Дмитрова О.С., Гончарова К.Г., Меренкова О.В., Медвідь Т.А., Бойко А.О., Вахнюк С.В.
під загальною редакцією д.т.н., професора Дмитрова С.О.

Моделювання оцінки операційного ризику комерційного банку

СУМИ 2010

УДК 336.711(477)
ББК 65.9(4Укр)262.101

Рекомендовано до друку вченою радою Державного вищого навчального закладу «Українська академія банківської справи Національного банку України», протокол №1 від 15.10.2010

Автори:
О.С.Дмитрова, К.Г.Гончарова, О.В.Меренкова, Т.А Медвідь., А.О.Бойко, С.В.Вахнюк

Рецензенти:
доктор економічних наук, професор, директор Центру наукових досліджень Національного банку України
В.І.Міщенко
доктор економічних наук, професор, проректор з навчальної роботи ДВНЗ «Українська академія банківської справи Національного банку України»
І.О.Школьник
доктор економічних наук, професор, завідувач кафедри фінансового аналізу і контролю обліково-економічного факультету Київського національного торговельно-економічного університету
Є.В.Мних

Моделювання оцінки операційного ризику комерційного банку [Текст]: монографія / за заг. ред. С.О.Дмитрова ; [О.С.Дмитрова, К.Г.Гончарова, О.В.Меренкова, Т.А Медвідь., А.О.Бойко, С.В.Вахнюк]. – Суми : Державний вищий навчальний заклад «Українська академія банківської справи Національного банку України», 2010. – 277 с.
ISBN 978-966-9858-55-7
Монографія присвячена висвітленню теоретичних підходів та методики оцінки операційного ризику комерційного банку на основі застосування бінарних показників, апарату теорії імовірності та теорії нечіткої логіки. Такий підхід дозволить забезпечити якісне регулювання та нагляд, сприятиме вчасному визначенню суттєвих існуючих або потенційних проблем в комерційних банках та Національному банку України.
Видання призначене для студентів,ю аспірантів економічних спеціальностей, викладачів і науковців, а також фахівців з питань банківського нагляду Національного банку України та комерційних банків.

УДК 336.711(477)
ББК 65.9(4Укр)262.101

ISBN 978-966-9858-55-7

ВСТУП

Що таке операційний ризик та чому їм слід управляти та оцінювати саме в комерційному банку? Таке питання виникає досить часто. Не будемо викладати загальновідомі теорії та постулати – наведемо лише один (до речі, відомий широкому загалові) приклад.

Таким прикладом є історія діяльності британського банку Берінгз, точніше, історія його банкрутства. Почнемо з того, що вказаний банк завдяки діям одного зі своїх трейдерів (Н. Лісон) протягом кількох років отримував надприбутки. Так, у 1993 р. британський банк Берінгз отримав 10% всього свого прибутку в розмірі близько 24 млн. дол. США завдяки проведенню арбітражних операцій на індекс НІККЕЙ225 між Осакською та Сінгапурською фондовими біржами шляхом купівлі-продажу ф'ючерсів та опціонів. Наступного року прибуток, отриманий банком завдяки діям зазначеного трейдера, сягнув 40 млн дол. США. Проте на початку 1995 р. землетрус в Японії змінив ситуацію на фондовому ринку, а прорахунки Н. Лісона призвели до збитків банку в розмірі 1,4 млрд дол. США, що більше ніж удвічі перевищило власний капітал банку. В результаті вкладники втратили близько 4 млрд дол. США. Берінгз було оголошено банкрутом та придбано голандською страховою групою ІНДж (ING) за один фунт стерлінг.

Розглядаючи аспекти з управління операційним ризиком банку, важливо відмітити, що його збитки були спровоковані не лише діями одного його співробітника. Сприятливі умови для виникнення такої ситуації були створені в значній мірі через помилки у побудові бізнес процесів, оскільки Н. Лісом виконував функції трейдера банку та операції бек-офіса, що є неприпустимим, але допомагало трейдерові приховувати реальний стан справ. Маючи кредит довіри від керівництва банку, Н. Лісон проводив несанкціоновані операції, збитки від яких перевищили власний капітал банку [7].

Підсумовуючи вищезазначене, можемо зробити однозначний висновок операційний ризику в банківській діяльності не можна ігнорувати.

