

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Кафедра банківської справи

Допущено до захисту

Завідувач кафедри

(підпис)

“ ____ ” _____ 202 ____ р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня магістра

зі спеціальності 072 «Фінанси, банківська справа, страхування та фондовий
ринок»

за магістерською програмою професійного/наукового спрямування

«Управління діяльністю банків на фінансовому ринку»

на тему: «Роль фінансового контролінгу в системі управління
операційним ризиком банку»

Виконавець:

студентка 63 групи, 6 курсу,
факультету фінансів та банківської
справи

Гогуленко Ніка Олександрівна

Науковий керівник:

д.е.н., професор

Коваленко Вікторія Володимирівна

ЗМІСТ

ВСТУП

РОЗДІЛ 1. Теоретичні основи фінансового контролінгу в системі управління операційним ризиком банківської установи

1.1. Економічний зміст фінансового контролінгу в системі управління операційним ризиком

1.2. Нормативно-правове забезпечення фінансового контролінгу в управлінні операційним ризиком у банківській системі

1.3. Методологічні підходи до впровадження фінансового контролінгу в систему управління операційними ризиками

Висновки до розділу 1

РОЗДІЛ 2. Оцінка практичних аспектів фінансового контролінгу в системі управління операційними ризиками АТ КБ «ПриватБанку»

2.1. Організаційна структура системи управління ризиками в АТ КБ «ПриватБанку»

2.2. Практика застосування інструментів фінансового контролінгу для виявлення та моніторингу операційного ризику

2.3. Оцінка ефективності діючих механізмів управління операційним ризиком у АТ КБ «ПриватБанку»

Висновки до розділу 2

РОЗДІЛ 3. Шляхи вдосконалення фінансового контролінгу в системі управління операційним ризиком АТ КБ «ПриватБанк»

3.1. Виявлення проблемних аспектів фінансового контролінгу в управлінні операційним ризиком в АТ КБ «ПриватБанку»

3.2. Напрями посилення ролі фінансового контролінгу в управлінні операційним ризиком банку

3.3. Прогнозування ефективності запропонованих заходів у контексті стабільності банківської діяльності

Висновки до розділу 3

ВИСНОВКИ

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

ДОДАТКИ

ВСТУП

Сучасний банківський сектор розвивається у швидкому темпі, постійно стикаючись із новими викликами та змінами у фінансовому середовищі. Зростання обсягів операцій, активна цифровізація, поява нових технологій та підвищення вимог до якості обслуговування клієнтів змушують банки переглядати підходи до організації своєї діяльності. В умовах такої динаміки особливого значення набуває здатність банку своєчасно реагувати на ризики, які можуть заважати його роботі. Одним із найважливіших серед них є операційний ризик, що супроводжує кожен етап виконання банківських операцій.

Операційний ризик виникає тоді, коли у внутрішніх процесах відбувається помилка, технічний збій, або коли працівники чи зовнішні чинники створюють загрозу стабільній роботі банку. Навіть одна невелика помилка може призвести до суттєвих фінансових наслідків, уповільнення діяльності, втрати клієнтів або пошкодження репутації. Тому управління операційним ризиком перестало бути допоміжним процесом і перетворилося на обов'язкову частину стратегічного розвитку кожної банківської установи.

У таких умовах важливою складовою стає фінансовий контролінг. Це не просто контроль за виконанням планів чи перевірка правильності операцій. Контролінг пов'язує між собою аналіз, планування, моніторинг і оцінку результатів, забезпечуючи єдиний підхід до управління діяльністю банку. Його головна роль полягає в тому, щоб завчасно виявляти ризики, знаходити їх причини, пропонувати шляхи усунення та допомагати керівництву приймати обґрунтовані рішення. З огляду на управління операційним ризиком, контролінг спрямований не на фіксацію вже допущених помилок, а на запобігання їх виникненню.

Актуальність обраної теми посилюється тим, що Національний банк України поступово удосконалює стандарти управління ризиками,

орієнтуючись на рекомендації Базельського комітету. Банки мають адаптуватися до цих вимог, розвиваючи власні системи внутрішнього контролю, створюючи бази даних операційних подій, модернізуючи ІТ-інфраструктуру та впроваджуючи нові методики оцінки ризику. Усе це підкреслює необхідність формування дієвого фінансового контролінгу як основи для ефективного управління операційними ризиками.

Таким чином, дослідження ролі фінансового контролінгу в системі управління операційним ризиком є важливим і своєчасним. Воно дозволяє глибше зрозуміти механізми стабільності банку, визначити слабкі місця у його внутрішніх процесах та запропонувати шляхи вдосконалення, які сприятимуть зміцненню фінансової стійкості та підвищенню конкурентоспроможності банківської установи.

Науковий інтерес до проблематики фінансового контролінгу та управління операційними ризиками відображений у працях як українських, так і зарубіжних науковців. Серед вітчизняних учених вагомий внесок зробили Коваленко В.В., Сергєєва О.С., Жердецька Л.В., Партин Г., Масленніков О., які досліджували методологію контролінгу, систему ризик-менеджменту та управлінські аспекти банківської діяльності. Зарубіжні науковці, такі як F. Freiberg, M. Knezevic, A.M. Dima, R. Stewart, приділяють увагу інтеграції контролінгу у загальну систему корпоративного управління та оцінці ефективності внутрішнього контролю в банках.

Мета кваліфікаційної роботи полягає в поглибленні теоретичних засад, удосконалення методичних підходів та розроблення практичних рекомендацій, спрямованих на підвищення ефективності фінансового контролінгу як ключового елемента системи комплексного управління операційними ризиками банку. Особлива увага приділяється формуванню дієвих інструментів моніторингу, аналізу та оцінки ризиків, що дозволяють своєчасно реагувати на можливі події операційного ризику банківської установи і забезпечувати безперервність діяльності банку.

Для досягнення поставленої мети передбачено **вирішення наступних завдань:**

- дослідити економічну сутність фінансового контролінгу та його роль у забезпеченні стабільності банківської діяльності;
- визначити нормативно-правові засади функціонування фінансового контролінгу в управлінні операційними ризиками у банківській системі України;
- проаналізувати існуючі методологічні підходи до впровадження фінансового контролінгу в систему управління ризиками банку;
- оцінити організаційну структуру управління ризиками в АТ КБ «ПриватБанк»;
- дослідити інструменти фінансового контролінгу операційного ризику АТ КБ «ПриватБанк»;
- оцінити ефективність діючих механізмів управління операційним ризиком у АТ КБ «ПриватБанк»
- обґрунтувати необхідність удосконалення фінансового контролінгу як інструменту мінімізації операційних ризиків банку;
- запропонувати напрями посилення механізму фінансового контролінгу в системі управління операційними ризиками банківської установи;
- розробити рекомендації щодо оптимізації системи фінансового контролінгу в системі управління операційним ризиком банку з урахуванням сучасних тенденцій цифровізації та регуляторних вимог.

Об'єктом дослідження є система управління операційним ризиком у банківській установі, у межах якого здійснюється застосування фінансового контролінгу як інструменту мінімізації впливу операційних ризиків на діяльність банку.

Предметом кваліфікаційної роботи є теоретико-методичні засади та практичні рекомендації застосування фінансового контролінгу операційного

ризик, який спрямований на підвищення ефективності механізму управління операційним ризиком банку.

Методи дослідження. Під час дослідження з метою розв'язання вищезазначених завдань було використано комплекс загальнонаукових та спеціальних методів, зокрема, методи аналізу, синтезу, індукції та дедукції, а також наукової абстракції й логіки, що сприяли розкриттю економічної сутності фінансового контролінгу, узагальненню наукових підходів та нормативно-правових засад управління операційними ризиками у банках. До того ж було застосовано системний підхід, що дозволив розглянути фінансовий контролінг як важливу складову комплексної системи ризик-менеджменту, визначити його основні елементи, функції та взаємозв'язки з іншими управлінськими процесами. Застосування методів класифікації та структурування допомогло впорядкувати підходи до організації фінансового контролінгу операційного ризику та описати модель його функціонування в межах «трьох ліній захисту» банківської установи. Використання порівняльного аналізу, під час написання кваліфікаційної роботи, дозволив зіставити підходи базових індикаторів та стандартизованого підходу до обчислення капіталу під операційний ризик, порівняти особливості побудови систем управління ризиками в українських і зарубіжних банках та визначити ефективність діючих механізмів фінансового контролінгу операційного ризику. З метою виявлення причин виникнення операційних ризиків й оцінки їхнього впливу на фінансові результати банку, було використано метод причинно-наслідкового аналізу. Метод моделювання дав змогу побудувати процес оцінки операційного ризику, розробити структуру системи фінансового контролінгу та візуалізувати взаємозв'язки між її елементами. Для зручності сприйняття аналізу використовувався графічний метод, який дозволив наочно відобразити динаміку операційного ризику, структуру системи контролінгу та її ключові компоненти. Статистичні методи, зокрема факторний аналіз, дозволили оцінити вплив кожного з факторів на бізнес-індикатор банку в стандартизованому підході з метою обчислення капіталу під

операційний ризик. Крім того, було застосовано метод експертних оцінок з метою виявлення слабких місць у функціонуванні фінансового контролінгу, а метод прогнозування – для оцінки майбутньої ефективності запропонованих удосконалень у системі управління операційними ризиками.

Для інформаційної бази дослідження використано нормативно-правові акти та закони України, що регулюють організацію та функціонування систем управління ризиками в банківських установах. Також застосовано положення та інструкції Національного банку України й рекомендації Базельського комітету з банківського нагляду. Для аналізу використовувалися фінансова звітність і звіти про управління АТ КБ «ПриватБанк», дані фінансово-інвестиційних порталів, публікації фахових періодичних видань, монографії та наукові роботи вітчизняних і зарубіжних дослідників.

Наукова новизна одержаних результатів полягає в поглибленні теоретичних засад та розробленні методичних підходів і практичних рекомендацій щодо підвищення ефективності фінансового контролінгу як ключового елемента системи управління операційним ризиком банку. До результатів, що визначають наукову новизну роботи, належать:

- уточнено економічну сутність фінансового контролінгу в системі управління операційним ризиком, акцентуючи на його ролі як комплексної системи, що поєднує аналіз, планування та моніторинг, забезпечуючи ранню діагностику потенційних ризиків у діяльності банку та своєчасне коригування управлінських рішень;

- узагальнено методологічні підходи до організації фінансового контролінгу операційного ризику та визначено модель його функціонування в межах концепції «трьох ліній захисту» банківської установи;

- доповнено зміст інструментарію фінансового контролінгу операційного ризику, зокрема щодо застосування факторного аналізу бізнес-індикатора у стандартизованому підході Базеля III, використання баз даних операційних подій;

– набули подальшого розвитку практичні рекомендації щодо оптимізації системи фінансового контролінгу операційного ризику банку в умовах активної цифровізації та посилення регуляторних вимог, що передбачають впровадження новітніх технологій, посилення внутрішньої культури ризик-орієнтованого управління та використання міжнародного досвіду для порівняльного аналізу навантаження на капітал.

Практична значимість кваліфікаційної роботи полягає у можливості безпосереднього використання результатів дослідження для підвищення ефективності системи управління операційними ризиками в банківських установах. Рекомендації, розроблені у роботі, можуть бути застосовані для вдосконалення внутрішніх процедур контролінгу, підвищення якості моніторингу операційних подій, оптимізації бізнес-процесів та покращення взаємодії між структурними підрозділами банку. Запропоновані заходи сприяють зміцненню системи внутрішнього контролю, підвищенню точності оцінки ризиків і зменшенню потенційних втрат, що є особливо важливим в умовах цифровізації та зростання кіберзагроз.

Структура та обсяг роботи. Робота складається із вступу, трьох розділів, висновків, списку використаної літератури та додатків.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ОСНОВИ ФІНАНСОВОГО КОНТРОЛІНГУ В СИСТЕМІ УПРАВЛІННЯ ОПЕРАЦІЙНИМ РИЗИКОМ БАНКІВСЬКОЇ УСТАНОВИ

1.1. Економічний зміст фінансового контролінгу в системі управління операційним ризиком

Конкуренція у вітчизняному банківському секторі з кожним роком набирає обертів, що змушує банківські установи постійно вдосконалювати свою діяльність та шукати нові шляхи підвищення ефективності. Для збереження стабільних позицій на ринку й отримання конкурентних переваг над іншими банками та небанківськими фінансовими установами, українські комерційні банки прагнуть оптимізувати структуру витрат, розширювати спектр банківських продуктів і послуг, підвищувати якість та швидкість обслуговування клієнтів, а також удосконалювати систему управління внутрішніми процесами.

Сучасні тенденції розвитку банківської діяльності зумовлюють активне впровадження інноваційних технологій, автоматизованих інформаційних систем, цифрових платформ і програмного забезпечення, що дозволяють забезпечити безперервність операцій та знизити кількість помилок, що виникають внаслідок людського фактору. Значного поширення набуває використання аутсорсингових послуг, що допомагає банківській установі ефективніше організувати технічну інфраструктуру та зосередитися на основних бізнес-процесах.

Разом з тим, активна цифровізація та автоматизація породжують нові виклики для вітчизняних банків. Зростає ризик технічних збоїв, кібератак, несанкціонованого доступу до даних, а також помилок персоналу, що безпосередньо підвищує рівень настання операційного ризику. Підходи до управління цими ризиками вже не відповідають динаміці сучасного

банківського сектору, тому потребують глибокої модернізації та інтеграції з сучасними системами контролю й моніторингу.

Успішне управління операційним ризиком сьогодні вимагає не лише своєчасного виявлення та оцінки ризикових подій, а й створення ефективної системи внутрішнього фінансового контролю, що поєднує аналітичні, управлінські, контрольні та прогностичні функції. Саме таку роль виконує фінансовий контролінг операційного ризику банку, який виступає інструментом комплексного управління ризиками, сприяє мінімізації можливих втрат.

Спершу визначмо тлумачення сутності «фінансовий контролінг». Незважаючи на те, що поняття «контролінг» співзвучний з терміном «контроль», однак їх зміст та функції відрізняються. Якщо за Орлюк О.П. «контроль» визначають як «невід’ємна частина регулюючого механізму, одна з форм зворотніх зв’язків, коли управляючий суб’єкт, одержуючи інформацію про стан фінансової системи, оцінює її та виносить рішення про необхідні заходи» [1]. У той час як «контролінг», на думку Терещенка О.О., окреслюють «спеціальною саморегулюючою системою методів та інструментів, яка спрямована на функціональну підтримку менеджменту підприємства і включає інформаційне забезпечення, планування, координацію, контроль і внутрішній консалтинг» [2]. Для більш точного розуміння понять порівняймо основні риси «контролю» та «контролінгу» на рис. 1.

Контроль	Контролінг
• перевірка ефективності використання ресурсів та збереження активів банку; • контроль за виконанням планових завдань і досягнення визначених цілей; • моніторинг дотримання внутрішніх політик, процедур та нормативів; • оцінювання фактичних результатів діяльності у порівнянні із запланованими показниками.	• розробка заходів щодо покращення роботи банку на основі аналітичних даних; • поєднання функцій фінансового аналізу та управління бізнес-процесами; • оцінка ефективності системи прийняття управлінських рішень; • запобігання впливу внутрішніх та зовнішніх загроз на діяльність банківської установи.

Рис. 1.1. Основні риси понять «контролю» та «контролінгу»

Джерело: розроблено та складено автором за матеріалами [3;4]

Тож «контроль» можемо визначити як процес перевірки та оцінювання вже досягнутих результатів діяльності. Його основна мета полягає у спостереженні за виконанням поставлених завдань, дотриманні внутрішніх процедур та досягненні запланованих фінансових показників. «Контролінг» навпаки представляє собою комплексну систему управління, що орієнтована на вдосконалення банківських бізнес-процесів та підвищення ефективності їх функціонування у майбутньому. Він поєднує фінансовий аналіз, планування, моніторинг і координацію управлінських рішень спрямованих на підвищення результативності діяльності банку. Тому поняття «контролінг» є ширшим порівняно з «контролем», оскільки він охоплює не лише процес перевірки та оцінювання діяльності банківської установи, а й передбачає застосування у системі управління таких функцій, як аналізу, планування та контролю з метою досягнення стратегічних цілей установи тощо.

В залежності від досліджуваного об'єкту розрізняють наступні види контролінгу: контролінг витрат, контролінг виробництва, контролінг інформаційних технологій, контролінг клієнтів, контролінг персоналу та

фінансовий контролінг [5; 6]. З метою дослідження системи управління операційним ризиком розглядатимемо саме фінансовий контролінг як інструмент ризик-менеджменту.

Єдиного визначення фінансового контролінгу не існує. Вітчизняні та закордонні науковці трактують його по-різному, зосереджуючись переважно на окремих його складових таких як функціональне призначення, роль у системі управління чи специфіка застосування в діяльності певних банківських установ. Розглянемо в табл. 1 основні поняття, що розкривають сутність фінансового контролінгу.

