МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ УПРАВЛІННЯ
КАФЕДРА МЕНЕДЖМЕНТУ ТА ФІНАНСІВ

До захисту допустити:
Завідувач кафедри
_____ Горбашевська М.О.
(підпис) *(ПІБ завідувача кафедри)*
« 29 **»** грудня **2023 р.**

«СИСТЕМА УПРАВЛІННЯ БЕЗПЕКОЮ ІНФОРМАЦІЙНИМИ ПОТОКАМИ В БАНКІВСЬКІЙ СФЕРІ»

Кваліфікаційна робота
здобувача вищої освіти другого (магістерського) рівня вищої освіти
освітньо-професійної програми «Менеджмент. Управління фінансово-економічною безпекою»
Єлісєєв Сергій Олександрович
(прізвище, ім'я, по батькові здобувача вищої освіти)
Науковий керівник:
Омельченко В. Я., професор кафедри менеджменту та фінансів, д.е.н.
(прізвище, ініціали, науковий ступінь, вчене звання,)
Рецензент:
Боєнко Олена Юріївна, кандидат економічних наук, доцент Донецький національний університет імені Василя Стуса (м. Вінниця)
(прізвище, ініціали, науковий ступінь, вчене звання, місце роботи)

Кваліфікаційна робота захищена
з оцінкою 90 А
Секретар ЕК_____
« 18 » січня 2024 р.

Київ – 2023

МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ УПРАВЛІННЯ
КАФЕДРА МЕНЕДЖМЕНТУ ТА ФІНАНСІВ

Рівень вищої освіти Магістр
Шифр та назва спеціальності 073 «Менеджмент»
Освітньо-професійна програма Менеджмент. Управління фінансово-економічною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри _____,
(науковий ступінь, вчене звання)
_____
(ПІП завідувача кафедри)
«_____»_____202__ р.

ПЛАН ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ

_____
(прізвище, ім'я, по батькові)

1. Тема роботи_____ Система управління безпекою інформаційними потоками в банківській сфері _____
керівник роботи___ Омельченко В. Я., в.о. завідувача кафедри менеджменту та фінансів, д.е.н., професор ___,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом Маріупольського державного університету від «___»_____ 20___року №_____
2. Строк подання здобувачем роботи_____
3. Вихідні дані до роботи (мета, об'єкт, предмет)_ мета роботи полягає в дослідженні управління безпекою банку, розкритті діючої практики з банківської системи України в умовах автоматизації та економічної нестабільності, запровадження напрямків удосконалення захисту системи безпеки банківської установи; об'єктом дослідження є управління системою захисту безпеки банківського сектору України; предметом дослідження являються теоретичні та прикладні аспекти ефективного захисту банківської системи України в умовах війни та економічної нестабільності___

4. Зміст роботи (перелік питань, які потрібно розробити)
Наприклад:
Розділ 1.__Розглянути сутність фінансово-економічної безпеки комерційного банку; визначити регуляторний вплив центрального банку (НБУ) на процес управління ризиками; дослідити методологічні аспекти управління ризиками електронного банківництва__
Розділ 2. __Провести фінансово-економічний аналіз банківського сектору України, зокрема дослідити наступні питання: макроекономічні та фіскальні ризики в умовах війни; фактори ризику ліквідності та фондування банківського сектору; ризик прибутковості та ризик високої частки державного капіталу в банківському секторі___
Розділ 3.__Запропонувати способи вдосконалення захисту банківської системи в сучасних умовах шляхом формування системи захисту інформаційної безпеки на базі міжнародних стандартів ISO, розробкою ефективного захисту топології мережевої системи комерційного банку___

5. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Омельченко В. Я., професор кафедри менеджменту та фінансів, д.е.н.	10.09.2023	10.09.2023
2	Омельченко В. Я., професор кафедри менеджменту та фінансів, д.е.н.	10.09.2023	10.09.2023
3	Омельченко В. Я., професор кафедри менеджменту та фінансів, д.е.н.	10.09.2023	10.09.2023

6. Дата видачі завдання____10 вересня 2023 р.___

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Обрання актуальної теми для написання роботи	10.09.23-15.09.23	виконано
2	Дослідження літературних джерел, складання та затвердження плану кваліфікаційної роботи	16.09.23-18.09.23	виконано
3	Встановлення мети та завдань для дослідження	19.09.23-28.09.23	виконано
4	Обробка фактичного матеріалу	29.09.23-14.10.23	виконано
5	Обговорення окремих частин роботи із науковим керівником на предмет правильності та коректності формулювань	15.10.23-21.10.23	виконано
6	Написання трьох розділів основної частини роботи, її подальше оформлення відповідно до наданих методичних рекомендацій	22.10.23-08.12.23	виконано
7	Подання зброшурованої та електронної версій кваліфікаційної роботи на кафедру з її подальшою перевіркою	09.12.23-12.12.23	виконано
8	Підготовка до захисту	13.12.23-18.12.23	виконано
9	Публічний захист кваліфікаційної роботи у ЕК	19.12.2023	виконано

Здобувач _____ _____Єлісєєв С. О._____
(підпис) (прізвище та ініціали)

Науковий керівник роботи _____ __Омельченко В. Я.___
(підпис) (прізвище та ініціали)

ЗМІСТ

ВСТУП

Процес забезпечення стійкості та системи захисту безпеки банків має значний вплив на зміцнення національної безпеки та її позицій у світовій фінансовій системі. На банківську систему покладено відповідальність за стабілізацію грошово-кредитної системи, регулювання руху фінансових ресурсів на всіх рівнях, гарантування конвертованості національної валюти, фінансування держави, бюджету та підприємств, підтримку інвестицій у країні та надання кредитів.

Актуальність обраної теми визначається тим, що через недосконаліть системи захисту виникають труднощі із безперебійним функціонуванням та зміцненням фінансово-економічної безпеки для банківських систем усіх країн, і Україна не є винятком. Розвиток банківського сектору в умовах підвищеного ризику, пов'язаного з економічною та політичною нестабільністю в країні, змушує його ефективно керувати та забезпечувати власну економічну безпеку. Це необхідно та важливе стратегічне завдання для України.

Мета роботи полягає в узагальненні теоретичних основ управління безпекою комерційних банків, розкритті діючої практики з банківської системи України в умовах автоматизації, появою інноваційних технологій та економічної нестабільності, а також пошуку напрямків удосконалення цієї роботи на основі систематизації існуючих пропозицій щодо цього питання.

Для досягнення поставленої мети в роботі вирішуються такі *завдання*:

- досліджено сутність, цілі та функції фінансово-економічної безпеки банку;
- узагальнено основні аспекти управління ризиками електронного банківництва;
- розглянуто вплив регуляторного процесу на управління ризику Національним банком України;

- проаналізовано макроекономічні та фіскальні ризики економічного сектору держави;
- досліджено фактори ризику ліквідності та фондування банківського сектору;
- охарактеризовано ризик прибутковості та високої частки державного капіталу в банківському секторі;
- запропоновано формування системи захисту інформаційної безпеки банку в сучасних умовах;
- надано рекомендації щодо розробки ефективного захисту топології мережевої системи комерційного банку;
- запропоновано методологію побудови системи забезпечення інформаційної безпеки банків на базі міжнародних стандартів.

Об'єктом дослідження є управління системою захисту безпеки банківського сектору України.

Предмет дослідження – теоретичні та прикладні аспекти ефективного захисту банківської системи України в умовах війни та економічної нестабільності.

Теоретичною основою роботи є наукові праці вітчизняних вчених та фахівців з питань проблем та перспектив забезпечення захисту банківської системи України в сучасних умовах. На вирішення цього наукового завдання спрямовані дослідження Зачосової Н. В., Кельдер Т. Л., Худолєй Л. В., Голобородько Ю. О., Щербатих Д. В., Соловйова В. І., Ляхович О. О., Добровольської В. В., Вдовиченко А. Р., Орос Г. С., Присяженко О. В., Синюк А. О., Коваленко В. В., Радової Н. В., Карчевою Г. Т., Ревенкова П. В., Костікової К. О та інших вітчизняних науковців.

Віддаючи належне внеску відомих вчених, слід відмітити, що недостатньо дослідженими залишаються питання щодо напрямів ефективного управління банківськими ризиками, формування системи захисту електронного банківництва на сучасному ринку банківських послуг та зменшення впливу

зовнішніх політично-економічних потрясінь. Значущість цього питання зумовила вибір теми, визначила мету, завдання, логіку та зміст дослідження.

У роботі було застосовано низку загальнонаукових та спеціальних *методів дослідження*, а саме: наукова абстракція – для визначення напрямів розвитку банківської діяльності в умовах зростаючих темпів ризику автоматизованих процесів та шахрайства через мережу; структурно-функціональний аналіз – для визначення причинно-наслідкових зв'язків між фінансовим станом та фінансовою стійкістю банків; графоаналітичний – для аналізу, порівняння й наочного відображення статистичних даних з метою дослідження стану функціонування банківського сектору України; статистичних порівнянь – для аналізу економічних показників діяльності банківської системи у період динамічних глобальних економічних трансформацій.

Вказаному питанню приділяється значна увага Національного банку України, що знайшло своє відображення у Законі Верховної Ради України «Про банки і банківську діяльність» № 2121-III (зі змінами та доповненнями) від 07.12.2000, Постанові «Про затвердження Положення про організацію та проведення інспекційних перевірок» від 17.07.2001 № 276, Постанові «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» від 28.09.2017 № 95, Постанові «Про затвердження Положення про Систему BankID Національного банку України» від 17.03.2020 № 32, Постанові правління Національного банку України «Про затвердження Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг» від 16.01.2021 року № 4 та інших нормативних джерелах. Інформаційною базою дослідження є дані Держкомстату України, Національного банку України, Асоціації українських банків та інших статистичних джерел.

У кваліфікаційній роботі з'ясовано сутність, принципи побудови та функції системи захисту банківської системи України; проведено аналіз

діяльності банківської системи України; розроблено конкретні рекомендації щодо підвищення економічно-фінансової безпеки банківської системи України, які містять у собі рекомендації щодо розробки та впровадження засобів і методів захисту ресурсів інформаційно-комунікаційних систем і мереж на організаційному та технічному рівні у контексті трансформації моделі бізнесу європейських банків на базі міжнародних стандартів; формування ефективного регуляторного контролю із забезпеченням системності та комплексності заходів безпеки інформації інституційного середовища; запропоновано напрями удосконалення топології комп'ютерної мережі в залежності від конкретних потреб, обмежень та мети мережі.

Впровадження пропозицій і рекомендацій, які є елементами *наукової новизни*, дозволить вибрати оптимальну стратегію розвитку захисту фінансово-економічної та інформаційної безпеки банківської системи України в умовах бойових дій.

Робота складається із вступу, трьох розділів, висновків та практичної частини, містить 100 сторінок, 31 рисунків, 6 таблиць, список літератури з 57 найменувань.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДИЧНІ ЗАСАДИ ПОБУДОВИ СИСТЕМИ ФІНАНСОВО-ЕКОНОМІЧНОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКІВСЬКИХ УСТАНОВ

1.1. Сутність фінансово-економічної безпеки комерційного банку

Фінансова стабільність одного банку тісно пов'язана з стабільністю банківської системи в цілому, бо діяльність однієї банківської структури негативно впливає на виникнення загальної банківської кризи. Це пов'язано з тим, що банки здебільшого працюють з запозиченим капіталом. І будь-яка негативна атмосфера в суспільстві може спричинити відтік фінансових ресурсів. Крім того, такий відтік може призвести до значного відтоку депозитів з банківської системи, якщо він відбудеться в одному з найбільших банків країни. Також недовіра до конкретного банку посилюється певними структурними проблемами в банківському секторі. Це засвідчує, наскільки важливим є забезпечення фінансової безпеки банків.

У цьому контексті слід зазначити, що фінансова безпека є ключовим фактором для забезпечення економічної безпеки банку. Таким чином, якщо економічна безпека перш за все відповідає за збереження матеріальних цінностей і здійснення банківських операцій, то метою фінансової її складової є попередження та уникнення загроз збереження та примноження фінансових ресурсів банку, забезпечення його стійкості, підвищення ефективності його діяльності та зміцнення його позицій на ринку. Фінансова стабільність і стійкість, ефективність фінансово-економічної діяльності, захист інтересів громадян і стійкість до внутрішніх і зовнішніх ризиків є ознаками фінансової безпеки.

Оскільки вищезазначені завдання є життєво важливими для діяльності банку, дослідження фінансово-економічної безпеки банку є пріоритетним. Для вирішення цього питання були систематизовані існуючі методи визначення

сутності цього поняття.

Як наслідок, основні підходи до розуміння фінансово-економічної безпеки включають такі визначення:

—сукупність заходів;

—стійкість до загроз, як внутрішніх, так і зовнішніх;

—здатність протистояти як наявним, так і імовірним загрозам [1].

Слід відмітити, що коли дослідники визначають основу забезпечення фінансово-економічної безпеки, вони звертають увагу на організаційні елементи. Тим не менш, у контексті зовнішніх і внутрішніх загроз слід приділяти більшу увагу питанням ліквідності, прибутковості, фінансової стійкості та управління банківськими ризиками.

Оскільки вищезазначені завдання є ключовими у діяльності банківської установи, то виникає необхідність дослідження саме фінансово-економічної безпеки банку. Для того, щоб розглянути це питання було систематизовано існуючі підходи до визначення сутності даного поняття у таблиці 1.1.

Таблиця 1.1

Підходи вітчизняних науковців щодо визначення фінансово-економічної безпеки банку

Автор, джерело	Визначення поняття
Кельдер Т. Л., Худолєй Л. В. [2]	Фінансово-економічна безпека банку – це стан, коли фінансова стабільність чи репутація не може бути підірвана цілеспрямованими діями певної групи осіб і організацій або фінансовою ситуацією, що складається всередині чи зовні банківської системи
Голобородько Ю.О. [3]	Фінансово-економічна безпека банку є станом, який характеризується оптимальним рівнем залучення і розміщення ресурсів при мінімізації загроз та негативних явищ і характеризує здатність банків до саморозвитку, підвищення ефективності та конкурентоздатності
Зачосова Н.В. [1]	Фінансовий стан комерційного банку при якому досягнуто збалансованість системи фінансових показників, дотримано стійкість до внутрішніх і зовнішніх загроз, що дозволяє своєчасно та в повному обсязі виконувати взяті на себе зобов'язання, а також забезпечує ефективний розвиток банку в поточному та наступних періодах

Продовження таблиці 1.1

Щербатих Д. В., Шпильовий Б. В. [4]	Безпека комерційного банку являється сукупністю заходів, спрямованих на запобігання збитку від негативних дій на їх економічну безпеку за різними аспектами фінансово-економічної діяльності
Соловйов В.І. [5]	Фінансово-економічна безпека банку – це стан під час якого забезпечується стабільність його функціонування, фінансова рівновага і регулярне одержання прибутку, можливість виконання поставлених цілей і завдань, здатність до дальшого розвитку й удосконалення

Джерело: розроблено автором за матеріалами [1-5]

Узагальнюючи наведені визначення вітчизняних науковців можна зробити загальний висновок їх трактувань, що фінансово-економічна безпека банку означає здатність виявити, попереджати та боротися з будь-якими загрозами для збереження фінансового стану банку та зміцнення його фінансово-економічного потенціалу. Таким чином, система фінансово-економічної безпеки банку повинна бути зосереджена на стабільності та ефективності банківської діяльності, виявленні ризиків, ліквідації криз і запобіганні банкрутству.

На етапі виявлення та прийняття банківськими ризиками процедура ідентифікації ризиків відіграє важливу роль у процесі управління банківськими ризиками. Ця процедура полягає у визначенні виду ризику, на який наражається банк під час своєї діяльності. Це означає, що для банківської діяльності потрібна комплексна класифікація ризиків. Якісна класифікація банківських ризиків є корисною, оскільки вона може бути корисною для пошуку внутрішніх методів підвищення ефективності управління ризиками банківських операцій.

У зв’язку з тим, що банк є відкритим і постійно змінюваним середовищем, ці фактори можна розділити на прогнозовані та непередбачувані. Цей метод лежить в основі класифікації банківських ризиків, яка розділяє їх залежно від того, наскільки добре банк може контролювати виникнення на внутрішні та зовнішні. Для наочного відображення ризиків банківської діяльності звернемося до схеми нижче.

Рис. 1.1. Класифікація ризиків банківських установ

Джерело: [6]

Зовнішні ризики мають значний вплив на ефективність банківської діяльності, і оскільки їх оцінювання базується на логічних методах аналізу,

управління такими ризиками складно та іноді навіть неможливо. Внутрішні ризики стосуються безпосередньо банківської діяльності. Чим ширше коло клієнтів, партнерів, зв'язків, фінансових операцій і послуг банку, тим більше внутрішніх ризиків супроводжує його роботу. Внутрішні ризики краще піддаються ідентифікації та квантифікації порівняно з зовнішніми, тому методики аналізу спрямовані на виявлення, оцінювання та вибір ефективних методів мінімізації та моніторингу цієї групи банківських ризиків.

Індекс фінансового стресу (IFS) використовується для визначення фінансової безпеки банків. Цей індекс надає комплексну кількісну оцінку стану фінансової системи та вимірює рівень стресу.

Індекс фінансового стресу дає змогу:

—виміряти рівень стресу фінансової системи;

—оцінити глибину та тривалість нестабільності фінансових ринків,

—порівняти його з рівнем стресу в минулих кризах;

—оцінити ефективність антикризових заходів, включно з іншими показниками;

—визначити характер потрясінь, які відбуваються в фінансовій системі та її окремих складових, будь то системні чи епізодичні [7].

Таким чином, індекс фінансового стресу не вказує на майбутні ризики в короткостроковій чи довгостроковій перспективі, а лише показує поточний стан справ у фінансовому секторі. Він дозволяє визначити більш точну оцінку ризику в реальному часі. Зокрема, це корисно для швидкого розробки антикризової політики центрального банку при відстежувані постійних динамічних змін стану фінансової системи нашої країни.

На графіку нижче відображені зовнішні та внутрішні загрози на фінансово-економічну безпеку комерційних банків та їх вплив зміну індексу фінансового стресу за більш ніж 10 років.

Рис. 1.2. Графік індексу фінансового стресу банківської системи

Джерело: [8]

На рисунку 1.2. показано основні події, які вплинули на фінансовий ринок України. Зокрема, позначка індексу досягла свого піку невдовзі після банкрутства «Lehman Brothers». Наступне стрімке зростання фінансового стресу спостерігається під час економічної кризи в 2014-2015 роках, хоча й на меншому рівні, але набагато триваліше за часом.

Рівень стресу почав значно зменшуватися лише після початку переговорів про реструктуризацію державного боргу у 2015 році. Після введення карантину в березні 2020 року індекс трохи зріс, але вже на початку червня знизився до рівня, який був до початку пандемії COVID-19.

Повномасштабне вторгнення Росії у 2022 році збільшило індекс. Усі його компоненти зросли, що свідчить про системний характер стресу для фінансового сектору. Спочатку зростання доходів на ринку цінних паперів, висока волатильність курсу готівкової валюти, високий рівень валютних інтервенцій і рефінансування комерційних банків Національним банком для підтримки їхньої ліквідності були причинами високого рівня показника фінансового стресу.

Завдяки збереженню довіри населення до банківської системи та відсутності відпливу вкладів, що стримало зростання загального індексу, лише рівень субіндексу поведінки домогосподарств залишився порівняно низьким.

Більшість субіндексів зменшилася. Однак дохідність державних і корпоративних цінних паперів стрімко зросла вже в липні, очікуючи реструктуризації державного боргу. Волатильність на готівковому ринку зберігалася, а ставки за депозитами населення зросли. Таким чином, індекс фінансової стійкості зріс до березневого рівня. Атаки на енергетичну інфраструктуру стали новим шоком для системи після успішної реструктуризації боргу та тимчасового зниження індексу. Оскільки коливання курсу готівки посилилися, банківські та валютні субіндекси значно зросли. Рівень стресу зріс через високі значення багатьох індексів. Однак індекс почав знижуватися вже з початку листопада, коли економіка пристосувалась до нових атак.

У поточному році волатильність на високих рівнях індексу фінансового стресу зберігалася, а основною причиною зростання був одночасний рух багатьох субіндексів. Субіндекс поведінки домогосподарств поступово зріс, головним чином завдяки підвищенню відсоткових ставок за гривневими депозитами. Незважаючи на те, що відпливи вкладень не є причиною підвищення ставок, воно не створює додаткового тиску на ліквідність. Тим не менш, воно демонструє жорсткіші монетарні умови, що посилює труднощі для фінансової системи. Зниження показників ліквідності призвело до зростання банківського субіндексу; однак він залишався найнижчим із всіх елементів фінанових показників. Зважаючи на високу дохідність суверенних єврооблігацій, субіндекс державних цінних паперів продовжує триматися на високих рівнях. У той же час валютний субіндекс поступово скорочується завдяки зменшенню різниці між офіційними та готівковими курсами валют, а також зменшенню кількості валютних інтервенцій, які проводить Національний банк України.

1.2. Дослідження регуляторного впливу центральним банком на процес управління ризиками

Формування сучасної банківської системи України почалось із формуванням її як самостійної, незалежної держави. Прийнятий у 1991 р. Закон України «Про банки і банківську діяльність» (№ 1586-VII від 04.07.2014) [9] зафіксував концептуальне положення, що банківська система України має бути дворівневою. Тобто було здійснено перебудову банківської системи, яка стала дворівневою, – монопольно регулював та контролював діяльність банківської сфери Національний банк України. Йому підпорядковувалися всі інші банки. Комерційні банки функціонують на основі приватного капіталу. Стосовно один одного вони є рівноправними та економічно самостійними. Вони слугують певним фундаментом усієї банківської системи, на чолі якої знаходиться центральний банк. Законодавство дає чітке розмежування прав та обов'язків кожному з рівнів банківської системи. Централізоване регулювання банківської системи перш за все визначається її регулятивною функцією.

Кожен банк має свою систему управління банківськими ризиками. При розробці системи ризик-менеджменту для окремого банку важливо враховувати масштаби та особливості його діяльності. Це пов'язано з тим, що впровадження та підтримка системи управління ризиками потребує значних витрат, таких як придбання нового програмного забезпечення та забезпечення відповідної технологічної підтримки. Якщо система неефективна, це може негативно вплинути на рівень прибутковості банку.

З іншого боку, для управління фінансовою стійкістю необхідно використовувати низку методів, основними з яких є:

—постановка цілей, визначення тактики та стратегії для забезпечення фінансової стійкості банку включає планування. Фінансове планування має на меті перетворити стратегічну мету в абсолютні та відносні фінансові показники за допомогою відповідних інструментів.

—аналіз основних факторів, які визначають стабільність фінансового стану банку. Аналіз дозволяє виявити зв'язки між різними елементами операцій банку. Аналіз є чудовим способом швидко визначити, як змінюються фінансові показники, які показують рівень фінансової стійкості, і прийняти розумні рішення для управління, щоб гарантувати її.

—оцінка та контроль банківської стійкості за допомогою різноманітних методів і процедур. У сфері регулювання та оцінки фінансової стійкості банків існують кілька підходів: зовнішнє – пряме регулювання та обов'язкова оцінка; по-друге, внутрішнє – саморегулювання й ініціативна оцінка.

—контролювати фінансовий стан банків. Контроль полягає в тому, щоб переконатися, що отримані результати відповідають запланованим показникам, оптимальні значення яких сприяють підвищенню фінансової стійкості банку. Усі етапи контролю повинні виконуватися як банками, так і органами нагляду, щоб забезпечити належний контроль за фінансовою стійкістю банків.

Організаційна будова і керівництво банком формулюють дієві підрозділи, службовий уряд та органи управління. Загальні зібрання акціонерів являються головним органом керівництва банку. Вони вирішують стратегічний план його подальшого функціонування. Реалізація ухвалених завдань вищим органом безпосередньо здійснюється через виконавчі органи, які цілковито підпорядковуються йому. В акціонерних банках виконавчим органом вважається правління, а структурою пайового банку являється дирекція. За функціонуванням правління слідкує голова, а за роботою дирекції доглядає генеральний директор. Їх становлять відповідно до статуту банку.

Нагляд за роботою правління або дирекції виконує ревізійна комісія. Загальний збір акціонерів встановлює склад такої комісії. За резолюцією зборів акціонерів ухвалюється наглядовий орган. Головна ціль наглядового органу полягає у керуванні діяльності банку і контроль роботи правління з ревізійною комісією. Таким органом є спостережна рада. Вона оберігає інтереси акціонерів у проміжку загальних зборів. Також виконує стратегічні завдання піднесення та

контролю банку.

Таким чином, необхідно розглянути основні компоненти ефективного управління банківськими ризиками, щоб максимально вплинути на фінансову стійкість банку. На наступній схемі показано основні структурні компоненти, які складають систему управління банківськими ризиками.

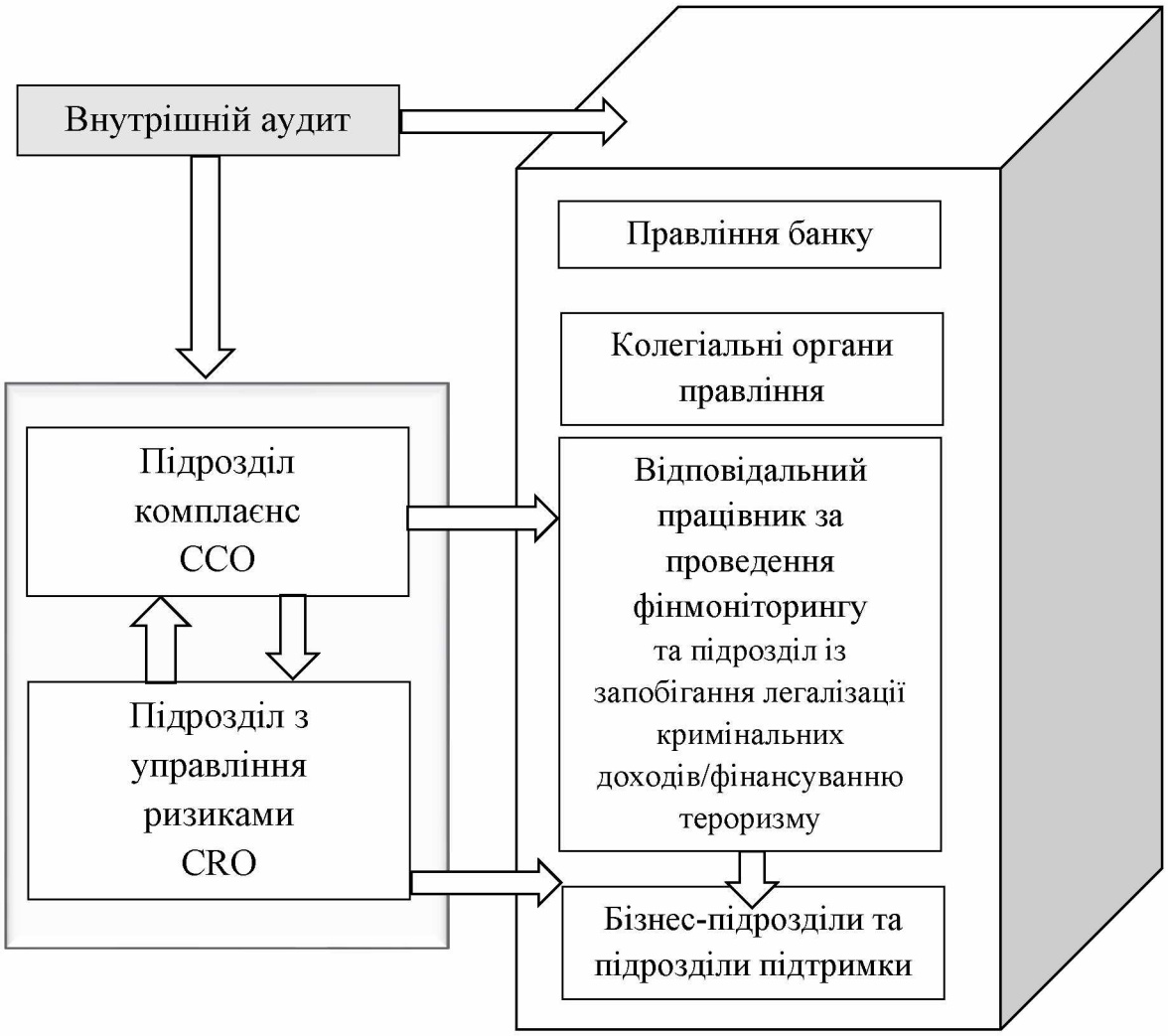

Рис. 1.3. Контроль ризиків банку та оцінка ефективності системи управління ризиками

Джерело: [10]

Виходячи з вищенаведеної інформації можна виокремити, що процес ризик-менеджменту повинен включати такі структурні та функціональні підрозділи банку:

—спостережна рада, яка виконує свої обов'язки перед власниками, вкладниками та органами банківського нагляду;

—правління банку, яке виконує свої обов'язки щодо виявлення, оцінки, контролю та нагляду;

—підрозділ ризик-менеджменту, який виконує свої обов'язки щодо виявлення, оцінки та контролю.