І. РОЛЬ ТА МІСЦЕ ОПЕРАЦІЙНОГО РИЗИКУ В СУЧАСНІЙ БАНКІВСЬКІЙ СПРАВІ

1.1 Основні причини та наслідки виникнення операційного ризику в банку

Проблема ризику та його впливу на суспільну діяльність цікавить людство досить тривалий час. Однак, лише порівняно нещодавно стала проявлятися підвищена увага до даної категорії, зокрема після низки економічних потрясінь таких, як світова фінансова криза, що розпочалася наприкінці 2007 року. При цьому, на особливу увагу заслуговує банківська діяльність, де ризик є чи не визначальним фактором успіху роботи на відповідну ринку.

Сьогоднішнє бізнес - середовище є більше складним, ніж будь-коли раніше. І господарюючі суб'єкти повинні співіснувати з невизначеністю у всіх аспектах операційної діяльності. І це природно, що є інтерес до того, яким чином керувати цією невизначеністю для досягнення конкурентних та стратегічних переваг.

Банківська справа, як і будь-який вид економічної діяльності, підкоряється загальним законам ринку і є вразливим по відношенню до численних загроз та ризиків. Саме тому для комерційних банків важливим аспектом є ефективне управління ризиками, яке включає як моніторинг, так і мінімізацію та оцінку ризиків, що впливає на прибутковість та розвиток банківської системи країни.

У самому широкому сенсі, ризик – це схильність до настання якоїсь несприятливої події, лиха. Словник «Cambridge Advanced Learner's Dictionary» визначає ризик як можливість настання чогось негативного. Подібна дефініція міститься і в інших словниках. Зокрема, «Compact Oxford English Dictionary». визначає ризик як:

1) ситуацію, що включає схильність до небезпеки;

2) можливість, що щось неприємне станеться. Словник «Merriam-Webster Online Dictionary» визначає ризик як можливість настання збитку чи шкоди.

Власне поняття «ризик» [1] визначає можливість настання несприятливої події та, здебільшого, трактується як імовірність чи загроза втрати суб'єктами господарювання частини своїх ресурсів, недоотримання доходів чи виникнення додаткових витрат в результаті здійснення певної виробничої чи фінансової діяльності. Ризик породжується невизначеністю та конфліктністю, що існують незалежно від їх усвідомлення особами, що приймають рішення, і визначається необхідністю прийняття рішення, результат реалізації якого може відрізнятись від очікуваного.

У роботі «Економічний ризик: ігрові моделі" під редакцією провідного вітчизняного вченого у сфері ризикології Вітлінського В.В. подано наступне визначення: «Ризик — це економічна категорія в діяльності суб'єктів господарювання, пов'язана з подоланням невизначеності, конфліктності в ситуаціях оцінювання, управління, неминучого вибору. Він має діалектичну об'єктивно—суб'єктивну структуру. Оцінка ризику є багатовимірною величиною, що характеризує можливі відхилення від цілей, від бажаного (очікуваного) результату, можливу невдачу (збитки) з урахуванням впливу контрольованих (керованих) і неконтрольованих (некерованих) чинників, прямих і зворотних зв'язків» [1].

Загалом концептуалізоване на цій основі поняття ризику сприймається трояко [3]:

1. Ризик як відображення об'єктивної непевності. Тут об'єктивна непевність сприймається як свідома інтерпретація непевності суб'єкта оцінювання, управління.

2. Визначення ризику як непевності через її психологічне сприйняття. У цьому розумінні ризик є комбінацією азарту та цілеспрямованих дій і вимірюється за допомогою показника ймовірності (ступеня, міри) переконаності особи. Разом з тим ризик супроводжує процес пізнання людиною світу.

3. Зв'язок «ризик — непевність» можна трактувати як суто психологічне явище, що проявляється лише в розрізі людських відчуттів і людського досвіду (поведінки суб'єкта). Послідовники психологічного підходу спираються на існуючий тісний зв'язок між суб'єктивними переживаннями людини та об'єктивною

дійсністю. Згідно з такою позицією величина ризику повинна змінюватися відповідно до психології та свідомості особи, яка наражатиметься на щось невідоме.

Таким чином, ризик — це об'єктивно-суб'єктивна категорія у діяльності суб'єктів, що пов'язана з подоланням невизначеності та конфліктності в ситуації неминучого вибору. Підводячи підсумки, слід зазначити, що категорію «ризик» можна розглядати в наступних ключових аспектах, зокрема як:

- ймовірність настання певної події;
- ступінь відхилення від бажаного результату;
- міру невдачі.

При цьому ризик, притаманний банківській діяльності, має свої особливості, тому надалі розглянемо вказану категорію детальніше.