Таблиця 1.1

Визначення фінансового контролінгу, що розкривають його сутність у фінансових установах

Сутність фінансового контролінгу	Науковці	Опис
Складова контролінгу або його різновид	Терещенко О.О., Фрейберг Ф.	Фінансовий контролінг виступає складовою частиною загальної системи корпоративного контролінгу та спрямований на підтримку фінансового менеджменту. Його головна мета полягає забезпеченні ліквідності та платоспроможності установи, досягнення максимального прибутку при одночасному зменшенні рівня фінансових ризиків.
Окрема інформаційна підсистема	Пушкар М.С., Карцева В.В.	Фінансовий контролінг реалізує свої завдання завдяки комплексному використанню знань і методів із таких сфер, як менеджмент, фінансовий аналіз, облік, статистика, маркетинг та контроль. Його основна роль полягає у формуванні надійної інформаційної та методичної основи, яка допомагає підприємству своєчасно приймати обґрунтовані та ефективні управлінські рішення.
Уподібнення до управлінського контролю	Масленніков О.Ю., Гонсьор О.Я.	Сутність фінансового контролінгу розглядається як форма управлінського контролю, що зосереджується на ключових напрямках фінансової діяльності підприємства. Його завдання полягає у своєчасному виявленні відхилень фактичних результатів від запланованих, коригуванні поточної роботи, запобіганні ризикам, дотриманні встановлених нормативів та забезпеченні безперервного вдосконалення процесу прийняття управлінських рішень.

Продовження таблиці 1.1

Основна ланка системи управління	Прокопенко О., Криворучко Л., Gonda G.	Фінансовий контролінг розглядається як ключовий елемент системи управління підприємством і водночас як особлива управлінська концепція, що формує філософію ефективного менеджменту. Його сутність полягає в забезпеченні якісної інформаційної підтримки управлінських рішень, адаптації підприємства до змін зовнішнього середовища та раціональному використанні ресурсів із урахуванням потенційних ризиків. Фінансовий контролінг являє собою безперервний процес, що включає три основні етапи – планування, реалізацію та контроль результатів.
Саморегулююча система	Дудар Д., Дяченко Н.М.	Фінансовий контролінг трактується як цілісна, саморегульована система, що має власну мету, набір функцій, завдань і інструментів реалізації. Його впровадження здійснюється через спеціалізований структурний підрозділ – службу контролінгу, яка координує та підтримує ефективність управлінських процесів у межах підприємства.

Джерело: складено та розроблено автором за матеріалами [2; 7; 8; 9; 10; 11; 12; 13; 14].

Отже, у банківській сфері фінансовий контролінг доцільно розглядати як комплексну систему управління, що поєднує аналіз, моніторинг і коригування бізнес-процесів у режимі постійного вдосконалення. Такий підхід забезпечує ефективну підтримку управлінських рішень, сприяє досягненню стратегічних цілей банку, збереженню його ліквідності та платоспроможності, а також мінімізації можливих ризиків.

Система фінансового контролінгу, будучи важливою складовою банківського ризик-менеджменту, виконує функцію ранньої діагностики потенційних проблем у змінні рівня ризику та дає змогу своєчасно скоригувати управлінські рішення, запобігаючи виникненню критичних ситуацій. Контролінг у банківській установі виступає ефективним інструментом управління ризиками, що реалізується через такі ключові функції:

– Розробка організаційних принципів, стратегій, політик, методик і процедур моніторингу ризиків, що супроводжують банківську діяльність;

- Оцінка ефективності системи управління ризиками та її оперативне вдосконалення;
- Аналіз і контроль рівня ризику, прийнятого окремими структурними підрозділами банку;
- Оцінка впливу зовнішніх факторів на структуру та величину ризикових позицій;
- Планування заходів хеджування ризиків;
- Формування оптимальної структури активів і пасивів, а також управління прибутковістю кредитного портфеля й портфеля цінних паперів;
- Встановлення лімітів на рівень ризику та контроль за їх дотриманням;
- Проведення аудиту і коригування управлінських дій у разі виявлення порушень у системі ризик-менеджменту;
- Введення обліку, складання та аналіз фінансової звітності, що відображає реальний стан ризикових позицій;
- Контроль за виконанням усіх затверджених процедур управління ризиками в межах банку [15].

Необхідність впровадження фінансового контролінгу операційного ризику в діяльність банків зумовлена постійним прагненням до підвищення ефективності бізнес-процесів, забезпечення конкурентоспроможності та відповідності фактичних результатів плановим показникам. Додатковим чинником є інтенсивна цифровізація банківських послуг, яка значно підвищує ймовірність виникнення операційних збоїв і вимагає створення комплексних систем контролю та управління ризиками.

Сучасні банки все частіше використовують фінансовий контролінг як основний інструмент управління бізнес-процесам, оскільки стабільність діяльності та досягнення стратегічних цілей неможливі без системного підходу.

Бізнес-процеси банку – це сукупність взаємопов'язаних операцій, що забезпечують виконання основних функцій установи, розвиток її діяльності

та отримання прибутку. Ефективне управління ними передбачає постійний аналіз, оптимізацію та контроль кожного етапу процесів, використання ресурсів, а саме людських, матеріальних, інформаційних та фінансових, із максимальною продуктивністю та мінімізацією втрат. У цьому контексті ключову роль відіграє компетентність виконавців і чітке розмежування відповідальності за окремі ланки процесу, що забезпечує узгоджену роботу всієї системи.

Таким чином, фінансовий контролінг операційного ризику виступає не лише інструментом ризик-менеджменту, а й стратегічним механізмом розвитку банку, що дозволяє йому підвищувати ефективність своїх бізнес-процесів, адаптувати банк до змін ринкового середовища та забезпечувати його конкурентні переваги.

Варто зазначити, що операційний ризик за своєю сутністю може проявитися на будь-якому етапі бізнес-процесів банку. Тож спершу визначимо суть операційного ризику.

Згідно з Постановою Правління Національного Банку України «Про затвердження Положення про організацію системи управління ризиками в банках України та банківських групах» операційний ризик характеризують як «імовірність виникнення збитків або додаткових втрат або недоотримання запланованих доходів унаслідок недоліків або помилок в організації внутрішніх процесів, навмисних або ненавмисних дій працівників банку або інших осіб, збоїв у роботі систем банку або внаслідок впливу зовнішніх факторів. Операційний ризик уключає юридичний ризик, однак має виключати ризик репутації та стратегічний ризик» [16].

За визначенням Базельського комітету з банківського нагляду операційним ризиком називають ймовірність понесення збитків через помилки або недоліки у внутрішніх процесах, людському факторі, технічних системах чи внаслідок впливу зовнішніх подій. Для управління операційним ризиком Базельський комітет також виокремлює вісім бізнес-процесів: корпоративні фінанси (Corporate Finance); продажі та спекулятивні операції

(Trading and Sales); роздрібний банкінг (Retail Banking); комерційний банкінг (Commercial Banking); платежі та розрахунки (Payment and Settlement); агентські послуги (Agency services); управління активами (Asset Management); роздрібні брокерські послуги (Retail Brokerage) [17].

При цьому кожен бізнес-процес має власні ключові показники ефективності (KPI), на які безпосередньо впливає операційний ризик. Тож, у даному випадку, фінансовий контролінг операційного ризику виступає комплексною системою, що поєднує у собі управління та контроль виконання завдань у внутрішніх фінансових бізнес-процесах з метою підвищення ефективності діяльності банку та запобігання реалізації операційного ризику, враховуючи як внутрішні, так і зовнішні чинники.

Фінансовий контролінг у банку, як і будь-яка система управління, виконує функції регулювання діяльності на двох рівнях – стратегічному та оперативному. Саме тому розрізняють стратегічний і оперативний фінансовий контролінг операційного ризику. Розглянемо їх більш детальніше.

Стратегічний фінансовий контролінг спрямований на забезпечення довгострокової стабільності та досягнення ключових цілей банку. Його завдання виходять за межі щоденного контролю та зосереджені на формуванні ефективної стратегії розвитку банківської установи. До його основних завдань належать: оцінка впливу внутрішніх та зовнішніх факторів на операційний ризик; аналіз конкурентного середовища та визначення сильних і слабких сторін банку; управління діяльністю банку для досягнення стратегічних цілей; оптимізація витрат у процесі операційної роботи тощо.

Натомість оперативний фінансовий контролінг банку зосереджений на щоденному управлінні бізнес-процесами та оперативній підтримці прийняття рішень. Він спрямований на забезпечення стабільності, ефективності та надійності поточної діяльності банку, зменшення ймовірності виникнення операційних ризиків та мінімізацію можливих втрат у разі їх реалізації. Його завдання включають: розробку та контроль виконання короткострокових

планів; порівняння фактичних результатів з плановими та підвищення продуктивності операцій; надання практичних рекомендацій щодо вдосконалення бізнес-процесів; підвищення кваліфікації та мотивації персоналу для зниження рівня операційного ризику.

Таким чином, стратегічний і оперативний контролінг взаємодоповнюють один одного. Перший формує довгострокові орієнтири та мінімізує загальні ризики, а другий забезпечує надійність, своєчасність та ефективність лише поточної діяльності банку, зменшуючи ймовірність реалізації операційних ризиків.

Спираючись на основні функції стратегічного та оперативного контролінгу, виокремимо завдання, що стоять перед системою фінансового контролінгу операційного ризику з метою мінімізації операційного ризику та запобіганню суттєвим втратам у разі його реалізації:

- Забезпечення досягнення коротко- та довгострокових цілей банку;
- Підвищення прозорості та ефективності внутрішніх бізнес-процесів;
- Формування комплексної системи управління операційними ризиками;
- Розробка та впровадження ключових показників для контролю та оцінки ризиків;
- Оптимізація використання ресурсів персоналу у взаємодії з технічними засобами;
- Організація збору, обробки та постійного доступу до даних про випадки операційного ризику.

Реалізацію зазначених завдань здійснюють контролінгові служби банку, які виконують роль координаційного та аналітичного центру управління ризиками. Вони займаються систематичним збором, обробкою та аналізом даних про бізнес-процеси та потенційні ризикові події, що дозволяє своєчасно виявляти загрози та прогнозувати їхній вплив на фінансовий стан

банку. Контролінгові підрозділи здійснюють аудит процедур та внутрішніх нормативів, перевіряють достовірність інформації, забезпечують відповідність діяльності банку законодавчим та регуляторним вимогам. Крім того, вони займаються адаптацією бізнес-процесів до змін зовнішнього середовища, оцінюють ефективність взаємодії між структурними підрозділами та впроваджують інноваційні підходи для підвищення прозорості та контролюваності операцій. Завдяки діяльності контролінгових служб отримує змогу не лише зменшувати вплив операційних ризиків, а підтримувати свої стратегічні пріоритети та зміцнювати конкурентні позиції на ринку.

Підсумовуючи все вищезазначене, можемо сказати, що фінансовий контролінг операційного ризику виступає ключовим інструментом управління бізнес-процесами банківської установи, забезпечуючи прозорість, ефективність та контроль за виконанням завдань. Завдяки діяльності контролінгових служб банк своєчасно реагує на потенційні загрози, оптимізує ресурси та бізнес-процеси, що сприяє підвищенню стабільності та досягненню стратегічних цілей. Таким чином, фінансовий контролінг та робота контролінгових служб є невід'ємною складовою ефективного управління операційними ризиками банку.

1.2. Нормативно-правове забезпечення фінансового контролінгу в управлінні операційним ризиком у банківській системі

Ефективне управління операційним ризиком є ключовим елементом стабільного функціонування банківської системи, оскільки саме цей вид ризику супроводжує всі бізнес-процеси банку – від внутрішніх операцій до взаємодії із зовнішнім середовищем. Для забезпечення належного контролю, запобігання втратам та підтримки фінансової стійкості банків надзвичайно

важливим є наявність чіткої та узгодженої нормативно-правової бази. Вона визначає основні принципи, вимоги та механізми фінансового контролінгу в управлінні операційним ризиком на різних рівнях – міжнародному, національному та внутрішньому. Саме тому доцільно розглянути структуру цієї нормативно-правової системи через призму трирівневого підходу, що охоплює метарівень, макрорівень та макрорівень регулювання. Такий підхід дозволяє комплексно оцінити взаємозв'язок між міжнародними стандартами, національними вимогами та внутрішніми політиками банків у сфері управління операційним ризиком. Розглянемо більш детальніше трирівневий підхід управління операційним ризиком.

– I рівень (метарівень) – охоплює міжнародні стандарти, норми та рекомендації, що визначають загальні принципи управління операційним ризиком у банківській сфері.

– II рівень (макрорівень) – представлений національною законодавчою базою, зокрема нормативними актами Національного банку України та законами, які прямо або опосередковано регулюють питання управління ризиками у банківських установах.

– III рівень (мікрорівень) – включає внутрішню нормативну документацію кожного окремого банку: політики, інструкції, положення та процедури, що враховують специфіку діяльності установи та визначають порядок контролю й управління операційними ризиками.

Більш докладний опис рівнів нормативно-правового регулювання управління операційним ризиком наведено нижче в табл. 1.2.

Таблиця 1.2

Нормативно-правове забезпечення управління операційним ризиком
банку

Рівень	Документ
I рівень – метарівень	Basel II: International convergence of capital measurement and capital standards: a revised framework 2004
	Basel III: A global regulatory framework for more resilient banks and banking systems
	Sound practices for the management and supervision of operational risk
	Основні принципи ефективного банківського нагляду

Продовження таблиці 1.2

	Директива 2006/48/ЄС Європейського Парламенту та Ради про започаткування та здійснення діяльності кредитних установ
II рівень – макрорівень	Постанова Правління НБУ №64 «Про затвердження Положення про організацію системи управління ризиками в банках України та банківських групах»
	Постанова Правління НБУ №156 «Про затвердження Положення про порядок визначення банками України мінімального розміру операційного ризику»
	Постанова НБУ №368 «Про затвердження Інструкції про порядок регулювання діяльності банків в Україні»
	Постанова Правління НБУ №75 «Про затвердження Положення про організацію бухгалтерського обліку, бухгалтерського контролю під час здійснення операційної діяльності в банках України»
	Методичні рекомендації щодо організації та функціонування систем ризик-менеджменту в банках України, затверджені Постановою Правління НБУ №361
	Методичні вказівки з інспектування банків «Система оцінки ризиків»: методичні вказівки, схвалені Постановою Правління НБУ №104
III – мікрорівень	Внутрішньобанківські документи, а саме політика та стратегія управління операційним ризиком, порядок та процедури управління операційним ризиком, методики виявлення суттєвих ризиків, декларації схильності до операційного ризику.
	Внутрішньобанківська документація з організації фінансового контролінгу операційного ризику банку

Джерело: складено та розроблено автором за матеріалами [18].

Метарівень нормативно-правового регулювання є фундаментом для побудови всієї системи управління операційним ризиком. Його документи задають стандарти, принципи та методологію, які застосовуються на національному та внутрішньобанківському рівнях. Завдяки цим міжнародним нормам банки отримують орієнтири для формування ефективних механізмів контролю й адаптуються до мінливих умов фінансового середовища.

Одним із ключових документів є Базель II «International convergence of capital measurement and capital standards: a revised framework», який визначив принципи розрахунку достатності капіталу банку з урахуванням різних видів ризиків, зокрема операційного. Фактично, Базель II встановив необхідність вимірювання операційного ризику як окремого виду ризику, що потребує покриття капіталом. Це стимулювало банки впроваджувати внутрішні

системи оцінки ризиків, автоматизовані процедури моніторингу та вдосконалювати контроль за бізнес-процесами.

Подальший розвиток підходів до управління ризиками відобразився в Базелі III «A global regulatory framework for more resilient banks and banking systems», який деталізував методи оцінювання операційного ризику, запровадивши стандартизований підхід (SA). Цей підхід базується на двох ключових елементах: бізнес-індикаторі (BIC) та внутрішньому мультиплікаторі втрат (ILM) [19]. Документ підвищив вимоги до прозорості розрахунків і стимулював банки до глибшого аналізу своїх операційних втрат. Таким чином, Базель III зміцнив зв'язок між ефективністю внутрішніх процесів і потребою в капіталі для покриття ризиків.

Окрему роль відіграє документ «Sound practices for the management and supervision of operational risk» (Комплексна практика управління та нагляду за операційним ризиком), який містить практичні рекомендації щодо ефективного управління операційними ризиками. Він визначає підходи до ідентифікації, оцінки, моніторингу та контролю ризиків, а також акцентує увагу на розвитку корпоративної культури управління ризиками [20]. У цьому контексті велика увага приділяється діджиталізації банківських процесів, впровадженню сучасних аналітичних інструментів та формуванню стратегії запобігання операційним ризикам на всіх рівнях управління.

Ваговим елементом міжнародної нормативної бази є «Основні принципи ефективного банківського нагляду», розроблені Базельським комітетом. У них визначено загальні вимоги до організації системи внутрішнього контролю, аудиту, управління ризиками та моніторингу діяльності банків. Документ підкреслює, що належний контроль і прозорість банківських процесів є запорукою фінансової стабільності як окремої установи, так і банківської системи загалом [21].

Важливе значення має Директива 2006/48/ЄС Європейського Парламенту та Ради, яка встановлює вимоги щодо ліцензування, нагляду та управління ризиками у діяльності кредитних установ країн Європейського

Союзу. Вона визначає, що всі банки мають ідентифікувати та оцінювати ризики, зокрема операційні, і підтримувати відповідний рівень капіталу для їх покриття. Документ також підкреслює важливість уніфікації підходів до управління ризиками серед банків різних країн та стимулює впровадження альтернативних методів розрахунку ризиків [22]. Таким чином, директива сприяє гармонізації європейської банківської системи та створює спільні стандарти управління ризиками.