Відділ з управління ризиками повинен підпорядковуватися голові Правління банку та повністю відокремлений від підрозділів, які безпосередньо приймають ризики і підрозділів, які реєструють ризики та контролюють їх розмір. Член Правління банку також повинен бути членом профільних комітетів і має право вето на рішення цих комітетів, якщо вони можуть завдати шкоди належному веденню банківської діяльності.

Регулятивний вплив полягає у тому, що на сьогодні Національний банк України вимагає від кожного українського банку розробити та визначити бізнес-модель, щоб краще зрозуміти перспективи функціонування банків і їхній вплив на економіку. Національний банк України проводить наглядову оцінку SREP на основі визначення бізнес-моделі банку.

Модель аналізу SREP стала дуже популярною в Європі. Ця модель є модифікацією раніше використовуваної ICAAP (Internal Capital Adequacy Assessment Process). CREP-аналіз базується на основних взаємопов'язаних напрямах аналізу, запропонованих Європейською банківською організацією ще у 2014 році. Проте запроваджений він був у систему банківського нагляду країн Європи тільки в 2015 році. ICAAP було розроблено в рамках Базеля II та спрямоване на дослідження внутрішніх процедур і процесів банку з метою визначення рівня достатності капітальних ресурсів у довгостроковій перспективі для покриття всіх можливих ризиків. Для цього використовується класифікація фінансових інституцій на основі результатів кластерного аналізу. Це включає постійний моніторинг показників діяльності банків, аналіз бізнес-моделі банку, оцінку системи внутрішнього управління та контролю, оцінку

адекватності капіталу, оцінку ризиків ліквідності та достатності джерел для підтримки ліквідності, визначення результатів оцінки фінансового стану та фінансової стійкості банку та визначення заходів, які необхідні виконати [11].

Аналіз бізнес-моделі є необхідним для визначення прибутковості діяльності банку в короткостроковій перспективі та його здатності зберігати стратегічну стійкість у довгостроковій перспективі.

Сьогодні Національний банк України вживає рішучих заходів щодо впровадження SREP-аналізу. Предметом обговорення є постанова Правління НБУ №47 від 2 травня 2018 року про внесення змін до «Положення про організацію та проведення інспекційних перевірок» [10]. Ця постанова враховує рекомендації Європейського банківського органу щодо організації єдиної процедури та методології процесу наглядових перевірок та оцінки.

Процес оцінки банків (SREP), який здійснюється одночасно за всіма банками, здійснюється шляхом оцінки розміру ризиків і якості управління ними на основі даних, отриманих від підрозділів НБУ, а також аналізу наявних тенденцій у діяльності банків.

З урахуванням змін, SREP-аналіз проводиться щороку 1 січня. Щоквартал оцінка коригується на основі аналізу змін кількісних показників і врахування нової важливої нефінансової інформації. Департамент банківського нагляду є відповідальним за проведення оцінки банків [12].

Оцінка банків SREP-аналізу визначає наступне:

—стратегію нагляду за банком, яка включає раннє втручання;

—життєздатність банку протягом наступних 12 місяців і стійкість стратегії протягом трьох років;

—достатній капітал і ліквідність для покриття ризиків;

—необхідність здійснення інспектування.

Загальний підхід до оцінки банків за методологією SREP-аналізу складається з чотирьох етапів (табл. 1.2).

Таблиця 1.2

Загальні підходи до проведення оцінки банків за методологією SREP за 4 елементами

Підхід	Характеристика
Аналіз та оцінка бізнес-моделі	Оцінка бізнес-моделі банку передбачає проведення оцінки життєздатності бізнес-моделі та визначення стійкості його стратегії розвитку. Життєздатність бізнес-моделі банку визначається на підставі оцінки її спроможності до генерації прийнятного рівня доходів протягом наступних 12 місяців, з огляду на значення показників ефективності, відповідність структури фінансування банку його бізнес-моделі, ризик-апетиту(схильність до ризику). Стійкість стратегії банку визначається на підставі оцінки її спроможності до генерації прийнятного рівня доходів упродовж щонайменше наступних 3-х років згідно із затвердженою стратегією банку та бізнес-планом, у тому числі з урахуванням виконання стратегії банку в минулому
Оцінка рівня організації корпоративного управління та внутрішнього контролю	Оцінка рівня організації корпоративного управління та внутрішнього контролю банку ґрунтується на результатах оцінювання ефективності функціонування, зокрема таких елементів: системи корпоративного управління в цілому; корпоративної культури та культури прийняття ризику; організаційної структури та функціонування органів управління (наглядова рада та правління банку); політики та практики винагород; системи управління ризиками; системи внутрішнього контролю; ризику AML
Достатність капіталу	Метою здійснення оцінки ризиків капіталу є визначення достатності капіталу (його розміру та структури)для покриття основних видів ризиків, притаманних діяльності банку, зокрема кредитного, процентного, ринкового та операційного ризиків протягом наступних 12 місяців, а також визначення необхідних заходів для врегулювання потенційної недостатності капіталу
Достатність ліквідності	Метою здійснення оцінки ліквідності є визначення достатності ліквідних активів для покриття ризиків ліквідності та фінансування, притаманних діяльності банку, а також необхідних заходів для врегулювання потенційного дефіциту ліквідності

Джерело: [12]

У рамках аналізу оцінюваних ризиків НБУ класифікує бізнес-моделі банків таким чином:

Універсальна — значна частина активів і зобов’язань пов’язана з іншими

банками та небанківськими фінансовими установами.

Роздрібна – більшість активів і зобов'язань пов'язані з людьми; корпоративна – більшість активів і зобов'язань пов'язані з юридичними особами, а більшість зобов'язань пов'язані з грошима юридичних осіб.

Корпоративна з роздрібним фінансуванням – активи здебільшого складаються з кредитів юридичним особам, а зобов'язання перевищують суму грошей, залучених фізичними особами.

Обмежене кредитне посередництво. Це означає, що частина кредитів, наданих юридичним та фізичним особам становить менше тридцяти відсотків, що є незначним результатом; або ж більшість кредитів надається обмеженому колу осіб чи фінансується власними коштами [14].

Якісні та кількісні показники використовуються для оцінки бізнес-моделей банку. Кількісні показники включають аналіз співвідношення між прибутковістю та ризиками банку, концентрацію його основних кредиторів, позичальників і пов'язаних осіб, конкурентоспроможність банку та аналіз досягнення банком планових показників; реалістичність; ризики репутації; дотримання вимог і правил НБУ; і ризики операцій із пов'язаними з банком особами. На схемі нижче зображено загальну систему оцінювання за методологією SREP-аналізу (рис. 1.4).

У 2018 році НБУ здійснив оцінку банків у рамках SREP за новою методологією. Більшість фінансових організацій, включаючи 40 середніх і малих банків, заявили, що оцінка фінансового стану банків була незадовільною. З іншого боку, основною проблемою, з якою стикаються невеликі банки, залишається відсутність стратегії розвитку та, як наслідок, нездатність бізнес-моделі функціонувати [15]. Повторна перевірка унеможливлює процес зіставлення даних, оскільки з початком повномасштабної війни 2022-го року більшість відділень позакривались на тимчасово окупованих територіях та зонах бойових дій.

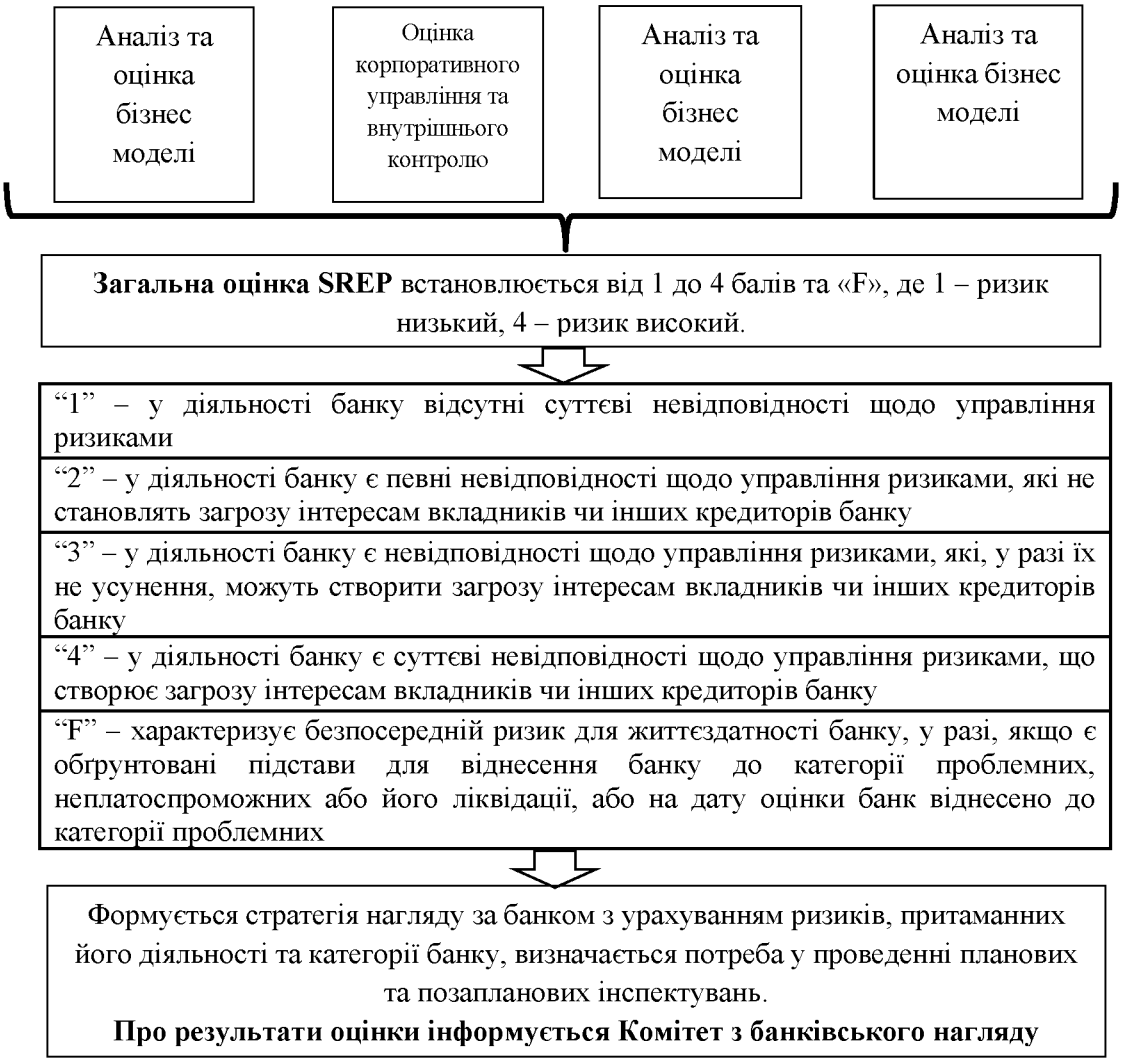

Рис. 1.4. Характеристики балів загальної оцінки SREP

Джерело: [16]

Отже, оцінювання банківського ризику за методологією SREP-аналізу виступає гарантом невипередженого, об'єктивного та поетапного контролю індивідуально щодо кожного банку з його власним інституційним середовищем відповідно до обраної бізнес-моделі на протидію ризикам фінансової стійкості. Для ефективності управління ризиками організаційна структура банку включає функціональні служби та підрозділи, кожен з яких виконує певні операції й має свої права та обов'язки за економічним змістом та обсягом операцій, які він виконує. Такі департаменти, управління, відділи формуються відповідно до

кваліфікації окремих банківських операцій або їхніх груп за функціональним призначенням, тому їх кількість і конкретна назва у різних банків можуть бути неоднаковими. Великі банки мають мережу філій і відділень та територіальні органи управління ними (дирекції).

1.3. Методологічні аспекти управління ризиками електронно-інформаційного банківництва

Ринок банківських послуг значно розвинувся завдяки швидкому розвитку Інтернет-технологій, які включили інформаційні системи в операційні процеси банків. Аби залишатися конкурентоспроможними на ринку банківських послуг, банки зараз переходять від традиційних форм банківського обслуговування до електронного банківського обслуговування. Електронний банкінг – це особливий, інноваційний інструмент дистанційного банківського обслуговування, який надає як традиційні послуги банківського обслуговування, так і інформаційні та комунікаційні послуги за допомогою різноманітних електронних каналів, які змінюються та вдосконалюються відповідно до розвитку інформаційних технологій.

На сьогодні ми маємо змогу отримати електронне банківське обслуговування за допомогою різних типів електронного банкінгу. На даний момент існує приблизно десять різних типів електронного банківництва. Вони пішли від банкоматів у магазинах і «домашніх» технологій до Інтернет-банкінгу, мобільного банкінгу та навіть відео-банкінгу, який можна використовувати коли завгодно, де завгодно за допомогою Інтернету.

Наразі багато фінансових установ в Україні використовують системи електронного банкінгу; мобільні та Інтернет-варіанти є найпоширенішими. Інтернет-сервіси Приватбанку, Альфа-Банку, VTBБанку, ПУМБ, Райффайзен Банку Аваль, УкрСиббанку, Укрсоцбанку та Ощадбанку вважаються найбільшими і найтехнологічнішими учасниками ринку. Однак Приватбанк традиційно залишається лідером на ринку онлайн-банкінгу та мобільного

банкінгу (рис. 1.5), оскільки усі операції в онлайн-банкінгу обслуговуються банком цілодобово та без вихідних у будь-який час. Платежі клієнтів банку здійснюються миттєво. Переказ коштів між клієнтами одного банку становить 0%, а між клієнтами інших банків – 1%. Передбачені цілодобові безкоштовні консультації онлайн і по телефону. Приватбанк досяг лідируючих позицій на ринку електронних банківських послуг, що підтверджується зростанням депозитної бази протягом останніх десяти років, включно з третім кварталом 2023 року. Однак через націоналізацію банку у четвертому кварталі 2022 року відтік коштів клієнтів спричинив скорочення депозитів фізичних осіб на 0,5 млрд грн і депозитів юридичних осіб на 2 млрд грн, що призвело до зниження довіри до банку. Наразі Приватбанк є єдиним банком в Україні та навіть у світі, який може виконувати більше сорока банківських операцій дистанційно через Інтернет.

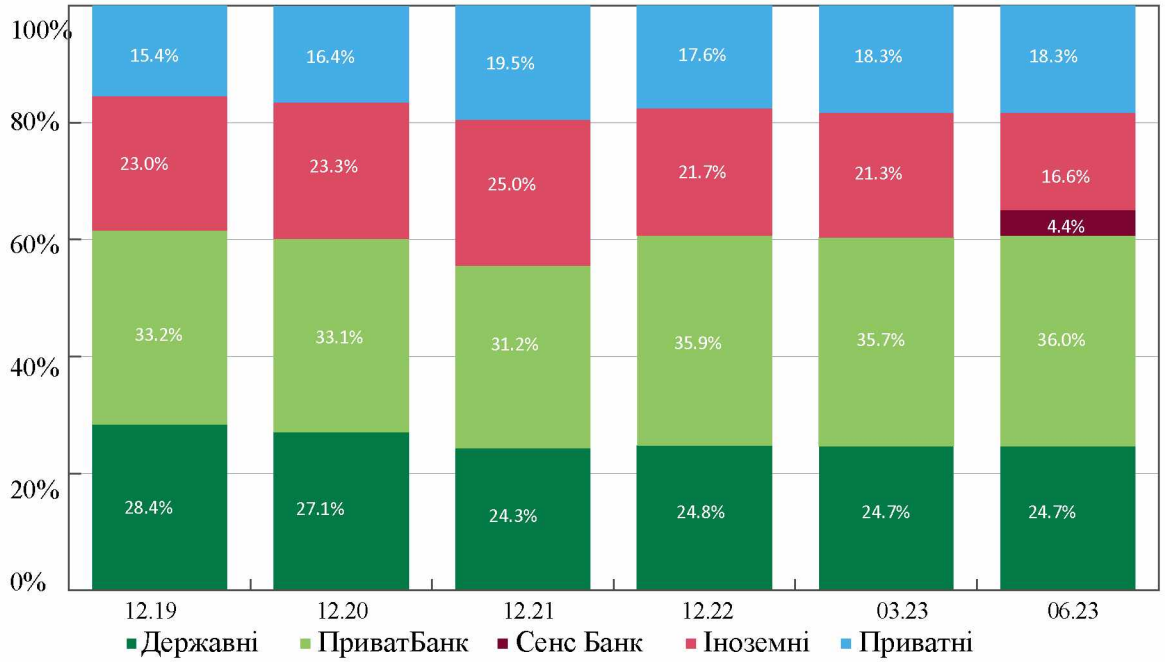

Рис. 1.5. Розподіл депозитів фізичних осіб за групами банків

Джерело: [17]

Слід відзначити, що впровадження електронного банкінгу призвело до появи нових джерел банківських ризиків, які раніше не існували в традиційних

банківських операціях. Через те, що технології електронного банкінгу та автоматизовані банківські системи, які використовуються в таких ситуаціях, недостатньо надійні, банківські установи та їхні клієнти опиняються беззахисними. У результаті було визначено три основні «системні» фактори, які сприяють появі нових елементів банківських ризиків під час впровадження систем електронного банкінгу:

1. поява у банку клієнтів нового типу, які часто самі виконують функції операціоністів;

2. залучення третьої сторони, зокрема провайдерів, для забезпечення формування та підтримки функціонування систем дистанційного банківського обслуговування (ДБО);

3. потенційна доступність банківських автоматизованих систем банків для [18].

Вважаю доцільним додати попередні «системні» елементи ще однією особливістю, а саме тим фактом, що клієнт не має доступу до банківської установи під час процесу обслуговування. Ця особливість пов'язана з тим, що банківські установи стикаються з труднощами в ідентифікації клієнтів під час дистанційного обслуговування. Це призвело до появи нових нестандартних джерел, які розширюють профіль банківських ризиків.

Незважаючи на те, що на даний момент не існує єдиної класифікації ризиків, пов'язаних з електронним банкінгом, дослідники з усього світу стверджують, що операційні, юридичні, стратегічні, репутаційні та ліквідні ризики є найбільш поширеними ризиками, пов'язаними з впровадженням електронного банкінгу.

З різних джерел виникають почуття ризику. Наприклад, шахрайство в системі електронного банкінгу, збої в системі обслуговування або компанії-провайдера, низька захист системи інформаційних технологій банку та провайдера та інші ситуації підвищують операційний ризик. У таких ситуаціях, як:

—розкриття або викрадення банківської таємниці або конфіденційної інформації про клієнта;

—нездатність забезпечити безперебійну роботу системи електронного банкінгу;

—впровадження незручної та складної системи електронного банкінгу тощо, – ризик для репутації зростає.

Варто зазначити, що переваги електронного банкінгу взаємодіють. Особливо помітна кореляція між ризиками репутації та банківськими ризиками, такими як юридичні та операційні. Банк може зазнати значних фінансових втрат через шахрайство, невиконання обов'язків перед клієнтами, розкриття конфіденційної інформації та збої в роботі автоматизованої системи електронного банкінгу. Реалізація стратегічного ризику може бути результатом помилок у стратегічному плануванні.

Ризик ліквідності є найважливішим ризиком, який часто пов'язаний з іншими ризиками, оскільки управління ліквідністю стає ще більш складним, оскільки клієнти завжди можуть отримати доступ до своїх грошей. Це може призвести до значної нестабільності грошей на рахунках. Репутаційні, правові та стратегічні ризики, як правило, опосередковано реалізуються ризиком ліквідності.

«Принципи ризик-менеджменту електронного банкінгу» [19], розроблені Базельським комітетом питань банківського нагляду, є основним міжнародним документом, який регулює процес управління ризиками в електронному банкінгу. Базельський комітет створив чотирнадцять основних принципів управління ризиками в електронному банківському секторі. Ці принципи були розроблені з метою створення міцної системи управління ризиками в електронному банківському секторі. Три групи включають стандарти управління ризиками електронного банкінгу:

—Група А: Регулятивний вплив збоку вищого керівництва банку (принципи 1-3);

—Група B: Дотримання безпеки банківської установи (принципи 4-10);

—Група C: Управління ризиками права та репутації (принципи 11-14).

Розпочнемо розгляд стандартів управління ризиками банку з першої А-групи. Нагляд з позиції вищого керівництва банку складається з перших трьох принципів, які наведено в таблиці 1.3. Ці принципи мають на меті контролювати дії Правління та Ради директорів банку, щоб розробити чіткі стратегічні бізнес-плани щодо впровадження електронного банкінгу, а також забезпечити їх узгодження та інтеграцію з загальнокорпоративними стратегічними цілями банку. Крім того, вище керівництво банку повинно забезпечити процес аналізу ризиків функціонування електронного банкінгу, створити ефективну систему контролю та моніторингу цих ризиків, а також розробити методи постійного оцінювання ефективності використання електронного банкінгу.

Таблиця 1.3

Принципи А-групи. Регулятивний вплив з боку керівництва

№	Назва принципу	Короткий зміст
1	Створення ефективної системи нагляду за операціями, що здійснюються через систему електронного банкінгу	а) Впровадження різних форм електронного банкінгу зумовлюють зростання ймовірності впливу на конфігурацію банківського ризику і реалізацію прийнятої стратегії банком, тому Рада директорів і Правління банку повинні враховувати ці особливості та піддавати їх глибокому стратегічного аналізу з точки зору співвідношення очікуваних витрат і прибутків у ретроспективі; б) Керівництво банку повинно впроваджувати електронне банківське обслуговування клієнтів лише за умови підготовки відповідного рівня кваліфікації менеджерів і персоналу у сфері ІТ; в) Управлінський нагляд повинен бути гнучким і ефективно реагувати на будь-які проблеми та інцидентів у цій сфері діяльності; г) Система ризик-менеджменту електронного банкінгу повинна бути інтегрована та узгоджена із загальним процесом управління банківськими ризиками.

Продовження таблиці 1.3

2	Створення всебічної процедури контролю за додержанням належного рівня безпеки	Найважливішим обов'язком Ради директорів і Правління банку є забезпечення процесу збереження активів банку, тому для виконання цього завдання керівництво банку повинно: 1) призначити конкретних осіб, які несуть відповідальність за стан справ у цій сфері; 2) розробити жорстві правил, що дозволяють відслідковувати спроби вторгнення в комунікаційні мережі банку та запобігати несанкціонованому доступу до комп'ютерних технологій, програмного забезпечення і баз даних; 3) здійснювати регулярний огляд та вдосконалення заходів щодо забезпечення безпеки з метою впровадження нових технологій і своєчасної модернізації програм, що використовуються банком.
3	Організація процесу всебічного нагляду за взаємодією з партнерами, які забезпечують процес надання певних видів електронних банківських послу	Керівництву банку слід здійснювати постійну оцінку доцільності та ефективності співпраці із компаніями-провайдерами та усвідомлювати пов'язані з аутсорсингом ризики. Також якісно оцінювати рівень професіоналізму і фінансового становища цих компаній та чітко прописувати межі відповідальності, план заходів у надзвичайних ситуаціях та частоту аудиторських перевірок з позиції ефективності управління ризиками обох сторін при укладанні контрактів.

Джерело: розроблено автором за матеріалами [20]

Що стосується другої групи В, то вона визначає управління безпекою та складається з семи принципів (табл. 1.4), описує дії та обов'язки спеціалістів, які безпосередньо керують процесом електронного банківського обслуговування в банківській установі. Ці принципи стосуються безпеки банку та його клієнтів.

Остання С-група стосовно управління правовим і репутаційним ризиком включає 11-14 принципи (табл. 1.5), які описують рівень відповідальності банківської установи перед клієнтами, включаючи захист їхньої конфіденційної та приватної інформації від третіх осіб, і спрямовані на підвищення довіри клієнтів до банків, які пропонують електронні платежі.

Таблиця 1.4

Принципи В-групи. Дотримання безпеки банківської установи

№	Назва принципу	Короткий зміст
4	Ідентифікація клієнтів електронного банкінгу	Банківська установа, яка здійснює обслуговування клієнтів у електронному режимі повинна: 1) вжити заходів для побудови ефективного процесу ідентифікації клієнта (засвідчення справжності особи, що здійснює транзакцію online) та його авторизації (встановлення легітимності доступу цієї особи до банківського рахунку або наявності у нього права на проведення операцій за рахунком) у системі електронного банкінгу; 2) ретельно контролюватись процес підключення до системи (для уникнення несанкціонованого доступу); 3)здійснювати повторну ідентифікацію у разі збоїв web-сеансів.
5	Недопущення відмови проведення фінансових операцій через канали електронного банкінгу та відповідальність за їх виконання	Банківська установа повинна забезпечити процес проведення фінансових операцій клієнтами не допускаючи відмов у їх здійсненні, тому важливим є розробити секретні та відкриті ключі для кожного клієнта. За допомогою секретного ключа генерується цифровий підпис і зашифровується текст, а за допомогою відкритого – здійснюється розшифровка і перевірка справжності документа. Банк може самостійно це здійснювати, або передати це партнерам (в останньому випадку необхідно вибирати такі організації, які забезпечують той же рівень ідентифікації, що і банк).
6	Належні заходи для забезпечення розмежування функцій	Між банківськими працівниками повинен існувати чіткий розподіл функцій при роботі у системах електронного банкінгу, базах даних та прикладних програмах. Права на ініціацію, авторизацію і завершення транзакції повинні розмежовуватись між працівниками чи партнерами. Різні працівники повинні збирати та перевіряти інформацію на цілісність і т. д. Банк повинен унеможливити нехтування цим принципом.
7	Ефективний контроль за авторизацією в системах електронного банкінгу, базах даних та прикладних програмах	Головна ціль даного контролю – забезпечити та гарантувати цілісність та збереженість баз даних, які містять інформацію про права на авторизацію та доступ до проведення тих чи інших операцій, оскільки неефективний контроль за розподілом функцій між працівниками (розподілення прав на авторизацію та доступ) збільшує ймовірність несанкціонованого доступу до баз даних.

Продовження таблиці 1.4

8	Забезпечення повноти даних про транзакції каналами електронного банкінгу, реєстрації цих даних, а також іншої інформації	Всі процеси, що здійснюються у системі електронного банкінгу повинні бути стійкими до злому та несанкціонованих змін. Банківська установа повинна розробити чіткий процес їх моніторингу та контролю для забезпечення цілісності даних. Цей принцип особливо актуальний в умовах модернізації програмного забезпечення банку.
9	Введення точного хронологічного простежування фінансових операцій електронного банкінгу	Служба внутрішнього контролю банку повинна здійснювати періодичний аудит операцій, що здійснюються в електронній формі. Найбільш важливим є процес аудиту операцій: відкриття, зміна і закриття клієнтського рахунку; проведення операцій, що показують зміни на балансі рахунку; оформлення заяв на збільшення раніше обумовленого з клієнтом ліміту; надання, модифікація або анулювання права на доступ до системи електронного банкінгу.
10	Збереження конфіденційності ключової банківської інформації	Банки повинні вжити заходів для забезпечення конфіденційності ключової банківської інформації, яка передається через системи електронного банкінгу і/або зберігається у базах даних, від доступу третіх осіб. Розроблені банком стандарти щодо збереження конфіденційності інформації слід використовувати і в організаціях, які залучаються до надання електронних послуг. Всі випадки доступу до такого роду даних необхідно реєструвати, а зареєстрованим файлам потрібно надати підвищену стійкість до розкрадань і спотворень.