Поняття «банківський ризик» автором роботи [2] визначається як загроза втрати банком частини своїх ресурсів, недоодержання доходів чи спричинення додаткових витрат у результаті здійснення фінансових операцій. Ризик виражається ймовірністю одержання таких небажаних результатів, як втрати прибутку і виникнення збитків внаслідок неплатежів по виданих кредитах, скорочення ресурсної бази тощо. Систему банківських ризиків можна подано на рис. 1.1.

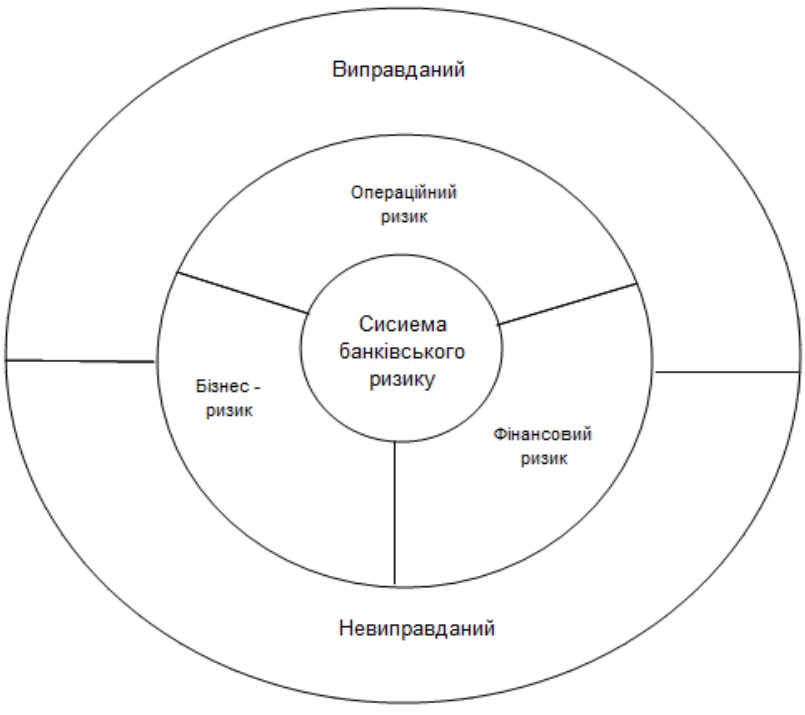


Рис. 1.1. Система банківського ризику

Існування ризику не обов'язково є причиною для занепокоєння. Ризики вважаються виправданими, якщо вони є зрозумілими, контрольованими, такими, які можна виміряти, і що відповідають здатності банку швидко реагувати на негативні обставини. Невиправданий ризик може випливати із навмисних або ненавмисних дій. Якщо ризики є невиправданими, ризик-менеджери мають взаємодіяти із керівництвом і спостережною радою банку, спонукаючи їх до пом'якшення або усунення цих невиправданих ризиків. Заходи, які в такому разі має здійснити банк, включають зменшення сум під ризиком, збільшення капіталу або зміцнення процесів управління ризиками. Категорії ризиків, властивих банківському бізнесу, за стандартами Базельського комітету з банківського нагляду (Базель ІІ), загалом класифікуються як фінансовий, операційний та бізнес-ризик (див. табл. 1.1).

Таблиця 1.1

Категорії ризиків, властивих банківському бізнесу

Категорія ризику згідно Базеля ІІ		Категорія ризику виділені НБУ	Характеристика
1		2	3
Фінансовий ризик	Ризик ліквідності	Ризик ліквідності	небезпека втрат у випадку нездатності банку покрити свої зобов’язання по пасивах балансу вимогами по активах
	Кредитний	Кредитний	невпевненість кредитора в тому, що боржник збереже намір виконати свої зобов’язання у відповідності з термінами й умовами кредитної угоди. У банківській діяльності варто розрізняти такі рівні кредитного ризику: – кредитний ризик за окремою згодою — імовірність збитків від невиконання позичальником конкретної кредитної угоди; – кредитний ризик усього портфеля — величина ризиків по всіх угодах кредитного портфеля
	Ринковий	* Ризик зміни процентної ставки; * Ринковий; * Валютний	наявний або потенційний ризик для надходжень та капіталу, який виникає через несприятливі коливання вартості цінних паперів та товарів і курсів іноземних валют за тими інструментами, які є в торговельному портфелі. Цей ризик випливає з маркетмейкерства, дилінгу, прийняття позицій з боргових та пайових цінних паперів, валют, товарів та похідних інструментів (деривативів).