На другому рівні, а саме макрорівні нормативно-правова база управління операційним ризиком формується відповідно до національного законодавства та нормативних актів НБУ, які визначають основні вимоги, принципи та методи організації системи управління ризиками в банках. Цей рівень забезпечує адаптацію міжнародних стандартів до умов національної банківської системи та слугує інституційною основою для реалізації вимог Базельського комітету у практичній діяльності українських банків.

Методичні рекомендації щодо організації та функціонування системи ризик-менеджменту, затвердженні Постановою Правління НБУ №361, визначають вимоги до побудови внутрішніх політик банків у площині управління ризиками. Також підкреслено роль капіталу банку як засобу покриття можливих ризиків, а також зазначено необхідність постійного вдосконалення процесів моніторингу та аналізу ризикових ситуацій. У цьому документі наведено положення щодо взаємозв'язку між системою ризик-менеджменту та корпоративним управлінням, що є важливою передумовою для забезпечення стабільності банківської діяльності [23].

Важливим документом на цьому рівні є Постанова Правління НБУ №64 «Про затвердження Положення про організацію системи управління ризиками в банках України та банківських групах». Її норми зобов'язують банки враховувати принципи комплексного управління операційними ризиками, забезпечуючи дотримання процесів ідентифікації, вимірювання, моніторингу, контролю та звітування. Документ наголошує на важливості

створення ефективної системи ризик-менеджменту, яка повинна охоплювати всі етапи управління та всі напрями діяльності банку [24].

Постанови правління НБУ № 156 та №75 регламентують порядок визначення банками мінімального розміру операційного ризику для розрахунку нормативів достатності капіталу, а також питання бухгалтерського обліку операційних втрат і контролю за їх відображенням у фінансовій звітності [25; 26]. Ці документи спрямовані на формування єдиної методології управління ризиками в межах вітчизняного банківського сектору та забезпечення прозорості процесів їх оцінки.

Крім того, Постанова НБУ №368 «Про затвердження Інструкції про порядок регулювання діяльності банків в Україні» розроблена з метою запобігання неефективному використанню ресурсів та зниження капіталу, що може виникнути внаслідок дії різноманітних ризиків, зокрема операційного, який є невід'ємною складовою банківської діяльності [27].

На макрорівні нормативно-правова база управління операційним ризиком формується безпосередньо всередині кожного банку з урахуванням його організаційного структури, масштабів діяльності та рівня ризиковості операцій. Вона охоплює внутрішньобанківські документи, що визначають стратегію, політику та процедури управління ризиками, зокрема декларації схильності до операційного ризику, методики ідентифікації та оцінювання ризиків, кодекс поведінки і порядок реагування на ризикові події. Важливим елементом є також внутрішня система контролінгу, яка забезпечує моніторинг ефективності управління ризиками на всіх етапах операційної діяльності банку.

Окрім того, внутрішньобанківська документація з організації фінансового контролінгу операційного ризику має включати вимоги до технічного та програмного забезпечення, інформаційної безпеки, кадрової політики, а також до створення надійної комунікаційної системи між структурними підрозділами. Такі внутрішні нормативи повинні відповідати

вимогам НБУ та міжнародним рекомендаціям, але водночас адаптуватися до індивідуальних потреб кожного банку.

Отже, українське нормативно-правове законодавство банківської діяльності тісно інтегроване у міжнародну нормативну систему та в багатьох випадках повністю відтворює її ключові положення. Це зумовлено необхідністю гармонізації національного банківського сектору з міжнародними стандартами, що забезпечує підвищення стійкості банківської системи та її конкурентоспроможності на глобальному рівні. У сучасних умовах діяльність банків неможлива без міжнародного співробітництва, яке потребує єдиних підходів до оцінювання, моніторингу та управління ризиками. Саме тому на основі рекомендацій Базельського комітету, а саме Базель II та Базель III, НБУ було розроблено «Положення про організацію системи управління ризиками в банках України та банківських групах», що визначає ключові принципи і вимоги до побудови ефективної системи управління операційними ризиками.

Завдяки впровадженню цих стандартів вітчизняні банки отримали можливість удосконалити внутрішні механізми контролінгу, забезпечити належну ідентифікацію та оцінку ризиків, а також підвищити рівень прозорості своєї діяльності. Це сприяє не лише зниженню ймовірності виникнення операційних втрат, а й зміцненню довіри інвесторів, клієнтів та міжнародних партнерів до національної банківської системи.

Наразі багато українських банків не мають власних систем обліку та баз даних для фіксації операційного ризику, що обмежує можливості використання сучасного стандартизованого підходу до визначення капіталу під цей вид ризику. Внаслідок цього виникає потреба в чіткому законодавчому врегулюванні цього питання. У більшості досліджень наголошується, що операційний ризик здебільшого розглядається банками як внутрішня та конфіденційна категорія, через що детальна інформація про його прояви рідко стає публічною.

Тому, доцільно розробити нормативний документ, який би зобов'язував банки вести облік операційного ризику та формувати відповідні бази даних. Це дозволило б створити єдиний реєстр операційного ризику для банківської системи і забезпечило б прозорість та доступність узагальненої інформації для зацікавлених сторін. Крім того, існує прогалина в правовому регулюванні щодо фінансового контролінгу операційного ризику. Необхідно запровадити комплексну стратегію управління, що включатиме внутрішні регламенти та правила реалізації цієї стратегії, методики кількісної оцінки ризику та його впливу на фінансові результати банку, розподіл відповідальності серед працівників, перелік технологій для обробки даних, а також чіткі процедури моніторингу та звітності на рівні підрозділів й банку в цілому.

Постійні кризові ситуації в банківському секторі, вплив зовнішніх економічних шоків, кіберзагрози та значні фінансові втрати, що виникають унаслідок цих факторів, свідчать про недостатню ефективність чинного законодавства в сфері управління операційним ризиком. Сучасні умови вимагають оновлення нормативної бази та запровадження більш гнучких та адаптивних механізмів регулювання.

До основних напрямків удосконалення українського законодавства можна віднести:

- Прискорене реагування законодавчих органів і керівництва банків на зовнішні й внутрішні загрози;
- Створення норм, що враховують специфіку діяльності окремих банківських установ;
- Інтеграцію вітчизняних норм управління ризиком із міжнародними стандартами з урахуванням особливостей національної банківської системи;
- Посилення захисту банківської інформації в умовах зростання кіберзагроз;

- Розробку уніфікованих алгоритмів переходу банків у надзвичайний режим роботи під час кризових подій;
- Створення комплексної бази даних щодо реалізації операційного ризику та її правове закріплення [18].

Отже, ефективне управління операційним ризиком є ключовою умовою стабільності банківської системи України. Недосконалість чинного законодавства потребує оновлення та адаптації до сучасних викликів і міжнародних стандартів. Створення єдиного реєстру ризиків, посилення контролю та захисту інформації сприятимуть підвищенню прозорості й надійності банківської діяльності.

1.3. Методологічні підходи до впровадження фінансового контролінгу в систему управління операційними ризиками

На сьогодні відсутній єдиний, універсальний підхід до управління операційним ризиком у банках, оскільки вибір конкретної моделі залежить від низки індивідуальних факторів, зокрема, від розміру установи, рівня її технологічного розвитку, структури активів та складності операцій. Важливу роль у цьому процесі відіграє регулятор, який оцінює, наскільки ефективно банк управляє власними ризиками, визначає рівень його готовності до прийняття ризику та межі толерантності до нього. Ефективна система управління операційним ризиком передбачає комплексну ідентифікацію ризиків за всіма напрямками діяльності банку, їх постійну оцінку, наявність внутрішніх політик, процедур і лімітів, а також розвинену систему моніторингу й звітності. Водночас важливим аспектом є створення культури ризик-менеджменту, коли відповідальність за управління ризиками розподіляється між усіма рівнями управління, а контроль стає невід'ємною частиною щоденної діяльності банку.

Еволюція підходів до управління операційним ризиком у банківській діяльності відбувалася поступово, проходячи кілька етапів, кожен із яких характеризувався зміною розуміння сутності ризику, його ролі в діяльності банків та методів управління ним. На початковому етапі, до 1990-х років, поняття «операційний ризик» фактично не існувало у теоретичному та практичному середовищі. Банки вважали такі ризики незначними або такими, що не потребують спеціального управління. Основна увага у цей час приділялася кредитним, ринковим і процентним ризикам. Натомість відсутність усвідомлення важливості операційного ризику призводила до відсутності його системного обліку та аналізу.

Період з 1991 по 2004 роки став етапом накопичення інформації про операційний ризик. Період характеризується поступовим усвідомленням значущості операційного ризику для стабільності банківської установи внаслідок ідентифікації та класифікації операційних ризиків, накопичення даних про випадки їх реалізації, створення перших внутрішніх баз даних. Саме в цей час у міжнародній практиці з'явилося офіційне визначення поняття «операційний ризик», що стало основою для подальшого розроблення методів його оцінювання та контролю [28].

Наступний етап, який тривав із 2004 до 2014 року, збігається з активним впровадженням вимог Базельського комітету. Основна увага була зосереджена на кількісному вимірюванні операційного ризику та його впливу на розмір регулятивного капіталу банку. Також розроблялися стандартизовані та внутрішні підходи до розрахунку ризику, формувалися моделі оцінки збитків від його реалізації. Водночас, у банках почали з'являтися окремі підрозділи з управління операційними ризиками, що сприяло підвищенню рівня контролю та управління [29, 30].

У період з 2014 по 2020 рік відбувся перехід до нової моделі управління, заснованої на стандартизованому підході Базель III. Основний акцент робився не лише на кількісних, а й на якісних аспектах оцінки ризику. Банки почали активно впроваджувати системи внутрішнього контролю,

автоматизацію процесів управління ризиками, а також політики та стратегії управління операційним ризиком.

Починаючи з 2020 року й дотепер, відбувається пошук інтегрований підхід до управління ризиками, де операційний ризик розглядається у взаємозв'язку з іншими видами ризиками. Основна увага приділяється побудові єдиного механізму оцінки, моніторингу та реагування на ризики, розвитку культури ризик-менеджменту серед усіх працівників банку. Заразом, цифровізація банківської діяльності та зростання кіберзагроз зумовили необхідність нових інструментів для виявлення, вимірювання та мінімізації операційних ризиків. Тому на цьому етапі операційний ризик перетворився з допоміжної категорії на стратегічний елемент системи управління банківською діяльністю.

Таким чином, розвиток підходів управління операційним ризиком у банках відбувався послідовно, а саме, від повного ігнорування цього виду ризику до усвідомлення його ключового значення для стабільності банківської діяльності. Кожна стадія відображала новий рівень зрілості банківської установи та посилення ролі ризик-менеджменту в корпоративному управлінні. На сучасному етапі управління операційним ризиком набуває стратегічного характеру, охоплюючи не лише контроль і вимірювання, а й формування ризик-культури в установах. Подальший розвиток підходів передбачає інтеграцію інноваційних технологій, аналітичних інструментів та міжнародних стандартів у систему управління ризиками.

У межах попередньо розглянутих етапів розвитку підходів управління операційним ризиком відіграло прийняття рекомендацій Базельського комітету. У Базелі II вперше на міжнародному рівні було офіційно визначено поняття операційного ризику та підкреслено необхідність його системного обліку. Згідно з вимогами Базельського комітету, банки повинні не лише визначати операційний ризик, а й ідентифікувати всі суттєві втрати, що можуть виникати внаслідок його реалізації. Це в свою чергу посприяло

формуванню єдиної структури ризик-менеджменту, у межах якої було виокремлено сім основних категорій операційних витрат. Це дало змогу банкам глибше аналізувати причини виникнення ризиків, узагальнювати дані про події, що спричиняють збитки, і створювати бази даних для подальшої кількісної оцінки операційного ризику. У результаті управління ризиками набуло більш системного та науково обґрунтованого характеру, що заклало основу для формування сучасних стандартів контролю та звітності у сфері банківського нагляду. Розглянемо більш детально категорії операційних витрат у табл. 1.3.

Таблиця 1.3

Характеристика категорій операційних витрат згідно з Базелем II

Категорії операційних витрат	Характеристика
Внутрішнє шахрайство	Збитки, спричинені навмисними діями співробітників банку з метою отримання особистої вигоди або приховування помилок.
Зовнішнє шахрайство	Втрати, пов'язані з незаконними діями сторонніх осіб, такими як крадіжки, хакерські атаки, підробка документів тощо.
Недосконалість кадрової політики	Витрати, пов'язані з порушенням трудового законодавства, дискримінацією працівників.
Клієнти та продукти банку	Збитки, що виникають через неналежне надання послуг, порушення договірних умов або невідповідність продукції банку нормативним вимогам.
Пошкодження матеріальних активів	Втрати, спричинені стихійними лихами, аваріями чи іншими фізичними впливами на майно банку.
Переривання діяльності внаслідок збоїв систем	Втрати, пов'язані з технічними збоями, кібератаками, відмовою ІТ-систем або інфраструктури.
Управління процесами	Витрати, що виникають унаслідок помилок персоналу, збоїв у внутрішніх процесах, неузгодженості дій чи неналежного контролю.

Джерело: складено та розроблено автором за матеріалами [31].

Класифікація операційних витрат, запропонована Базелем II, стала фундаментом для побудови ефективної системи ідентифікації та контролю ризиків у банківській діяльності. Вона дозволяє не лише визначати джерела

потенційних збитків, а й формувати механізми контролю, попередження та мінімізації ризиків. Водночас, це забезпечує більш глибоке розуміння природи операційного ризику та створює основу для розробки дієвих стратегій зниження втрат.

Проте для зменшення негативних наслідків від операційного ризику та мінімізації фінансових втрат однієї лише класифікації недостатньо. Необхідним стало створення механізму покриття можливих збитків капіталом банку.

Саме з цією метою у 2004 році Базельський комітет з банківського нагляду запропонував низку підходів до визначення обсягу капіталу, який має бути зарезервований для покриття операційних ризиків. Відповідно до рекомендацій Базеля II, існує три основні методи розрахунку капіталу під операційний ризик: підхід базового індикатора (BIA), стандартизований підхід (TSA) та поглиблений підхід до вимірювання (AMA).

Таблиця 1.4

Методи розрахунку капіталу для покриття операційного ризику згідно з
Базелем II

Метод розрахунку	Капітал для покриття операційного ризику	Опис	Інформаційна база для розрахунку
The Basic Indicator Approach (BIA)	$K_{BIA} = \frac{[\sum(GI_{1..n} \times \alpha)]}{n},$ де GI – валовий дохід банку за останні три роки; n – кількість попередніх трьох років, для яких валовий дохід є позитивним; α – коефіцієнт операційного ризику.	Необхідний розмір капіталу банку під покриття операційним ризиком визначається шляхом добутку коефіцієнта операційного ризику (складає 15%) на річний валовий дохід за останні 3 роки, коли цей дохід мав додатне значення.	Публічні дані
The Standardized Approach (TSA)	$K_{TSA} = \frac{\{\sum_{years_{1-3} \max[\sum(CI_{1-8} \times \beta_{1-8}), 0]\}}{3},$ де CI_{1-8} – річний валовий дохід для кожної з восьми бізнес-ліній; β_{1-8} – коефіцієнт рівня	Розмір капіталу під покриття операційного ризику знаходиться шляхом зважування усередненого річного валового доходу по кожній бізнес-лінії за 3 роки помноженого на коефіцієнт рівня необхідного капіталу до	Власні внутрішні дані банку

	необхідного капіталу до рівня по кожній з 8 бізнес-ліній.	рівня по відповідній бізнес-лінії.	
The Advanced Measurement Approach (AMA)	$K_{AMA} = Expected\ Loss + Unexpected\ Loss,$ де $Expected\ Loss$ – очікувані втрати від операційного ризику; $Unexpected\ Loss$ – непередбачувані втрати від операційного ризику.	Розмір необхідного капіталу під покриття операційного ризику визначається шляхом моделювання використовуючи кількісні та якісні критерії.	Власні внутрішні детальні дані банку

Джерело: складено та розроблено автором за матеріалами [32].

Відповідно до рекомендацій Базельського комітету, кожен із трьох запропонованих підходів до розрахунку капіталу під операційний ризик має власні особливості, рівень складності та чутливості до ризику. Вони розташовані у порядку зростання точності вимірювання ризику, але водночас й у порядку зменшення простоти розрахунків. Найбільш доступним для використання є підхід базового індикатора (BIA), який ґрунтується на фінансовій звітності банку та застосуванні фіксованого коефіцієнта (15%) до середнього річного валового доходу за три попередні роки. Цей метод вважається найпростішим, проте й найменш чутливим до реальних умов функціонування банку, оскільки не враховує специфіку окремих напрямів діяльності.

Стандартизований підхід (TSA) передбачає більш детальну оцінку операційного ризику за кожним із восьми видів банківського бізнесу. Для кожного напрямку встановлюються власні коефіцієнти, які коливаються від 12% до 18%, що дозволяє більш точно враховувати рівень ризику у різних сферах банківських операцій. Разом із тим, даний метод є складнішим у реалізації, оскільки потребує внутрішнього аналізу валових доходів і ретельного ведення внутрішньої звітності.

Найбільш глибоким та точним є підхід розширеного вимірювання (AMA), який ґрунтується на внутрішніх моделях оцінки ризиків. У цьому випадку банки самостійно розробляють системи збору та аналізу даних про

операційні втрати, поєднуючи внутрішні й зовнішні джерела інформації. АМА дозволяє не лише розраховувати необхідний обсяг капіталу, а й розподіляти його між окремими напрямками діяльності для підвищення ефективності управління ризиками. Такий підхід потребує високого рівня організації, наявності компетентного підрозділу з управління ризиками, а також регулярних перевірок з боку внутрішнього та зовнішнього аудиту.