Джерело: розроблено автором за матеріалами [20]

Слід відмітити, що більшість із наведених принців спрямовані регулювати управління безпекою, що має важливе місце в процесі впровадження новітніх інформаційних систем до складу основної діяльності банківської установи. Серед актуальних загроз користувачів банківськими послугами є фішинг. Фішинг — це тип інтернет-шахрайства, який намагається отримати доступ до конфіденційних даних клієнтів банку, таких як номер карти, термін дії карти, тризначний код безпеки (CVV2/CVC2) і код з банківських SMS-повідомлень. Збільшення кількості фішингових веб-ресурсів є проблемою, яка стосується всіх країн, а не лише України. Міжнародна організація із захисту кібербезпеки Anti-Phishing Working Group повідомила, що

з 2022 по 2023 рік кількість фішингових сайтів зросла на 29,3%. Кількість шахрайських сайтів в Україні зросла на 26% у 2023 році (107680 фішингових ресурсів у 2022 році проти 136400 у 2023 році). [21].

Таблиця 1.5

Принципи С-групи. Управління правовим і репутаційним ризиком

№	Назва принципу	Короткий зміст
11	Розкриття необхідної інформації стосовно електронних банківських послуг	Банківська установа повинна на власному сайті у відкритому доступі розмістити адекватну інформацію про банк: назва банку та фізичне розташування головного офісу та відділень; інформацію про членів Правління банку; інформація про зворотній зв'язок збанком у питаннях обслуговування, надсилання скарг та пропозицій; інформація про систему електронного банкінгу; інформація про політику конфіденційності клієнтів та захист клієнтської інформації; інформація про страхування депозитів і т. д. На сайті повинна зображатьсяінформація, яка допоможе сформувати клієнту позитивну думку про банківську установу.
12	Збереження таємниці інформації про клієнта	Ключовою відповідальністю банківської установи перед клієнтом є збереження його конфіденційної інформації. База даних інформації про клієнтів, що накопичується банком у процесі надання онлайнових послуг, повинна відповідати всім вимогам законодавчих актів про збереження приватної інформації клієнтів тих держав, на території яких функціонує електронний банкінг. Провайдери, з якими співпрацює банк, також повинні дотримуватись цих стандартів. Банк зобов'язаний дати своїм вкладникам і позичальникам право забороняти передачу відомостей про себе третім особам, які бажають використовувати їх у маркетингових цілях.
13	Підтримання системи електронного банкінгу в режимі експлуатаційної готовності	Банки повинні забезпечити безперервний процес надання обслуговування через різні форми електронного банкінгу та розробити план дій для підтримки роботи системи в критичних умовах, тому банківським установам потрібно: забезпечити безперебійну подачу потужного рівня електроенергії та використовувати потужні сервери для обробки даних; постійно оцінювати та переоцінювати рівень потужності електромереж необхідних для якісного функціонування електронного банкінгу та здійснювати прогноз в динаміці; системи слід періодично випробовувати на стійкість до стресових ситуацій та атак.

Продовження таблиці 1.5

14	Створення ефективного механізму реагування на неочікувані інциденти	Плани реагування на неочікувані інциденти повинні містити наступну інформацію: методи виявлення негативного інциденту (зовнішньої чи внутрішньої атаки) та рівня загроз; шляхи відновлення функціонування систем електронного обслуговування; шляхи взаємодії банку з клієнтами та засобами масової інформації; взаємозв'язок з керівництвом банку та регулятором банківської системи; формування команди для ліквідації інциденту та наслідків; збір та аналіз інформації про кризову ситуацію після її ліквідації та притягнення до відповідальності винних осіб.

Джерело: розроблено автором за матеріалами [20]

Банкомати – ще одна область, яка має високий рівень ризику. Причому обсяг шкідливого програмного контенту в банкоматах у 2023 році зріс на 12% порівняно з 2022 роком, а лише 19 відсотків банків повідомили про загрозу атак на них. Проте, у середньому витрати комерційних банків на кібербезпеку становлять 2,204 млрд грн на рік, що утричі перевищує подібні статті витрат нефінансових установ [22].

Ця статистика наголошує на тому, що банківська установа повинна створити систему управління ризиками електронного банкінгу. Це означає, що він повинен мати окремий відділ, який займатиметься ідентифікацією, оцінкою, керівництвом, контролем і моніторингом ризиків електронного банкінгу. Ризики, пов'язані з електронним банкінгом, ймовірно, зростуть у міру розвитку інформаційних технологій у банківській галузі. Міжнародні рекомендації вимагають створення системи управління ризиками, щоб ідентифікувати, керувати та контролювати ризики електронного банкінгу більш ефективно та запобігати їх поширенню на всіх рівнях функціонування банківської установи.

У процесі управління ризиками цієї категорії потрібно чітко та конкретно розмежовувати обов'язки відповідальних осіб відділу управління ризиками електронної форми банківництва з метою підвищення точності та своєчасності ідентифікації, одночасно зберігаючи розуміння того, наскільки вони пов'язані один з одним. Система управління ризиками електронного банкінгу,

розроблена банком, повинна відповідати міжнародним стандартам і забезпечувати:

1. у повній мірі нагляд та контроль здійснюваних операцій, які проходять через різні канали електронного банкінгу на відповідний рівень безпеки;

2. ретельний контроль процесу ідентифікації та авторизації клієнтів у системі електронного банкінгу, щоб уникнути вторгнення третіх осіб;

3. збереження конфіденційної інформації клієнтів.

Під час розробки з подальшим впровадженням системи ризик-менеджменту електронного банкінгу надзвичайно важливо розробити стратегію оцінки, контролю та нагляду за діями провайдера електронного банкінгу. Це пов'язано з тим, що кваліфікація та фінансовий стан провайдера будуть прямо корелювати з якістю роботи систем електронного банкінгу.

Базельський комітет з питань банківського нагляду запропонував стандарти, які допоможуть визначити основні джерела ризиків у сфері електронного банкінгу та створити основу для управління цими ризиками. Крім того, ще на етапі формування стратегічних цілей банку, відповідно із здійсненням аналізом цих принципів, які надалі слід враховувати під час розробки методів управління ризиками електронного обслуговування, дозволить оцінити можливість і доцільність банківської установи впроваджувати електронне банківське обслуговування.

В умовах сьогодення електронні банківські послуги слугують необхідною мірою з метою конкурентоспроможності на банківському ринку послуг, хоч впровадження цих технологій збільшує ймовірність виникнення банківських ризиків, якщо виникнуть певні події чи збої в програмному забезпеченні, які ускладнять або унеможливлять клієнтам виконувати банківські операції чи послуги дистанційно. Операційні, юридичні, стратегічні, репутаційні та ліквідні ризики є основними ризиками електронного банкінгу. Їх відрізняє від традиційних банківських ризиків те, що вони мають абсолютно нові джерела несприятливих подій. Через особливості електронного обслуговування клієнтів цей профіль банківських ризиків значно розширюється.

Висновки до першого розділу

В першому розділі кваліфікаційної роботи розглянуто дослідження сучасних підходів вітчизняних науковців щодо визначення сутності та забезпечення фінансово-економічної безпеки банківських установ. Оцінка сучасної банківської фінансово-економічної безпеки залежить від повноти, ефективності та своєчасності управлінських заходів із ліквідації, спрямованих на запобігання існуючим і потенційним ризикам для банківської системи. Внутрішні та зовнішні фактори сприяють ризикам для економічної безпеки банків.

В роботі розглянуто ризики, які можуть спричинити в умовах сьогодення електронні банківські послуги, які є мірою забезпечення конкурентоспроможності на сучасному банківському ринку послуг, проте їх впровадження збільшують ймовірність виникнення певних подій чи збоїв в програмному забезпеченні, які ускладнять або унеможливлять клієнтам виконувати банківські операції чи послуги дистанційно.

Банківська система зазнала значних змін через значну кількість подій, які виникали останнім часом в Україні. Зокрема, їх початок береться з часів банкрутства «Lehman Brothers», оскільки наступне зростання фінансового стресу відбулося під час економічної кризи в 2014-2015 роках. Рівень стресу почав значно зменшуватися лише після початку переговорів про реструктуризацію державного боргу у 2015 році, але введення карантину в березні 2020 року спричинило новий зріст індексу фінансового стресу. Останні події повномасштабного вторгнення Росії значно збільшило індекс і усі його компоненти зросли. Наведені події свідчать про системний характер стресу для фінансового сектору нашої країни.

На основі проведеного дослідження можна зробити висновок, що необхідна додатково оцінка бізнес-моделі, яка допоможе надати оцінку ефективності функціонування системи безпеки банківської основі на перспективній основі за допомогою SREP-аналізу, що охоплює основні

напрями роботи банку, його діяльність, профіль ризиків і бізнес-модель функціонування. Сьогодні для проведення таких аналізів і оцінок життєздатності бізнес-моделей банків потрібні додаткові дослідження, доопрацювання та адаптація до поточної економічної та політичної ситуації в нашій країні.

РОЗДІЛ 2
ФІНАНСОВО-ЕКОНОМІЧНИЙ АНАЛІЗ БАНКІВСЬКОГО СЕКТОРУ УКРАЇНИ ТА ЙОГО ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ

2.1. Макроекономічні, фіскальні та інформаційні ризики в умовах війни

Одним із найважливіших елементів стабілізації макроекономіки є стан державного бюджету. Його формування значною мірою впливає на макроекономічні ризики, пов'язані з накопиченим державним боргом, державними гарантіями та діяльністю підприємств у державному секторі економіки. Фінансовий ризик полягає в тому, щоб компенсувати додаткові втрати держави, особливо втрати, спричинені військовими діями, під час економічних труднощів.

Прогнози щодо цьогорічного зростання економіки покращуються завдяки стійкості української енергетичної системи. Прогнозується зростання ВВП на 2%, а інфляція буде знижена на 15%. Незважаючи на дефіцит торгівлі товарами та послугами, значна і постійна міжнародна фінансова підтримка дозволяє збільшити міжнародні резерви. Ситуація на валютному ринку покращилася, оскільки інтервенції НБУ зменшилися, курс готівки наближається до безготівкового, а очікування бізнесу та населення покращилися [23]. Але українська економіка слабка та схильна до безпекових ризиків, а попит на банківські послуги знижений.

Незважаючи на поступове відновлення економіки, вона все ще є чутливою. Економіка України почала поступово відновлюватися, незважаючи на продовження бойових дій і повітряні атаки Росії на українські міста. У 2024 році реальний ВВП має зрости на 2%. Порівняно з початком року НБУ покращив прогноз, головним чином через те, що енергетичний сектор не постраждав від повітряних атак Росії. Таким чином, показники діяльності підприємств в роздрібній торгівлі та сфері послуг покращилися (рис. 2.1).

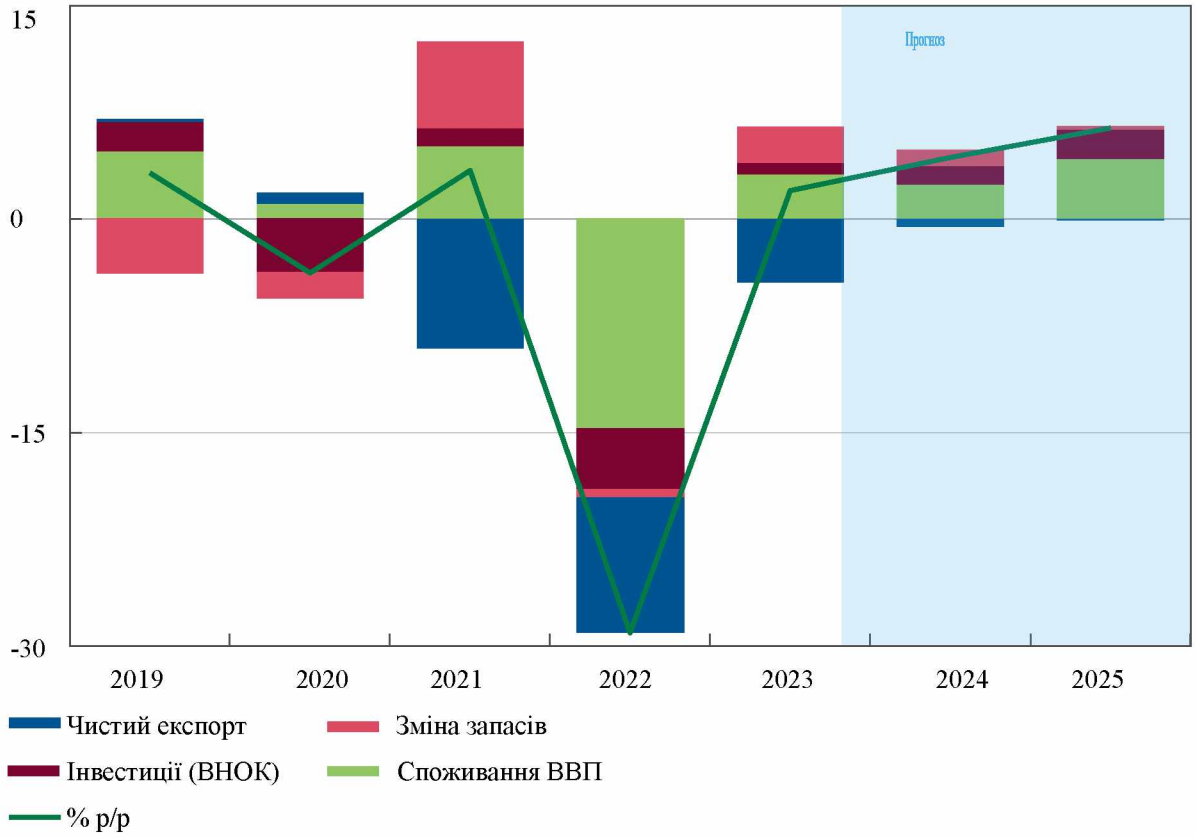

Рис. 2.1. Внески категорій кінцевого використання в зміну реального ВВП, в. п.

Джерело: [24]

Країни партнерів надалі забезпечуватимуть зростання видатків держбюджету та зростання очікувань домогосподарств продовжуватиме стимулювати споживчий попит. Тим не менш, руйнування виробничих потужностей та інфраструктури, особливо енергетичної, продовжуватиме обмежувати економічну активність, і необхідні значні ресурси для їх відновлення.

У результаті війни економіка продовжує нести втрати і залишається уразливою до безпекових ризиків, як це було продемонстровано підривом Каховської ГЕС російськими військами. Небезпека належного функціонування «зернового коридору» та перспективи збільшення пропускної здатності сухопутних експортних шляхів залишаються невизначеними [25]. Обмеження на імпорт харчових продуктів з України до країн ЄС, які сусідять з Україною, є

ще однією проблемою. Інвестори бояться ризиків. У зв'язку з повільним відновленням економіки попит на певні банківські послуги, особливо кредити, залишається низьким.

Слабша інфляція дозволить швидше знижувати ставки, оскільки її падіння відбувається швидше, ніж очікувалося. Даному ефекту сприяє достатня пропозиція пального та продовольства, менший дефіцит електроенергії та покращені інфляційні очікування через сприятливі умови на валютному ринку. Свій внесок у сповільнення росту цін продовжуватиме призводити до зниження світової інфляції. Прогнози НБУ передбачають, що зростання споживчих цін до кінця року не перевищуватиме 15%.

Зниження облікової ставки є результатом зниження інфляції, стабільності на валютному ринку та комфортного рівня міжнародних резервів. Відповідно до поточних оцінок, це може статися вже цього року, і навіть раніше, ніж передбачалося в квітневому макропрогнозі. Таким чином, високі номінальні процентні ставки поступово зникнуть із фінансової системи. Фінансові установи матимуть достатньо часу, щоб змінити ціни на свої основні товари завдяки швидкості та прогнозованості цього процесу.

Міжнародна допомога сприяє нарощуванню резервів і покриває розриви платіжного балансу. За прогнозом НБУ торгівля товарами та послугами продовжує демонструвати значний дефіцит, який становив 9.3 млрд дол. у I кварталі, що становить 27.8% ВВП. Порівняно з IV кварталом 2022 року надходження від експорту низки товарів скоротилися. Це стосується продовольства, оскільки світові ціни знизилися, а також хімічної промисловості, оскільки внутрішній попит на добрива зріс.

Зменшилися також обсяги експорту послуг у секторі IT. Витрати громадян України за кордоном мали значний негативний вплив на поточний рахунок. Ці фактори будуть присутні й надалі. З квітня поточний рахунок зазнав додаткового тиску через додаткові труднощі, пов'язані з роботою «зернового коридору», а також запровадження європейськими країнами обмежень на імпорт української їжі. Тим часом надходження від міжнародних

партнерів значною мірою покриють дефіцит торгівлі товарами та послугами. (рис. 2.2).

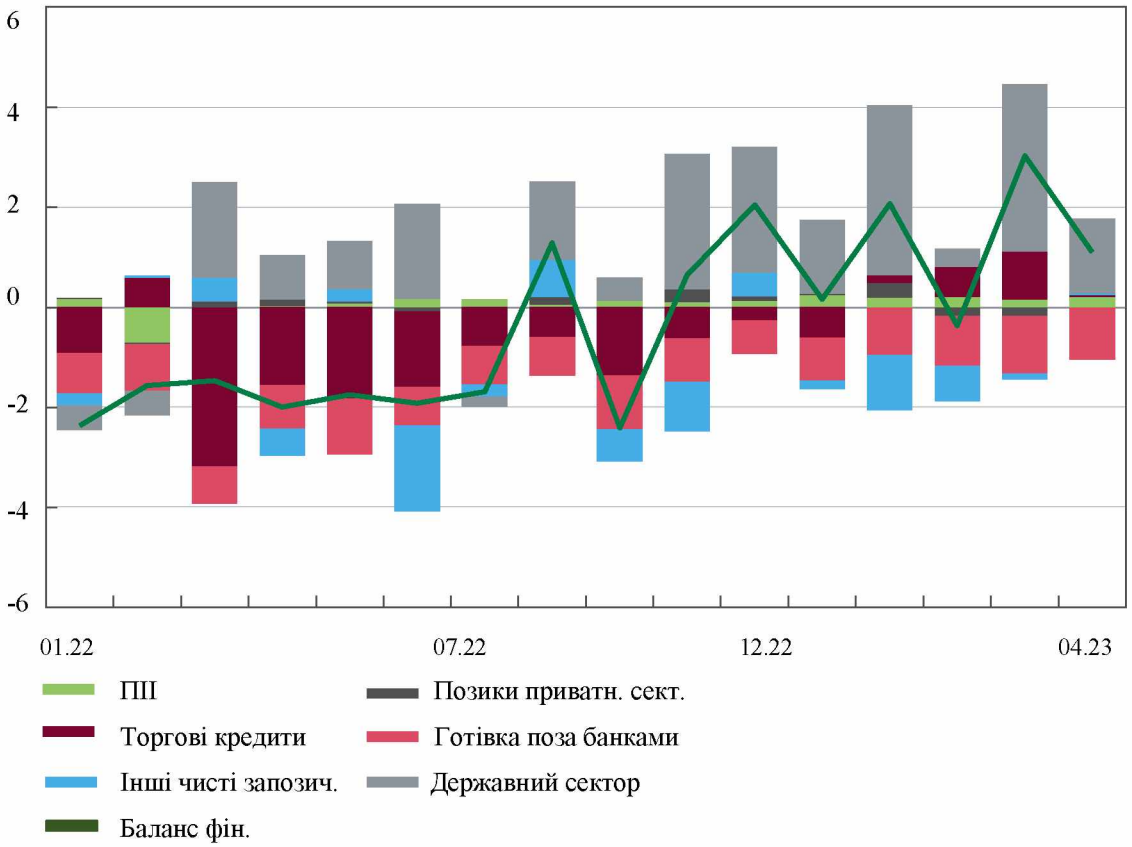

Рис. 2.2. Баланс фінансового рахунку, млрд дол.

Джерело: [24]

Надходження капіталу у вигляді позик за фінансовим рахунком слугує результатом забезпечення міжнародної фінансової допомоги. Крім того, заборгованість нерезидентів за торговими кредитами зменшилася. Приватний бізнес приходить в країну завдяки потребі в фінансуванні бізнесу та стабільності валютного ринку. Цей тренд залишиться.

Умови міжнародних резервів покращують курсові очікування. На валютному ринку ситуація покращилася. В порівняні з періодом місяців грудня-лютого кількість дій НБУ зменшилася. Це призвело до збільшення продажу валюти аграрними підприємствами під час посівної кампанії, одночасно зменшуючи попит на валютні ресурси весною зі сторони імпортерів

енергоресурсів.

Крім того, було введено обмеження на гральні заклади, що призвело до зменшення відпливу коштів за операціями з картками. Отже, з початку року гривня зміцнилася на 9 відсотків, а курс практично зрівнявся з безготівковим. Різниця між ними наприкінці минулого року становила десять відсотків. Таким чином, курсові очікування як бізнесу, так і населення покращилися. Це зменшує попит населення на гроші. Зокрема, у травні населення купувало найменшу кількість валюти з серпня.

Міжнародні резерви зросли до найвищого рівня за останні 11 років завдяки значній міжнародній допомозі та меншим інтервенціям НБУ. Їхній обсяг наприкінці травня становив 37.3 млрд дол., – результат еквівалентний майже п'яти місяцям потенційному обсягу майбутнього імпорту (рис 2.3). Такий запас міцності відкриває нові можливості для поступового перегляду обмежень на валюту.

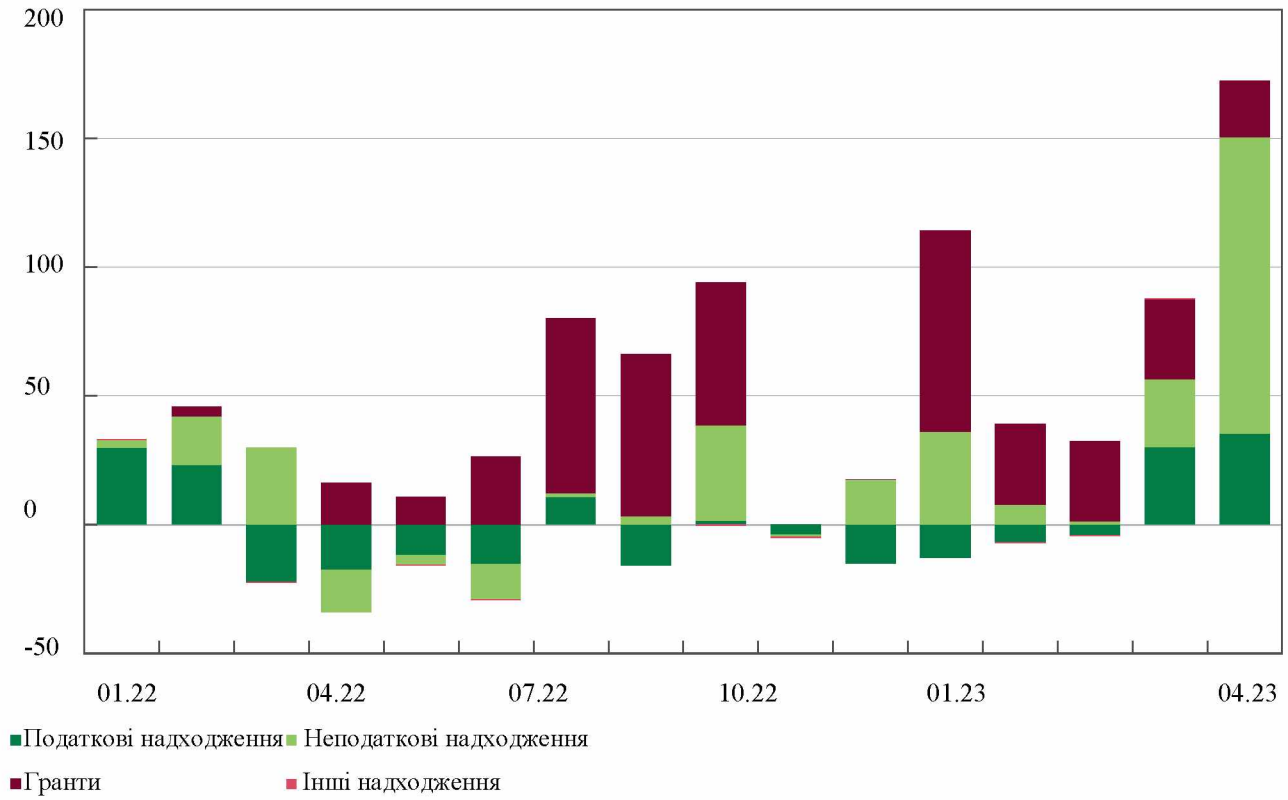

Рис. 2.3. Внески в річну зміну доходів зведеного бюджету, в. п.

Джерело: розроблено автором за матеріалами [24, 26]

Ліквідність уряду підтримується постійними надходженнями коштів від донорів. Унікальний рівень дефіциту державного бюджету є результатом значних потреб у забезпеченні обороноздатності. Прогноз НБУ передбачає, що на 2023 рік загальний дефіцит державного бюджету без грантів становитиме понад 1.7 трлн грн, що становить 26% ВВП. Водночас існує загроза його розширення; цього року плановий дефіцит вже двічі переглянули. З об'єктивних причин існує обмежена ймовірність скорочення видатків. Натомість вони можуть збільшитися, якщо буде потрібно більше грошей на військові сили, соціальну допомогу та відновлення пошкодженої інфраструктури. Що стосується енергетичного сектору, підвищення тарифів лише частково пом'якшить накопичення квазіфіскальних дефіцитів.

Бюджетні потреби продовжують залежати від міжнародної допомоги. Затверджена в березні нова чотирирічна програма МВФ є важливою для бюджету. Крім отримання значних фінансових ресурсів, його реалізація сприятиме структурним реформам, особливо щодо управління державними фінансами. Ліквідність уряду значно зросла завдяки постійному надходженню міжнародної допомоги. Буфер ліквідності дозволяє своєчасно виконувати зобов'язання та збільшити горизонт планування витрат. Покращення графіка платежів за державною програмою «Доступні кредити 5-7-9%» має бути одним із позитивних наслідків.

Збільшення ролі внутрішніх залучень у фінансуванні дефіциту бюджету є очікуваним. Беземісійне фінансування забезпечує наповнення бюджету поточного року. Цьогоріч роловер внутрішнього боргу значно перевищує сто відсотків як у національній, так і в іноземній валюті, після низьких показників минулого року. (рис. 2.4).

Таким чином, залучення уряду до гривневих надходжень вже перевищило весь 2022 рік. З початку року портфель ОВДП банків зріс на 60 млрд грн. Тим не менш, значною мірою це зростання було зумовлено діями Національного банку Японії, які включали дозвіл на часткове покриття обов'язкових резервів банків за допомогою бенчмарк-ОВДП. Однак наразі цей вплив майже

завершено. Натомість значний запас ліквідності в банківському секторі буде створений завдяки подальшому збільшенню залучень. Сповільнення інфляції, що призводить до зростання реальної дохідності гривневих боргових інструментів, є ще одним фактором. Ринок має продовжувати залучати уряд.