Продовження табл. 2.8

1		2	3
Операційний ризик	Ризик персоналу	Операційно-технологічний	людський фактор може бути джерелом ризику внаслідок дії конкурентів, таємниці, конфіденційності, що можуть породжувати невизначеність знань про об’єкт керування (ризик вивчення) або помилкової дії менеджера чи оператора (ризик дії), конфліктів
	Технологічний ризик		пов'язаний з використанням у діяльності банку технічних засобів, високотехнологічного обладнання та технологій. Цей вид ризику породжується помилками в застосуванні комп'ютерних програм, у математичних моделях, формулах і розрахунках.
	Системний		пов'язаний зі зміною цін на акції, їх прибутковістю, поточним і очікуваним відсотком по облігаціях, очікуваними розмірами дивіденду і додатковим прибутком, викликаними загально ринковими коливаннями
	Ризик зовнішнього середовища		ризик, безпосередньо не пов’язаний з діяльністю банку чи його партнерів, а визначається впливом великої кількості політичних, економічних, демографічних, соціальних, географічних та інших факторів
Бізнес—ризик	Стратегічний	Стратегічний	ризик розроблення неефективних довгострокових планів, основних і глобальних цілей, задач, обсягу, видів, принципів управління
	Ризик дій акціонерів		можливість прийняття рішень мотивованих конфліктом інтересів окремих акціонерів
	Ризик дій менеджменту		можливість неправильних дій у процесі досягнення поставлених цілей з використанням визначених інструментів
	Юридичний	Юридичний	ризик зменшення активів або збільшення зобов’язань банку через неадекватний чи неправильний юридичний висновок або документацію; ризик неврахування змін законодавства та ризик, пов’язаного з цим, застосування штрафних санкцій
	Репутаційний	Ризик репутації	потенційне зменшення клієнтської бази через несприятливе сприйняття іміджу банку, даний ризик може призводити як до зменшення клієнтської бази, так і до ускладнення у встановленні нових відносин із партнерами

Джерело: складено авторами на підставі [4]

Очевидно, що прихильність до ризику можна розглядати як функцію від двох параметрів: імовірності настання негативної події і масштабу можливого збитку,

тобто чутливості активів до наслідків цієї події. По-перше, очевидно, що ризик, це невизначеність. По-друге, ризик несе в собі нові можливості, які необхідні для досягнення конкурентних переваг. По-третє, ризик може надавати руйнівний вплив на діяльність банку. У зв'язку з цим, окремі західні аналітики умовно поділяють все розмаїття ризиків на три категорії: ризики події (бізнес-ризики), фінансові ризики та операційні ризики.

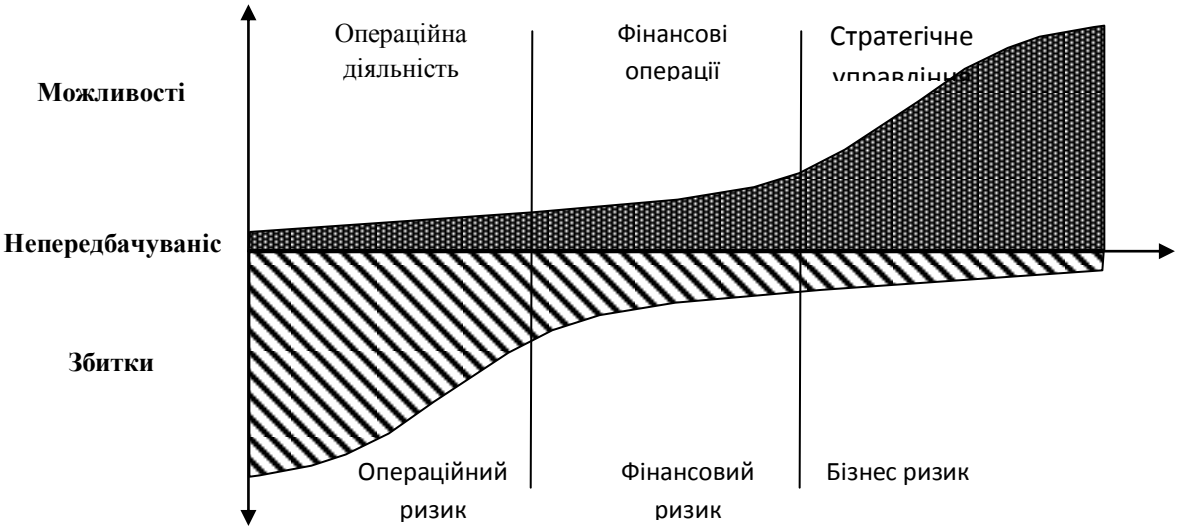


Рис. 1.2. Співвідношення фінансових і інших видів ризиків

Відповідно до цієї моделі, управління ризиком події повинно бути органічною частиною стратегічного управління у банку, в рамках якого оцінюються можливості банку, нові тенденції у зовнішньому середовищі, визначаються основні конкурентні переваги і плануються заходи щодо досягнення поставлених цілей.