Попередньо розглянуті підходи Базеля II, зокрема підхід АМА, протягом певного часу вважалися найефективнішими інструментами вимірювання операційного ризику. Проте з накопиченням практичного досвіду виявилось, що навіть найскладніші моделі не завжди забезпечують точність і стабільність оцінок ризику. Особливо це стало очевидним після глобальної фінансової кризи 2007-2008 років, коли виявилися значні недоліки підходу АМА. Зокрема, він не враховував можливі зміни у структурі ризиків. Крім того, більшість банків фіксували збитки від операційного ризику лише через кілька років після самої події, що спотворювало результати оцінки. Додатковими проблемами стали відсутність уніфікованої системи звітності та значна варіативність підходів, через що результати різних банків були практично не порівнювальними.

Наведені недоліки створили передумови для переходу до нового, більш узгодженого та гнучкого підходу. У відповідь на виявлені проблеми Базельський комітет з банківського нагляду у 2016 році запропонував універсальний стандартизований підхід до вимірювання операційного ризику (SMA) згідно з Базелем III. Ця методика поєднує переваги попередніх моделей, забезпечуючи кращу чутливість до ризику, прозорість та можливість порівняння результатів між банками. Відповідно до нових вимог, усі три підходи, передбачені Базелем II, було поступово скасовано, а банки зобов'язано перейти на використання єдиного стандартизованого методу оцінки капіталу під операційний ризик.

На відміну від попередніх підходів, у Базелі III акцент зроблено на більш прозорий і логічний механізм визначення капіталу для покриття

операційного ризику – через поєднання двох ключових компонентів: бізнес-індикатора (BIC) та внутрішнього мультиплікатора збитків (ILM) (формула 1.1).

$$K_{SMA} = BIC \times ILM, \quad (1.1)$$

де BIC – компонент бізнес-індикатора;

ILM – внутрішній мультиплікатор збитків.

Компонент бізнес-індикатора (BIC) складається з бізнес-індикатора та граничного коефіцієнта (формула 1.2). Бізнес-індикатор (BI) відображає масштаби діяльності банку і включає три складові: процентні доходи, доходи від надання послуг та фінансовий результат (формула 1.3). Для визначення обсягу капіталу цей індикатор множиться на граничний коефіцієнт, який коливається від 12% до 18% залежно від величини BI. Таким чином, більші банки з вищими обсягами операцій повинні резервувати більше капіталу для покриття ризиків, що створює більш реалістичну та пропорційну систему оцінювання.

$$BIC = BI \times \alpha_j, \quad (1.2)$$

де BI – сума трьох складових, усереднених за 3 роки;

α_j – граничний коефіцієнт.

$$BI = ILDC + SC + FC, \quad (1.3)$$

де $ILDC$ – складова процентних доходів;

SC – складова послуг;

FC – фінансова складова.

Додаткову гнучкість і точність забезпечує внутрішній мультиплікатор збитків (ILM), який враховує історичні дані про операційні втрати за останнє десятиліття. Наявність цього показника дозволяє банкам із якісною базою даних точніше оцінювати власний рівень операційного ризику. Якщо ж така інформація відсутня, тоді для розрахунку капіталу застосовується лише компонент бізнес-індикатора, а значення ILM прирівнюється до 1.

Для українських банків цей аспект має особливе значення, адже у вітчизняних банківських установах поки що бракує достовірних і

структурованих даних про фактичні збитки від операційного ризику. У звітах банки зазвичай подають лише описову інформацію про природу ризиків, без конкретних кількісних показників. Відповідно, у таких умовах внутрішній мультиплікатор не може бути повноцінно використаний, що знижує точність оцінювання ризику [33].

Попри це, запровадження підходу SMA можна вважати значним кроком уперед, адже він забезпечує більшу узгодженість між різними банками, спрощує процес розрахунків і водночас підвищує чутливість системи до реального рівня ризику. Його універсальність робить можливим застосування як для великих міжнародних банків, так і для менших установ, створюючи єдині стандарти управління операційним ризиком на глобальному рівні.

Розвиток системи управління операційним ризиком у рамках Базеля III створив підґрунтя для пошуку більш ефективних практичних рішень. В українських банках останніми роками зростає усвідомлення важливості впровадження сучасних механізмів управління ризиками, особливо в умовах активної цифровізації процесів. Адже збільшення використання інформаційних технологій посилює вразливість до операційних ризиків (кіберзагроз, технічних збоїв та помилок персоналу).

Одним із найефективніших інструментів комплексного управління такими ризиками є фінансовий контролінг операційного ризику, який поєднує аналітичні, управлінські та контрольні функції. Проте на практиці вітчизняні банки ще не приділяють достатньої уваги цьому аспекту. Наразі відсутній єдиний методичний підхід до організації фінансового контролінгу, що призводить до неповноти механізмів в системі управління ризиками.

Запроваджений стандартизований підхід (SMA) дозволяє оцінювати операційний ризик на основі відкритої фінансової звітності, враховуючи показники доходів і витрат банку. Однак управління ризиками не повинно обмежуватися лише фінансовими розрахунками або аналізом збитків. Воно має бути інтегрованим у кожен бізнес-процес. Ефективний фінансовий

контролінг повинен забезпечувати контроль і моніторинг ризиків на всіх етапах діяльності банку, передбачати єдині стандарти внутрішньої звітності, чітку термінологію, узгоджені процедури оцінювання та обліку ризикових подій.

У сучасних умовах постійних змін і підвищеної невизначеності фінансового середовища доцільно створювати цілісну систему фінансового контролінгу операційного ризику, орієнтовану на випереджувальні дії. Вона має забезпечувати безперервність процесу управління ризику, формування внутрішньої ризик-культури серед працівників, вдосконалення програмного забезпечення для аналітики ризикових подій, а також гармонійне поєднання стратегії банку з його ризик-апетитом.

РОЗДІЛ 2

ОЦІНКА ПРАКТИЧНИХ АСПЕКТІВ ФІНАНСОВОГО КОНТРОЛІНГУ В СИСТЕМІ УПРАВЛІННЯ ОПЕРАЦІЙНИМИ РИЗИКАМИ АТ КБ «ПРИВАТБАНК»

2.1. Організаційна структура системи управління ризиками в АТ КБ «ПриватБанк»

Система управління ризиками є ключовим елементом ефективного функціонування будь-якої банківської установи, адже саме вона забезпечує своєчасне виявлення, оцінку та мінімізацію потенційних загроз, які можуть вплинути на стабільність, ліквідність і репутацію банку. Для АТ КБ «ПриватБанку», як найбільшого та системно важливого банку України, роль цієї системи має особливе значення, адже вона не лише забезпечує безперервність операцій, а й сприяє підтримці фінансової стійкості банку.

В умовах військового стану система управління ризиками в банках, зокрема у АТ КБ «ПриватБанку», зазнала суттєвих змін і розширення своїх функцій. Повномасштабна війна створила нові джерела ризиків, які потребують швидкої адаптації методів контролю та прогнозування. Водночас, значно зросла частка операційного ризику, який охоплює втрати через непередбачувані події, технічні збої, кібератаки, шахрайство та порушення безпеки даних.

У результаті військових дій українські банки зіткнулися з масштабними збитками, пов'язаними із втратою та пошкодженням майна, зниження ділової активності та необхідністю додаткових витрат на забезпечення безперервної роботи. Так, наприкінці 2022 року загальні збитки банківського сектору через втрату або пошкодження активів сягнули 757 млн. грн. [34]. Крім того, значні фінансові втрати банки зазнали через тимчасове припинення роботи відділень, скорочення клієнтського попиту та

підвищення операційних витрат на підтримку діяльності, а саме придбання генераторів, засобів зв'язку, додаткові витрати на персонал тощо.

Не менш важливим джерелом стали шахрайські дії та кібератаки, що у воєнний період набули масового характеру. Ці події мають кумулятивний ефект, тобто їхні наслідки накопичуються і впливають на фінансові результати банків у середньо- та довгостроковій перспективі. У зв'язку з цим суттєво зросла роль систем моніторингу операційних інцидентів, кіберзахисту та внутрішнього контролю.

Загалом, рівень операційних збитків банківської системи у 2022 році збільшився до 13 млрд. грн., що значно перевищує показники довоєнного періоду. Серед усіх банків найбільший рівень операційного ризику зафіксовано у АТ КБ «ПриватБанку», який оцінюється приблизно у 4 млрд. грн. [35]. Це пояснюється масштабами діяльності банку, високим рівнем автоматизації бізнес-процесів, великою клієнтською базою та активним використанням цифрових каналів обслуговування, що, своєю чергою, підвищує ймовірність кіберзагроз і технічних збоїв.

Підвищення рівня операційного ризику, додаткові витрати на підтримку безперервності роботи, кіберзахист та адаптацію бізнес-процесів до умов воєнного стану суттєво вплинули на структуру доходів і витрат банку. Для більш об'єктивного розуміння фінансового стану АТ КБ «ПриватБанк» варто розглянути динаміку його основних показників за останні п'ять років (табл. 2.1).

Таблиця 2.1

Динаміка доходів і витрат АТ КБ «ПриватБанку» станом на 01.01.2021
– 01.01.2025 роки

Показники	01.01.2021	01.01.2022	01.01.2023	01.01.2024	01.01.2025
Доходи	53 463	50 938	73 233	101 638	110 509
- процентні доходи	33 563	35 854	43 686	66 237	77 594
- комісійні доходи	27 649	35 057	32 945	41 589	46 602
- інші операційні доходи	1 066	1 370	2 759	3 075	2 609
- інші доходи	338	424	612	746	636
Витрати	29 166	15 870	38 561	28 872	29 505
- процентні витрати	11 961	6 537	3 768	6 616	10 706

Продовження таблиці 2.1

- комісійні витрати	8 888	11 840	12 505	17 150	18 834
- адміністративні та інші операційні витрати	18 597	21 569	22 234	24 373	26 689
- податок на прибуток	-6	17	4 474	35 001	40 863
Чистий прибуток (збиток)	24 302	35 050	30 198	37 765	40 141

Джерело: складено та розроблено автором за матеріалами [36; 37; 38; 39; 40].

Упродовж досліджуваного періоду простежується тенденція постійного збільшення доходів, зокрема процентних й комісійних, що забезпечується розширенням спектра банківських послуг, зростанням обсягів кредитування та розвитком цифрових каналів обслуговування клієнтів. Якщо станом на 01.01.2021 рік загальний обсяг доходів становив 53 463 млн. грн., то вже до 01.01.2025 року він зріс до 110 509 млн. грн., тобто більш ніж удвічі.

Процентні доходи демонструють найбільшу частку у структурі доходів, що підтверджує активну кредитну діяльність банку, тоді як комісійні доходи свідчать про успішний розвиток розрахунково-платіжної діяльності банку та активне використання цифрових каналів обслуговування клієнтів. Водночас спостерігається зростання інших операційних доходів, що відображає диверсифікацію джерел прибутку.

З боку витрат простежується схожа тенденція, а саме, поступове їх зростання у зв'язку з підвищенням вартості ресурсів, витратами на забезпечення операційної діяльності в умовах війни та зростанням витрат на кіберзахист і підтримку IT-інфраструктури. Найбільшу частку у структурі витрат займають адміністративні витрати, які зросли з 18 597 млн. грн. у 2021 році до 26 689 млн. грн. у 2025 році, що пов'язано з необхідністю адаптації до нових умов функціонування, відновлення відділень, забезпеченням енергетичної незалежності та збільшенням витрат на персонал.

Позитивною тенденцією є те, що темпи зростання доходів переважають темпи зростання витрат, що забезпечує банку збереження високої прибутковості. Так, чистий прибуток АТ КБ «ПриватБанку» зріс із 24 302

млн. грн. у 2021 році до 40 141 млн. грн. у 2025 році, що є свідченням успішної реалізації стратегії управління ризиками та ефективного використання ресурсів банку.

Отже, незважаючи на підвищення навантаження на систему управління ризиками, АТ КБ «ПриватБанк» не лише зберіг платоспроможність, а й забезпечив приріст чистого прибутку, що свідчить про ефективність його системи фінансового контролінгу операційного ризику. Виявлена тенденція підтверджує, що операційний ризик має прямий вплив на фінансові результати банку, формуючи обсяг витрат і рівень прибутковості. Зниження впливу цього ризику можливе завдяки вдосконаленню механізмів управління, посиленню моніторингу операційних процесів, створення бази даних подій ризику та розвитку внутрішнього контролю.

Водночас важливим чинником ефективності управління операційним ризиком є визначення його мінімального розміру, оскільки саме він дає змогу банку підтримувати баланс між рівнем ризику та досягненням стратегічних цілей. Оптимальне визначення мінімального операційного ризику дозволяє більш точно оцінювати потенційні втрати, встановлювати межі ризик-апетиту та забезпечувати достатній рівень капіталу для їх покриття. Важливо також враховувати вимоги НБУ, який регламентує порядок розрахунку мінімального розміру операційного ризику при визначенні нормативів достатності капіталу.

Згідно з чинними положеннями НБУ, поступове введення коефіцієнтів розрахунку мінімального розміру операційного ризику відбувалося поетапно:

- до 30 грудня 2021 року включно коефіцієнт становив 0;
- з 31 грудня 2021 року коефіцієнт становив 0,5;
- з 29 грудня 2023 року коефіцієнт становить 1 [41].

Таке поетапне підвищення показників свідчить про прагнення регулятора забезпечити більш точну оцінку ризикової позиції банків і підвищити рівень їхньої фінансової стійкості.

Таким чином, встановлені НБУ коефіцієнти поступово підвищили вимоги до розрахунку операційного ризику, що стимулює банки до вдосконалення систем управління ризиками та підвищення прозорості їхньої звітності. Для АТ КБ «ПриватБанк» це означає необхідність постійного моніторингу змін у нормативних показниках і своєчасного коригування внутрішньої політики управління ризиками.

З метою оцінки ефективності реалізації цих вимог та виявлення тенденцій у розвитку фінансового контролінгу операційного ризику доцільно проаналізувати динаміку мінімального розміру операційного ризику АТ КБ «ПриватБанк», що наведена у табл. 2.2.

Таблиця 2.2

Мінімальний розмір операційного ризику АТ КБ «ПриватБанк» станом на 01.01.2021-01.01.2025 роки, млн. грн.

Показники	01.01.2021	01.01.2022	01.01.2023	01.01.2024	01.01.2025
Мінімальний розмір операційного ризику, тис. грн.	0	41 254	41 254	82 509	135 700
Регулятивний капітал, тис. грн.	19 224	40 843	54 523	64 843	59 942
Покриття капіталом операційного ризику, %	X	99,00%	132,16%	78,59%	44,17%

Джерело: складено та розраховано автором за матеріалами [37; 38; 39; 40; 42].

Наведені у таблиці 2.2 дані свідчать про поступове зростання мінімального розміру операційного ризику АТ КБ «ПриватБанк» у станом на 01.01.2021-01.01.2025 роках. Таке збільшення пов'язане як із загальним посиленням регуляторних вимог НБУ, так і з розширенням масштабів діяльності банку, що зумовлює підвищення потенційних операційних втрат. Водночас спостерігається поступове зростання регулятивного капіталу, що свідчить про здатність банку ефективно покривати ризики власними ресурсами.

Для більш наочного відображення змін у покритті капіталом операційного ризику на рис. 2.1 подано динаміку даного показника у співвідношенні до регуляторного капіталу.

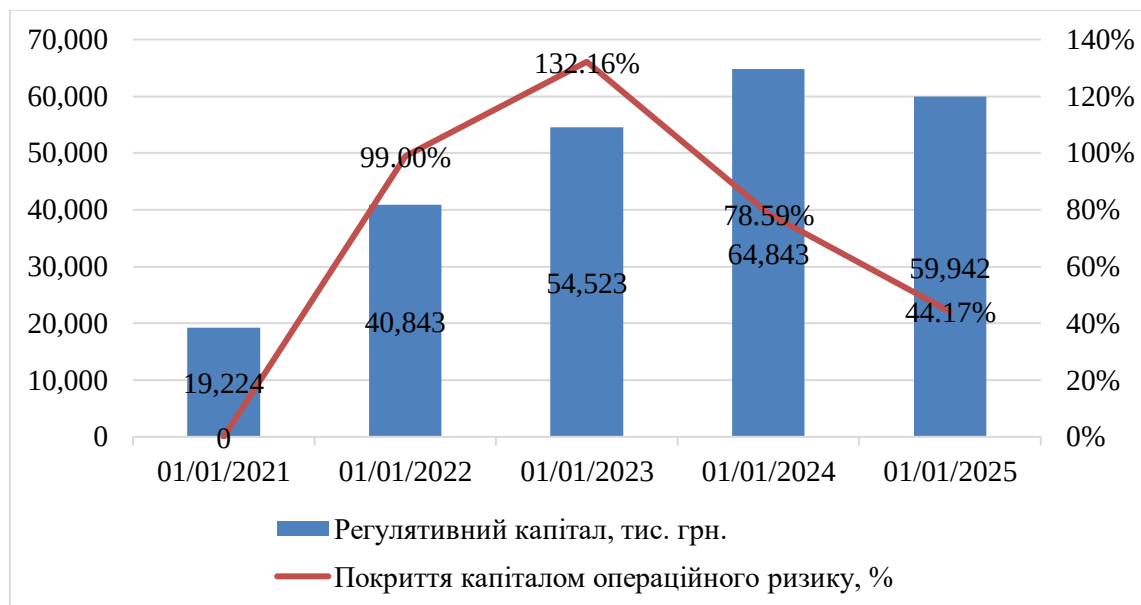


Рис. 2.1. Динаміка покриття капіталом операційного ризику станом на 01.01.2021–01.01.2025

Джерело: складено та розраховано автором за матеріалами [37; 38; 39; 40; 42].