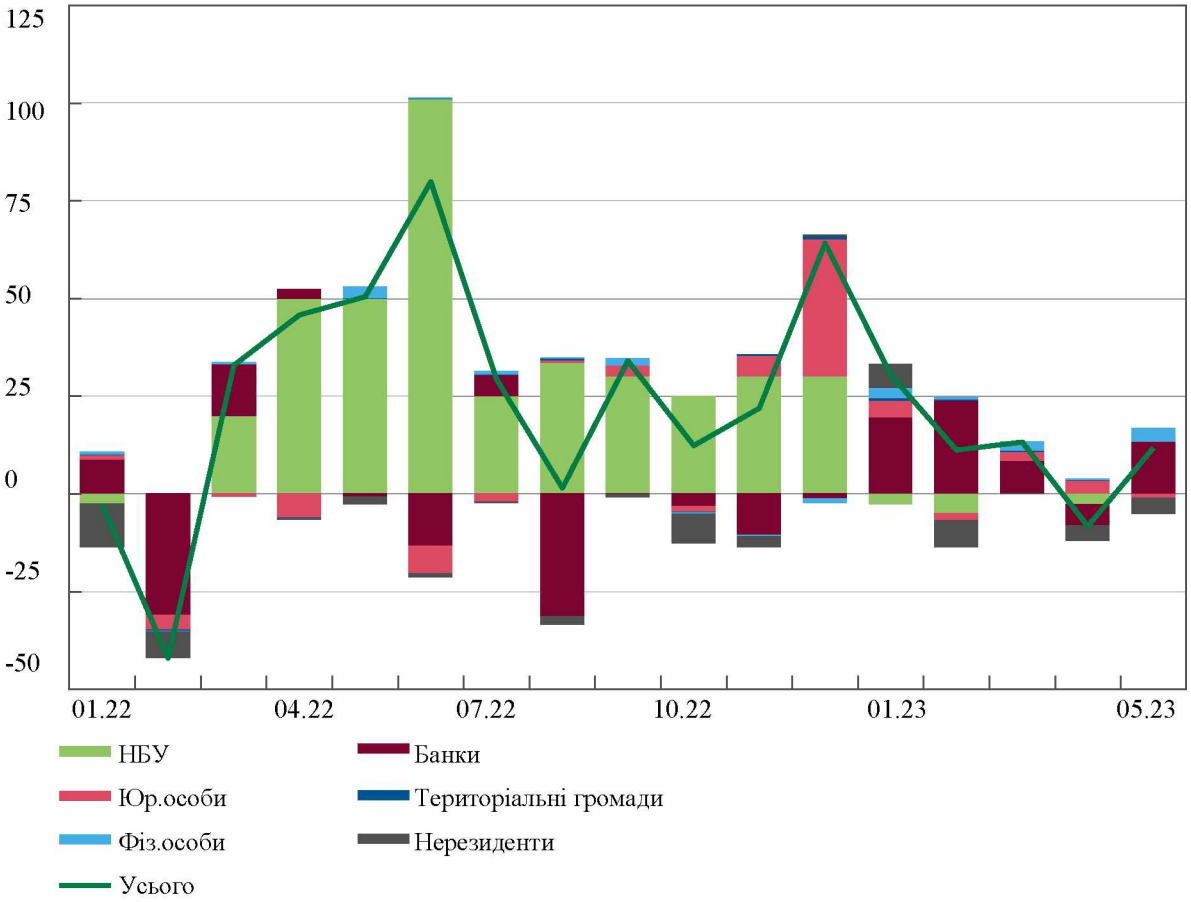

Рис. 2.4. Зміна обсягів ОВДП в обігу, за номінальною вартістю, млрд грн

Джерело: розроблено автором за матеріалами [24, 26]

Отже, шляхом системного вдосконалення механізму державного управління центральними та місцевими органами виконавчої влади можна досягти підвищення рівня раціонального розпорядження фінансових ресурсів країни, яке є вирішальним в питаннях економічно зросту нашої держави.. Таким чином, з метою зменшення ризиків у фінансовому секторі України виникає необхідність щодо розробки програми та рекомендацій з додержанням послідовних дій з питань забезпечення бюджету держави безперебійними

надходженнями. Це можливо за чітким реформуванням видаткової частини бюджету та удосконалення бюджетного процесу, щоб зробити бюджетні рішення більш якісними та ефективними.

2.2. Фактори ризику ліквідності та фондування банківського сектору

В сучасних умовах банківський сектор страждає від постійних фінансових криз, невизначеності та нестабільності в економіці. В таких умовах функціонування комерційних банків все частіше піддається ризику, що може зашкодити фінансовій стійкості банку. Здатність банку якісно та ефективно виконувати свої основні функції безпосередньо пов'язані з ліквідністю, яка є одним із основних критеріїв, що визначають стабільність банківської діяльності.

Сьогодні українські банки змушені працювати в умовах зростання ризиків. Це пов'язано з погіршенням операційного середовища в Україні, недостатністю капіталу банківської системи, нестабільністю ресурсної бази та великою кількістю недіючих кредитів у кредитному портфелі. Навіть попри значне підвищення вимог НБУ до обов'язкових резервів, банки зберегли значну кількість високоліквідних активів. Коефіцієнти ліквідності як у національній, так і в іноземній валюті перевищують мінімальні вимоги.

Банки вклали велику кількість грошей у бенчмарк-ОВДП та тримісячні депозитні сертифікати, що призвело до переваги довших інструментів. Ресурси бізнесу стали основним джерелом поповнення коштів останнім часом, тоді як темпи залучення коштів серед населення значно сповільнилися [27]. Натомість банки покращили строкову структуру вкладів населення. Крім того, для системи притаманний помірний ризик ліквідності.

Банківська система зберігає значну кількість ліквідності. У середньому по сектору норматив короткострокової ліквідності LCR у всіх валютах більше ніж втричі перевищує мінімальний. Завдяки припливу коштів клієнтів банки усіх груп мають достатній запас високоякісних ліквідних активів. Останніми

формується понад 90 відсотків зобов'язань. Банки повертають кредити рефінансування НБУ та скорочують зовнішні борги, оскільки їм не потрібні додаткові ресурси. У червні частка рефінансування зобов'язань уже становила менше 1%. Зовнішні борги банків також скоротилися на майже 14% з початку 2022 року, їхня частка в зобов'язаннях вже менше 2%. Це найнижча динаміка з першої половини 2004 року. Для банків ринок зовнішніх залучень фактично закритий під час війни [28]. З іншого боку, вітчизняні фінансові установи не відчувають нестачі ресурсів на внутрішньому ринку, у тому числі в іноземній валюті.

Рішення Національного банку України змінює структуру гривневих високоліквідних активів. Обсяг високоякісних ліквідних активів знизився на 9% наприкінці травня порівняно з початком року (рис. 2.5). Зміна, спричинена запровадженням НБУ заходів для зв'язування ліквідності, є основною причиною.

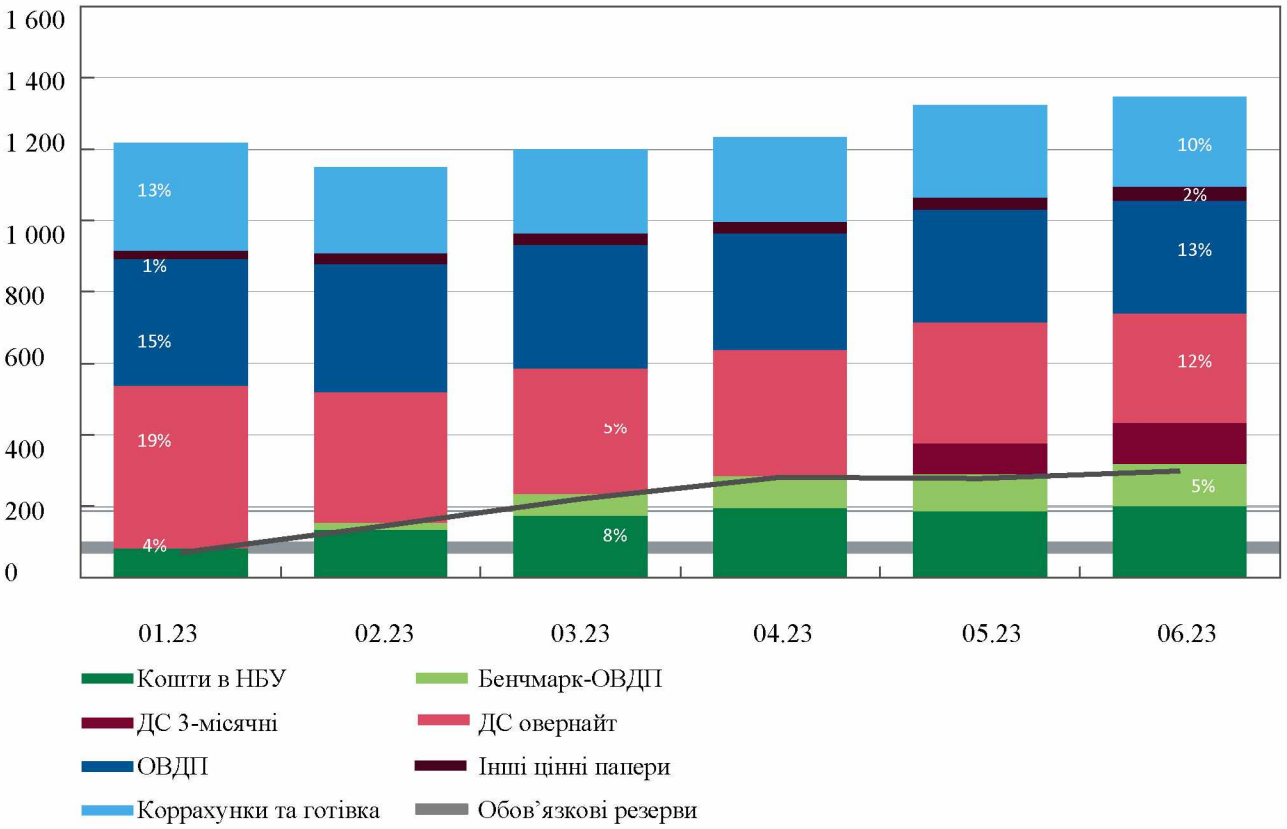

Рис. 2.5. Високоліквідні активи та їхня частка у чистих активах, млрд грн

Джерело: [29]

Таким чином, з початку 2023 року вимоги до обов'язкового резервування зросли. Це було особливо помітно для короткострокових коштів населення. Крім того, банки були змушені перевести певну кількість високоякісних ліквідних активів у кошти на коррахунку в Національному банку.

З іншого боку, спеціальні бенчмарк-ОВДП, які приносять ринкову дохідність, дали банкам можливість задовольнити частину вимог до обов'язкових резервів. Тобто, ліміт придбання бенчмарк-ОВДП для покриття обов'язкових резервів був майже повністю використаний більшістю банків. Ці активи становили 4,7% чистих активів, або 116 млрд грн. Через обмеження, встановлені материнськими банками на інвестування в державні цінні папери, іноземні банки менш активно купували бенчмарк-ОВДП.

У квітні 2023 року Національний банк України змінив структуру операційної монетарної політики та запровадив тримісячні депозитні сертифікати з дохідністю, вищою за дохідність інструментів овернайт. Крім того, банки вже вклали 117 мільярдів гривень у новий більш довший інструмент. Банки докладають понад три місяці, щоб залучити кошти фізичних осіб, щоб отримати доступ до цього інструменту. Збільшення частки високоліквідних активів, представлених довшими інструментами, не збільшує тиску на ліквідність банків, оскільки під заставу цих паперів легко отримати рефінансування.

Склад високоліквідних активів у валюті складався переважно з готівки, валютних ОВДП та коштів на кореспондентських рахунках в іноземних банках інвестиційного класу. Для цілей розрахунку LCR в іноземній валюті з 1 січня 2023 року введено правило, що частка коррахунків у банках інвестиційного класу не повинна перевищувати 80% високоліквідних активів (рис. 2.6). Можна виявити циклічні зміни, аналізуючи динаміку показників у межах одного ділового циклу. Банк може відчути додаткову потребу в ліквідних коштах, оскільки попит на кредити зазвичай збільшується швидше, ніж депозитна база, коли бізнес розвивається.

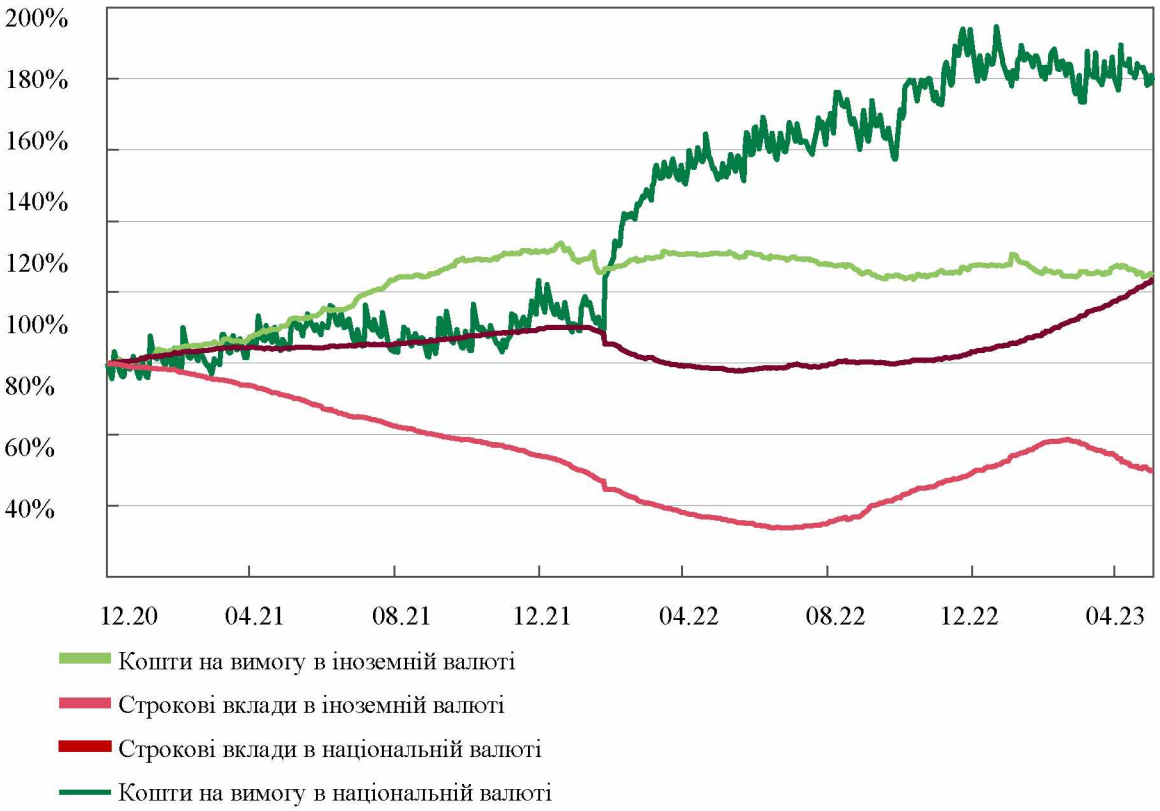

Рис. 2.6. Вкладені кошти фізичних осіб в комерційних банках

Джерело: [29]

Це змусило банки інвестувати частину своїх грошей із рахунків в іноземних банках у суверенні облігації, особливо в Сполучених Штатах. Банки продовжують проводити валютні операції, незважаючи на високу дохідність за цими цінними паперами. Зростають вимоги до короткострокової ліквідності LCR в іноземних валютах, а медіанне значення сектора перевищує мінімальні вимоги втричі [30]. Банки з іноземним капіталом зберігають більшість високоліквідних коштів в іноземній валюті.

Незважаючи на те, що грошові кошти вкладників серед звичайного населення майже не зростають, їхня строкова структура покращується. З початку року гроші населення в банках лише незначно зросли. Насамперед це пов'язано зі змінами, внесеними до політики оплати праці військових, які торік були основним джерелом зростання ліквідності. Навіть попри надходження більшості коштів населення до державних і приватних банків, все ще існує нерівномірність припливу коштів населення до різних груп банків. Приплив

строкових депозитів сприяв незначному збільшенню вкладів протягом останніх місяців.

Значного приросту набули строкові депозити населення у національній валюті з самого початку року (рис. 2.7).

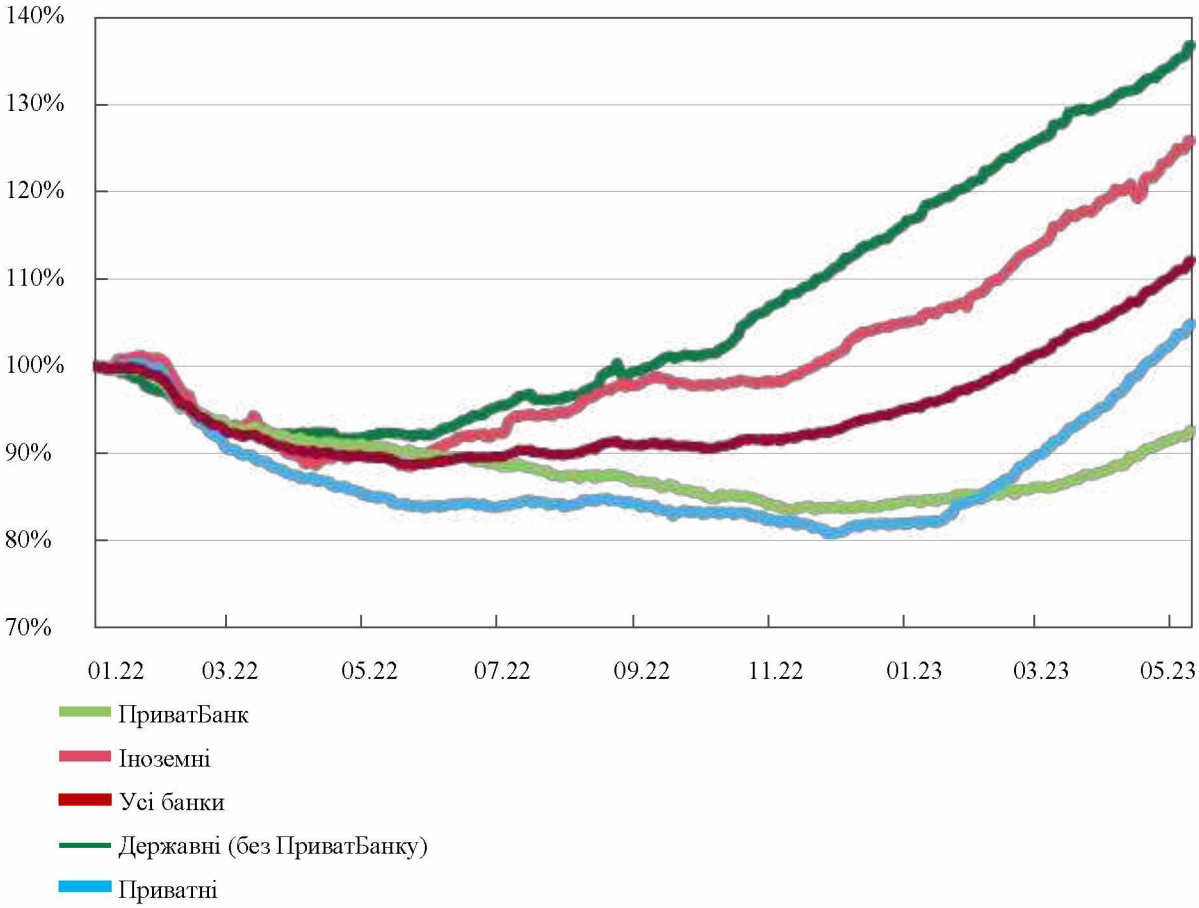

Рис. 2.7. Строкові гривневі кошти фізичних осіб

Джерело: [31]

Сталося подібне лише завдяки підвищенню процентних ставок комерційними банками за депозитами на довший період, а іноді зі зниженням за короткими, у відповідь на зміни в монетарній політиці Національного банку України. Роздрібні строкові кошти в гривні зросли на 19% з початку року, а їхня частка зросла на близько 5% до 35%. Цей тренд є результатом зусиль Національного банку України збільшити строкові вкладення у загальному потоці коштів населення.

Загалом, у більшості країн ЄС частка строкових депозитів у вкладах населення невелика (рис. 2.8).

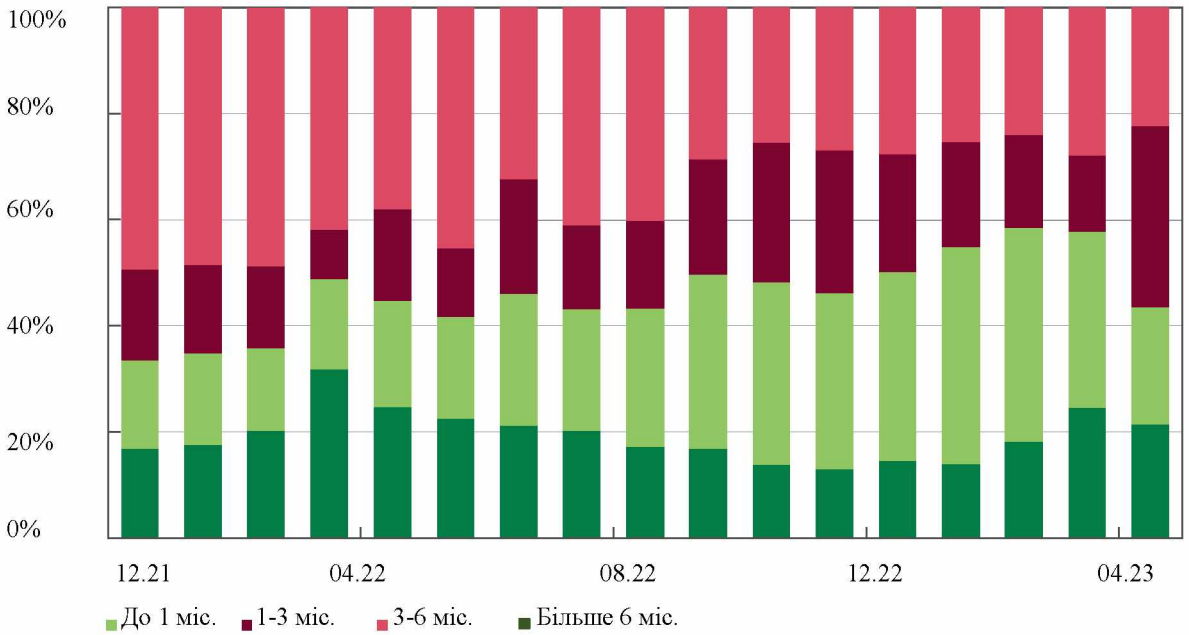

Рис. 2.8. Структура нових депозитів домашніх господарств

Джерело: [31]

У Єврозоні частка поточних рахунків і депозитів на вимогу приблизно 61%, а в ЄС 76%. Відповідно до європейських стандартів для визначення нормативів ліквідності навіть поточні вклади населення вважаються стабільними.

Тільки у трьох країнах ЄС більше 50% строкових депозитів становлять вкладення з можливістю дострокового розірвання договору. Крім того, банки в Україні пропонують такі вклади, які можуть становити до 14% усіх строкових депозитів суспільства [32]. Близько 40% цих вкладів зосереджено в шести найбільших банках, з яких один є державним. Частка цих коштів останнім часом зросла незначно. В сучасних умовах наростаючої нестабільності право на строкове розірвання депозиту може приваблювати клієнтів. За таке право клієнти зазвичай не отримують доходу.

Нарощення фондування фінансується корпораціями, бо останнім часом гроші корпорацій ростуть швидше, ніж гроші населення. Це пов'язано з

відновленням доходів з одного боку, а з іншого – з помірними вимогами бізнесу до їх використання. Банки кажуть в опитуванні про умови фондування, що пропозиція корпорацій є основним двигуном приросту. З початку року до червня грошові кошти корпорацій зросли майже на 20%. У банках усіх груп збільшуються залишки (рис. 2.9).

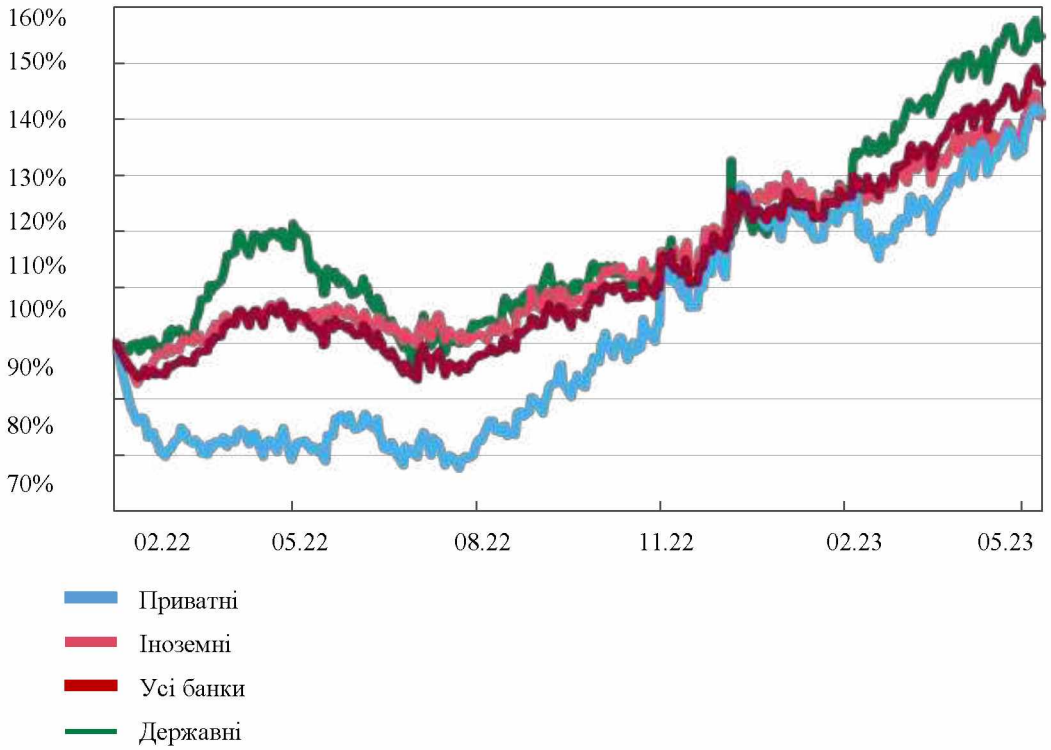

Рис. 2.9. Гривневі кошти суб'єктів господарювання за групами банків, 23.02.2022 = 100%

Джерело: [31]

Загалом, з січня частка депозитів бізнесу в загальній структурі зобов'язань банків зросла на 5% до понад 49%. З початку війни це вперше перевищило частку коштів населення. Насамперед нарощують залишки банків, які базуються на коштах бізнесу як основному джерелі фінансування. Банки активно конкурують за кошти підприємств, що змушує їх підвищувати ставки, щоб утримати клієнтів. Бізнес продовжуватиме отримувати гроші, якщо не буде значних економічних потрясінь.

Валютні вклади стали менш популярні серед населення. Сталося це у зв'язку зі стабілізацією валютного ринку та зменшенням спредів між офіційним і готівковим курсами населення більше не бажає купувати безготівкову валюту на депозити. Зважаючи на підвищення депозитних ставок, строкові вклади в гривні виглядають привабливішими, ніж валютні вклади.

Таким чином, існує тенденція до зниження обсягів строкових депозитів в іноземній валюті через закінчення строків старих вкладів і значне сповільнення припливу нових вкладів. З іншого боку, гроші не знімаються з поточних рахунків. Як наслідок цього, обсяг фінансування населення банками в іноземній валюті майже не змінився. У зв'язку з відсутністю валютного кредитування банки зберігають більшість цих коштів у високоліквідних активах, як і раніше. Крім того, банки майже не зберігають валютні ставки, оскільки не вважають за потрібне збільшувати свої вклади в валюту. Ця складова фондування не створює додаткових ризиків ліквідності для банків.

2.3. Ризик прибутковості комерційних банків

Визначальним фактором фінансової стійкості будь-якого комерційного банку є його дохід. З початком бойових дій банківському сектору вкрай необхідно було пристосовуватися до нових умов функціонування в ризиковому середовищі. Незважаючи на важку ситуацію банки отримали значні операційні та чисті прибутки завдяки високим процентним ставкам. Торік чистий процентний дохід значно зріс і залишається високим за допомогою направлення коштів до пропонованих депозитних сертифікатів від НБУ та стабільному процентному доходу від корпоративного кредитування. Поступове зниження ставок за процентами не повинно мати значного впливу на дохідність, оскільки чиста процентна маржа достатньо висока [33]. Незважаючи на зниження комісійних і валюто обмінних доходів, банки зберігають високу операційну ефективність за допомого. Обсягу чистих процентів доходів і контрольованим адміністративним витратам. Банки стають більш стійкими під

час війни, коли отримують прибуток і запас капіталу. Ці кошти також можуть бути використані з метою погашення втрат від кредитних операцій та бути вагомою підтримкою у період відновлення після бойових дій.