Протягом останніх років, особливо в умовах глобальної економічної та фінансової криз, існує зростаючий інтерес з боку суб’єктів господарювання до виявлення та запобігання втрат, викликаних операційними ризиками.

Операційний ризик не є новим ризиком, він існує стільки ж, скільки існує бізнес. Але, у зв’язку з нерегулярністю втрат, його повний потенціал донедавна не усвідомлювався. Таким чином, операційний ризик не привертав значної уваги до 90-х років XX століття, коли відбулася серія фатальних операційних втрат, що надало нового акценту операційному ризику. При цьому вражає те, що колосальні операційні втрати спіткали відомі та респектабельні фірми США та Європи, що

підкреслює небезпеку ігнорування цієї сфери. Зокрема, слід згадати такі два приклади щодо понесених величезних операційних втрат, що мали місце саме у фінансовому секторі: по-перше, Канадіан Імперіал Бенк оф Комерс (Canadian Imperial Bank of Commerce (CIBC)), який заплатив 2,4 млрд. доларів США за позовом акціонерів «Енрон», по-друге, 690 млн. доларів США збитків, завданих Олфьост (Allfirst (Allied Irish Banks)) шахрайською торговельною діяльністю. Також сюди можемо додати сумно відомий американський хедж-фонд Лонг-Терм Кепітал Менеджмент (Long-Term Capital Management, LTCM), у якому працювали два нобелівських лауреати і чиє банкрутство після дефолту в Росії в 1998р. ледь не призвело до колапсу світових фінансових ринків. LTCM був створений у 1994 р. з капіталом більш 1 млрд. доларів США і швидко перетворився в один з ведучих хедж-фондів. Не дивно, адже його засновником і керівником був відомий інвестиційний банкір Джон Меріуезєр, а серед його партнерів фігурували два лауреати Нобелівської премії по економіці Р.Мертон і М.Шоулз[1]. Саме вони розробили складну стратегію інвестування активів LTCM. У середині 1998р. капітал фонду складав 5 млрд. доларів США, а активи під управлінням — 100 млрд. доларів США. Але через дефолт в Росії, де LTCM вів масштабні операції з державними цінними паперами і форвардними контрактами «рубль — долар», фонд утратив 4 млрд. доларів США. У жовтні 1998 р. LTCM виявився на грані краху, і завмерла вся світова фінансова система: на той момент у фонду були відкриті позиції по усьому світу на 1,25 трлн. доларів США. Його врятував лише стабілізаційний кредит у 3,625 млрд. доларів США, наданий консорціумом з 14 американських банків, об'єднаних з ініціативи Федеральної резервної системи США. У грудні 1999р. LTCM виплатив банкам усі борги і тихо закрився.

Наведені приклади показують масштаби небезпеки операційних ризиків. Чому саме операційних, а не фінансових? Тому, що фінансові ризики піддаються кількісному вимірюванню з подальшим їх коригуванням. На сьогодні економісти доволі вправно навчились маніпулювати ризиками, які мають чіткі кількісні

[1] Разом з Ф. Блеком (він помер у 1995р.) вони розробили модель опціонного ціноутворення Блека — Шоулза, за яку в 1997р. одержали Нобелівську премію.

параметри. Проте, масштаби та швидкість руху коштів в рамках сучасної фінансової системи (більше того – за умов глобалізації) загострили та висвітили загрози дещо іншої природи, які не мають чітких кількісних індикаторів – це й є операційний ризик. Крім можливих величезних втрат, операційний ризик також загрожує всім видам діяльності та операціям як окремих господарюючих суб'єктів, так і фінансової системи в цілому. Втрати від операційного ризику можуть бути суттєвішими, ніж втрати від ринкового або кредитного ризиків. Це можна пояснити, зокрема нерегулярністю його управління і як наслідок – ігнорування в багатьох випадках.