Аналіз динаміки покриття капіталом операційного ризику АТ КБ «ПриватБанк» за зазначений період свідчить про суттєві коливання рівня співвідношення між регулятивним капіталом і мінімальним розміром операційного ризику. Станом на 01.01.2021 рік обсяг операційного ризику був відсутній через нульове значення коефіцієнта, встановленого НБУ, однак у наступні роки, після поступового впровадження нормативних змін, показник почав активно зростати.

Зокрема, на початку 2022 та 2023 роках рівень покриття операційного ризику капіталу приблизно дорівнював або перевищував 100%, що свідчить про високу здатність банку покривати потенційні операційні втрати за рахунок власних ресурсів. Проте станом на 01.01.2024 та 01.01.2025 спостерігається поступове зниження цього показника, що пояснюється як

зростанням мінімального розміру відповідно до регуляторних вимог, так і збільшенням операційних витрат, пов'язаних із воєнним станом, кібератаками та підвищенням вартості підтримання банківської інфраструктури.

Попри зниження показника покриття, АТ КБ «ПриватБанк» продовжує дотримуватися вимог НБУ щодо достатності капіталу, що свідчить про ефективну політику управління ризиками та гнучкість системи контролінгу. У цілому, динаміка демонструє, що банк здатний адаптувати свою ресурсну базу до змін зовнішнього середовища, забезпечуючи стабільне покриття операційного ризику на належному рівні. Це підтверджує його стратегічну стійкість, а також високий рівень організації процесів управління ризиками в умовах невизначеності.

Високий рівень стійкості та адаптивності банку до зовнішніх викликів пояснюється не лише ефективною фінансовою політикою, але й наявністю розгалуженої системи контролю ризиків, у межах якої кожен орган виконує визначену функцію в загальній структурі ризик-менеджменту (Додаток А). Для більш повного розуміння побудови та взаємодії елементів системи управління ризиками розглянемо організаційну структуру суб'єктів управління ризиками в АТ КБ «ПриватБанк» (табл. 2.3).

Таблиця 2.3

Організаційна структура суб'єктів управління ризиками в АТ КБ
«ПриватБанк»

Суб'єкт системи управління ризиками	Характеристика
1. Наглядова рада	Ключовий орган управління ризиками в банку, який несе повну відповідальність за формування, контроль і вдосконалення системи ризик-менеджменту. Затверджує політику управління ризиками, визначає рівень ризик-апетиту, контролює дотримання лімітів і своєчасне оновлення внутрішніх документів. Крім того, забезпечує незалежність функцій контролю, ухвалює стратегічні рішення щодо запобігання ризикам і конфліктам інтересів, а також здійснює загальний нагляд за ефективністю управління ризиками в усіх підрозділах банку.

Продовження таблиці 2.3

1.2. Комітет з питань ризиків Наглядової ради	Постійно діючий дорадчий орган, що підтримує Наглядову раду у формуванні та реалізації політики управління ризиками банку. Його основна роль полягає у моніторингу дотримання рівня ризик-апетиту, контролі ефективності системи ризик-менеджменту та наданні рекомендацій щодо вдосконалення процесів управління ризиками.
2. Правління Банку	Відповідає за практичну реалізацію стратегії управління ризиками, затвердженої Наглядовою радою, та за забезпечення ефективного функціонування системи внутрішнього контролю. Координує розробку внутрішньобанківських документів з управління ризиками, контролює їх виконання, а також забезпечує своєчасне інформування структурних підрозділів про зміни у політиці ризик-менеджменту.
2.1. Кредитний комітет	Наділений правом самостійно ухвалювати рішення щодо доцільності та умов проведення активних операцій.
2.2. Комітет з питань управління активами та пасивами	Функціонує з метою самостійно ухвалювати рішення щодо управління активами й пасивами банку.
2.3. Комітет з управління операційними ризиками та інформаційної безпеки	Забезпечує комплексне та ефективне управління операційними та юридичними ризиками, а також координацію впровадження системи внутрішнього контролю та інформаційної безпеки.
2.4. Комітет з питань управління непрацюючими активами	Діє з метою зниження рівня і обсягу проблемних активів банку завдяки оперативного прийняття управлінських рішень і підвищення ефективності процесів роботи з проблемною заборгованістю.
3. Напрямок Внутрішній аудит	Основними завданнями є виявлення, оцінка та моніторинг основних ризиків, перевірку адекватності систем контролю та розподілу повноважень, а також надання рекомендацій щодо підвищення ефективності управління ризиками.
4. Блок підрозділів з питань управління ризиками	Діяльність спрямована на підвищення кваліфікації персоналу, удосконалення методології оцінки ризиків і розробку кількісних моделей, що забезпечують ефективний контроль та своєчасне реагування на ризики.
5. Напрямок «Compliance»	Підрозділ забезпечує моніторинг відповідності діяльності банку вимогам законодавства, координує роботу всіх структурних підрозділів у сфері комплаєнсу, а також має право ініціювати зупинення рішень органів управління, якщо їх реалізація може призвести до порушення нормативних вимог чи етичних стандартів.
6. Відділ Офіс уповноваженого з антикорупційної діяльності	Підрозділ організовує розробку й упровадження Антикорупційної програми, проводить оцінку корупційних ризиків, розглядає повідомлення про можливі порушення та бере участь у службових розслідуваннях.

Джерела: складено та розроблено автором за матеріалами [43].

Представлена організаційна структура системи управління ризиками в АТ КБ «ПриватБанк» демонструє чіткий розподіл повноважень між суб'єктами ризик-менеджменту, що забезпечує ефективну координацію процесів виявлення, оцінки та мінімізації ризиків. Взаємодія наглядових, управлінських та контрольних органів сприяє формуванню культури управління ризиками, що дозволяє своєчасно реагувати на зміни зовнішнього середовища та зменшувати вплив операційних загроз.

Ключовою складовою системи є модель трьох ліній захисту, яка забезпечує багаторівневий підхід до контролю ризиків і підвищує надійність функціонування банківських процесів [43]:

- Перша лінія захисту представлена бізнес-підрозділами та службами підтримки, які є безпосередніми власниками ризиків. Вони відповідають за виявлення, оцінку та управління ризиками у своїй повсякденній діяльності, впроваджуючи заходи для їх запобігання та мінімізації.

- Друга лінія захисту включає Департамент управління операційними ризиками, який здійснює розробку політик, методик та внутрішніх процедур, координує діяльність першої лінії, а також контролює дотримання вимог регулятора та внутрішніх стандартів банку. Саме цей рівень формує систему моніторингу ризиків і забезпечує їх аналітичну оцінку.

- Третя лінія захисту реалізується підрозділом внутрішнього аудиту, який виконує незалежну перевірку ефективності системи управління ризиками та внутрішнього контролю. Внутрішній аудит забезпечує об'єктивну оцінку функціонування всієї системи захисту, виявляє слабкі місця та надає рекомендації щодо їх усунення.

Загалом система управління ризиками в АТ КБ «ПриватБанк» не обмежується лише розподілом відповідальності між органами управління чи контролю. Її ефективність значною мірою визначається дієвістю фінансового контролінгу операційного ризику. Саме цей елемент забезпечує постійний

моніторинг фінансових результатів та виявляє потенційні джерела ризику тощо.

До компетенції служби фінансового контролінгу операційного ризику входить проведення глибокого аналізу ключових фінансових показників банку, визначення зон підвищеного ризику та оцінка їх впливу. Її діяльність спрямована не лише на ідентифікацію операційних ризиків, але й на розробку рекомендацій щодо мінімізації негативних наслідків та запобігання майбутнім втратам.

Крім того, служба фінансового контролінгу виступає важливою ланкою у забезпеченні прозорості фінансових потоків і підвищенні довіри до банку з боку регуляторів, клієнтів і партнерів. Незалежність цієї служби гарантується тим, що вона підзвітна Головному ризик-менеджеру та Наглядовій раді, що дозволяє забезпечити об'єктивність оцінок і узгодженість управлінських рішень.

Таким чином, налагоджена система фінансового контролінгу операційного ризику є невід'ємною складовою загальної структури ризик-менеджменту АТ КБ «ПриватБанк», забезпечуючи ефективне поєднання стратегічного аналізу та практичних заходів з управління ризиками.

2.2. Практика застосування інструментів фінансового контролінгу для виявлення та моніторингу операційного ризику

Для АТ КБ «ПриватБанк», як у однієї із найбільших банківських установ країни, ефективне управління ризиком стало не просто частиною внутрішньої політики, а необхідною умовою стабільності та довіри клієнтів. Зростання рівня цифровізації, поява нових фінансових технологій і посилення кіберзагроз формують потребу у створенні комплексної системи контролю, здатної своєчасно виявляти ризики та мінімізувати їх наслідки.

Фінансовий контролінг у цій системі відіграє ключову роль, оскільки поєднує функції аналізу, управління та нагляду. Саме через механізми фінансового контролінгу банк має можливість оцінювати рівень ризику на основі реальних фінансових показників, виявляти потенційні відхилення від нормативних значень і своєчасно вживати коригувальних заходів. Такий підхід дозволяє забезпечити не лише стабільність операційної діяльності, а й підвищити ефективність управління ресурсами, що є особливо важливим в умовах війни.

У АТ КБ «ПриватБанк» фінансовий контролінг операційного ризику реалізується через цілу систему інструментів: бази даних внутрішніх й зовнішніх подій операційного ризику, ключові індикатори ризику (KRI), самооцінка операційного ризику, сценарний аналіз, аналіз результатів перевірок, здійснених підрозділом внутрішнього аудиту та зовнішнім аудитором, аналіз значних подій операційного ризику, аналіз та оцінка ризиків нових продуктів та значних змін в діяльності Банку, аналіз ризиків аутсорсингу [43].

Система управління операційним ризиком у банку передбачає створення ефективної бази даних, яка фіксує як внутрішні, так і зовнішні події операційного ризику. Формування та введення таких баз дозволяє банку накопичувати, систематизувати й аналізувати інформацію про інциденти, що можуть впливати на операційну діяльність установи та її репутацію. Збір інформації зовнішніх подій операційного ризику здійснюється підрозділами другого рівня захисту на основі відкритих джерел, спеціалізованих баз даних, а також у межах обміну даними між банками. Така інформація включає аналогічні складові, що й база внутрішніх подій, і дає змогу порівнювати тенденції та виявляти нові ризики, характерні для ринку в цілому. Водночас, внутрішня база операційного ризику є основою для управління ризиками банку. Вона повинна містити детальну інформацію про кожну ризикову подію: дату та час виникнення, виявлення, реєстрації та оцінку її реалізації (збитки, штрафи, компенсації, неодержані доходи) [44]. Також важливо

фіксувати перелік структурних підрозділів, у яких сталася подія, хто відповідає за її розслідування та усунення наслідків, а також опис причин її виникнення. Окрім цього, слід оцінювати потенційний вплив події на інші види ризиків – кредитний чи репутаційний тощо.

Систематичний аналіз як внутрішніх, так і зовнішніх подій дозволяє підрозділам ризик-менеджменту своєчасно виявляти слабкі місця в операційних процесах, визначати тенденції повторення інцидентів і формувати ефективні профілактичні заходи.

Разом із тим, ефективне управління операційним ризиком неможливе без використання ключових індикаторів ризику (KRI), які виконують роль раннього попередження про можливі порушення у конкретних бізнес-процесах. Ці показники розробляються для кожного напрямку діяльності банку, а саме від касових операцій до ІТ-інфраструктури. Їхня основна мета своєчасно сигналізувати про потенційне зростання ризику та допомогти запобігти його реалізації.

Розглянемо орієнтовні ключові індикатори операційних ризиків, які можуть використовувати АТ КБ «ПриватБанк».

Таблиця 2.4

Приклади ключових індикаторів операційних ризиків у банку

Вид ризику	Ключові індикатори операційних ризиків	Джерела формування даних
Ризик операцій та процесів	– кількість затримок виконання операцій; – кількість помилок у транзакціях; – кількість претензій клієнтів; – сума збитки через порушення процесу.	Звіти операційних відділів, журнали операцій (тразакцій), звіти внутрішнього аудиту.
Ризик персоналу	– рівень плинності кадрів; – кількість дисциплінарних порушень; – кількість випадків перевищення повноважень; – сума витрат на безпеку персоналу та охорону праці.	HR-звітність, результати перевірок служби комплаєнсу.
Ризик продуктів і послуг	– кількість скарг клієнтів; – кількість випадків некоректного стягнення комісій;; – кількість помилок при ціноутворенні; – сума повернення комісій.	Аналітичні звіти фронт-офісу; скарги клієнтів; CRM-система.

Продовження таблиці 2.4

Інформаційний ризик	– кількість збоїв ІТ-систем; – кількість випадків втрати даних; – кількість несанкціонованих змін; – сума збитків від порушень інформаційної безпеки.	Звіти департаменту інформаційної безпеки та ІТ-департаменту, системи моніторингу, журнали подій.
Кіберризик	– кількість спроб несанкціонованого доступу; – кількість фішингових атак; – кількість випадків використання шкідливих програм; – сума збитків від кібератаки.	Звіти ІТ-департаменту, системи кіберзахисту, інцидент-репорти.
Зовнішній ризик	– кількість зовнішніх подій, що завдали збитки; – кількість випадків пошкодження майна; – сума збитків внаслідок пошкодження майна	Звіти підрозділів безпеки, акти комісій із розслідуванням інцидентів, інвентаризаційні акти або технічні огляди.

Джерела: складено та розроблено автором за матеріалами [44].

Для кожного KRI встановлюється граничне значення, яке визначає рівень ризику, що вимагає підвищеної уваги. Якщо індикатор перевищує цей поріг, банк повинен негайно провести аналіз причин, оцінити масштаби можливих втрат і вжити коригувальних заходів. Наприклад, якщо показник «кількість випадків неправильно переданих даних» перевищує встановлений рівень (скажімо, 3 випадків), це сигналізує про підвищений операційний ризик у підрозділі інформаційної безпеки.

Таким чином, база даних подій операційного ризику та ключові індикатори ризику функціонують у взаємозв'язку. У той час перший інструмент забезпечує глибокий аналіз фактів реалізації ризику, тоді як другий запобігає його виникненню, фіксуючи відхилення ще до появи втрат. Поєднання цих інструментів формує інтегровану систему фінансового контролінгу, яка дозволяє АТ КБ «ПриватБанк» не лише оперативно реагувати на ризики, а й прогнозувати їх.

Використання додаткових інструментів управління операційним ризиком дозволяє сформувати всебічну та узгоджену систему контролю, яка охоплює всі етапи ідентифікації, оцінки та мінімізації ризиків. Зокрема,

самооцінка операційного ризику дозволяє керівникам бізнес-процесів самостійно оцінювати рівень ризику та ефективність установлених контрольних заходів. У процесі самооцінки визначаються основні операційні ризики, аналізується притаманний (ризик до впровадження заходів реагування) та залишковий (ризик після впровадження заходів реагування) рівні ризику, оцінюється дієвість існуючих заходів та визначаються напрями їх посилення. Такий підхід забезпечує замученість відповідальних осіб до управління ризиками та сприяє підвищенню ризик-культури в банку.

Сценарний аналіз використовується для оцінки малоймовірних, але потенційно значних подій. На основі експертних оцінок моделюються ситуації, які не завжди відображені у статистиці: масштабні кібератаки, тривалі збої IT-інфраструктури, випадки внутрішнього шахрайства або ризики, пов'язані з воєнними діями. Такий аналіз дозволяє заздалегідь визначати можливий обсяг збитків і потребу в капіталі для покриття цих ризиків [45].

Важливим джерелом інформації для контролінгу є результати перевірок внутрішнього та зовнішнього аудиту. Внутрішній аудит виявляє недоліки у процесах, оцінює якість впроваджених механізмів контролю, тоді як зовнішні аудитори підтверджують об'єктивність роботи системи ризик-менеджменту та її відповідність вимогам НБУ. Результати аналізу та аудиторських оцінок використовуються банком для оптимізації внутрішніх процесів, усунення виявлених недоліків та підвищення ефективності механізмів контролю.

Аналіз значних подій операційного ризику дозволяє оцінити причини та наслідки інцидентів, що призвели до значних фінансових втрат або операційних збоїв. Для кожної такої події здійснюється визначення першопричини, аналіз масштабів впливу, оцінка можливого впливу на інші види ризиків та формування рекомендацій щодо недопущення повторення подібних ситуацій у майбутньому. Аналіз таких інцидентів є обов'язковою вимогою національного регулятора.

Окремим напрямом контролінгу виступає оцінка ризиків нових продуктів і значних змін у діяльності банку. Перед впровадженням нового продукту здійснюється аналіз його технологічних, операційних та компласнс-ризиків. Враховуються особливості операційної обробки, облікових систем, організації взаємодії між підрозділами, також визначається необхідність додаткових контрольних заходів для мінімізації операційних ризиків. Такий підхід дозволяє зменшити вразливість ще до запуску продукту банку.