Банківський сектор загалом закінчив минулий рік із прибутком, незважаючи на значні втрати, пов'язані з війною, зокрема через кредитний ризик. На початку 2023 року фінансовий результат значно покращився. Банки отримали більше операційних доходів завдяки збереженню високих процентних ставок і доступу до високоякісних ліквідних інструментів. За результатами діяльності минулого року кількість підприємств, які зазнали збитків, невелика, приблизно така ж, як у 2021 році. Це дрібні банки з активами, які складають менше 1% активів сектору. Під час цього періоду рентабельність капіталу сектору становила 54% на рік. Банки нарощують капітал за рахунок поточних прибутків. Цей капітал можна надалі використовувати для підтримки кредитування та покриття потенційних втрат активів.

Після швидкого збільшення у період другого півроку 2022-го процентні доходи банків залишаються високими. Процентні доходи цього року були на 51% вищі, ніж за той самий період минулого року (рис. 2.10). Банки отримали найбільший прибуток минулого року від надходжень за депозитними сертифікатами, за якими вони розміщували вільну ліквідність. Цього року кількаразовий перегляд правил обов'язкового резервування Національного банку України запровадив обмеження щодо вкладення комерційних банків до депозитних сертифікатів і трохи зменшив доходи від цих інструментів. У свою чергу, дозвіл на часткове виконання вимог щодо обов'язкового резервування за рахунок бенчмарк-ОВДП призвів до більшої кількості державного боргу, які були придбані. Так, доходи у травні місяці від ОВДП мали збільшення з 5% до 22% порівняно з груднем минулого року. У травні загальний процентний дохід від депозитних сертифікатів і ОВДП становив 53%.

Процентні доходи від корпоративного кредитування зросли на 23 відсотки за п'ять місяців порівняно з попереднім роком. Результатом є більші

кредитні ставки за період довоєнних часів та більший обсяг портфеля, незважаючи на його останнє скорочення. Надходження від процентів від кредитів компанії складають приблизно чверть усіх процентних доходів. Банки отримують понад 20 відсотків від кредитування бізнесу за державної програми доступних кредитів під ставкою у 5, 7 або 9 відсотків. Натомість стрімке скорочення портфеля, яке тривало донедавна, було головною причиною скорочення процентних доходів від роздрібного кредитування. У травні їхні процентні доходи становили лише 17 відсотків.

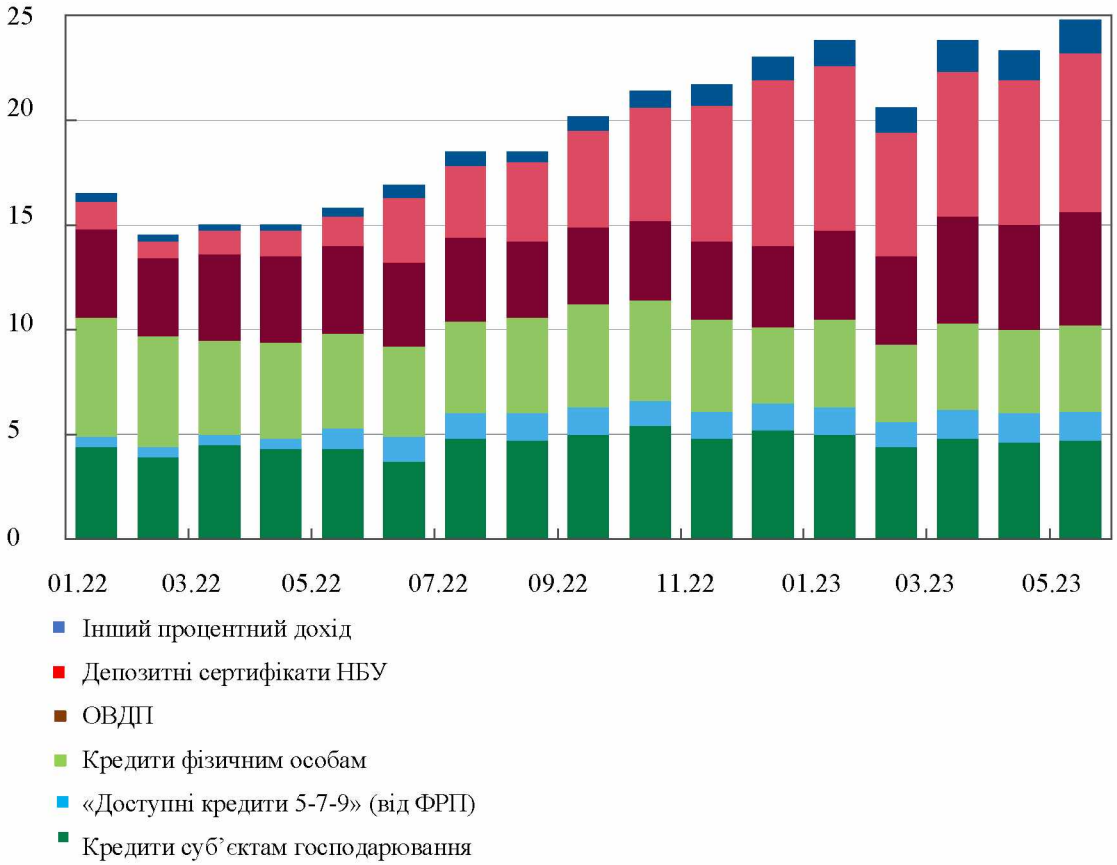

Рис. 2.10. Складові процентних доходів, млрд грн

Джерело: [34]

Співвідношення між отриманими та нарахованими процентними доходами від кредитування все ще становить приблизно сто відсотків. Це коливання значною мірою залежить від нерівномірного надходження компенсацій за процентами 5, 7 або 9 відсотків державної програми доступних

кредитів, коли сплата від клієнтів відбувається частіше. Таким чином, відображені банками процентні доходи найбільш точно показують, скільки коштів надходить.

Найшвидше зростає вартість фондування в корпоративному секторі. За останні п'ять місяців фінансові установи докладали зусиль, щоб збільшити кількість строкових вкладів серед клієнтів. До цього НБУ спонукав банки змінити монетарну політику та підвищити обов'язкові резерви за коштами у період до 3 місяців. Крім того, банки підвищили депозитні ставки для строкових вкладів. (рис. 2.11).

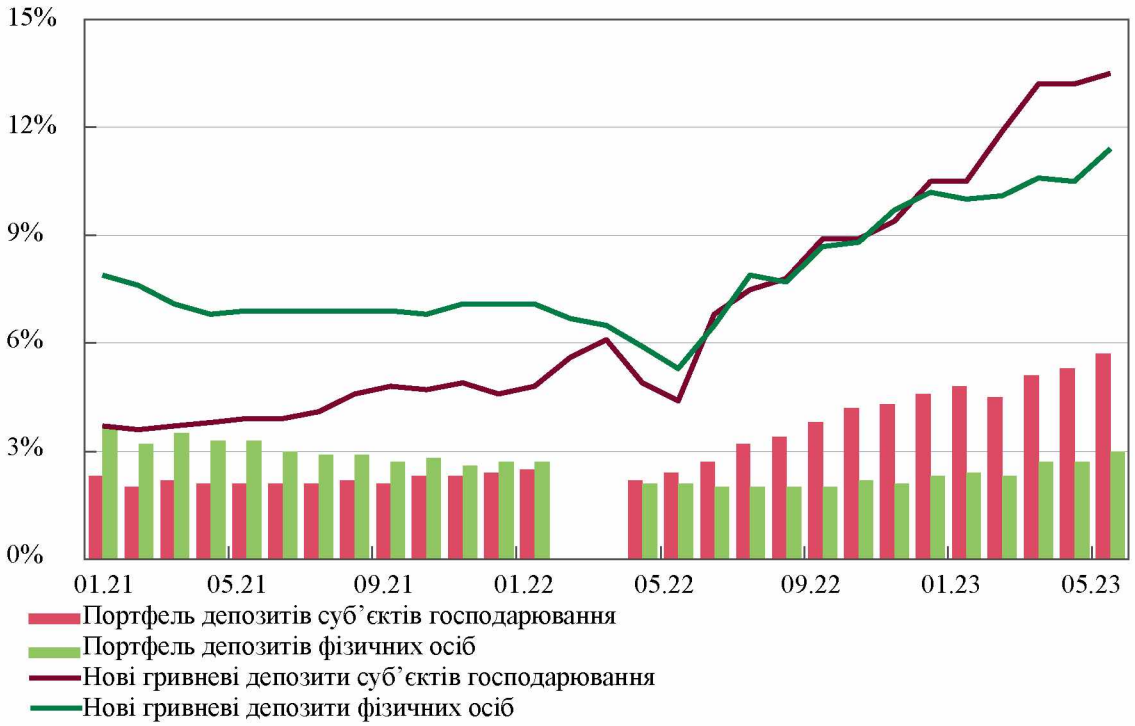

Рис. 2.11. Вартість нових депозитів та наявних портфелів депозитів бізнесу та населення, % річних

Джерело: [35]

Таким чином, можемо вбачати ріст вартості гривневих депозитів за вкладеннями від населення на 2,5 відсотка у період закінчення попереднього року. У результаті UIRD для 12-місячних вкладів зросла до 15% річних, а для тримісячних вкладів – до 14% річних. У той же час дохідність банку

знижувалася, а доступ до коротших інструментів зменшувався. Поєднання цих заходів призвело до збільшення суми строкових коштів населення. З іншого боку, за цей час ставки поточних та короткострокових вкладів лише незначно знизилися, що призвело до незначного підвищення вартості нових роздрібних депозитів. Витрати банківський установ за процентами роздрібного фондування почали поступово зростати через дещо більшу кількість залучених строкових коштів і поступове заміщення дешевших вкладів, залучених торік.

Порівняно з роздрібними депозитами, вартість корпоративних депозитів піддається меншому контролю з боку банківської установи. У бізнес-сегменті багато банків конкурують один з одним, клієнти мають сильніші переговорні позиції та мають незначну різницю між ціновими умовами поточних і строкових вкладів. Банки повинні покривати всю діяльність компанії, щоб утримати клієнтів.

Останніми місяцями банкам стало дорожче приймати фондування від корпорацій, ніж вклади населення. Вартість корпоративного фінансування має зріст майже у два рази більше порівняно з показниками минулого року. Зростали також корпоративні вклади. Крім того, структура процентних витрат значно змінилася за останній рік. За перші п’ять місяців цього року процентні виплати банків на користь бізнесу зросли на 22% порівняно з попереднім роком.

Під час зниження ключової ставки висока процентна маржа захистить прибуток банків. Різке зростання процентної ставки в економіці забезпечили національним банкам сприятливі умови для функціонування (рис. 2.12). Процентні активи банків зростали помітно швидше за вартість фондування. Таким чином, показник чистої процентної маржі мав стрімке зростання в період минулого року.

Банківські системи багатьох інших країн, які зараз переживають цикл підвищення ставок, демонструють такі тенденції. Маржа вітчизняних банків трохи знизилася лише на початку 2023 року. Основним фактором є зниження середньозважених ставок депозитних сертифікатів, яке було спричинено

змінами в структурі монетарної політики. Підвищення вартості фондування та витрати на підтримку обов'язкових резервів є додатковим фактором.

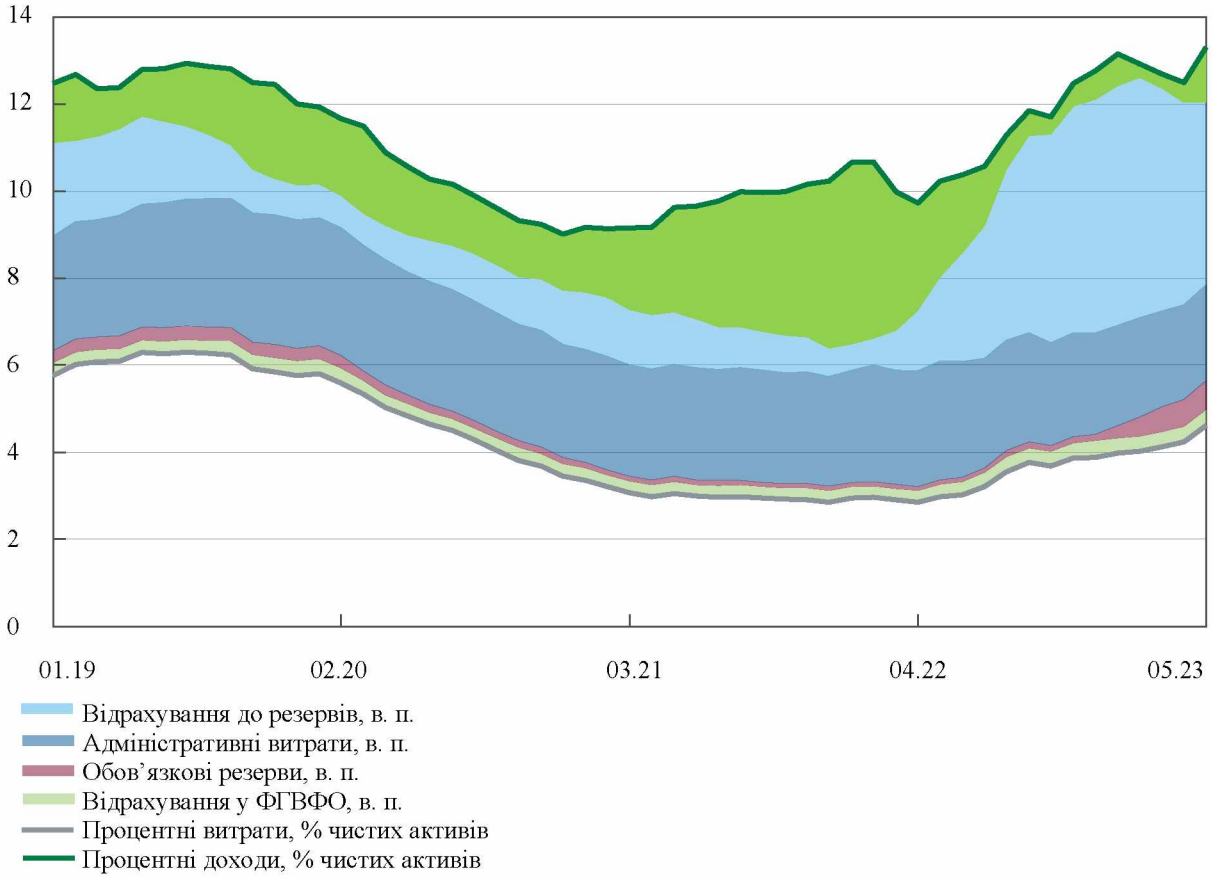

Рис. 2.12. Декомпозиція чистої процентної маржі банків

Джерело: [36]

Зниження ключової ставки, яке очікується, скоротить дохідність активів, особливо безризикових інструментів. З іншого боку, подальший зріст обсягу строкових вкладів разом із нульовою ставкою за поточними коштами знижує маневреність банків у управлінні вартістю фондування. Таким чином, чиста процентна маржа скорочуватиметься. Але оскільки поточні прогнози показують поступову зміну ключової ставки, то банкам буде легше адаптуватися до цих самих змін. Крім того, актуальний показник процентної маржі гарантуватиме достатню дохідність протягом тривалого періоду часу.

Операційні прибутки покривають кредитні втрати. Торік прибутковість банків значно знизилася через високі витрати на формування резервів. В період

майже усього минулого року не відбувалося забезпечення через банківські операції з причин втрат доходу від кредитного ризику. Цьогоріч фінансові установи значно сповільнили процес формування резервів. (рис. 2.13).

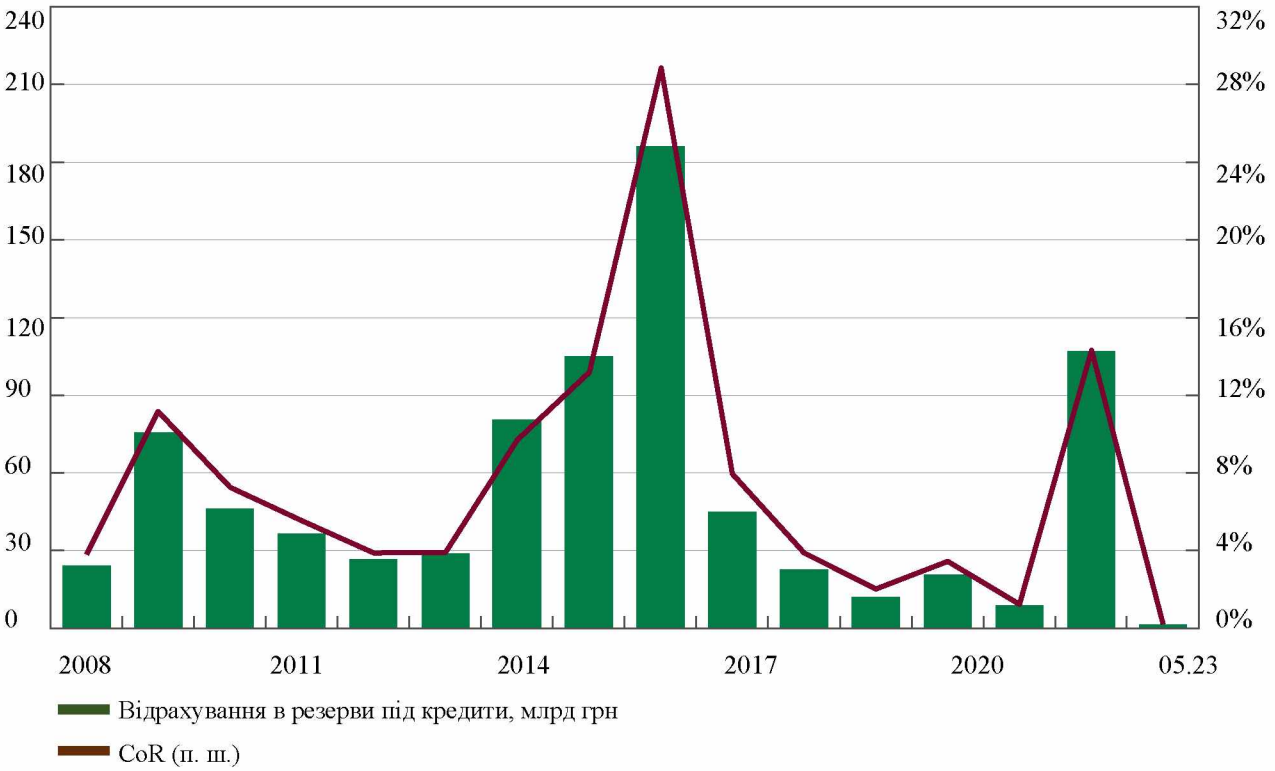

Рис. 2.13. Вартість ризику (CoR)

Джерело: [36]

За п'ять місяців відношення відрахувань на збільшення резервів під кредити відносно чистого кредитного портфеля (CoR) склало менше 1% на рік порівняно з 14% за минулий рік. Вартість ризику, ймовірно, ще зросте протягом року, хоча вона надалі матиме показник у декілька разів менше за минулий рік. Центральним банком було розпочато оцінювання фінансової стійкості 20 найбільших банківських установ, щоб визначити, чи потрібне збільшення фінансових резервів і пруденції. Це можна зробити, не втрачаючи значної прибутковості, завдяки поточній високій маржинальності.

Що стосується комісійного доходу, то обсяги платіжних операцій та чистий комісійний дохід банків майже не постраждали, незважаючи на відсутність економічної активності в період осінні та зими через пошкодження

енергетичної інфраструктури. Середній чек зріс, а кількість здійснених операцій досягла рівня 2021 року. Однак не вдалося зберегти комісійний дохід, позначки якого майже досягали до показників довоєнного періоду. Останнім часом кількість українських мігрантів, які користуються платіжними картками за кордоном, зменшилася. Крім того, кількість транзакцій готівкою в банківських установах самообслуговування в Україні зменшилася та як наслідок, комісійний дохід також зменшився.

Зменшується вплив надходжень від операцій з обміну валюти на прибуток банків, оскільки в останні місяці прибуток банків від цих операцій значно знизився. В період з червня 2022 року до травня поточного року його частка чистого операційного доходу втричі знизилася до 8%. Спред між офіційним і готівковим курсами скоротився після стабілізації на валютному ринку, що призвело до зменшення попиту населення на купівлю валюти. Незважаючи на незначне зниження в останні місяці, кількість транзакцій карткою залишається більшою, ніж довоєнна. Таким чином, надходження від операцій з обміну валюти прибуток буде вищим, ніж до війни, навіть якщо сальдо буде низьким.

Операційні витрати залишаються низькими. Операційні витрати зросли на 7,4% за перші півроку порівняно з аналогічним періодом минулого року (рис.2.14). Додаткові ресурси були потрібні для забезпечення безперебійної роботи відділень під час масованих обстрілів енергетичної інфраструктури та відновлення своєї діяльності в регіонах, які раніше не були окуповані.

Тож за останні п’ять років загальні операційні витрати банків перевищили загальні витрати на утримання основних засобів і нематеріальних активів. Це приблизно п’ята частина всіх операційних витрат. Тим часом банки продовжували скорочувати кількість своїх відділень, намагаючись оптимізувати свою мережу. У той час витрати на співробітників банківського сектору, які з початку року продовжували знижуватися, майже не змінилися.

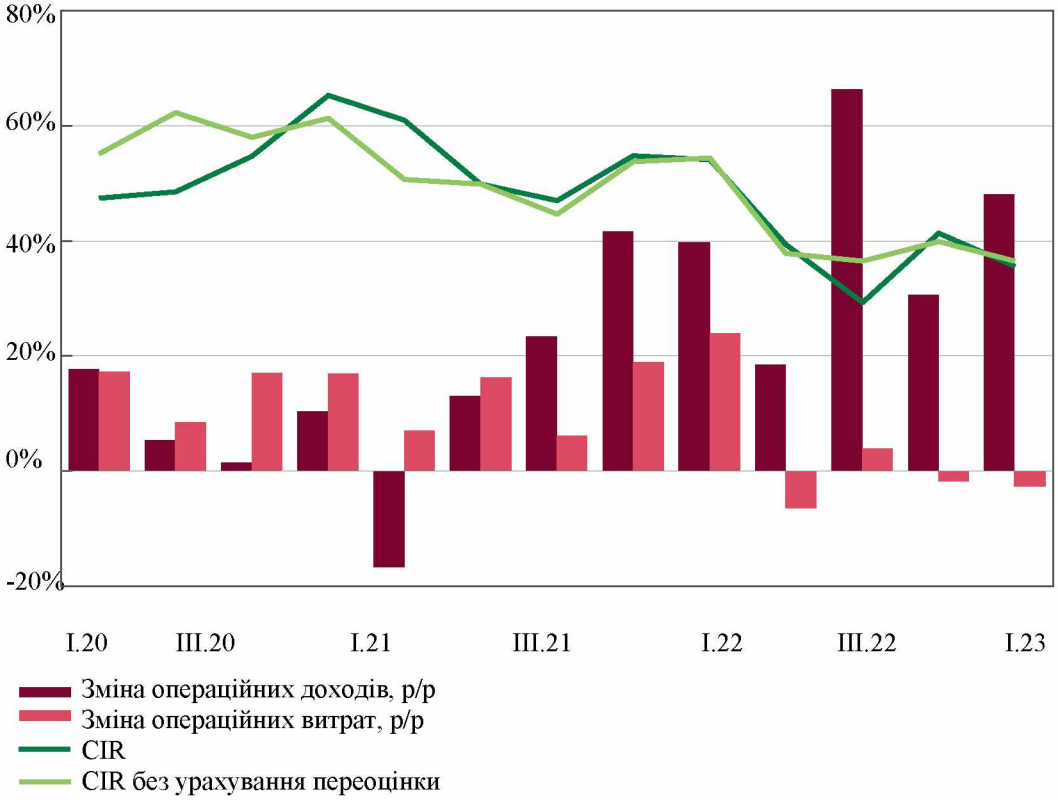

Рис. 2.14. Операційна ефективність банків

Джерело: [36]

Таким чином, відношення витрат від здійснюваних операцій до доходів (CIR) мали все ще кращі показники, ніж вони було до широкомасштабної атаки, оскільки операційний дохід значно зріс. За півроку ця цифра зросла на 38 відсотків, що є найвищим показником за більш як 15 років. Поточна операційна ефективність дає банкам значний запас міцності для потенційного покриття збитків із операцій з кредитними коштами та інших потенційних збитків, які пов'язані з війною.

2.4. Ризик високої частки державного капіталу в банківському секторі

Банки з державною участю відіграють важливу роль у соціально-економічному розвитку країни. Збереження значної частини національного капіталу, що лежить в банківській системі залежить від цих банків. Однак під

час серйозних економічних криз дуже важливо швидко вивчити та визначити, наскільки добре працює державний капітал у банківській системі України, а також розробити подальші дії держави щодо збільшення чи зменшення частки державного капіталу до наявного капіталу комерційних банків.

Робота та функції державних банків змінилися з початком повномасштабної війни Росії проти України. Державні банки підтримують кредитування, особливо державних підприємств, у періоди воєнних ризиків і значної невизначеності, утримують рахунки для державних виплат і залишають належний рівень до надання послуг банківськими установами за допомогою найширших мереж філій. У результаті частка державних банків у всіх базових показниках діяльності комерційних банків значно зросла. Зростання під час кризи є виправданим, але під час відновлення банківського ринку воно створює великі ризики для конкурентів. Таким чином, стратегії державних банків вже зараз потрібно змінювати, щоб вони могли вирішити основні недоліки своєї діяльності та підготувати велику частку банківського сектору до процедури приватизації у післявоєнний період.

У фінансовій системі значна частина держави є основним джерелом додаткових ризиків. Зокрема, дослідження ЄБРР показує, що державні банки дуже схильні до політичного впливу, що значно знижує їхню продуктивність [37]. Розвинені країни, особливо європейські, прагнуть зменшити присутність держав у фінансовому секторі. Цьому сприяють правила ЄС щодо конкуренції та державної допомоги. В Європі державна власність переважно складається з спеціалізованих установ, таких як банки розвитку або експортно-імпортні (наприклад, у Чехії, Словаччині чи Румунії), які надають послуги фінансового сектору, в яких приватні фінансові установи недостатньо активні (рис.2.15).

Але в умовах кризи держава може виявитися найнадійнішим акціонером, оскільки вона має ресурси та бажання допомогти своїм банкам. Таким чином, вкладники відносяться до державних банків із більшою довірою, куди вони часто зберігають свої гроші під час криз. Крім того, державні устрої повинні періодично втручатися в діяльність системно важливих приватних банків з

метою їх порятунку у часи криз. У Східній Європі та Балканах є чудові приклади того, як банки Словенії та Латвії вистояли після світової економічної кризи у 2007-2009 роках.