Вони також виступають в якості імперативного попереджувального сигналу всім суб'єктам господарювання, які повинні визначати, вимірювати та управляти цим ризиком. Ці події в поєднанні зі змінною природою ризику можливо назавжди змінили сприйняття та пріоритети банківського менеджменту.

Більше того, одне з останніх досліджень КПМДжі (KPMG) показало, що банкам слід приділяти більше уваги управлінню ризиками, щоб не допустити повторення теперішньої ситуації, однак, лише нечисленні банки планують істотно змінити свої підходи до цього процесу [5]. З такими результатами дослідження процесу управління ризиками, проведеного експертами ЕІЮ (EIU) за завданням КПМДжі Інтернешнл (KPMG International), змушені погодитися чимало закладів банківського сектору. Згідно з дослідженням, 90% із 400 опитаних банківських інститутів провели (або планують провести) аналіз власних систем управління ризиками. Однак, при цьому лише 42 % істотно змінюють цей процес або планують здійснювати істотні зміни. Судячи з усього, банки переконані, що такі антикризові заходи можуть виявитися не настільки дієвими, як очікується, або ж вони ще не до кінця усвідомили всю масштабність негативних наслідків кризи для банківської галузі.

Представники банків, котрі брали участь у дослідженні, практично не сумніваються, що відсутність відповідної дисципліни у процесі управління ризиками стала одним із чинників, які обумовили фінансову кризу. Однак, говорячи про антикризові заходи, лише четверо з десяти респондентів повідомили, що в їхніх

організаціях плануються достатньо серйозні зміни, на які заслуговує криза таких масштабів. Позитивним чинником можна вважати визнанням банками того, що проблема полягає саме у невдалому управлінні ризиками. Коли криза лише розпочиналася, багато хто називав причиною втрат загальне прагнення банків до гонитви за підвищенням доходів, коли політика легкого доступу до кредитів або політика винагород не сприяли створенню стійкої цінності для акціонерів у довготерміновій перспективі. Ці чинники, ставши своєрідними індикаторами, справді відіграли свою роль, однак надійні системи управління ризиками мусили б знизити їх вплив. Тому ключовим елементом подолання кризи має стати перебудова всієї системи управління ризиками — недостатнім виявиться зосередження уваги лише на якихось окремих проблемах.

У дослідженні виокремлюють кілька проблем, які слід вирішити у межах поліпшення якості управління ризиками: відсутність у вищого керівництва відповідних професійних знань із управління ризиками; недостатньо ефективна взаємодія служб виявлення та управління ризиками з іншими підрозділами організацій, а також недостатній авторитет підрозділів, які відповідають за управління ризиками. Виявлення та управління ризиками 75% респондентів вважають своєрідною допоміжною функцією. Тим не менше, сім із десяти респондентів визнають, що авторитет цієї служби виріс порівняно з тим, що спостерігалося 2 роки тому. Ще більший відсоток респондентів упевнений в тому, що високий рівень роботи з ризиками може бути значною конкурентною перевагою для банку. Крім того, чимало респондентів вважають, що рівень відповідальності й авторитету керівників трьох підрозділів, котрі відповідають за роботу з ризиками, тепер значно зросте, особливо під час розроблення стратегій розвитку та розміщення капіталу. Однак для того, аби це справді відбулося, слід зробити так, щоб ці підрозділи більше не вважалися допоміжними.

Дуже непростою є проблема професійних знань членів ради директорів у галузі управління ризиками. В цілому, до нестачі таких спеціальних знань у керівництва найвищої ланки ставляться доволі толерантно. Тим не менше, деякі респонденти висловили думку, що цей чинник сприяв погіршенню ситуації у

багатьох банках. Особливо серйозним такий недолік вважають керівники середньої ланки. Що стосується чинника недостатньої взаємодії, важливим його вважають менше 20% респондентів. Проте під час докладного аналізу виявилось, що політика компанії або банку з управління ризиками недостатньо чітко транслюється на рівень операційних підрозділів. Таким чином, взаємодію з бізнес-одиницями, з підрозділами внутрішнього аудиту та Комітетом з аудиту можна вдосконалити.

Дослідження продемонструвало, що банкам слід сформувати серйозніше ставлення до ризиків та впроваджувати культуру управління ризиками на всіх рівнях. По суті, кожен працівник банку має стати ризик-менеджером. У зв'язку з цим вимагається розуміння та усвідомлення працівниками рівня прийнятності ризиків для їхньої конкретної компанії. Сучасні структури з управління ризиками мають ґрунтуватися на трьох основних засадах: працівники, котрі працюють із клієнтами; функціональний підрозділ із управління ризиками та служба внутрішнього аудиту та нормативно-правової відповідності. Для того, щоб втілити на практиці правильне ставлення до ризиків, необхідна послідовна увага до цих проблем із боку найвищого керівництва. Це могло би підвищити статус цієї функції. Водночас поточну роботу в цьому напрямку можна передати на середній рівень керівництва.