Аналіз ризиків аутсорсингу охоплює оцінку надійності та відповідності вимогам третіх сторін, які надають банку послуги та виконують окремі операційні функції. Банки повинні досліджувати фінансову стабільність контрагента, рівень його інформаційної безпеки, відповідність стандартам ISO 27001, можливість забезпечення безперервності діяльності та виконання умов договору.

У комплексі застосування цих інструментів забезпечує цілісний підхід до управління операційним ризиком, у якому поєднується аналіз подій ризику, прогнозування майбутніх загроз, контроль та оцінка ефективності заходів реагування на ризик. Це, в свою чергу, забезпечує відповідність сучасним вимогам національного регулятора, рекомендаціям Базельського комітету та власним цілям щодо мінімізації операційних втрат.

Застосування якісних інструментів управління операційним ризиком створює основу для глибшої кількісної оцінки, яка дозволяє визначити ступінь впливу окремих чинників на формування ризикового профілю банку. На цьому етапі особливої важливості набувають кількісні статистичні методи, які забезпечують можливість точної оцінки та прогнозування операційних втрат.

На даний етап найбільш поширеним інструментом є стандартизований підхід SMA, передбачений Базелем III. Він поєднує у собі показники бізнес-індикатора (BI) та історичні дані щодо операційних збитків, забезпечуючи об'єктивну оцінку капіталу, необхідного для покриття операційного ризику.

Використання SMA дозволяє банку точніше визначати, які процеси є найбільш ризикованими та порівнювати власний рівень ризику з міжнародними стандартами.

Враховуючи стандартизований підхід до розрахунку капіталу для покриття операційного ризику, доцільно використати факторний аналіз, який дозволяє оцінити, як кожен окремий компонент бізнес-індикатора (BI) впливає на його загальне значення, а відповідно, і на обсяг капіталу, що має бути сформований для покриття операційних ризиків.

У даному випадку застосовується адитивна факторна модель, оскільки підсумковий показник BI формується як сума його складових: процентних доходів (ILDC), послуг (SC) та фінансової (FC).

$$BI = ILDC + SC + FC \quad (2.1)$$

Для оцінювання впливу кожного фактора у формування бізнес-індикатора використаємо метод елімінування, а саме ланцюгових підстановок, який передбачає послідовне визначення впливу окремого фактору шляхом виключення інших змінних. Суть підходу полягає в тому, що всі фактори фіксуються на одному рівні, за винятком того, який аналізується, адже саме його зміна дозволяє визначити частку впливу на кінцевий результат. За базові значення складових BI візьмемо станом на 01.01.2021 рік, а фактичні – 01.01.2025 рік.

Таблиця 2.5

Визначення впливу факторних складових на бізнес індикатор АТ КБ
«ПриватБанк» методом ланцюгових підстановок станом на 01.01.2021 –
01.01.2025 роки

Підстановки	Складова процентних доходів (ILDS)	Складова послуг (SC)	Фінансова складова (FC)
Всі фактори на базовому рівні	21 939	19 827	11 696
ILDC на фактичному рівні, SC та FC на базовому рівні	67 524	19 827	11 696
ILDC та SC на фактичному рівні, FC на базовому рівні	67 524	30 377	11 696
Всі фактори на базовому рівні	67 524	30 377	12 608

Зміна ВІ внаслідок зміни фактору	45 585	10 550	912
Перевірка	ВІ фактичний - ВІ базисний	Сума впливу факторів ILDS, SC, FC	
	57 047	57 047	

Джерело: складено та розраховано автором за матеріалами [36; 37; 38; 39; 40; 42].

З наведених результатів видно, що кожна зі складових бізнес-індикатора АТ КБ «ПриватБанк» має різний рівень впливу на його підсумкове значення. Найбільший внесок у формування ВІ забезпечує складова процентних доходів, тоді як вплив складової послуг та фінансової складової є порівняно меншим. Така динаміка пояснюється специфікою бізнес-моделі банку, орієнтованої на високий рівень кредитних операцій та обслуговування роздрібного сегменту. Аналіз методом ланцюгових підстановок дозволив кількісно оцінити, наскільки зміна кожного окремого фактору зумовила зростання або зниження бізнес-індикатора, а отже, необхідного капіталу для покриття операційного ризику в межах стандартизованого підходу SMA. Розглянемо більш детально кожний компонент бізнес-індикатора (рис. 2.2).

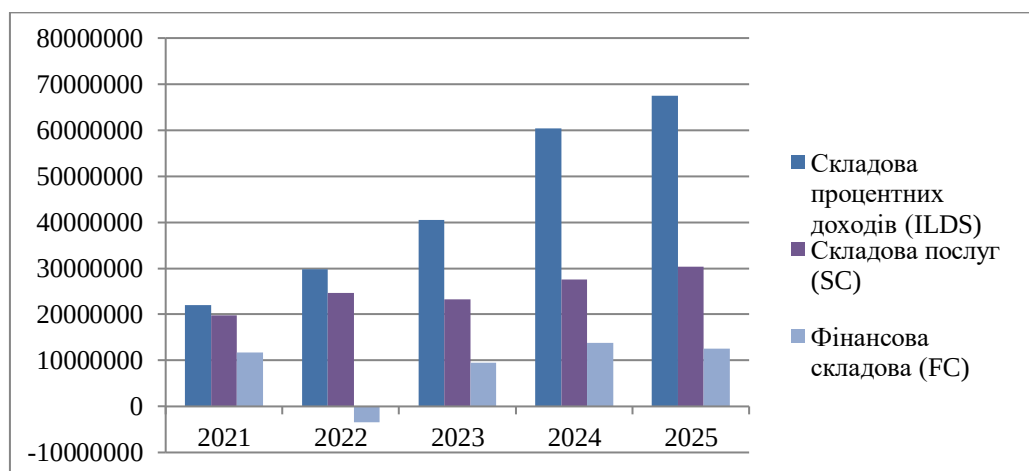


Рис. 2.2. Динаміка компонент бізнес-індикатора АТ КБ «ПриватБанку» станом на 01.01.2021 – 01.01.2025 роки

Джерело: складено та розраховано автором за матеріалами [37; 38; 39; 40; 42].

Отримані дані свідчать, що основним фактором, з огляду впливу на ВІ, є складова процентних доходів, адже саме їх стрімке зростання після 2022 року забезпечило основну частину приросту показника. Водночас зміна складової послуг протягом досліджуваного періоду також демонструє поступове зростання, однак її вплив є суттєво меншим порівняно з процентними доходами. Це свідчить про нарощення обсягів операційної діяльності банку, розвиток сервісів та розширення клієнтської бази. Фінансова складова характеризується рівномірністю та відсутністю значних стрибків, що відображає дотримання стратегії помірному ризику банку.

Загалом, порівняння числових даних із графічним матеріалом підтверджує, що структура ВІ формується нерівномірно, найбільша частка його приросту зумовлена саме процентними доходами, тоді як інші складові мають менш вагомий вплив. Така структура формує відповідний профіль операційного ризику банку, оскільки коливання у найвагомій складовій ВІ прямо визначають обсяг капіталу, який має бути сформований відповідно до стандартизованого підходу SMA. Це підкреслює необхідність постійного удосконалення системи контролінгу, зокрема механізмів попередження та мінімізації операційних втрат.

Тому важливою складовою системи управління операційним ризиком є правильний вибір стратегії реагування на потенційні інциденти. АТ КБ «ПриватБанк» застосовує чотири основні методи управління ризиком, а саме прийняття, передачу, пом'якшення та уникнення ризику, що відповідає рекомендація Базельського комітету та вимогам Положення НБУ №64.

Метод прийняття ризику використовується у випадках, коли можливі втрати є незначними, а ймовірність їх настання низькою. За таких умов банк свідомо допускає існування ризику, не змінюючи процеси чи структуру операційної діяльності. Цей підхід є раціональним у ситуаціях, коли витрати на запобігання ризику перевищують очікувані збитки.

Метод передачі ризику передбачає делегування частини або всього ризику зовнішнім сторонам. Найпоширенішими інструментами є

страхування операційних подій та передача окремих функцій на аутсорсинг. Таким метод застосовується у випадках, коли ризик може призвести до значних фінансових втрат, але ймовірність настання цього дуже низька, або ризик перебуває поза повним контролем банку. У межах операційної діяльності АТ КБ «ПриватБанк» активно використовує аутсорсинг ІТ-послуг, сервісів інкасації, мережевої інфраструктури, що дозволяє мінімізувати вплив технічних ризиків.

Метод пом'якшення ризику орієнтований на зменшення ймовірності та розміру втрат шляхом удосконалення внутрішніх процесів і провадження додаткових контрольних заходів. До таких заходів належить автоматизація операцій, підсилення контрольних точок у процесах, підвищення кваліфікації персоналу, запровадження резервних та альтернативних процедур, які забезпечують безперервність операцій у разі збоїв основних процесів. Цей метод є найбільш використовуваним, оскільки дозволяє банку системно впливати на якість бізнес-процесів та підвищувати їх стійкість.

Метод уникнення ризику застосовується тоді, коли подія може мати критичні наслідки та високу ймовірність реалізації. У таких випадках банк відмовляється від певних видів операцій, послуг або рішень, що можуть спричинити неприйнятно високі втрати. Це може стосуватися запуску продуктів з надмірною операційною складністю, співпраці з ненадійними контрагентами чи здійснення операцій у несприятливому регулятивному середовищі.

Застосування цих методів у комплексі підсилює загальну систему контролінгу операційного ризику та забезпечує гнучкість управлінських рішень. Їх ефективність зростає у поєднанні з такими інструментами, як базаю подій, KRI, самооцінкою ризику та сценарним аналізом, що запобіжні заходи, оптимізувати структуру капіталу та забезпечувати стабільність функціонування банку навіть у ризикованому середовищі.

2.3. Оцінка ефективності діючих механізмів управління операційним ризиком у АТ КБ «ПриватБанк»

Стійкість та надійність АТ КБ «ПриватБанк» значною мірою залежить від того, наскільки ефективно банк управляє операційними ризиками в умовах динамічного та нестабільного ринкового середовища. Вчасне виявлення подій ризику, якісна система контролю та достатній рівень капіталу дозволяють мінімізувати можливі втрати й забезпечувати безперервність роботи установи. Тому аналіз дієвості впроваджених механізмів ризик-менеджменту є важливим елементом оцінки фінансового контролінгу банку.

Ефективність системи управління операційним ризиком у банку доцільно оцінювати з двох позицій, а саме відповідності регуляторним вимогам та її реального впливу на рівень капіталу й стійкість установи в умовах воєнного часу. Для АТ КБ «ПриватБанк», як найбільшого банку за активами, операційний ризик є системно важливим, оскільки банк обслуговує значну частину населення та бізнесу, має розгалужену мережу відділень і одним з лідерів цифрового банкінгу.

У такому випадку важливим є розуміння того, в якій нормативно-правовій площині функціонує система ризик-менеджменту банку. Національний банк України встановлює єдині правила організації управління ризиками постановою № 64 «Про затвердження Положення про організацію системи управління ризиками в банках України та банківських групах», яка визначає вимоги до трирівневої моделі захисту та ролей ключових органів управління. Додатково порядок розрахунку операційного ризику і його вплив на достатність капіталу врегульовано постановою № 156 «Про затвердження Положення про порядок визначення банками України мінімального розміру операційного ризику», внаслідок поетапного переходу до національної адаптації стандартизованого підходу SMA. У межах цього переходу НБУ

установив поступове збільшення коефіцієнта, що застосовується під час визначення мінімального розміру операційного ризику: до 30.12.2021 він дорівнював 0, із 31.12.2021 був підвищений до 0.5, а з 29.12.23 становить 1.

У межах цих вимог АТ КБ «ПриватБанк» забезпечує функціонування однієї з найрозвиненіших систем управління операційним ризиком в українському банківському секторі. У річних звітах банк зазначає, що застосовує комплексну модель, яка включає базу внутрішніх і зовнішніх подій, ключові індикатори ризику KRI, механізм регулярної самооцінки процесів, сценарний аналіз, оцінку ризиків нових продуктів, а також аналіз значних подій та висновків внутрішнього та зовнішнього аудиту. Важливу роль відіграє й чітка організаційна структура, а саме модель трьох ліній захисту, що забезпечує узгоджену взаємодію Наглядової ради, Комітету з питань ризиків, Правління, профільних комітетів, комплаєнсу та внутрішнього аудиту.

Особливої ваги ця система набула після початку повномасштабної війни, коли банк зіткнувся зі зростанням операційних загроз. У відповідь було посилено захист ІТ-інфраструктури, переведено критичні системи на хмарні платформи, забезпечено безперервність роботи відділень та контакт-центрів, а також розширено практику стрес-тестування [46]. Завдяки цьому банк зміг підтримувати стабільну роботу цифрових сервісів і мінімізувати ризики втрати даних та коштів клієнтів. Такі дії підтверджують високу і дієвість системи управління ризиками навіть у надзвичайно складних умовах воєнного часу.

Для оцінки ефективності управління операційним особливе значення є порівняння капіталу для покриття операційного ризику за різними методиками, а саме міжнародними BIA та TSA й національним підходом НБУ, що є адаптацією стандартизованого підходу SMA. Загалом, це дозволяє не лише визначити відповідність внутрішніх процесів вимогам регулятора, але й оцінити, наскільки коректно банк ідентифікує та покриває ризики у своїй діяльності.

Таблиця 2.6

Мінімальний розмір резерву для покриття операційного ризику АТ КБ
«ПриватБанк» за міжнародними та національним підходами

Підходи	01.01.2021	01.01.2022	01.01.2023	01.01.2024	01.01.2025
BIA	4893	5771	6796	8967	11136
TSA	5872	6925	8155	10760	13363
НБУ	0	3820	10985	15246	16576

Джерело: складено та розраховано автором за матеріалами [36; 37; 38; 39; 40; 42; 47].

Методики BIA і TSA відображають міжнародний підхід, що базується на зв'язку між рівнем операційного ризику та величиною доходів банку. Проте їх чутливість до змін у структурі доходів різна. Якщо BIA відображає загальну динаміку доходів, то TSA є більш деталізованим, оскільки враховує особливості операцій за бізнес-процесами. Саме тому показники для покриття операційного ризику за TSA стабільно перевищують результати BIA.

Національний підхід НБУ, що ґрунтується на SMA, демонструє іншу динаміку. Його результати суттєво зростають у 2023-2025 роках унаслідок підвищення коефіцієнта врахування операційного ризику в капіталі до рівня 1. Це означає, що банк повинен забезпечувати повне покриття операційних ризиків регулятивним капіталом, без застосування знижувальних коефіцієнтів. Таким чином національна методика стає більш жорсткою порівняно з міжнародними підходами, особливо з BIA, який найменш чутливий до змін.

Порівняння цих підходів у динаміці за 2020-2025 роки дозволяє чітко визначити, наскільки ефективно АТ КБ «ПриватБанк» реагує на зміни нормативної бази, а також оцінити ступінь навантаження на капітал. Зростання різниці між підходом НБУ та міжнародними методами після впровадження коефіцієнта 1 свідчить про підвищення вимог до фінансової стійкості банків. Фактично банк має акумулювати більше капіталу під

операційні ризики, що підкреслює важливість якісної роботи механізмів ризик-менеджменту.

Доречно розглянути порівняння впливу різних підходів на капітал за останні роки у таблиці 2.7.

Таблиця 2.7

Порівняння навантаження на капітал мінімальних розмірів резервів для покриття операційного ризику АТ КБ «ПриватБанк» за міжнародними та національним підходами

Роки	Різниця TSA та BIA та	Різниця НБУ та BIA	Різниця НБУ та TSA	Навантаження на капітал		
				TSA-BIA	НБУ- BIA	НБУ- TSA
01.01.2021	979	-4893	-5872	2,77	-13,88	-16,65
01.01.2022	1154	-1950	-3104	2,82	-4,77	-7,60
01.01.2023	1359	4189	2830	2,49	7,68	5,19
01.01.2024	1793	6279	4485	3,29	11,52	8,22
01.01.2025	2227	5440	3213	3,43	8,39	4,95

Джерело: складено та розраховано автором за матеріалами [36; 37; 38; 39; 40; 42; 47].

Отримані результати демонструють суттєві відмінності у навантаженні на капітал залежно від застосованого підходу до розрахунку капіталу необхідного для покриття операційного ризику. Зокрема, вплив показників за TSA на капітал стабільно перевищують результати BIA на 2,5-3,4%, що підтверджує значно вищу ризик-чутливість стандартизованого підходу. TSA враховує специфіку діяльності банку за окремими бізнес-лініями, тому точніше відображає реальну структуру ризикових операцій АТ КБ «ПриватБанк», який характеризується широкою клієнтською базою, високою часткою цифрових транзакцій та складними операційними процесами.

Найпомітніші зміни відбуваються після 2023 року, коли відповідно до вимог НБУ коефіцієнт для визначення мінімального розміру операційного ризику було підвищено до 1. Як наслідок, вплив показників на капітал за національним підходом випереджають результати BIA на 7,7-11,5%, а TSA на 5,2-8,2%. Це свідчить про те, що український регулятор установив

жорсткіші вимоги до покриття операційного ризику, ніж класичні міжнародні методики. Розрахунок за національним підходом стає не просто інструментом контролю, а механізмом забезпечення стійкості банківської системи умовах підвищеної невизначеності.