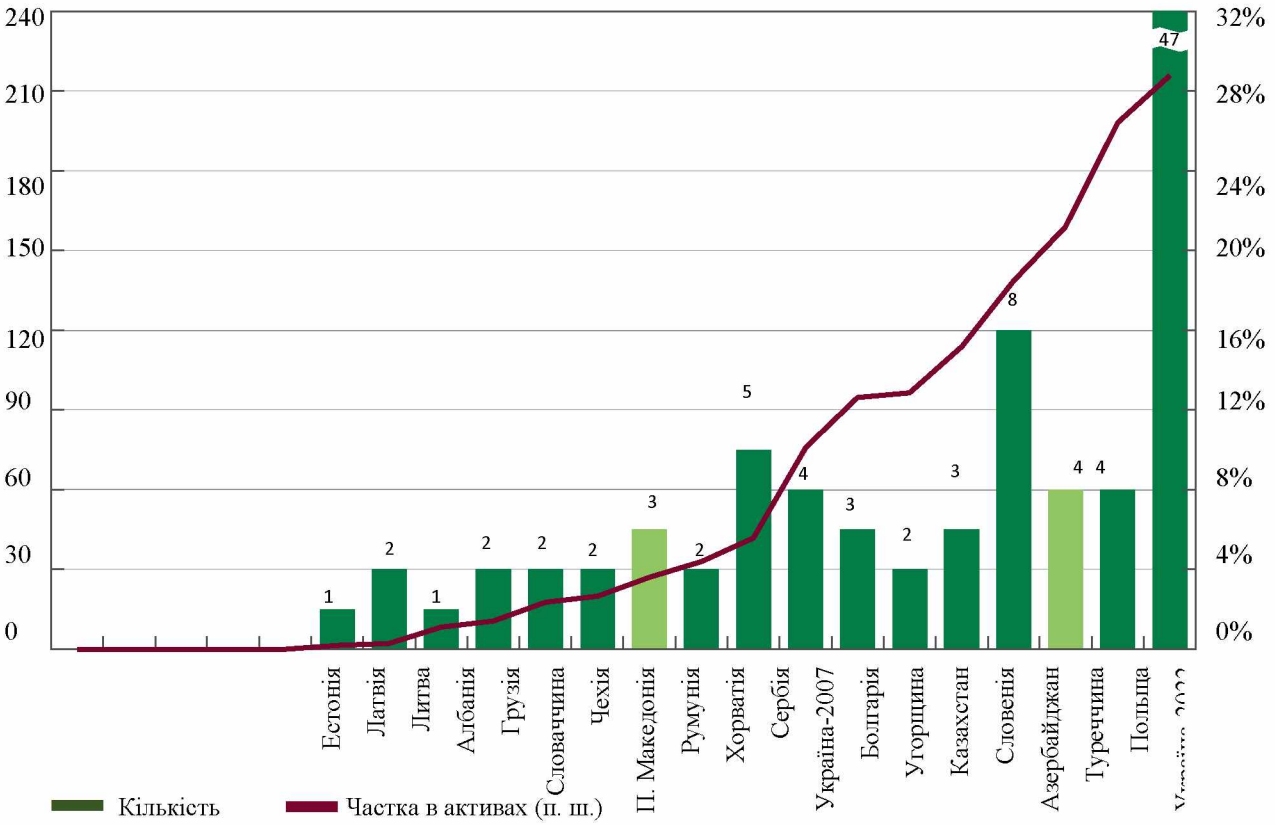

Рис. 2.15. Частка та кількість банків із державним капіталом у банківському секторі країн Центральної та Східної Європи

Джерело: [37]

Участь банківських установ із державним капіталом у країн Європи має тенденцію поступового зниження після кризи за сприятливих ринкових умов. У багатьох сусідніх країнах (в Молдові та країнах Балтії), банки з великою часткою державного капіталу були повністю приватизовані. Виключеннями з цього регіону є Угорщина, у якій збільшення державної частки у приватних банківських установах було пов'язане з політичними причинами, а також Польща, де це зростання було результатом виходу приватних банків з ринку.

Плани приватизації українських державних банків вчергове були відкладені через війну. У минулі кризи банківські установи з великим

капіталом, які за державним втручанням вдалося врятувати від банкрутства, стали державними, що призвело до значної частини державних банків в банківському секторі України. Водночас з 2016 року стратегія вирішального реформування у державному банківському секторі, передбачала приватизацію більшості державних банків. Відтоді було вжито низку заходів, спрямованих на підтримку приватизації (рис.2.16).

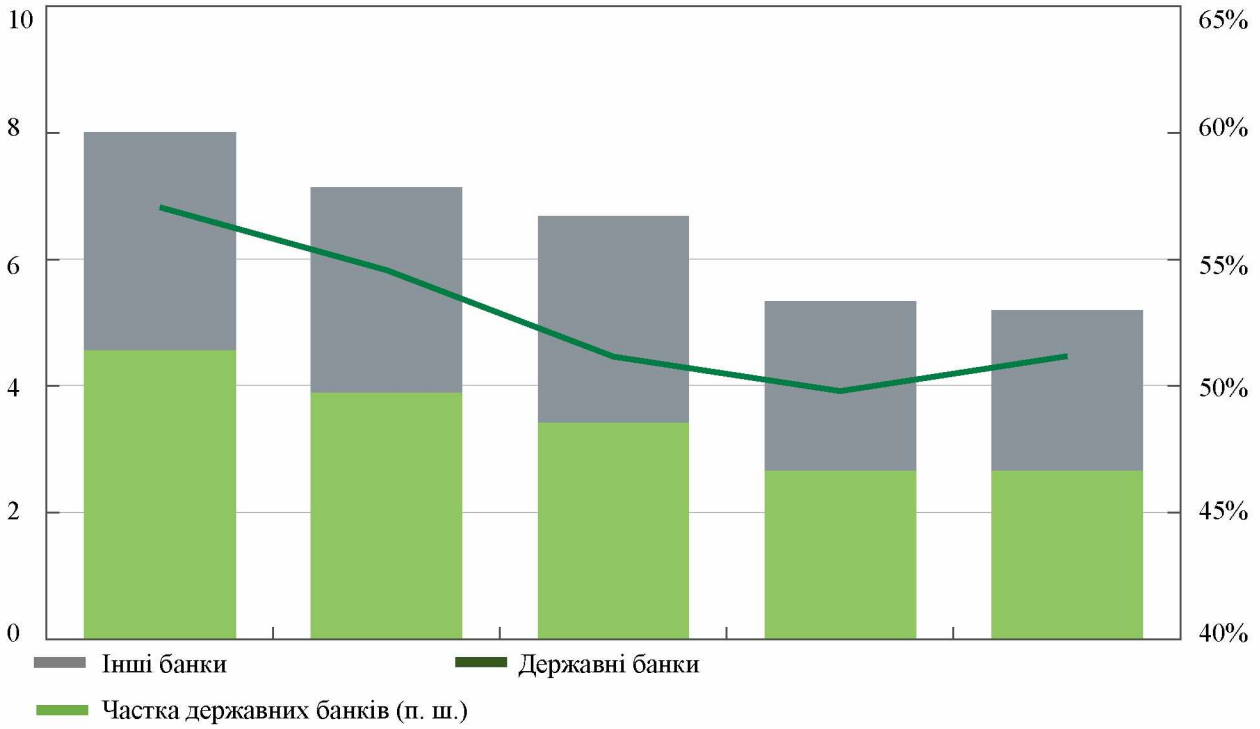

Рис. 2.16. Кількість (тис. одиниць) та частка (%) структурних підрозділів банків

Джерело: [38]

Зокрема, було вдосконалено корпоративне управління, створено автономні спостережні структури, встановлено план дій щодо кожного державного банку та розпочато очищення балансів банків від застарілих активів, які були проблемними. IFC надала Укргазбанку позику в розмірі 30 млн євро з подальшою можливістю перетворення у власний капітал. Напередодні вторгнення Росії Ощадбанк вів переговори про отримання позики від ЄБРР розміром 100 млн євро з подібною можливістю перетворення

отриманих коштів у капітал. Банки встановили рівні цільової ефективності із визначенням своєї частки на ринку. Незважаючи на те, що державні банки не підійшли до приватизації безпосередньо, їхня частка в секторі природним чином скорочувалася через активну конкуренцію з банками з приватним капіталом.

Плани приватизації були відкладені через початок повномасштабної війни. З іншого боку, діяльність державних банків була зосереджена на задоволенні економічних потреб воєнного періоду, зокрема на збереженні вкладів, обслуговуванні рахунків у державному секторі та кредитуванні підприємств, особливо стратегічно важливих секторів. Історія свідчить про те, що державні компанії завжди добре обробляли кредити.

Державні банки продовжують бути лідерами як у розмірі мережі, так і у вкладах населення. Приватбанк і Ощадбанк, найбільші державні банки, складають понад половину всієї банківської мережі країни. Напередодні вторгнення державні біли активні в оптимізації своїх філій для зменшення витрат і впровадження безготівкових платежів. Через бої із тимчасовою окупацією Росією багатьох територій кілька відділень банків, особливо державних, були закриті з лютого 2022 року. Тим не менш, кількість відділень державних банків поступово зменшилася. Багато з них також були переобладнані, щоб вони могли працювати навіть під час тривалих відключень електроенергії. Частка державних банківських установ за даним показником збільшується через подальшу оптимізацію мережі відділень іншими банками.

Наприкінці 2021 року 56% депозитів населення належали державним банкам, більшість із яких були в Ощадбанку та Приватбанку. З початком повномасштабної війни військові виплати зросли в рази. Зважаючи на те, що більшість рахунків, призначених для отримання таких виплат, були відкриті саме в цих двох банках, то основні надходження коштів спрямовувалися саме до них. Таким чином, розмір частки вкладених депозитів серед клієнтів в усіх державних банках перевищила 60%. Ці гроші майже ніколи не потрапляють в інші комерційні банки країни.

Державні банківські установи продовжували надавати кредит через катастрофічне падіння економіки та безпрецедентні ризики для безпеки внаслідок війни з початку минулого року, які знизили необхідність ризикувати та надавати кредити фінансовим установам. У травні 2022 року уряд надав державним банкам інструкції щодо того, як діяти під час воєнного стану. Зокрема, ці рекомендації підтримували продовження надання державними банками фінансової допомоги ряду галузей економіки та підприємствам, які мають вирішальне значення для інфраструктури.

Навесні 2022 року державні банки активно підтримували аграріїв через кредитування під посівну. Розгалужена мережа відділень із доступом до програми доступного державного кредитування під ставкою 5, 7 або 9 відсотків сприяли цьому (рис.2.17).

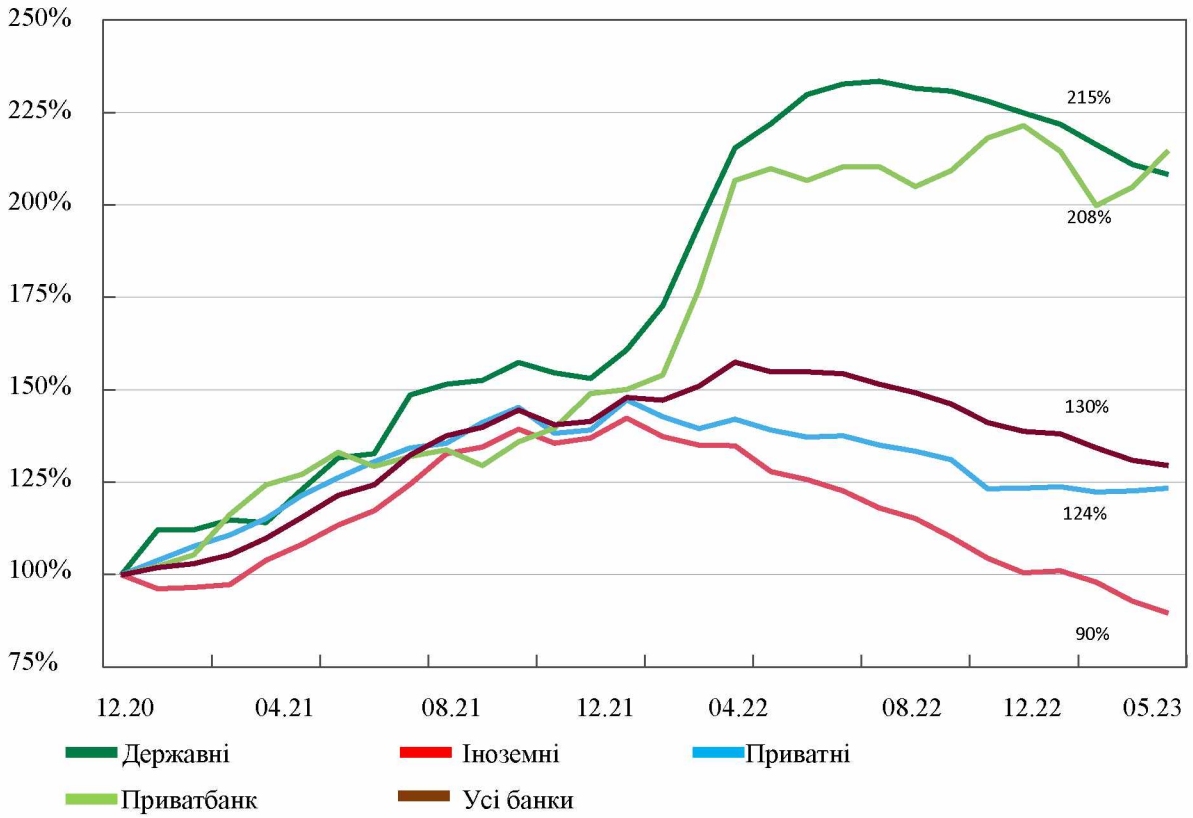

Рис. 2.17. Чисті кредити суб'єктам господарювання в гривнях, 2020 = 100%

Джерело: [39]

Державна програма іпотечного кредитування «єОселя» залучає найбільшу кількість банків-учасників. Оскільки програма фінансується пільговими групами людей, такими як військові, правоохоронні органи, медики, вчителі та науковці, її робота спрямована на вдоволення соціальних потреб цих груп людей. З іншого боку, процентний спред, який отримують банки за програмою, не забезпечує банкам дохідності від цих операцій; оскільки за його допомогою покриваються тільки витрати операційної діяльності із частковою вартістю ризику за кредитуванням.

У приватних банках маржинальність і операційна ефективність вищі, ніж у більшості державних. Зважаючи на значну частку ринку, державні банки є «маркет-мейкерами» за кількома критеріями. Зокрема, вони встановлюють референтні депозитні ставки. Держбанки донедавна підтримували низькі депозитні ставки завдяки значним надходженням грошей на депозити населення. (рис.2.18).

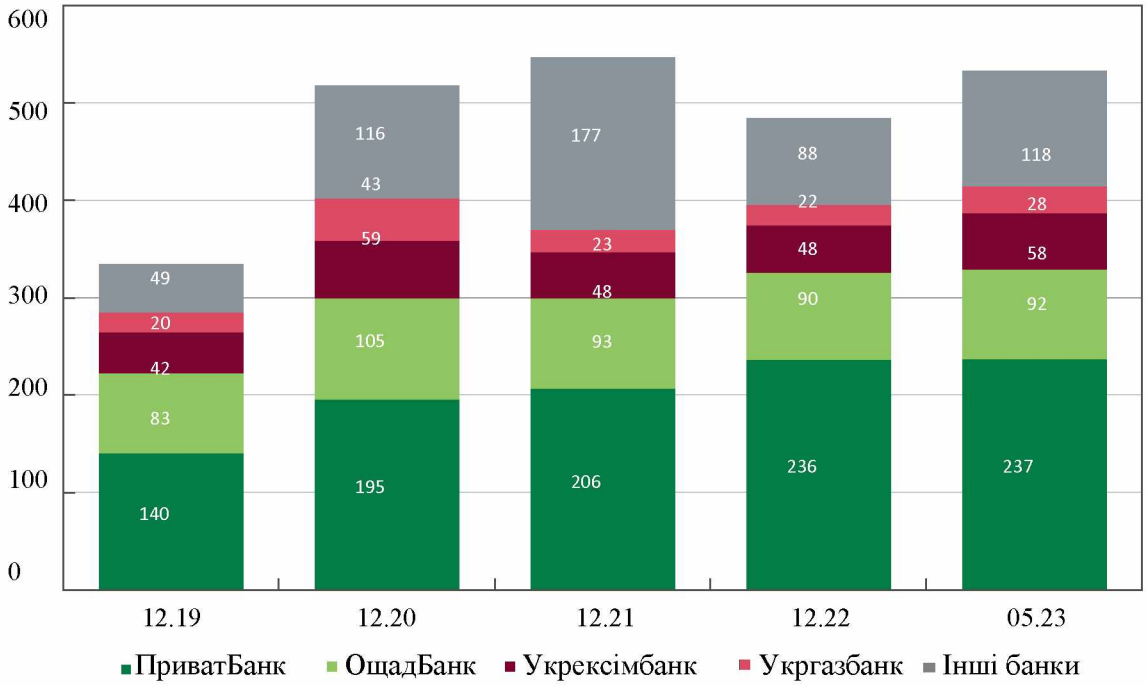

Рис. 2.18. Обсяги ОВДП у розрізі банків, млрд грн

Джерело: [39]

Такий рух депозитних ставок підвищив маржинальність банків. Приватбанк повністю скористався дешевим фондуванням, а Ощадбанк меншою мірою. Вони почали збільшувати ставки за депозитами для своїх клієнтів лише з березня по квітень цього року в відповідь на заходи, вжиті НБУ, але вартість ресурсу цих банків продовжує бути однією з найнижчих на ринку. Натомість окремі державні банки збільшили вартість коштів компаній, які суперничають між собою за право надання послуги корпоративних вкладів з метою утримання ліквідності із поверненням значного рефінансування. Укргазбанк і Укрексімбанк мали значно нижчу чисту процентну маржу, ніж приватні банки з подібними бізнес-моделями через підвищення вартості фондування.

Державні банки надали понад 50% схвалених кредитних заявок. Приватбанк також дуже швидко кредитував підприємства, хоча доти він лише поволі збільшував свій портфель корпоративних кредитів. Кредити компанії зараз становлять майже 37% її кредитного портфеля, у порівняні з 26% на початок 2022-го року. Крім того, державні банки використовують понад дві третини гарантій портфельного кредитування від держави за встановленими лімітами. Фінансування державних підприємств є ще одним видом кредитування, який підтримують саме державні банки. Майже третина цих кредитів знаходиться в складі чистого корпоративного портфеля державних банківських установ, що майже втричі більше, ніж у секторі в цілому. Нині єдині державні банки готові надавати кредити державним організаціям в потребуючих великих обсягах, виходячи з розміру та пріоритетів уряду.

Окремі державні банки зазнали збитків і втрати капіталу в результаті реалізації кредитного ризику. До розгортання бойових дій загострені проблеми з якістю активів державних банків були частково вирішені. Напередодні вторгнення кількість непрацюючих кредитів у державних банках була значно вищою, ніж у банках інших груп. Війна також призвела до значних втрат кредитного ризику для сектора та державних банків. (рис.2.19).

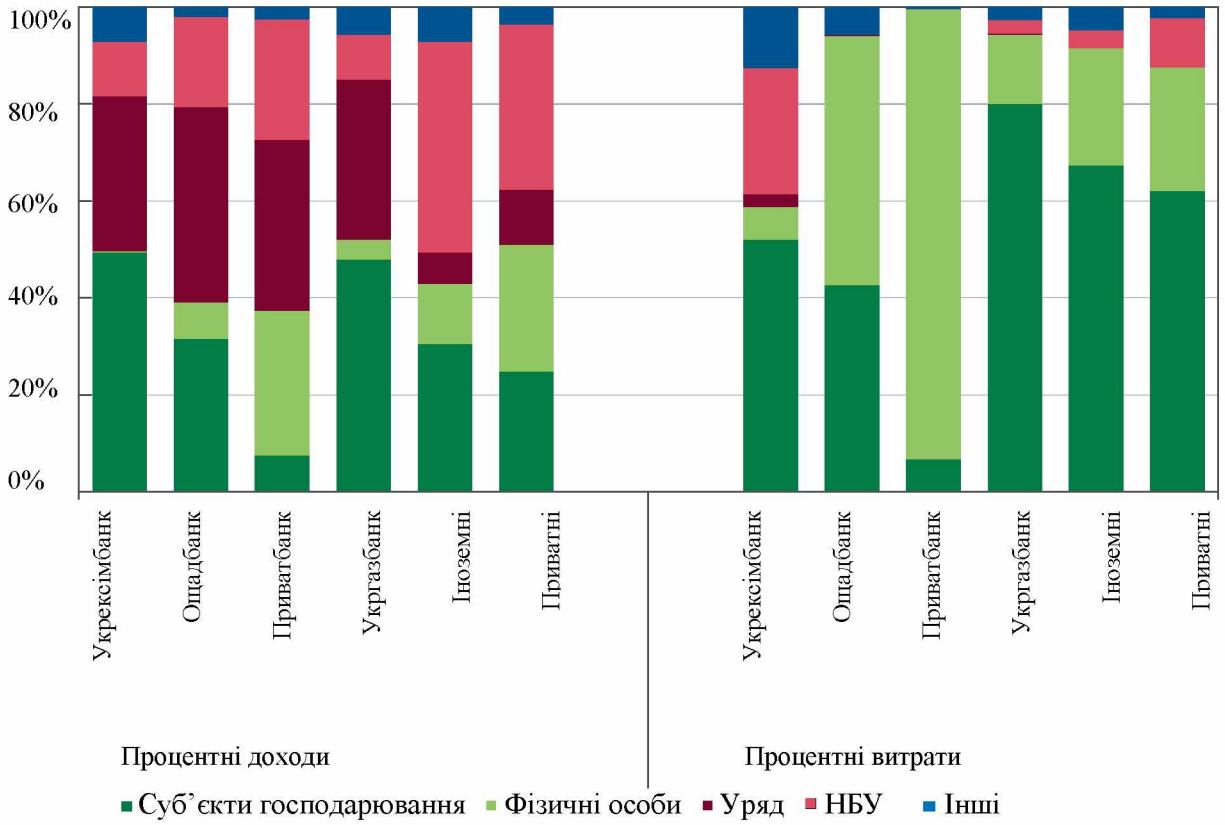

Рис. 2.19. Структура процентних доходів та витрат

Джерело: [39]

Рівень ризику зріс у результаті значної концентрації портфеля. Однак реструктуризація та значна кількість гарантійних кредитів від держави підтримали діяльність державних банків. Але торік Укрексімбанк і Укргазбанк отримали збитки, а Ощадбанк отримав низьку рентабельність через зниження маржинальності та операційної ефективності. Наразі Укрексімбанк є єдиним банком, який не дотримується вимог до достатності капіталу. Перераховані державні банківські установи потрапили до десяти найгірших фінансових установ у галузі за показником достатності основного капіталу в травні. Відповідно до оцінки стійкості деяких державних банків може знадобитися додатковий капітал. НБУ надасть банкам достатньо часу, щоб компенсувати цю потребу, враховуючи власні прибутки банків. Досі накопичені фінансовими установами збитки поглинають майже дві третини коштів, проінвестованих державою. Досвід України свідчить про те, що управління урядом банківською установою є більше витратою, ніж інвестицією.

Стратегії державних банків повинні бути оновлені. Конкретніші цілі діяльності банків у найближчій перспективі мають доповнити короткі стратегічні (основні) напрями діяльності банків державного сектору під час стану ведення бойових дій та повне відновлення економіки після них. Відповідно до цих цілей новообрані наглядові ради державних банків мають розробити комплексні стратегії, які визначать місце та функції кожного банку під час тривалої війни. Новою проблемою може слугувати націоналізація банку, акціонери якого потрапили під санкції через російську агресію.

Стратегічні зміни повинні враховувати зобов'язання України перед МВФ і практику ЄС щодо поступового скорочення зниження участі уряду в приватних банківських установах після кризи. Зважаючи на ймовірність воєнних подій, період часу, необхідний для зниження участі держави в банківському сегменті буде досить довгим. У той же час, як найбільший акціонер, державі необхідно дотримуватись дій щодо уникнення умов не конкурентоспроможності банківських установ. Втрата суперництва із повною монополізацією певних видів кредитування будуть продовжувати перешкоджати інвесторам, особливо для придбання державних банків.

Висновки до другого розділу

В другому розділі кваліфікаційної роботи проаналізовано фінансово-економічний стан банківського сектору України. Слід відмітити, що фінансовий сектор добре підготувався до повномасштабної війни, оскільки банки продовжували безперебійно надавати послуги населенню, зберігати функціонування філіалів, підтримувати операційну ефективність, прибутковість і нарощення капіталу. Накопичений запас міцності підтримує фінансову стабільність, підвищує стійкість банків до подальших труднощів, пов'язаних із тривалою війною, і готує до повного відновлення кредитування. Осінньо-зимовий енергетичний терор від Росії для економіки виявився меншим, ніж очікувалося. Економічна активність зросла завдяки стабільності

енергосистеми.

Багато грошей потрібно на тривалі бойові дії, що призвело до рекордного бюджетного дефіциту. Наявні внутрішні ресурси недостатні для покриття всіх бюджетних потреб. Таким чином, підтримка з боку інших країн продовжує бути життєво важливою для України. У наступні чотири роки ініціатива МВФ сприятиме отриманню 115 млрд дол. від партнерів, що робить міжнародну фінансову підтримку системнішою. Завдяки виконанню зобов'язань, які взяла на себе Україна перед міжнародними партнерами, можна очікувати подальшого стабільного надходження фінансових ресурсів.

Немає причин для занепокоєння щодо ліквідності банківської системи, оскільки коефіцієнти короткострокової ліквідності в середньому втричі перевищують мінімальні вимоги. Люди мають стабільні рахунки в банках. Результати роботи Національного банку звітують щодо покращення строкової структури вкладень населення. Банки збільшили витрати на фінансування бізнесу через підвищення ставок і більше рахунків. Зобов'язання банків зменшили частку зовнішніх позик і кредитів рефінансування. Після різкого падіння з початку вторгнення роздрібний кредитний портфель нарешті повернувся до нормального стану, але поки рано говорити про повне відновлення.

РОЗДІЛ 3
ШЛЯХИ ВДОСКОНАЛЕННЯ ЗАХИСТУ ІНФОРМАЦІЙНОЇ БАНКІВСЬКОЇ СИСТЕМИ В СУЧАСНИХ УМОВАХ

3.1. Формування системи захисту інформаційної безпеки банку

Банківська установа є комплексом інформаційних елементів, які взаємодіють між собою для досягнення спільної мети. Ці елементи включають у себе структурні зв'язки та технології обміну інформацією. Під час функціонування банку ці складові можуть змінюватися під впливом внутрішніх і зовнішніх факторів, які часто бувають непередбачуваними та складними для оцінки. Як об'єкт інформатизації, банк зумовлюється сукупністю таких груп компонентів: технічні засоби, документація, програмне забезпечення та персонал. Під різного роду факторами впливу та під впливом один одного під час взаємодії дані компоненти формують відповідний стан інформаційної безпеки банку, покращуючи якості безпеки за одними параметрами і погіршуючи за іншими. Саме такий взаємозв'язок між компонентами в умовах взаємного впливу, зумовлює необхідність комплексного підходу до забезпечення інформаційної безпеки банку.

Комплексність підходу полягає у регулярному процесі забезпечення інформаційної безпеки на кожному етапі та на всіх напрямках діяльності банку. При створенні системи безпеки необхідно організовувати та об'єднувати заходи, методи та засоби безпеки таким єдиним механізмом, який забезпечуватиме захист не тільки ззовні, від зловмисників та шахраїв, але й від некомпетентних працівників та непередбачуваних внутрішніх ситуацій.

Системність та комплексність заходів безпеки інформації має передбачати [40]:

—Головна характеристика якості системи безпеки – високий ступінь захищеності відповідної інформації банку;

—Заходи з безпеки охоплюють усі інформаційні ресурси банку з усієї структури;

—Забезпечення інформаційної безпеки є безперервним і плановим процесом, заснованим на єдиній концепції безпеки;

—Забезпечення безпеки інформації вплетено в робочі процеси банку, утворюючи єдину систему.

Виходячи з наведеного, можна сформувати основне поняття системи захисту банківських даних – це комплекс об'єктів, суб'єктів, заходів і методів, спрямованих на забезпечення безпечного зберігання та використання інформації у банку. Головна мета цієї системи полягає в гарантуванні надійності обробки та збереження інформації. Враховуючи важливість та складність побудови функціональної та ефективної системи захисту інформації, її створення повинно базуватись на таких головних принципах: законність (відповідність планових заходів захисту діючому законодавству), повнота інформації (захист не тільки конфіденційної, але й тієї інформації, втрата якої може негативно вплинути на діяльність установи), обґрунтованості (визначення доцільності надання доступу до інформації), повної участі та відповідальності (поширення відповідальності за захист інформації на усіх залучених осіб), превентивності (плановість заходів щодо захисту інформації).

Здебільшого при формуванні системи безпеки використовується метод метод захисту з використанням принципів AAA (authentication, authorization, accounting). Протокол AAA дозволяє мінімізувати шанси використання порушниками захищеної інформації наступним чином:

—Автентифікація (authentication) є контрольним етапом, на якому користувач має надати докази своїх прав на доступ. Звершується за допомогою введення логіну та паролю, використання системних запитів, ідентифікаційних карт тощо;

—Авторизація (authorization) полягає у визначення переліку ресурсів, до яких сервіс дозволяє доступ визначеному користувачу;

—Облік (accounting) є записом активності користувача, його дій та параметрів доступу. Здійснюється з метою аналізу використання мережевих ресурсів, практики доступу й виявлення сторонніх вторгнень.