Банкам також слід приділяти більше уваги якісному аспекту аналізу ризиків, пов'язаних із будь-яким стратегічним рішенням. Це викликано тим, що пропозиції банків зараз стали настільки складними, що якісні методи аналізу самі по собі не забезпечують необхідний рівень оцінки ризиків, особливо в умовах сучасних мінливих та непередбачуваних ринків. Недостатня обґрунтованість рішень, коли основний акцент робився на короткотерміновому виграші, а здорового скептицизму під час оцінки прийнятих рішень не вистачало, стала однією з причин кризи. Процес прийняття стратегічних рішень слід удосконалити, і для банків першим кроком у цьому напрямку має стати зміцнення дисципліни у галузі управління ризиками. А для втілення вказаної цілі, на наш погляд, необхідно, зокрема усвідомити роль саме операційного ризику.

В економічній літературі поки що не склалося однозначного уявлення про операційний ризик, що приводить до різних трактувань суті даного виду ризику та

способів управління ним. Розглянемо декілька підходів до визначення поняття «операційний ризик банку».

Перший підхід відбито у назві, й він полягає в тому, що під цим терміном розуміють ризики, які виникають у процесі операцій, котрі здійснює фінансовий інститут (банк). Такий підхід охоплює помилки персоналу, недотримання процедур виконання операцій, збої комп'ютерних систем тощо. Разом із тим, не йдеться про навмисне порушення систем внутрішнього контролю (наприклад, свідоме порушення лімітів та резервів співробітниками банку), внутрішні та зовнішні шахрайства. За такого підходу не враховують ризик, пов'язаний із неадекватною організацію процедур виконання операцій та, власне, організацією бізнес-процесів у банку (наприклад, надання одному підрозділів одночасно повноважень прийняття рішень та контролю за ними). Викладений підхід також не враховує ризик, пов'язаний із використанням неадекватних моделей оцінки ризику (ринкового та кредитного).

Другий поширений підхід полягає у розбитті ризиків банку на фінансові й нефінансові та визначенні операційних ризиків як «нефінансових». Під фінансовими ризиками розуміють ризики, що виникають при виконанні банками функцій фінансових посередників. До них відносять ринковий, кредитний, ризик ліквідності, ризик невідповідності активів та зобов'язань, а також страховий ризик. На відміну від фінансових, нефінансові ризики притаманні не тільки фінансовим посередникам, а й є загальними для багатьох суб'єктів господарювання. Нефінансові ризики класифікують на три категорії: ризики внутрішніх подій, ризики зовнішніх подій та бізнес-ризики.

До першої категорії відносяться шахрайствами, відсутність належного внутрішнього контролю, збої інформаційних систем, правові помилки та порушення. Ризики зовнішніх подій пов'язані катастрофами, терористичними актами, землетрусами, цунамі тощо. Бізнес-ризики охоплюють збитки від нереалізованих конкурентних переваг, неправильного вибору стратегії розвитку та місця на ринку, втрати від регуляторних змін, від змін у попиті тощо.

На нашу думку, другий підхід не зовсім адекватно відображає сутність операційних ризиків. Так, бізнес-ризики породжують втрати через звичайні економічні причини, тому мають бути предметом аналізу бізнес-діяльності банку в цілому, а не ризик-менеджерів. Окрім цього, необхідно відокремити безпосередні втрати, пов'язані з певною подією, від побічних втрат. Наприклад, окрім 85 млн. доларів США прямих збитків банк Нью-Йорка (США) від терористичних актів 11 вересня 2001 р., також зазнав опосередкованих збитів через порушення звичайног перебігу економічної діяльності на кілька днів (зокрема, біржа не працювала 4 дні).

Третій підхід полягає в тому, що операційний ризик – це ризик прямих та побічних збитків у результаті неправильної побудови бізнеспроцесів, неефективності процедур внутрішнього контролю, технологічних збоїв, несанкціонованих дій персоналу або зовнішніх впливів. Ми вважаємо, що дане визначення здається найґрунтовнішим і узагальнює підходи, спрямовані на перераховані сфери виникнення операційних ризиків, що широко представлені в західній літературі з банківської практики.