Для АТ КБ «Приватбанк» це означає необхідність формувати більший обсяг регулятивного капіталу для покриття операційного ризику та підтримувати постійний моніторинг процесів ризик-менеджменту. Підвищене навантаження на капітал вимагає від банку максимальної точності в оцінці ризиків, підвищення ефективності контролю, вдосконалення внутрішніх процедур, а також розвитку системи раннього виявлення подій та індикаторів ризику. Тому впровадження жорсткіших нормативних вимог стимулює банк до посилення культури ризик-менеджменту та впровадження інноваційних управлінських інструментів.

Це підтверджується також змістом річної звітності за 2022 та 2023 роки, де АТ КБ «ПриватБанк» докладно описує розгалужену систему інструментів управління операційним ризиком. Так, наприклад, самооцінка операційного ризику проводиться на рівні бізнес-підрозділів, які визначають ключові ризики у своїх процесах, оцінюють імовірність та масштаб можливих втрат. За результатами самооцінки формуються карти ризиків і плани дій зі зниження ризику, що безпосередньо інтегруються в систему управлінської звітності банку. Використання цього інструменту відповідає рекомендаціям Базельського комітету щодо залучення «першої лінії захисту» до процесів ризик-менеджменту [48].

Під час війни використання банком сценарного аналізу операційного ризику має особливе значення, оскільки дає змогу завчасно оцінити можливі фінансові втрати та потребу в капіталі для покриття операційного ризику внаслідок реалізації подій операційного ризику, наприклад, масштабних кібератак, фізичного зниження інфраструктури та тривалих відключень енергопостачання. Окремі елементи таких сценаріїв враховуються й у внутрішніх стрес-тестах банку.

Внутрішній аудит та зовнішні аудитори забезпечують незалежну оцінку ефективності системи внутрішнього контролю й управління операційним ризиком. У протязі 2022-2024 роках банк не отримував від зовнішніх аудиторів зауважень, що свідчили б про критичні недоліки в системі управління ризиками. Водночас НБУ застосовує до банку регулярні наглядові заходи, результати яких публічно не розкриваються, але відсутність жорстких санкцій свідчить про відповідність системи управління ризиками вимогам регулятора.

Важливим елементом є аналіз значних подій операційного ризику та інцидентів інформаційної безпеки. АТ КБ «ПриватБанк» в звіті наголошує, що в перший рік повномасштабного вторгнення основними джерелами операційних втрат були знищення фізичних активів і перебої в роботі електроенергетичної інфраструктури. Частина цих втрат компенсувалася за рахунок страхування та резервів, а інша частина за рахунок переорієнтації процесів у дистанційні канали [49].

З метою комплексної оцінки ефективності чинних механізмів управління операційним ризиком доцільно узагальнити їх сильні та слабкі сторони, а також можливості та загрози у таблиці 2.8.

Таблиця 2.8

SWOT-аналіз фінансового контролінгу системи управління операційним ризиком АТ КБ «ПриватБанку»

Сильні сторони	Слабкі сторони
– розвинена система трьох ліній захисту, чіткий розподіл повноважень і функцій у системі управління ризиком; – комплексний набір інструментів (база внутрішніх і зовнішніх подій, KRI, самооцінка, сценарний аналіз, аналіз аутсорсингу тощо); – суттєвий запас регулятивного капіталу для покриття операційного ризику банку; – активне застосування сучасних цифрових технологій, що підвищує якість моніторингу, швидкість реагування на інциденти та рівень автоматизації процесу контролю;	– залежність від складних цифрових систем, що підвищує чутливість до технічних збоїв та кібератак; – частина процесів управління операційним ризиком потребує подальшої автоматизації, зокрема інтеграції KRI у єдину цифрову платформу та підвищення точності прогнозних моделей; – підвищення навантаження на підрозділи унаслідок зростання кількості реалізації подій операційного ризику під час війни; – складність контролю за контрагентами аутсорсингу та їх відповідності стандартам інформаційної безпеки;

Продовження таблиці 2.8

– розвинена ІТ-інфраструктура та кіберзахист, посилені після 2022 року через перенесення даних у хмарне середовище, застосування резервних майданчиків; – наявність висококваліфікованого персоналу, що забезпечують контроль за всіма процесами.	– додаткові витрати на підвищення кваліфікації персоналу; – складність ідентифікації подій операційного ризику з низькою частотою їх реалізації та збитків.
Можливості	Загрози
– розширення співпраці з банками задля обміну даними про зовнішні події операційного ризику; – розвиток системи безперервності бізнесу і кіберстійкості, включаючи масштабування хмарних рішень, резервних каналів зв'язку; – підвищення точності оцінювання операційних ризиків шляхом інтеграції нових інструментів контролю ризиків; – удосконалення процесів управління аутсорсингом.	– некоректне використання або приховування співробітниками інформації про події операційного ризику; – порушення конфіденційності даних через залучення контрагентів до розробки й підтримки програмного забезпечення; – зловживання правами до внутрішніх систем може призвести до несанкціонованих мін або витоку даних.

Джерело: розроблено автором.

Отже, система управління операційним ризиком АТ КБ «ПриватБанк» показує, що банк володіє розвиненою та комплексною системою контролю, яка ґрунтується на використанні сучасних технологій та чіткій моделі рьох ліній. Сильні сторони забезпечують здатність ефективно реагувати на операційні загрози, тоді як можливості відкривають перспективи для подальшої цифровізації процесів та залучення нових інструментів управління операційним ризиком. Водночас слабкі сторони та загрози свідчать про необхідність постійного оновлення ІТ-інфраструктури, посилення контролю за доступами до внутрішніх систем та зменшення залежності від контрагентів. Загалом результати аналізу підтверджують, що система управління операційним ризиком АТ КБ «ПриватБанк» є ефективною та здатною функціонувати в умовах підвищеної невизначеності, однак потребує безперервного вдосконалення.

РОЗДІЛ 3

ШЛЯХИ ВДОСКОНАЛЕННЯ ФІНАНСОВОГО КОНТРОЛІНГУ В СИСТЕМІ УПРАВЛІННЯ ОПЕРАЦІЙНИМ РИЗИКОМ АТ КБ «ПРИВАТБАНК»

3.1. Виявлення проблемних аспектів фінансового контролінгу в системі управління операційним ризиком АТ КБ «ПриватБанк»

АТ КБ «ПриватБанк» реалізовує власну стратегію управління ризиками, сформовану відповідно до вимог Постанови Правління НБУ № 64, яка передбачає підтримання ризиків на прийнятному рівні та забезпечення оптимального співвідношення між сукупним ризиком та фінансовими показниками банку шляхом його підтримання на заздалегідь визначеній прийнятній межі. Досягнення цієї мети забезпечується через формування ефективної системи управління ризиками, ключові функції якої включають своєчасну ідентифікацію, точне вимірювання та оперативне інформування про всі суттєві ризики.

Разом з тим, масштаб і особливості діяльності АТ КБ «ПриватБанк» створюють низку додаткових викликів для фінансового контролінгу операційних ризиків. По-перше, банк є найбільшим постачальником платіжних послуг, що створює істотне операційне та технологічне навантаження на ІТ-системи та внутрішні процеси. По-друге, банк обтяжений специфічною категорією проблемних активів, пов'язаних із попередніми акціонерами, що суттєво обтяжує систему управління операційним ризиком.

Одним із вагомих викликів для фінансового контролінгу в АТ КБ «ПриватБанк» залишається необхідність суворого дотримання вимог фінансового моніторингу. Згідно з Положенням НБУ № 65 «Про здійснення банками фінансового моніторингу», банки зобов'язані застосовувати ризик-орієнтований підхід до обслуговування клієнтів, враховуючи комплекс

критеріїв ризикованості, визначених регулятором. Найчастіше Національний банк України у своїх звітах наголошує, що основні порушення у банківському секторі пов'язані саме з недоліками систем протидії відмиванню доходів та фінансування тероризму, зокрема з неправильною оцінкою ризикованості клієнтів або недостатнім контролем їх операцій.

Попри те, що у 2024 році АТ КБ «ПриватБанк» потрапив до переліку банків, охоплених плановими виїзними перевірками НБУ у сфері фінансового моніторингу, результати перевірки не засвідчили наявності критичних порушень або системних недоліків [49; 50]. Однак, це не означає відсутність проблем у цьому напрямку, адже в умовах посилення регуляторних вимог банк змушений працювати із значною кількістю оновлених критеріїв ризику, що постійно доповнюються відповідно до міжнародних стандартів та змін у законодавстві України. Механізми фінансового контролінгу мають оперативно оновлюватися, адаптуючись до нових індикаторів підозрілих операцій, що вимагає значних ресурсів, як технологічних, так і кадрових.

Крім того, необхідність безперервного вдосконалення автоматизованих систем моніторингу створює постійне навантаження на ІТ-інфраструктуру банку. АТ КБ «ПриватБанк» оперує однією з найбільших клієнтських баз серед інших банків, що робить процес скринінгу та верифікації клієнтів особливо складним. Навіть незначні помилки у визначенні статусу клієнта або затримки у виявленні підозрілих транзакцій можуть спричинити реалізацію операційного ризику.

Згідно з аналітичними звітами Європейського банківського управління (ЕВА), у 2024 році найбільш критичними серед операційних ризиків для фінансових установ ЄС залишаються кіберризики та захист даних. Вони стабільно очолюють рейтинг загроз протягом кількох останніх років, випереджаючи ризики помилок персоналу, юридичні ризики та різноманітні форми внутрішнього та зовнішнього шахрайства. Понад 47% європейських банків повідомили, що у другій половині 2023 року зазнали принаймні однієї

кібератаки, що демонструє системний характер цієї проблеми та її зростаючу масштабність [52].

Для АТ КБ «ПриватБанк» ці тенденції мають особливе значення, адже банк виступає технологічним лідером серед українських банків, активно розширює цифрові сервіси тощо. Проте інтенсивне розширення цифрових каналів неминуче супроводжується збільшенням операційного навантаження на ІТ-інфраструктуру та зростанням вразливості до кіберзагроз. В умовах війни ці ризики посилюються, адже щороку фіксується рекордна кількість кібератак на фінансові установи, що змушує банк працювати у режимі підвищеної оборони. Надмірна залежність від безперебійної роботи платіжних систем, мобільного банкінгу та систем дистанційної автентифікації робить будь-який технічний збій або кібератаку потенційно критичною подією операційного ризику.

В умовах зростання кіберзагроз та ускладнення операційного середовища особливої ваги набуває якість фінансового контролінгу, який має забезпечувати не лише фіксацію та аналіз ризикових подій, а й їх попередження через інструменти управління операційним ризиком. Проте в українській банківській практиці, у тому числі АТ КБ «ПриватБанк» простежуються недоліки у взаємодії окремих суб'єктів системи контролінгу, що ускладнює формування цілісної та узгодженої системи управління операційним ризиком. Це пов'язано з тим, що різні структурні підрозділи можуть використовувати неоднакові підходи до ідентифікації та оцінки ризикових подій, застосовувати різні класифікаційні ознаки, методики розрахунку збитків та формати звітності. Така розбіжність призводить до неповної інформації, й у результаті знижується точність прогнозування потенційних загроз, а процес ухвалення управлінських рішень стає повільним та більш затратним. Дана проблема стає ще більш актуальною з огляду на впровадження нових вимог Базель III, які зобов'язують банки розраховувати капітал під операційний ризик за стандартизованим підходом, що потребує угоджених і достовірних даних.

Також повномасштабне вторгнення суттєво загостило проблеми фінансового контролінгу операційного ризику в АТ КБ «ПриватБанк». Руйнування інфраструктури, перебої в роботі відділень та нестабільність безпосередньо впливають на якість збору даних, повноту реєстрації подій операційного ризику та швидкість їх аналізу. Це призвело до неповноти даних, затримок у реєстрації подій та зниження точності оцінювання потенційних втрат. Посилення навантаження на ІТ-інфраструктуру додатково підвищили ризик технічних збоїв, що ускладнює підтримання безперервності процесів контролю. У такій ситуації різні методики оцінки ризику між підрозділами, недостатня інтегрованість даних в єдину систему стали ще більш відчутними. Особливо критично з огляду на вимоги Базель III та національного регулятора, які потребують точних даних для розрахунку капіталу під операційний ризик.

Міжнародна практика управління операційним ризиком демонструє значно вищий рівень узгодженості процесів контролю, ніж це спостерігається у вітчизняних банках. У країнах ЄС, США та Великої Британії управління операційним ризиком базується на стандартах Базельського комітету, де використовують єдину методику визначення капіталу під операційний ризик SMA. Для системно важливих європейських банків використання SMA є обов'язковим, його запровадження супроводжується формуванням стандартизованих класифікацій ризикових подій і єдиних методів збору даних.

У 2024 році Європейська банківська асоціація (ЕВА) опублікувала розширений пакет технічних стандартів, де детально визначено правила побудови баз даних операційних подій, порядок розрахунку бізнес-індикатора, методи коригування показників у разі реструктуризації чи злиттів банківських установ, а також процедури наглядової оцінки операційних ризиків [53]. Паралельно Європейський центральний банк (ЕЦБ) застосовує комплексну SPER-методологію, що включає автоматизовані моделі ризик-скорингу, аналіз ключових показників ризику (KRI) та

ефективності (KPI), а також індивідуальні експертні оцінки системи управління ризиків кожного банку [54].

Тож ефективний фінансовий контролінг операційного ризику неможливий без високого рівня стандартизації, автоматизації та інтеграції інформаційних систем. Саме ці елементи є ключовими відмінностями між міжнародною банківською системою та вітчизняною. Хоча Національний банк України впроваджує вимоги до Базель III та поступово впроваджує підхід SMA в банківську діяльність, але вітчизняні банки, у тому числі АТ КБ «ПриватБанк», все ще стикаються з неузгодженістю внутрішніх інформаційних систем, неоднорідністю методик оцінювання ризиків та недостатньою автоматизацією процесів контролінгу.

У зв'язку з цим доцільним є порівняння ключових характеристик системи управління ризиком АТ КБ «ПриватБанку» з міжнародними стандартами, що дозволяє чітко окреслити проблемні аспекти фінансового контролінгу.

Таблиця 3.1

Порівняння систем управління операційним ризиком АТ КБ
«ПриватБанк» та міжнародні стандарти країн ЄС та США

Критерій	АТ КБ «ПриватБанк»	Міжнародні стандарти
Методика розрахунку операційного ризику	Використовується національний підхід НБУ, інтегрований зі стандартизованим підходом SMA (повне застосування коефіцієнта ризику 1 з 29.12.2023р)	У всіх системно важливих банках діє стандартизований підхід SMA як обов'язковий міжнародний стандарт згідно з Базелем III.
Якість та узгодженість внутрішніх даних про події операційних ризиків	Дані про події операційного ризику збираються у внутрішній централізованій системі, але рівень стандартизації ще недостатній. Існують різні формати звітування між підрозділами, що перешкоджає повній уніфікації даних та швидкій аналітиці.	Дані зберігаються в єдиній базі за класифікацією ЕВА та подаються в стандартизованому форматі (ITS/RTS)
Інтегрованість систем контролінгу	Система контролінгу охоплює всі три лінії захисту, однак внутрішні системи не повністю інтегровані між собою (ризик, комплаєнс, ІТ-ризик, аудит). Частина процесів виконується в різних програмних комплексах, що ускладнює консолідацію даних та управлінських рішень.	Використовуються інтегровані системи контролінгу, що забезпечують автоматичний моніторинг ключових показників ефективності (KPI) та ризику (KRI), а

Продовження таблиці 3.1

		також централізовані системи для нагляду (SREP) та обліку операційних витрат (OPEX)
Ступінь автоматизації управління операційними ризиками	Банк має системи автоматичного моніторингу транзакцій у режимі реального часу та автоматизованої реєстрації інцидентів. Використовується поведінкова аналітика («поведінкова біометрія») для боротьби з шахрайством. Однак рівень автоматизації в частині інтегрованого контролінгу ризиків залишається нижчим, ніж у провідних міжнародних банків.	Високий рівень автоматизації завдяки використанню машинного навчання, поведінкової аналітики, автоматичного виявлення загроз та повної інтеграції IT- та ризик-систем.
Рівень IT- та кіберзахисту	Банк використовує багатофакторну автентифікацію (OTP, Push-ID, Smart-ID), шифрування даних на рівні міжнародних стандартів, хмарні резервні середовища для критичних систем (після початку війни). Рівень його кіберзахисту відповідає вимогам НБУ та ISO/IEC 27001.	Розвинені моделі управління ІКТ-ризиками згідно з стандартами DORA, NIST. Повністю автоматизовані процеси виявлення подій операційного ризику

Джерело: складено та розроблено автором за джерелами [43; 52; 53; 54; 55].

Порівняння підходів до управління операційним ризиком, наведених у табл. 3.1, показує суттєву різницю між системою управління АТ КБ «ПриватБанк» та банків ЄС та США. Хоча АТ КБ «ПриватБанк» належить до найбільш технологічних банківських установ України і демонструє значні успіхи у провадженні сучасних інструментів контролю, однак рівень інтегрованості, автоматизації та стандартизації процесів залишається нижчим порівняно з міжнародними стандартами.