Апаратно-програмні системи ідентифікації та автентифікації (CIA) для персональних комп'ютерів відіграють значну роль серед засобів AAA. Через них працівник може отримати доступ до певних даних у кооперативній мережі тільки після проходження автентифікації та ідентифікації, що знижує ризики несанкціонованого доступу. За видами використання ідентифікаційних ознак сучасні CIA поділяються на електронні, біометричні, комбіновані та разові паролі. Детальна класифікація наведена на рисунку 3.1.

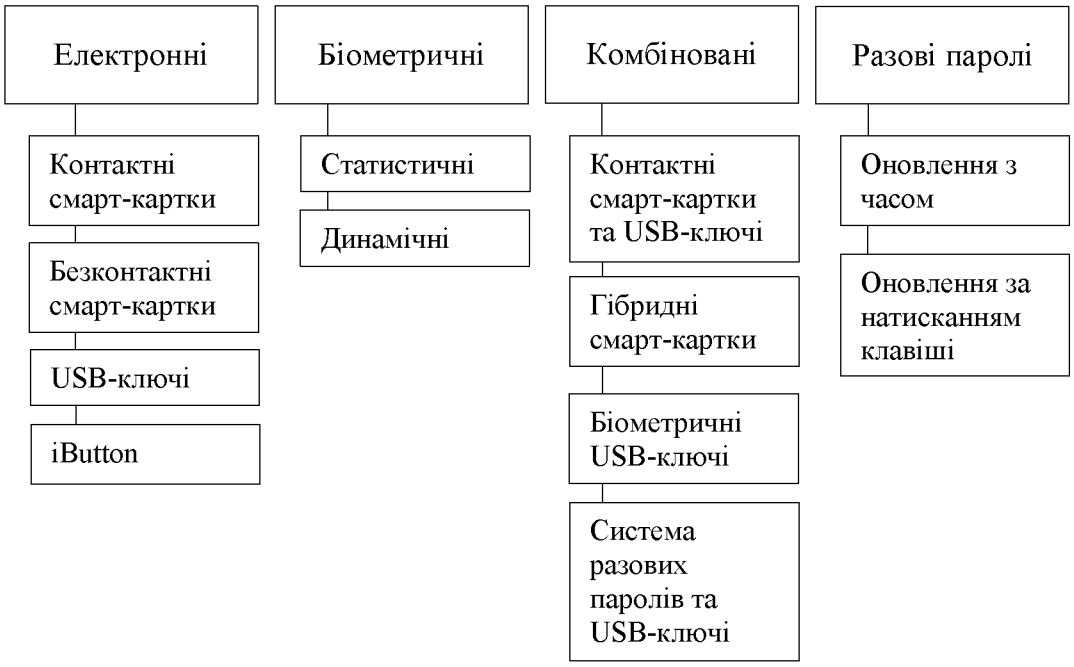

Рис. 3.1. Системи автентифікації та ідентифікації

Джерело: розроблено автором за матеріалами [42]

В результаті збільшення обсягів фінансових траншів за останні роки, з'явилась нагальна потреба у розробці способів додаткового захисту персональних даних споживачів банківських та фінансових послуг. Сучасні розробки українських інженерів GlobalLogic допомагають захистити фінансовий сектор та зменшити ризики банків від шахрайських дій. Детальний розгляд новітніх технологій захисту зображено у таблиці 3.1.

Як зазначає віцепрезидентка GlobalLogic, банківські системи, які автоматизовані, проявляють більшу стійкість до кібератак та шахрайства, однак основною слабкістю для зламу залишаються люди. Частіше користувачі встановлюють однакові паролі та пін-коди для різних облікових записів, сприяючи злочинцям, або навіть надають персональні дані шахраям. Внаслідок цього для більшого захисту розроблюються та встановлюються більш персоналізовані системи автентифікації та ідентифікації клієнта.

Таблиця 3.1

Сучасні технології захисту інформації у банківському секторі

Назва методу	Визначення	Мета використання
Криптографія	Спосіб захисту інформації через перетворення інформації за використанням спеціальних даних з метою приховування змісту інформації, підтвердження її цілісності, справжності, авторства.	Підвищення конфіденційності транзакцій, захист передачі даних між банківською установою та клієнтом у мобільних платежах.
Технологія блокчейна	Система запису та передачі інформації, що зберігає дані у вигляді ланцюжка блоків, де кожен блок містить інформацію про певну кількість транзакцій та хеш попереднього блоку.	Забезпечення прозорості та безпеки транзакцій. Внутрішня мережа різко реагує на будь які зміни та втручання ззовні, що дозволяє оперативно реагувати на них.
Системи багатофакторної автентифікації	Метод контролю доступу до інформації, в якому користувачеві для отримання доступу необхідно надати більше одного «доказу механізму автентифікації».	Додатковий захист від зловмисників. Окрім звичного логіну та паролю використовуються додаткові чинники: цифровий підпис, СМС, карти доступу тощо.
Системи на основі штучного інтелекту та машинного навчання	Системи і комплекси з елементами штучного інтелекту та моделюванням інтелектуальної діяльності людини, покликані виконувати завдання, що потребують людського інтелекту, набагато швидше та ефективніше, ніж людина самостійно.	Виявлення та запобігання підозрілим операціям. Обробка великих обсягів даних та виокремлення аномалій в транзакціях миттєво за допомогою ШІ.

Джерело: розроблено автором за матеріалами [43]

Побудова системи безпеки сучасних українських базуються на вимогах та правилах щодо її організації від НБУ. Головні принципи та заходи безпеки затверджено Положенням про організацію заходів із забезпечення інформаційної безпеки в банківській системі України від Правління Національного банку України №95 від 28.09.2017 р [44]. Даним положенням затверджено перелік обов'язкових заходів із забезпечення інформаційної безпеки та кіберзахисту, з урахуванням актуальних кіберзагроз.

Першочергово до таких заходів відноситься впровадження системи управління інформаційною безпекою (СУІБ) до усіх критичних бізнес-процесів банку. Відповідно до даної системи необхідним є впровадження процесного та ризик-орієнтованого підходу до забезпечення інформаційної безпеки. Також обов'язковою умовою є налаштування системи криптографічного захисту інформації від несанкціонованого доступу та дій.

Діюча на сьогодні система BankID від НБУ є яскравим прикладом дистанційної ідентифікації, що забезпечує функціонування моніторингу та верифікацію клієнта без фізичної присутності та паперової документації. Дана система розпочала свій активний розвиток у 2020 році з затвердженням Положення про систему BankID №32 від 17.03.2020р [45]. Реалізація норм цього документа призвела до позитивних наслідків у банківській сфері: це сприяло додатковій мотивації абонентів для підключення до системи та сприяло підвищенню рівня якості послуг і поліпшенню її функціонування. Абоненти-ідентифікатори (банки) монетизували передачу даних на користь абонентів-надавачів послуг, які дистанційно надають комерційні послуги (адміністративні послуги залишилися безкоштовними). За рахунок зростання кількості абонентів-ідентифікаторів та їх клієнтів зросла і кількість надавачів послуг. Тепер тарифікуються лише ті операції, під час яких дані для ідентифікації клієнта успішно передалися між абонентами. Водночас абонент-надавач послуг сплачує кошти за отримані послуги абоненту-ідентифікатору.

Вже за місяць роботи система налічувала 33 абоненти, з яких 14 – банківські установи, 19 – інші фінансові (портали послуг) [46].

Дистанційна ідентифікація фізичних осіб за допомогою Системи BankID НБУ полягає у передачі особистих даних від ідентифікатора (банку, де відкрито рахунок) до постачальника послуг, який безпечно надає доступ користувачам. Цей процес може бути ініційований лише власником особистих даних, тобто це може зробити лише ви, інші особи не мають такої можливості. Згідно з законодавством України, інформація передається у зашифрованому вигляді.

Система BankID НБУ має наступні особливості:

- Інтернет-канал, яким передаються дані, захищений.
- Дані користувачів захищені шифруванням і передаються через Систему BankID НБУ з кваліфікованим електронним підписом або печаткою банку, що передає інформацію.
- Інформація передається лише одному постачальнику послуг, який обробляє запит, і лише цей постачальник зможе розшифрувати дані від ідентифікатора.
- Особисті дані користувачів не зберігаються в Системі BankID НБУ.

Система має інтеграції з найважливішими для користувачів установами: банки, небанківські фінансові та комерційні установи, державні установи та громадські організації [47]. У цьому полягає її універсальність, яка зменшує кількість вимог щодо подачі документів до кожної з перелічених установ та надає швидкий доступ до важливої персональної інформації з мінімальними ризиками злому або викрадення інформації.

Система BankID стала важливим елементом сучасних електронних фінансових послуг, демонструючи значну ефективність у забезпеченні безпеки та надійності транзакцій. В рамках цього контексту, дослідження статистичних даних безпечних транзакцій та швидкого поширення системи BankID стає ключовим для усвідомлення успіху та впливу цієї інноваційної платформи в електронному фінансовому середовищі.

Уже з початку 2021 року 94% користувачів платіжних карток на українському ринку отримали можливість використання Системи BankID. Це свідчить про активний інтерес банків до державної системи віддаленої ідентифікації. Приєднання все більшої кількості банків до системи як ідентифікаторів сприяє розширенню спектру послуг, що стають доступними українським користувачам. Крім того, спостерігається підвищена співпраця між банками, оскільки для ідентифікації клієнта банк може отримувати дані від інших установ. Ефективність діяльності розглянутої системи можна визначити за кількістю успішних ідентифікацій, представлених на рисунку 3.2.

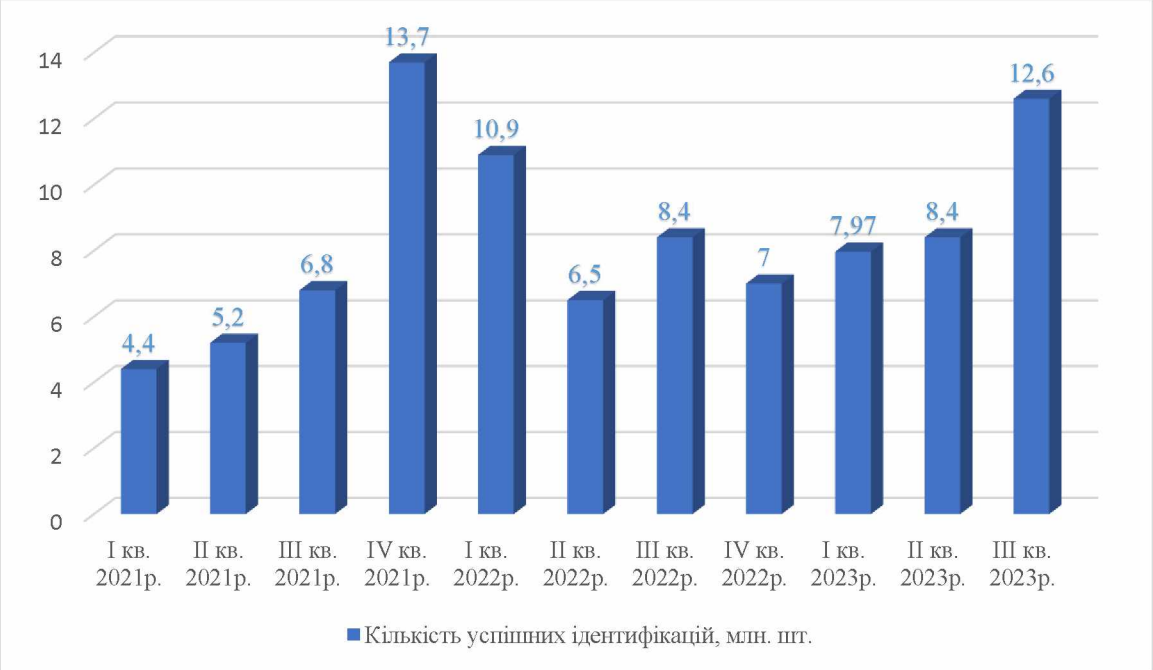

Рис. 3.2. Динаміка успішності ідентифікацій через систему BankID

Джерело: розроблено автором за матеріалами [48]

Для подальшого розвитку системи BankID у вересні 2023 року Національний банк вжив заходів щодо підвищення захисту даних користувачів та уточнення вимог до відповідальності учасників системи. Зокрема, введено обов'язкову багатофакторну автентифікацію для всіх банківських установ, що передбачає використання двох чи більше факторів різних категорій (наприклад, знання, володіння, притаманність). Також розширено повноваження НБУ та Ради системи з метою збільшення відповідальності банків за виконання умов

користування системою, а також збільшено період зберігання інформації про передачу даних користувачів через систему BankID.

3.2. Розробка ефективного захисту топології мережевої системи комерційного банку

Топологія комп'ютерної мережі визначає структуру з'єднання між пристроями і метод їх розташування. Ця структура є важливою, оскільки вона визначає, як інформація буде передаватися від одного пристрою до іншого. Існує кілька основних типів топологій комп'ютерних мереж, кожна з яких має свої унікальні особливості [49]:

—Зіркова топологія (Star Topology): у даній топології кожен пристрій підключений до центрального вузла (зазвичай це концентратор або комутатор). Всі комунікації відбуваються через центральний вузол. Вона дозволяє легко додавати нові пристрої, але в разі відмови центрального вузла мережа може припинити роботу.

—Шина (Bus Topology): всі пристрої підключені до одного загального кабеля (шини). Дані передаються по цьому кабелю, і всі пристрої отримують інформацію, але одночасна передача може призвести до конфліктів та зниження швидкості.

—Кільцева топологія (Ring Topology): у такій мережі пристрої утворюють кільце, де кожен пристрій підключений до двох сусідніх пристроїв. Дані переміщуються від одного пристрою до іншого в напрямку за годинниковою стрілкою або проти годинникової стрілки.

—Деревоподібна топологія (Tree Topology): ця топологія є комбінацією зіркової та шинної топологій. Вона має центральний вузол, який об'єднує групи зіркових топологій посередництвом шини.

—Мешковина (Mesh Topology): кожен пристрій підключений безпосередньо до кожного іншого пристрою в мережі. Це забезпечує найвищий рівень надійності, оскільки відмова одного зв'язку не перерве зв'язку в цілому.

—Гібридна топологія (Hybrid Topology): це поєднання двох або більше видів топологій. Наприклад, поєднання зіркової топології кільцевою може створити більш складну, але більш надійну мережу.

Кожен з цих типів має свої переваги та недоліки, і вибір конкретної топології залежить від потреб, масштабу та вимог конкретної мережі. Схематичне зображення даних топологій наведено на рисунку 3.3.

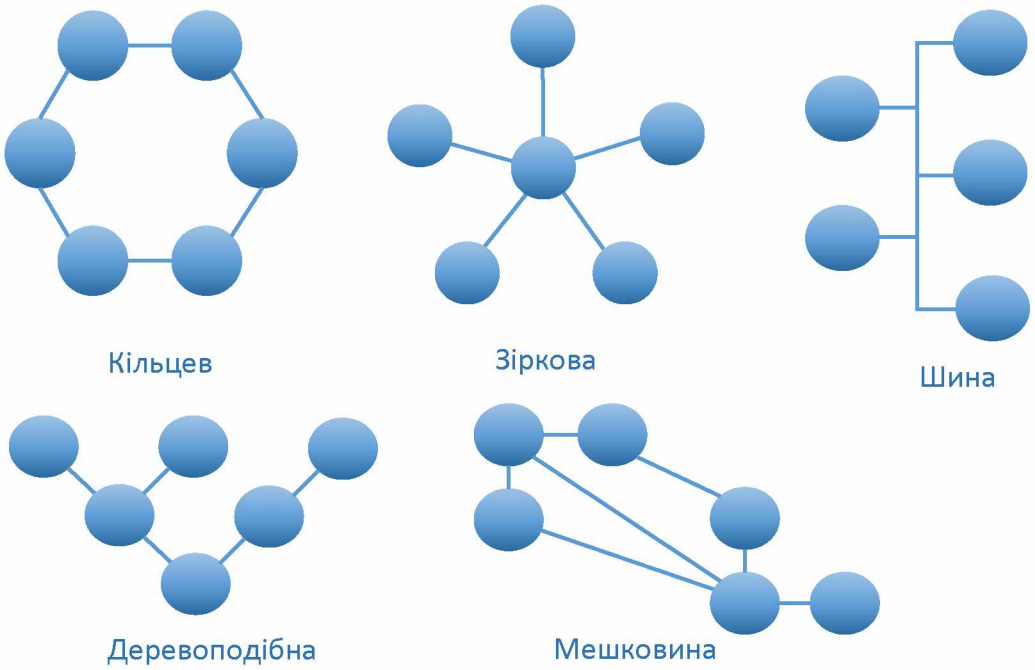

Рис. 3.3. Топології комп'ютерних мереж

Джерело: [50]

Вибір правильної топології комп'ютерної мережі залежить від конкретних потреб, обмежень та мети мережі. Компанії та організації повинні аналізувати ці критерії для обрання оптимальної топології, яка задовольнить їхні вимоги щодо продуктивності, надійності, безпеки та масштабованості. Обрання правильної топології комп'ютерної мережі ґрунтується на таких аспектах:

Ефективність передачі даних: Топологія визначає шлях, по якому дані будуть пересилатися між пристроями. Правильно підібрана топологія може забезпечити ефективну передачу даних, запобігаючи переповнення мережі та зниження швидкості передачі.

Надійність: Деякі топології, наприклад, мережа з резервними шляхами (redundancy), можуть забезпечити надійність в разі відмови обладнання або з'єднання. Вони дозволяють дані обходити по альтернативних маршрутах, уникнувши втрати зв'язку в разі проблеми на одному зв'язку.

Масштабованість: Топологія повинна бути такою, щоб легко можна було додавати нові пристрої до мережі без значного зниження її продуктивності. Деякі топології легше масштабуються, ніж інші.

Управління мережею: Особливості топології можуть впливати на здатність до управління мережею. Наприклад, в деяких топологіях (наприклад, зірка або дерево) керування мережею може бути простішим через централізовану точку.

Вартість реалізації: Реалізація різних типів топологій може вимагати різних витрат на обладнання, кабельні системи та підтримку. Важливо обрати топологію, яка відповідає бюджету і потребам конкретної мережі.

Забезпечення конфіденційності та безпеки: Деякі топології можуть мати вплив на рівень безпеки мережі. Наприклад, мережі з ділянками (subnetting) можуть допомагати в ізоляції трафіку та забезпеченні безпеки даних.

Фізичну топологію мережі можна розглянути більш докладно, використовуючи схематичне зображення вузлів та з'єднаннь між вузлами в комп'ютерній мережі або, загальніше, в будь-якій телекомунікаційній мережі (рис. 3.4). Дана топологія – звичайний граф, на якому вузлам мережі відповідають вершини, а з'єднанням — неорієнтовані або орієнтовані ребра. Схеми комп'ютерних мереж є важливою частиною мережевої документації.

Розглянемо фізичну побудову системи безпеки або мережі в банку[51].

1. Сервери:

1.1. Центральні сервери: Зазвичай це потужні комп'ютери або серверні комплекси, які використовуються для зберігання та обробки великих обсягів даних. Вони можуть включати сервери баз даних, сервери додатків та інші.

1.2. Сервери безпеки: відповідають за різноманітні аспекти безпеки, такі як аутентифікація, шифрування, моніторинг, контроль доступу тощо.

2. Центри управління:

2.1. Security Operations Center (SOC): Це центр управління безпекою, де відбувається моніторинг та реагування на потенційні загрози безпеці. Він може бути обладнаний спеціалізованими системами для виявлення інцидентів безпеки та відповіді на них.

3. Мережеве обладнання:

3.1. Фаєрволи (Firewalls): Вони контролюють трафік мережі, фільтруючи його та блокуючи небажані підключення чи атаки зовнішніх джерел.

3.2. Мережеві комутатори та маршрутизатори: Використовуються для передачі даних між різними компонентами мережі.

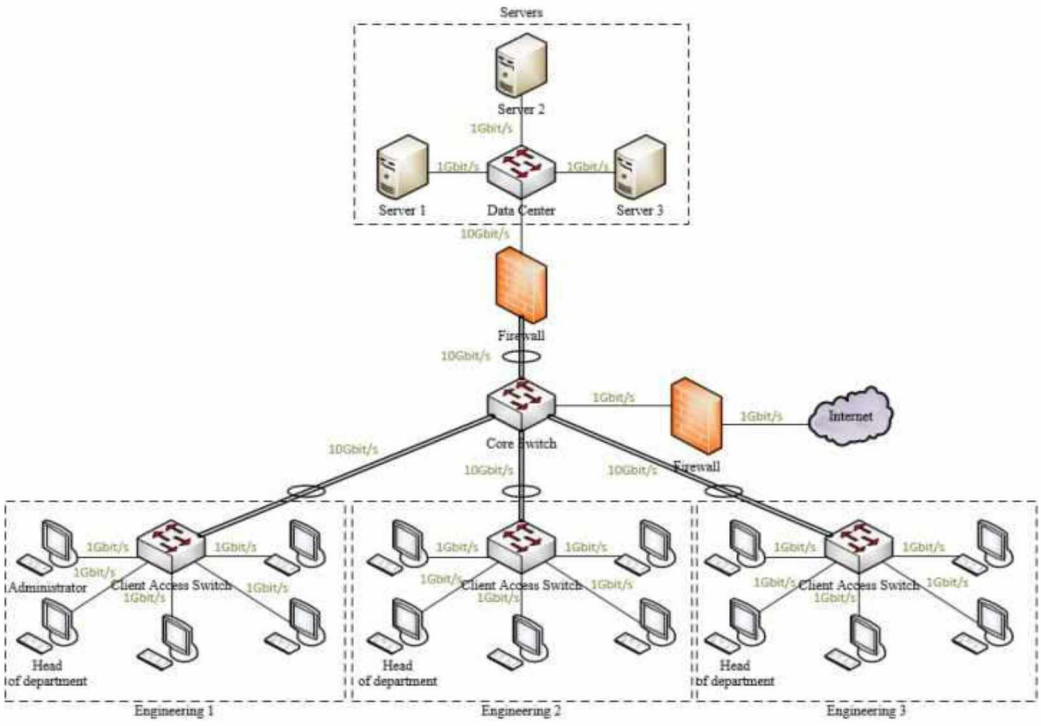

Рис. 3.4. Фізична топологія структурованої мережі

Джерело: [51]

4. Сховища даних:

4.1. Центри обробки даних (Data Centers): Вони містять сервери для зберігання та обробки інформації, забезпечують резервне копіювання та відновлення даних в разі потреби.

5. Звичайні комп'ютери та пристрої:

5.1. Робочі станції та ноутбуки працівників: Використовуються для роботи з банківською інформацією та здійснення банківських операцій.

Передача інформації у даній системі відбувається через мережеві з'єднання між такими компонентами:

– Локальна мережа (LAN): внутрішня мережа банку, яка об'єднує всі компоненти в одну систему. Для передачі даних використовуються мережеві кабелі (Ethernet) або бездротові з'єднання (Wi-Fi).

– Внутрішні мережеві канали: можуть бути захищені шифруванням та іншими методами безпеки для запобігання несанкціонованому доступу до інформації.

– Зовнішні мережі: це зв'язок з іншими банками, клієнтами, партнерами чи іншими системами, який також потребує захисту та безпеки.

Усі ці компоненти співпрацюють для створення і забезпечення безпечної і надійної інфраструктури, яка захищає конфіденційні дані та забезпечує операційну діяльність банку. Як вже зазначалось, за будь якої системи захисту використовується кодування інформації для запобігання стороннього (зовнішнього) втручання та додаткові етапи автентифікації (мультифакторна автентифікація). Найпоширенішим способом шифрування інформації є криптографічний метод захисту – перетворення звичайного тексту (початкових даних) у криптографічно захищений вигляд (шифротекст), який може бути прочитаний лише тими, хто має відповідний ключ для розшифрування. Поетапно процес шифрування та розшифрування розглянуто на рис. 3.5.

Для звершення шифрування використовуються відкритий ($К_1$) та секретний ($К_2$) ключі, що генеруються попарно. Ключ $К_2$ в обов'язковому порядку зберігається у власника, так як має бути захищений від зловмисників,

тоді як копії ключа $К_1$ можуть поширюватись серед користувачів мережі, серед яких йде обмін інформації. Після першого етапу шифрування ключем К1 отримується деякий текст Х, який передається отримувачу і розшифровується ключем $К_2$. Так, отримуємо текст Т як на вході, так і на виході, проте під час його передачі він є повністю захищеним від несанкціонованого доступу. Така система захисту називається крипостійкою – при зламі каналу зв'язку неможливо розшифрувати текст Х без відповідного ключа для використання тексту М не за призначенням.

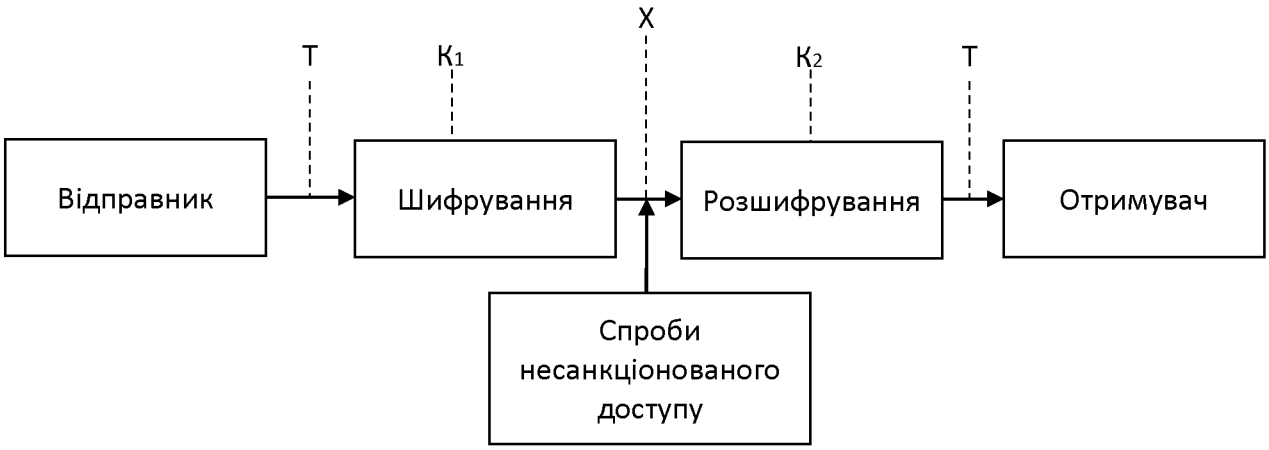

Рис. 3.5. Узагальнена схема асиметричною криптосистеми

Джерело: [52]

Як підсумок, криптографія грає ключову роль у забезпеченні трьох основних аспектів безпеки даних під час їх передачі через мережу: конфіденційності, цілісності та автентичності.

1. Конфіденційність: криптографія допомагає зберегти конфіденційність даних, тобто забезпечує, що інформація залишається недоступною для несанкціонованих осіб під час передачі по мережі. Шифрування даних дозволяє перетворювати інформацію в такий формат, який може бути розшифрований лише відповідним отримувачем, зберігаючи при цьому відсутність доступу для сторонніх осіб, які можуть перехоплювати дані під час передачі.

2. Цілісність: забезпечується цілісність даних, тобто гарантується незмінність інформації або пошкодження під час передачі по мережі. Це досягається за допомогою цифрових підписів або методів хешування, які дозволяють перевірити, чи була інформація змінена під час передачі.

3. Автентичність: дозволяє перевірити, що інформація надійшла від визначеного відправника і не була підроблена під час передачі. Це досягається за допомогою цифрових підписів, які можуть бути перевірені для підтвердження відправника та цілісності даних.

3.3. Методологія побудови системи забезпечення інформаційної безпеки банків на базі міжнародних стандартів ISO

Сучасні інформаційно-комунікаційні системи та мережі схильні до різноманітних мережних загроз, включаючи несанкціонований доступ і розкриття, викривлення або зміну інформації. Застосування відповідних заходів управління безпекою необхідно для сучасного захисту інформаційних ресурсів та послуг банківських установа від потенційних небезпек.

Під управлінням інформаційною безпекою ми розуміємо циклічний процес, який включає:

—постановку завдань щодо захисту інформації;

—підготовка збору та подальшого аналізу отриманих даних про рівень безпеки інформації в автоматизованих банківських системах та мережах;

—оцінювання інформаційного ризику;

—розробку плану дій для запобігання ризику;

—реалізація та впровадження розроблених механізмів регулювання;

—призначення відповідальних осіб за розподіленими обов’язками;

—політика безпеки;

—навчання та мотивація персоналу;

—оперативне виконання захисних дій.

Етапи забезпечення банківської установи системи безпеки інформаційної бази містять оцінювання поточного рівня захисту інформації в інформаційно-комунікаційних системах та мережах, а також розробку комплексу заходів для забезпечення оптимального рівня на основі оцінки ризиків.

Після виявлення вимог безпеки необхідно вибрати та включити розроблену методику управління із забезпеченням впевненості, щоб запобігти несанкціонованому доступу. Засоби управління можуть бути розроблені згідно з обраною політикою безпеки інформаційного середовища. Вони також можуть бути побудовані на основі стандартів або різноманітних інших документів і заходів управління, визначених для конкретного класу систем.

Міжнародний стандарт ISO 27001 визначає систему управління інформаційною безпекою як компонент загальної системи управління організації. Ця система базується на оцінці ризиків і забезпечує створення, реалізацію, експлуатацію та моніторинг загальної інформаційної безпеки, а також підтримку, перегляд, супровід і вдосконалення. Відповідно до стандарту ISO/IEC 27001 склад системи управління безпеки інформаційного середовища повинен складатися із наступних чотирьох етапів [54]:

- перший етап – планування, яке пропонує створення переліку інформації, оцінку ризиків і вибір заходів і механізмів захисту;
- другий етап – дія, яка включає реалізацію та впровадження відповідних заходів;
- третій етап – перевірка, яка містить оцінку ефективності та надійності наявного функціоналу. Тобто, провести внутрішній аудит системи, щоб знайти проблеми.
- четвертий етап – удосконалення, яке складається з впровадження коригувальних заходів для покращення функціонування системи на чотири етапи.

З метою підвищення ефективності захисту сучасних інформаційно-комунікаційних систем і мереж необхідно вжити відповідних заходів під час

розробки системи управління інформаційною безпекою. Заходи управління повинні враховувати витрати на виконання послуг і впровадження систем безпеки, а також зниження ризиків і потенційних збитків при умові періодичних порушень систем безпеки автоматизованого програмного забезпечення через мережу. У стандартах і нормативних документах можна знайти принципи управління, які можна використовувати для розробки політики безпеки інформації. Розглянемо законодавчі аспекти управління інформаційною безпекою, а також узагальнені для сучасних інформаційних мереж і систем [55].

З законодавчої точки зору заходи управління включають:

—захист даних і особистої інформації;

—охорону інформаційних ресурсів організації;

—право інтелектуальної власності;

—документи щодо політики інформаційної безпеки;

—розподіл обов'язків щодо інформаційної безпеки;

—структура підрозділів і навчання щодо інформаційної безпеки;

—повідомлення про інциденти та безперервність;

—постійне управління;

Необхідно враховувати всі заходи управління, які описані в стандартах, оскільки вони є вкрай важливими. Однак використання будь-якого методу управління має бути розроблено, щоб враховувати ризики та потенційні загрози, пов'язані з даними інформаційно-комунікаційних систем і мереж.

Загалом, система з управління безпекою банківського інформаційного потоку повинна складатися з наступних чинників (рис.3.6):

—автентифікація клієнтів та співробітників, усілякого роду інформаційних даних щодо послуг або додатків;

—авторизація основних документів клієнтів та партнерів, переліку цін, управлінської ланки;

—проведення аудиту інформаційного ресурсу та наданих послуг.

Рис. 3.6. Система управління інформаційною безпекою банку

Джерело: розроблено автором за матеріалами [56]

Переваги використання системи управління інформаційною безпекою, яка базується на міжнародних стандартах серії ISO:

1. Гарантія неперервності (застосування сучасних технологій для захисту інформації залежить від того, наскільки надійно зберігаються конфіденційність і цілісність даних, а також від того, наскільки добре працюють певні програми, сервіси та сервіси в галузі інформаційних і телекомунікаційних технологій);

2. Зменшення ризиків (за рахунок обмеження фізичного доступу та впровадження процедур моніторингу та аудиту стану інформаційної безпеки система управління інформаційною безпекою дозволяє зменшити ризик втрати інформацію, розкрадання та користування обладнанням не за призначенням, завдання шкоди або порушення роботи інформаційних систем організації. Проведення оцінювання із мінімізацією ризику дозволяють визначити загрози для інформаційних ресурсів і послуг, оцінювати їх уразливість і ймовірність виникнення загроз, а також оцінювати потенційний руйнівний вплив, який може бути спричинений несанкціонованим доступом);

3. Зниження витрат на охорону інформації (застосування сучасних технологій у сфері створення, моніторингу та покращення системи безпеки інформаційного простору надає змогу зменшити витрату бюджету, пов'язану з інформаційною безпекою);

4. Забезпечення захисту, конфіденційності та доступності важливих інформаційних ресурсів у мережах та системах інформаційно-комунікацій;

5. Забезпечити комплексний і централізований контроль ступеня захисту даних.

Інформаційна система управління за міжнародними стандартами серії ISO розкриває сутність підходу щодо регулювання ризиків інформаційної безпеки, який активно та ефективно допомагає інформаційним системам організацій будь-якого розміру та рівня розвитку вирішувати проблеми, що виникають у процесі забезпечення відповідності стандартам інформаційної безпеки. Загальні критерії безпеки інформаційних технологій та сім'я стандартів ISO є найважливішими стандартами для управління інформаційною безпекою та включають у свій склад:

- критерії безпеки комп'ютерних систем;
- європейські критерії безпеки інформаційних технологій;
- федеральні критерії безпеки інформаційних технологій;
- канадські критерії безпеки інформаційних технологій.

Усі вони розуміють важливість процесу управління ризиками та основні методи, а також ідеї щодо того, як створюється, впроваджується, використовується, спостерігається, перевіряється, підтримується та вдосконалюється система захисту організації.

Ідентифікація та управління різноманітними процесами, включаючи процес управління ризиками інформаційного об'єкту, є необхідним для того, щоб організація працювала ефективно. Регуляторний спосіб дотримання інформаційної безпеки надає можливість організаціям поєднувати максимальну економічну ефективність із прийнятним рівнем ризику. Це також дозволяє

керівникам різних рівнів зрозуміти процес організації та пріоритизації ресурсів, які мають обмежений доступ для впровадження управління ризиками. Упровадження управління ризиками інформаційної безпеки надає можливість суб'єкта господарювання, які розподілені на корпоративні мережі, економічно ефективно контролювати рівень ризику [56].

Не існує універсального рішення, і різні організації використовують різні моделі управління ризиками. Тому визначення допущеного ризику та підхід до управління ризиками залежать від структури інформаційної системи та її розподіленості. Кожна модель має своє унікальне поєднання точності, ресурсів, часу, складності та суб'єктивності. Інвестиції в процес управління ризиками повинні базуватися на перевіреній ідеї та чітком визначенні ролей і завдань. Крім того, ефективна програма управління ризиками дозволить розподіленим корпоративним мережам забезпечити достатню інформаційну безпеку. Оцінка ризиків організації є першим кроком у створенні та функціонуванні захищених інформаційних систем. Оцінка ризиків використовується для визначення загроз для активів, оцінки їхньої уразливості та ймовірності виникнення загроз, а також можливого руйнівного впливу, який може виникнути в результаті несанкціонованих дій. Вище наведено сценарій для управління ризиками інформаційного об'єкту (рис. 3.6).

Сценарій розрахунку ризиків, запропонований для інформаційної системи, складається з наступних основних компонентів:

1. розробка методології оцінювання ризику для інформаційної системи;

2. розробка критеріїв прийняття ризиків і визначення прийнятого рівня ризику;

3. визначення активів;

4. виявлення небезпек для активів;

5. виявлення вразливих місць у системі захисту;

6. виявлення дій, які порушують конфіденційність, цілісність і доступність інформаційної системи.

Відповідно до вимог процесу оцінки ризиків і скорочення ризиків згідно з ISO 27002 завдання та методи управління мають бути обрані та впроваджені відповідно. Для прийняття такого рішення необхідно враховувати критерії допустимості ризику, а також юридичні, регулятивні та договірні вимоги. Використання цього сценарію дозволяє створити систему захисту інформації, яка використовує оцінку ризиків, яка визначає загальну організацію, класифікацію даних, системи доступу, напрями планування, методи забезпечення безпеки, практичні правила та вимоги, відповідальність співробітників і використання оцінки ризиків у контексті інформаційної безпеки підприємств. У цьому сценарії створюється система управління інформаційною безпекою. Система управління інформаційною безпекою була розроблена з метою зменшення матеріальних втрат, пов'язаних з порушеннями інформаційної безпеки. Розроблено структурну схему оцінювання інформаційних ризиків на основі запропонованого сценарію (рис. 3.7).

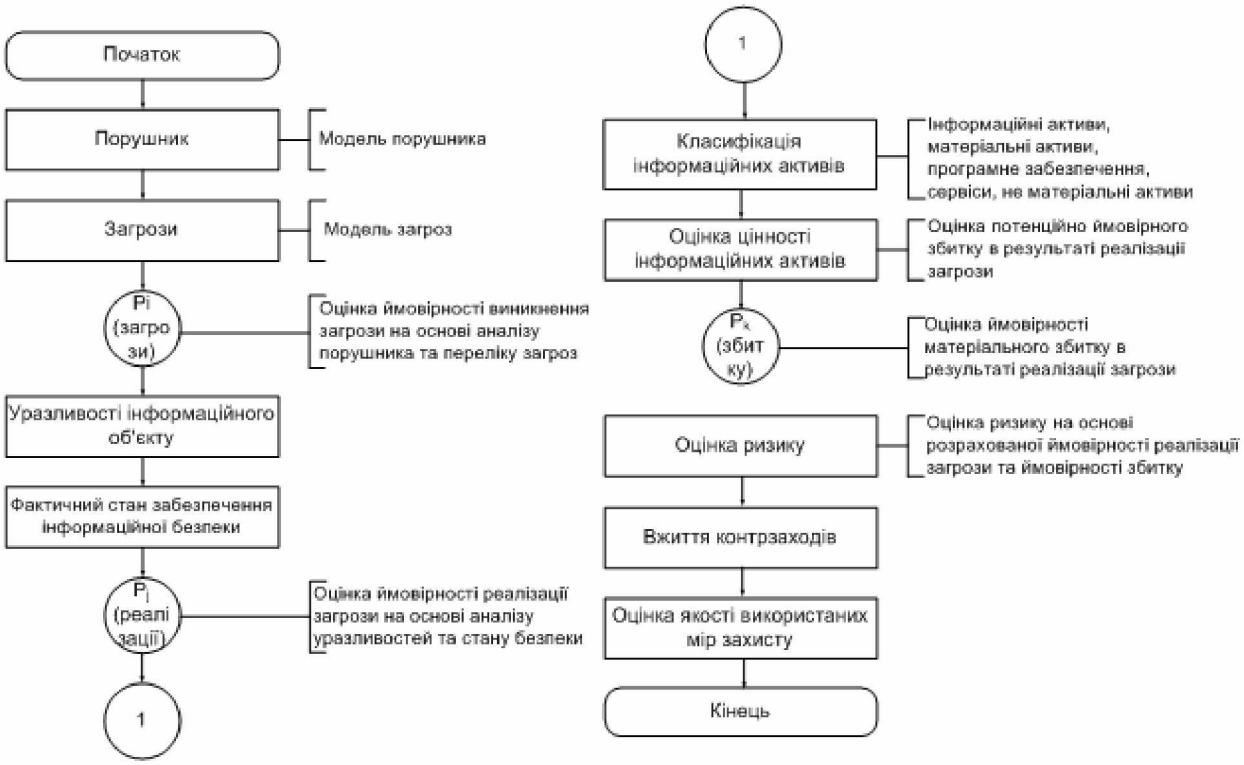

Рис. 3.7. Структурна схема оцінювання інформаційних ризиків

Джерело: [57]

Відповідно до міжнародних стандартів ISO, аналіз сучасних заходів управління інформаційною безпекою інформаційно-комунікаційних систем і мереж показав, що забезпечення безпеки властивостей інформаційних ресурсів і послуг у мережах передачі даних є важливим компонентом. Для забезпечення та підтримки безпеки інформаційно-комунікаційних систем і мереж необхідно використовувати широкий спектр засобів і заходів управління. В роботі показано, що впровадження системи управління інформаційною безпекою, яка базується на міжнародних стандартах серії ISO, має багато переваг для сучасних інформаційно-комунікаційних систем і мереж. Крім того, було запропоновано сценарій управління ризиками інформаційної безпеки, а також розроблено структурну схему оцінювання інформаційних ризиків мережі підприємства.

Висновки до третього розділу

В третьому розділі кваліфікаційної роботи надані практичні рекомендації щодо вдосконалення розвитку захисту банківської системи із урахуванням сучасних змін економічного середовища. Збільшення обсягів фінансових траншів за останні роки викликало потребу розгляду додаткового захисту персональних даних споживачів банківських та фінансових послуг. З цього приводу було розглянуто сучасні розробки вітчизняних інженерів GlobalLogic, які допомагають захистити фінансовий сектор та зменшити ризики банків від шахрайських дій.

Не менш важливою залишається вивчення системи BankID, яка є основним елементом сучасних електронних фінансових послуг. В рамках цього контексту, дослідження статистичних даних безпечних транзакцій та швидкого поширення системи BankID стає ключовим для усвідомлення успіху та впливу цієї інноваційної платформи в електронному фінансовому середовищі.

Досліджено методи вибору відповідної топології комп'ютерної мережі під конкретні потреби, обмеження та мети мережі в розрізі потреб

комерційного банку. Запропоновано методологічні аспекти застосування правильної топології комп'ютерної мережі за ключовими елементами ефективності передачі даних, надійності, масштабованості, управління, вартістю реалізації та забезпечення конфіденційності.

Розроблено методичні рекомендації системи управління фінансово-економічною безпекою банківської установи система, яка базується на міжнародних стандартах серії ISO, визначає оцінку ризиків і забезпечує створення, реалізацію, експлуатацію та моніторинг загальної інформаційної безпеки, а також підтримку, перегляд, супровід і вдосконалення управління інформаційною безпекою.

ВИСНОВКИ

Проведені в роботі дослідження дозволяють зробити такі висновки.

Потужна банківська система є необхідною умовою забезпечення сталого економічного зростання в Україні. Враховуючи значну відкритість національної економіки, високий рівень вразливості банків до несприятливих змін кон'юнктури фінансового ринку, обумовлену гострою нестачею капіталу в межах країни та тиском з боку політично-економічних перетворень, національному банківському сектору необхідна виважена розробка рекомендацій та дій щодо розвитку захисної функції фінансово-економічної безпеки кожного інституційного середовища.

Фінансово-економічна безпека банку є специфічним завданням з елементами організаційно-правової структури, яка призначена забезпечувати своїми особливими методами надійне регулювання банківської діяльності та ефективне функціонування грошового ринку. У наукових дослідженнях по-різному трактують поняття фінансово-економічної безпеки комерційного банку, але усі існуючі визначення включають здатність виявлення, предостереження та боротьби з будь-якими загрозами для збереження фінансового стану банку із зміцненням його фінансово-економічного потенціалу. Таким чином, система фінансово-економічної безпеки банку повинна бути зосереджена на стабільності та ефективності банківської діяльності, виявленні ризиків, ліквідації криз і запобіганні банкрутству.

Однією з найважливіших сфер прояву боротьби із фінансово-економічними ризиками є електронне банківництво. Одночасно з позитивними перевагами використання мережі містить у собі недоліки: з одного боку – сприяє розвитку фінансової установи та підвищує конкурентоспроможність, з іншого – підвищує ризик фінансово-економічної безпеки, що зумовлює необхідність розробки надійної системи захисту банківської системи в національному фінансово-економічному просторі.

За результатами аналізу сучасного стану фінансового сектору України

помітно стійкість у банківській діяльності. Перш за все, цьому посприяв накопичений запас міцності, який підтримує фінансову стабільність, підвищує стійкість банків до подальших труднощів, пов'язаних із тривалою війною, і готує до повного відновлення кредитування. Проблеми залишаються у тому, що зростання потреби фінансування на тривалі бойові дії призвело до рекордного бюджетного дефіциту.

Результати дослідження ліквідності банківської системи не дають причин для занепокоєння щодо банкрутства, оскільки коефіцієнти короткострокової ліквідності в середньому втричі перевищують мінімальні вимоги. Люди мають стабільні рахунки в банках. Результати роботи Національного банку звітують щодо покращення строкової структури вкладень населення. Банки збільшили витрати на фінансування бізнесу через підвищення ставок і більше рахунків. Зобов'язання банків зменшили частку зовнішніх позик і кредитів рефінансування. Після різкого падіння з початку вторгнення роздрібний кредитний портфель нарешті повернувся до нормального стану, але поки рано говорити про повне відновлення.

Розгляд та аналіз викладених вище питань зумовив необхідність пошуку шляхів удосконалення досліджуваного процесу. Автором проаналізовано існуючі пропозиції щодо цього питання та систематизовано у наступних напрямках.

По-перше. Надано рекомендації щодо формування практичні рекомендації щодо вдосконалення розвитку захисту банківської системи із урахуванням сучасних змін економічного середовища. Збільшення обсягів фінансових траншів за останні роки викликало потребу розгляду додаткового захисту персональних даних споживачів банківських та фінансових послуг. З цього приводу було розглянуто сучасні розробки вітчизняних інженерів, які допомагають захистити фінансовий сектор та зменшити ризики банків від шахрайських дій.

По-друге. Представлено розробку дієвої методики обрання топології комп'ютерної мережі в залежності від актуальних потреб банківської установи,

її обмеження та мети створеної мережі. Запропоновано методологічні аспекти застосування правильної топології комп'ютерної мережі за ключовими елементами ефективності передачі даних, надійності, масштабованості, управління, вартістю реалізації та забезпечення конфіденційності.

По-третє. На методичні рекомендації системи управління фінансово-економічною безпекою банківської установи система, яка базується на міжнародних стандартах серії ISO, визначає оцінку ризиків і забезпечує створення, реалізацію, експлуатацію та моніторинг загальної інформаційної безпеки, а також підтримку, перегляд, супровід і вдосконалення управління інформаційною безпекою.

Таким чином, сучасний стан банківської системи України вимагає прийняття трансформаційних заходів щодо покращення функціонування системи захисту безпеки фінансово-економічного середовища. Дані напрями необхідно структурувати за проблемами, з якими стикнулася банківська система, а саме: вирішення питання кібербезпеки інформаційного простору банківської системи; стимулювання структурних перетворень в управління фінансовими ризиками; розвиток інноваційних платформ в електронному фінансовому середовищі банківського сектору України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Зачосова Н. В. Теоретико-методичні засади побудови системи економічної безпеки фінансових установ / Н. В. Зачосова. // Науковий вісник: Економічні науки. – 2016. – №4. – С. 47–51.

2. Кельдер Т. Л. Економічна безпека банківської системи України в умовах глобальної фінансової кризи / Т. Л. Кельдер, Л. В. Худолєй. // Держава та регіони: Економіка та підприємництво. – 2012. – №2. – С. 181–185.

3. Голобородько Ю. О. Теоретичні підходи до розкриття сутності та складових фінансової безпеки банківських установ / Ю. О. Голобородько. // Науковий вісник НЛТУ України. – 2012. – №22. – С. 194–198.

4. Щербатих Д. В. Підходи та загрози до формування фінансово-економічної безпеки банківських установ / Д. В. Щербатих, Б. В. Шпильовий. // Вісник Черкаського університету: Економічна. – 2016. – №1. – С. 141–148.

5. Соловйов В. І. Банківська безпека України: вдосконалення методики оцінки / В. І. Соловйов // Вісник Бердянського університету менеджменту і бізнесу. – 2012. – № 1(17). – С. 171–176.

6. Ляхович О. О. Сутність та забезпечення фінансово-економічної безпеки банківських установ / О. О. Ляхович, В. В. Добровольська // Вісник НУВГП: Економічні науки. – 2020. – №1(89) – С. 25–29. – Електронний ресурс. – Режим доступу до ресурсу: http://surl.li/nzeqc

7. Вдовиченко А. Р. Індекс фінансового стресу: оцінка і застосування в емпіричних дослідженнях в Україні / А. Р. Вдовиченко, Орос Г. С. // Журнал Європейської економіки. – 2015. – №2 – С. 207-210. – Електронний ресурс. – Режим доступу до ресурсу: http://surl.li/nzeru

8. Організаційна структура системи управління ризиками: Офіційне інтернет-представництво Національного банку України [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/nzeto

9. Про банки і банківську діяльність [Електронний ресурс]: Закон Верховної Ради України № 2121-III (зі змінами та доповненнями) від 07.12.2000. – Режим доступу до ресурсу: http://surl.li/nzeup

10. Про затвердження Положення про організацію та проведення інспекційних перевірок [Електронний ресурс]: Постанова від 17.07.2001 № 276 – Режим доступу: http://zakon.rada.gov.ua/laws/show/z0703-01

11. Синюк А. О. Оцінювання фінансової стійкості банків із використанням бізнес-моделей / А. О. Синюк // Науковий погляд: економіка та управління. – 2018. – № 2(60). – С. 176–188.

12. НБУ почав впроваджувати нові оцінки ризиків при обстеженні банків: Офіційне інтернет-представництво Національного банку України [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/nzfbh

13. Коваленко В. В. Моніторинг фінансової стабільності банківської системи України / В. В. Коваленко, Н. В. Радова. // Східна Європа: економіка, бізнес та управління. – 2019. – №2. – С. 321–330. – Електронний ресурс. – Режим доступу до ресурсу: http://surl.li/nzfco

14. Аналіз бізнес-моделей банків у рамках Supervisory review and evaluation process (SREP): Офіційне інтернет-представництво Національного банку України [Електронний ресурс] – Режим доступу до ресурсу: https://old.bank.gov.ua›doccatalog›document

15. Кожен другий комерційний банк не пройшов перевірку НБУ: Офіційне інтернет-представництво Національного банку України [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/nzfdq

16. Здійснення Національним банком України безвиїзного банківського нагляду: Офіційне інтернет-представництво Національного банку України [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/nzfex

17. Огляд банківського сектору 2023 року: Офіційне інтернет-представництво Національного банку України [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/lgzju

18. Карчева Г. Т. Теоретичні та практичні аспекти управління ризиками

електронного банкінгу / Г. Т. Карчева // Науковий вісник Полісся. – 2015. – № 2(2). – С. 121-126.

19. Ревенков П.В. Актуальні направлення регулювання електронного банківництва / П. В. Ревенков, А.Л. Поспєлов // Фінанси та кредит. – 2015. – № 24(648). – С. 2–13.

20. Нечипоренко А. В. Адаптація зарубіжних практик фінансового ризик-менеджменту до діяльності українських підприємств / А. В. Нечипоренко, К. О. Костікова // European scientific journal of Economic and Financial innovation. – 2023. – №1(11). – С. 46–53. – Електронний ресурс. – Режим доступу до ресурсу: http://surl.li/nzfne

21. Аналіз шахрайських та фішингових сайтів 2022-2023 [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/nzgha

22. Кібербезпека: Матриця платіжного шахрайства [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/nzgil

23. Данилишин Б. Бюджет 2023: реалістичність та ризики [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/nzgjq

24. Звіт про фінансову стабільність 2023 року: Офіційне інтернет-представництво Національного банку України [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/nzgkh

25. Війна і державні фінанси: скільки потрібно грошей на відновлення і де їх брати [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/nzgmd

26. Статистика щодо продажу та погашення ОВДП: Офіційне інтернет-представництво Національного банку України [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/nzgmx

27. Банкіри назвали головні виклики та ризики для банківської системи [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/nzgoa

28. У 2023 році банки почали нарощувати роздрібне кредитування [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/nzgrf

29. Звітність фінансового сектору 2023 року: Офіційне інтернет-

представництво Національного банку України [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/nzgrw

30. Павлюк О. О. Вплив коефіцієнта LCR на контроль за банківською ліквідністю / О. О. Павлюк // Економіка і суспільство. – 2016. – №7. – С. 36–41. – Електронний ресурс. – Режим доступу до ресурсу: http://surl.li/nzgtk

31. Тенденції банківського сектору : Офіційне інтернет-представництво Національного банку України [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/nzguq

32. Береславська О. І. Депозитні операції банків України: сучасний стан та напрямки розвитку / О. І. Береславська, В. А. Овсяник // Фінансово-кредитна діяльність: проблеми теорії та практики. – 2018. – №1. – С. 54-60. – Електронний ресурс. – Режим доступу до ресурсу: http://surl.li/nzgwp

33. Правдиковська І.І. Вплив війни на банківську систему України / І. І. Правдиковська, Н. О. Дорошенко // Молодий вчений. – 2022. – № 9(109). – С. 150–153. – Електронний ресурс. – Режим доступу до ресурсу: http://surl.li/nzgyb

34. Прибуток українських банків за 8 міс. 2023 сягнув рекордних 95 млрд грн [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/nzgyz

35. Грошово-кредитна та фінансова статистика банківського сектору: Офіційне інтернет-представництво Національного банку України [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/bypoo

36. Процентний ризик банку: Офіційне інтернет-представництво Національного банку України [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/nzhcj

37. Transition report 2020-21 the state strikes back: European Bank for Reconstruction and Development [electronic resource] – link: http://surl.li/nzhit

38. Кількість комерційних банків в Україні з 2008 по 2023 роки: Офіційне інтернет-представництво Міністерства фінансів України [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/lmqyw

39. Рисін В. В. Трансформація ролі банків на ринку державних боргових цінних паперів / В. В. Рисін, С. Є. Папірник // Економіка і

суспільство. – 2022. – №44. – С. 57–63.

40. Система захисту інформації в банку [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/nzhpf

41. Протокол AAA [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/nzhqa

42. Кавуненко Я. О. Дослідження методів багатофакторної автентифікації та їх практичного застосування / Я. О. Кавуненко // Науковий вісник ХНУРЕ. – 2022. – №1. – С. 112–119.

43. Як банки захищають кошти від кіберзагроз [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/nzhsj

44. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України: Постанова від 28.09.2017 № 95. – Режим доступу: http://surl.li/nzhui

45. Про затвердження Положення про Систему BankID Національного банку України: Постанова від 17.03.2020 № 32. – Режим доступу: http://surl.li/nzhvh

46. Створені передумови для запровадження комерційної моделі використання Системи BankID НБУ: Офіційне інтернет-представництво Національного банку України [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/nzhwh

47. Про Систему BankID Національного банку: Офіційне інтернет-представництво Національного банку України [Електронний ресурс] – Режим доступу до ресурсу: https://bank.gov.ua/ua/bank-id-nbu

48. Результати діяльності Системи BankID НБУ, 2022 рік: Офіційне інтернет-представництво Національного банку України [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/nzhxv

49. Топологія комп'ютерних мереж [Електронний ресурс] – Режим доступу до ресурсу: http://marytisna.blogspot.com/2017/10/blog-post.html

50. Базові топології комп'ютерних мереж [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/nziad

51. Напора І. Ю. Система інформаційної безпеки банку / І. Ю. Напора // Економічні науки. – 2021. – №4. – С. 81–84.

52. Технології криптографічного захисту інформації [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/nzick

53. Технології захисту інформації [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/lmxdk

54. Стандарт ISO 27001. Система менеджменту інформаційної безпеки [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/nzidl

55. Про затвердження Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг: Постанова Правління Національного банку України від 16.01.2021 року № 4. – Режим доступу до ресурсу: http://surl.li/nziei

56. Коваль Я. С. Вдосконалення інформаційно-аналітичної системи економічної безпеки банків на державному рівні / Я. С. Коваль // Вчені записки Університету «КРОК». – 2019. – №2(54). – С. 212–220.

57. Загальна схема процесу управління ризиком [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/nzigq