У країнах ЄС управління операційним ризиком базується на уніфікованій методиці SMA, яка є обов'язковою для всіх системно важливих банків згідно з вимогами Базель III (Basel III Endgame). Це забезпечує однаковий підхід до оцінки ризиків та формування капіталу, незалежно від розміру та структури банку. Натомість АТ КБ «ПриватБанк» використовує національний підхід на основі підходу SMA, який хоч і наближений до європейського підходу, але все ще не забезпечує повної гармонізації з міжнародними вимогами.

Суттєвою перевагою міжнародної практики є висока стандартизація та централізований збір даних. Європейські банки зберігають інформацію про операційні події у єдиній базі згідно з класифікацією ЕВА та формують звітність у стандартизованих форматах ITS/RTS. Це дає змогу отримувати повну та узгоджену інформацію, що суттєво полегшує аналіз ризиків. У банку дані хоч і накопичуються централізовано, однак стандарти звітності та методики аналізу між підрозділами все ще відрізняються, що негативно впливає на процес збору інформації.

Автоматизація є ще однією ключовою відмінністю. У міжнародних банках значна частина процесів контролю та ризиків виконується автоматично, як від моніторингу подій операційного ризику, так і до формування KRI та KPI. Машинне навчання та поведінкова аналітика застосовуються не лише для виявлення шахрайства, а й для прогнозування майбутніх ризиків. АТ КБ «ПриватБанк» також активно впроваджує нові технології, зокрема поведінкову біометрію та моніторинг у режимі реального часу, проте рівень інтеграції між системами ризик-менеджменту, комплаєнсу, ІТ та аудиту залишається недостатнім.

Щодо кіберзахисту, АТ КБ «ПриватБанк» дотримується вимог НБУ та міжнародних стандартів, застосовує багатофакторну автентифікацію, шифрування та резервні хмарні середовища. Однак іноземні банки додатково керуються нормами DORA та NIST, які встановлюють більш комплексні та жорсткі вимоги до управління ІКТ-ризиками. Це забезпечує широкий спектр інструментів виявлення загроз і швидшу реакцію на реалізацію подій ризику.

Тому узагальнення міжнародного досвіду дає змогу чітко окреслити проблемні аспекти, у яких система фінансового контролінгу АТ КБ «ПриватБанк» потребує подальшого вдосконалення.

По-перше, окремі підрозділи банку використовують різні методи для процесу збору й опрацювання даних, що унеможливорює формування повного розуміння ризиків банку. Відсутність єдиного стандарту аналізу та

звітування призводить до розрізненості інформації, через що точність оцінки операційного ризику знижується.

По-друге, недостатня автоматизація окремих етапів контролінгу призводить до затримки у процесі виявлення та обробці подій операційного ризику. Це негативно впливає на ефективність системи управління ризиками, особливо в умовах зростання кількості кіберзагроз та частки транзакцій, які обслуговує банк.

По-третє, взаємодія між комплаєнсом, ризик-менеджментом, ІТ-структурами та внутрішнім аудитом потребує глибшої інтеграції. У міжнародній практиці саме взаємопов'язаність цих блоків забезпечує повноцінну систему захисту, тоді як у АТ КБ «ПриватБанк» вони часто працюють у рамках власних інформаційних середовищ.

Тож, у сукупності усі вищезазначені проблеми свідчать про те, що система управління операційного ризику потребує подальшого вдосконалення. Чітке визначення цих проблем дає змогу окреслити напрями, у яких АТ КБ «ПриватБанк» має посилити фінансовий контролінг та підвищити ефективність управління ризиками.

3.2. Напрями посилення ролі фінансового контролінгу в управлінні операційним ризиком банку

Ефективність системи управління операційним ризиком значною мірою залежить від того, наскільки глибоко фінансовий контролінг впроваджений у щоденне управління банком. Якщо контролінг обмежується лише обліком факту втрат від реалізації ризику, то він не виконує функції його запобігання. Тому для АТ КБ «ПриватБанк» важливо не просто виконувати формальні вимоги регулятора, а перетворити фінансовий контролінг на активний інструмент виявлення, оцінки та зниження операційного ризику.

Міжнародні рекомендації Базельського комітету з банківського нагляду підкреслюють, що операційний ризик має виглядати як невід’ємна частина загальної системи управління ризиками, а аналітика, звітність та контроль мають бути системними, регулярними та пов’язаними з фінансовими показниками діяльності [56]. У країнах ЄС саме через фінансовий контролінг забезпечується зв’язок між подіями операційного ризику, бізнес-процесами та обсягом капіталу, який банк має тримати для покриття таких втрат.

Тому до ключових напрямів, за якими доцільно посилювати роль фінансового контролінгу в управлінні операційним ризиком, з урахуванням міжнародного досвіду та вимог НБУ, належать:

- посилення зв’язку між фінансовим контролінгом та розрахунком капіталу під операційний ризик;
- підвищення якості та повноти даних операційного ризику;
- розвиток аналітичних інструментів фінансового контролінгу управління операційним ризиком;
- інтеграція контролінгу в управління ІТ-систем;
- посилення інституційної ролі контролінгу в моделі «трьох ліній захисту»;
- використання міжнародного досвіду з метою покращення системи управління операційним ризиком;
- формування культури ризик-орієнтованого управління.

Першим важливим напрямом є поглиблення зв’язку між фінансовим контролінгом і розрахунком капіталу під операційний ризик. Згідно з оновленими вимогами Базельського комітету, капітал під операційний ризик визначається на основі бізнес-індикатора (BI), що розраховується за складом валового доходу банку. Національний банк України, по суті, впроваджує цей підхід у національну банківську систему, зокрема через введення 100% урахування операційного ризику в норматив достатності капіталу з 29 грудня 2023 року. Для АТ КБ «ПриватБанк» це означає, що фінансовий контролінг має не просто відслідковувати доходи й витрати, а системно аналізувати, як

кожен його напрям діяльності формує ВІ та впливає на навантаження на капітал. Практично це означає побудову регулярних звітів, де ВІ та пов'язані з ним показники зіставляються з даними про події операційного ризику й витрати на їх покриття.

Другий напрям стосується якості та повноти даних, на яких базується фінансовий контролінг. У міжнародних банках управління операційним ризиком спирається на стандартизовані бази даних, де фіксуються всі події ризику, їх фінансові наслідки та причини, а формат даних стандартизований для всієї установи. Для АТ КБ «ПриватБанк» важливо не лише вести внутрішній реєстр подій операційного ризику, а й підвищити його результативність для контролінгу завдяки впровадженню єдиних правил заповнення, чіткого кодування типів подій, обов'язкову прив'язку кожної події до статей доходів і витрат. У річних звітах банку вже зазначено, що операційний ризик регулярно виноситься на розгляд Наглядової ради, формуються окремі звіти та ключових показників ризику. Тому наступним кроком має стати повна інтеграція цієї інформації у систему фінансового контролінгу, коли будь-яке відхилення у витратах або доходах автоматично пов'язується з конкретними групами операційних подій.

Третій напрям полягає у розвитку аналітичних інструментів фінансового контролінгу. Міжнародна практика показує, що найбільший ефект дають не окремі звіти подій операційного ризику, а постійний аналіз бізнес-процесів, включаючи сценарний аналіз, аналіз чутливості та факторний аналіз впливу окремих складових ВІ на капітал. Для АТ КБ «ПриватБанку» це може означати запровадження регулярних перевірок за основними бізнес-напрямами, де фінансовий контролінг оцінює, які саме продукти, канали або процеси найбільше збільшують навантаження на капітал за операційним ризиком, які види операційних подій найчастіше призводять до витрат, як зміна ІТ-інфраструктури, нових цифрових сервісів чи аутсорсингу впливає на витрати. Такі оцінки мають супроводжуватися

конкретними пропозиціями, наприклад, змінити тарифну політику, переглянути ліміти, інвестувати в автоматизацію певних операцій [57].

Четвертий напрям полягає у посиленні ролі фінансового контролінгу в управлінні ІКТ- та кіберризиком. Європейська банківська асоціація (ЕВА) вказує, що інформаційно-комунікаційні технології та безпека даних є невід'ємною частиною операційного ризику, а відповідні ризики мають оцінюватися в єдиній системі управління. Для АТ КБ «ПриватБанк», який активно розвиває цифрові продукти, впроваджує поведінкову біометрію, автоматичні системи моніторингу шахрайства та кіберзахисту, фінансовий контролінг має також оцінювати економічний ефект цих рішень. Тобто не лише враховувати витрати на ІТ-захист, але й зіставляти їх зі зменшенням кількості реалізації подій операційного ризику, сумою відвернених збитків та зниженням навантаження на капітал у довгостроковій перспективі. Такий підхід дозволяє приймати більш обґрунтовані рішення щодо інвестицій у кібербезпеку, резервні центри обробки даних та модернізацію інфраструктури.

П'ятий напрям пов'язаний з організаційною роллю фінансового контролінгу у моделі «трьох ліній захисту». Постанова НБУ №64 вимагає, щоб система управління ризиками була побудована як узгоджений механізм, де бізнес-підрозділи, функції контролю та внутрішній аудит чітко взаємодіють і не дублюють одна одну. У цьому контексті фінансовий контролінг може стати «зв'язуючою ланкою» між ризик-менеджментом, комплаєнсом, ІТ та внутрішнім аудитом. Для АТ КБ «ПриватБанку» доцільно посилити інституційну роль підрозділу фінансового контролінгу операційного ризику шляхом закріплення за ним повноваження не лише формувати звіти, а й ініціювати перегляд процедур, лімітів, внутрішніх регламентів на основі результатів аналізу. Це означає регулярну участь контролінгу у роботі комітетів, підготовку консолідованих аналітичних висновків для Правління та Наглядової ради та узгодження ризик-апетиту з реальними фінансовими результатами.

Шостий напрям передбачає використання міжнародного досвіду з метою покращення системи управління операційним ризиком. Звіти Європейського банківського управління щодо впровадження Basel III показують, що банки ЄС поступово підвищують здатність покривати операційний ризик капіталом, а стандартизований підхід дозволяє порівнювати навантаження на капітал між установами. Для АТ КБ «ПриватБанку» важливо не лише виконувати мінімальні нормативи НБУ, а й зіставляти власні показники з показниками інших вітчизняних банків та, наскільки можливо, іноземних. Фінансовий контролінг може готувати аналітичні огляди, з метою оцінити, чи не є навантаження на капітал за операційним ризиком вищим у порівнянні з аналогічними банками та у яких напрямках виникають додаткові ризики.

Сьомий напрям стосується розвитку внутрішньої культури ризик-орієнтованого управління на основі даних. Міжнародні стандарти наголошують, що ефективна система управління операційним ризиком неможлива без участі всіх рівнів персоналу та готовності керівництва приймати рішення, спираючись на якісну аналітику. У АТ КБ «ПриватБанк» фінансовий контролінг може посилити цю культуру шляхом регулярних презентацій для персоналу, підготовки зрозумілих візуальних матеріалів (графіки, діаграми впливу на капітал), проведення внутрішніх тренінгів щодо того, як операційні помилки або збої в ІТ-процесах трансформуються у реальні фінансові втрати. Це сприятиме тому, що операційний ризик сприйматиметься не як формальний показник, а як конкретний чинник, що безпосередньо впливає на прибутковість та стабільність банку.

Отже, посилення ролі фінансового контролінгу в управлінні операційним ризиком АТ КБ «ПриватБанк» передбачає підвищення якості даних та детальний їх аналіз, а також інтеграцію контролінгу у всі управлінські процеси. Використання сучасних інструментів та орієнтація на міжнародні стандарти дозволять банку ефективніше реагувати на ризики, зміцнювати фінансову стійкість і забезпечувати стабільність своєї діяльності.

3.3. Перспективи застосування запропонованих заходів фінансового контролю у діяльності АТ КБ «ПриватБанк»

Стабільність роботи банку в умовах швидких змін банківського ринку, цифрових загроз та воєнних ризиків значною мірою залежить від того, наскільки ефективно він може передбачати та контролювати операційні ризики. У випадку АТ КБ «ПриватБанк» це має особливе значення, оскільки він є найбільшим банком України за обсягом активів та має велику клієнтську базу. Саме тому прогноз ефективності запропонованих заходів з удосконалення фінансового контролінгу є важливим етапом оцінки майбутньої стійкості банку. Для цього необхідно враховувати вимоги Національного банку України, досвід країн Європейського Союзу та реальні тенденції розвитку банківського сектору.

Одним із ключових факторів, що визначають ефективність удосконалення системи управління операційним ризиком, є відповідність підходів банку вимогам НБУ. Це означає, що банки повинні вдосконалювати збір даних, підвищувати якість внутрішнього контролю та забезпечувати точність оцінки ризиків відповідно до вимог регулятора.

Тому результативність запропонованих заходів для АТ КБ «ПриватБанк» можна розглядати через призму цих вимог. Посилення внутрішнього контролю, вдосконалення обліку подій операційного ризику, а також розвиток системи ключових індикаторів ризику підвищують здатність банку визначати точний рівень ризику та формувати необхідний обсяг капіталу. Це в свою чергу дозволяє банку уникати надмірного навантаження на капітал, яке може виникати через недостатню точність розрахунків. Таким чином, удосконалення внутрішніх процесів безпосередньо пов'язано з майбутньою стабільністю установи.

Також важливу роль у впровадженні цих заходів відіграє цифровізація процесів ризик-менеджменту. У звіті АТ КБ «ПриватБанку» за 2023 рік

зазначено, що банк активно розвиває системи кіберзахисту, впроваджує поведінкову біометрію, багатофакторну автентифікацію та моніторинг операцій у режимі реального часу [46]. Подібні інструменти використовують теж провідні міжнародні банки, оскільки вони дозволяють зменшити кількість шахрайських операцій, швидше реагувати на порушення та скоротити вплив людського фактор на бізнес-процеси [58]. Водночас, банки, що застосовують автоматизовані системи моніторингу, підвищують ефективність виявлення подій операційного ризику і зменшують можливі збитки від його реалізації. Подальша цифровізація контролінгу, впровадження нових систем моніторингу та розвиток алгоритмів аналізу поведінки користувачів дозволять зміцнити стійкість АТ КБ «ПриватБанк» до кіберризиків. Таким чином, перспектива застосування цих заходів полягає в підвищенні безпеки цифрових сервісів і збереженні довіри клієнтів.

Значний вплив на ефективність впровадження заходів має також міжнародний досвід. У Європейському Союзі підхід до управління операційним ризиком ґрунтується на стандартизованих вимогах Базельського комітету. У країнах ЄС запроваджено єдину методику оцінки операційного ризику, саме стандартизованого підходу (SMA), а також вимоги регламенту DORA щодо операційної стійкості і кіберзахисту. Стандарти Європейської банківської асоціації (EBA) 2024 року уточнюють порядок збору даних про інциденти та вимоги до звітності [59]. Порівнюючи ці вимоги з вітчизняними, можна зробити прогноз, що АТ КБ «ПриватБанк», маючи розвинений рівень цифровізації та значний досвід роботи з великою клієнтською базою, здатний швидко адаптуватися до європейських підходів у разі їх запровадження в Україні. Це, у свою чергу, підвищить конкурентоспроможність банку, особливо після завершення процесу євроінтеграції фінансової системи України.

НБУ у звіті про фінансову стабільність за червень 2024 року наголошує, що операційні ризики банків залишаються підвищеними через загрози інфраструктурі, перебої електропостачання та кіберзагрози [60].

Тому для АТ КБ «ПриватБанк», який має понад тисячу відділень і широкий спектр цифрових сервісів, ці виклики особливо важливі. Запропоновані заходи, а саме автоматизація процесів контролю, посилення безпеки ІТ-систем, розширення резервування та розвиток хмарних технологій, здатні значно підвищити стійкість банку до зовнішніх загроз. Це свідчить, що банк зможе швидше відновлювати роботу після реалізації операційних подій, зменшити залежність від фізичної інфраструктури та забезпечити безперервність обслуговування клієнтів.

У довгостроковій перспективі, вдосконалення фінансового контролінгу сприятиме зниженню витрат на покриття збитків від операційних подій, підвищенню точності оцінки ризику та оптимізації використання капіталу. Покращення якості даних, своєчасне виявлення відхилень та впровадження сучасних методів аналізу дозволять банку точніше оцінювати імовірність настання операційних подій та масштаб можливих втрат. Це, у свою чергу, забезпечить ефективніше планування потреби в капіталі та уникнення його надмірного резервування.

Оптимізовані процеси контролінгу дозволять спрямовувати вивільнені ресурси на інші стратегічні напрями діяльності, такі як розвиток нових послуг, інвестиції у цифрові технології, підвищення якості сервісу. Завдяки цьому банк отримує змогу не лише відповідати регуляторним вимогам, а й посилювати свою конкурентоспроможність на ринку. Крім того, ефективний фінансовий контролінг створює стабільне аналітичне підґрунтя для прийняття управлінських рішень, що знижує ймовірність помилок та сприяє формуванню культури активного управління операційним ризиком.

З огляду на всі ці аспекти, вплив запропонованих заходів на систему управління операційним ризиком можна оцінити як позитивний. Вони здатні суттєво підвищити якість управління операційним ризиком, зміцнити операційну стійкість банку, зменшити рівень можливих втрат і забезпечити стабільність діяльності навіть у складних умовах. Інтеграція ІТ-систем, стандартизація процесів обліку даних і врахування міжнародного досвіду

створюють підґрунтя для того, щоб АТ КБ «ПриватБанк» і надалі залишався лідером банківської системи України та відповідав вимогам сучасного банківського середовища.