До аналогічного контексту належить визначення, що запропонував Базельський комітет у редакції Угоди з капіталу: «Операційний ризик визначають як ризик виникнення збитків у результаті недоліків та помилок у ході здійснення внутрішніх процесів у банку, допущених із боку співробітників, через інформаційні системи, а також зовнішніх подій».

Отже, ми бачимо, що підходи до визначення операційного ризику – різноманітні, що й зумовлює специфічність їх сприйняття. Особливо така складність прослідковується у вітчизняних банках банках, оскільки управління операційним ризиком характерне для банківської справи в країнах США та Західної Європи [8].

Що стосується причин виникнення операційного ризику, то їх є велика кількість. Для можливості ефективного контролю та відстеження рівня операційного ризику дуже важливо правильно розподілити види та його прояви за причинами виникнення.

Причини виникнення операційного ризику поділяються на зовнішні та внутрішні. Головною причиною найчастіше виступають дії людини. Навіть, коли

проблема виникає з системами та технологіями, які використовуються у банківській системі, перед цим людина приймає рішення, яку програму використовувати, або дії некваліфікованого фахівця призводять до проблем з технікою чи системами. Класифікатор операційного ризику повинен мати найбільш спрощену форму - яка на практиці дозволить чітко виначати причини виникнення операційного ризику [9].

Зазвичай, сфера операційних ризиків знаходиться в компетенції тих підрозділів банку, які є допоміжними для основного виду бізнесу (служби внутрішнього контролю, безпеки, аудиту тощо). Проаналізуємо причини виникнення операційних ризиків за даними табл. 1.2

Таблиця 1.2

Причини виникнення операційних ризиків

Причини	Перші за важливістю	Другі за важливістю	Треті за важливістю
Комп'ютерні збої та недосконалість програмного забезпечення	57%	19%	22,5%
Помилки персоналу	38%	43%	5,5%
Шахрайство (внутрішнє та зовнішнє)	5%	14%	33,5%
Недосконалість побудови внутрішніх бізнес-процесів	-	19%	5,5%
Втручання зовнішніх факторів (аварійного типу)	-	5%	-
Зловживання персоналу без шахрайства	-	-	11%
Неповне використання можливостей систем	-	-	11%
Відсутність єдиного інформаційного поля	-	-	5,5%
Проблеми каналів зв'язку між філіями	-	-	5,5%

Джерело: [9].

Згідно даних таблиці можна зробити висновки, що серед найважливіших причин виникнення операційних ризиків – три: комп'ютерні збої – 57%, помилки персоналу – 38%, шахрайство – 5%. Поміж причин операційних ризиків другої пріоритетності (тобто таких, що експерти поставили на друге місце) домінують

помилки персоналу (43%). Найважливіша причина третьої пріоритетності – внутрішнє та зовнішнє шахрайство.

Як свідчать результати експертного дослідження, операційні ризики мають різний ступінь важливості в загальній структурі сукупного банківського ризику, що видно з табл. 1.3.

Таблиця 1.3

Ранг операційних ризиків серед дев'яти категорій ризиків

Групи банків	Середній ранг (ступінь важливості) операційних ризиків для банків)
Банківська система України вцілому	5
Найбільші банки	4
Великі банки	6
Середні банки	6
Невеликі банки	6

Джерело: [9].

У середньому в банківській системі даний вид ризику займає за пріоритетністю пяте місце серед девяти категорій ризику, визначених Методичними рекомендаціями щодо організації та функціонування систем ризик менеджменту в банках України. Однак пріоритетність даного виду ризику – на четвертому місці щодо найбільших банків і шостому для всіх інших.

Теоретичне пояснення даного факту випливає із загальної теорії систем, тому що зі зростанням величини банку він стає складнішим як система. Практично це виявляється в якісних та кількісних відмінностях характеристик ризиків. Із збільшенням банку зростають обсяг операцій, їх різноманітність, збільшується кількість філій, банкоматів тощо.

Цікавим є співвідношення об'єктивної та суб'єктивної складових в операційних ризиках банків. Відомо, що ризик має як об'єктивну, так і суб'єктивну складову. Перша породжена ризикованістю, що природно притаманна банківській діяльності. Друга – особливостями прийняття рішень зацікавленими суб'єктами в умовах невизначеності. Результати експертного дослідження показують, що в середньому у банківській системі об'єктивна складова та суб'єктивна приблизно однакові, з невеликою перевагою останньої. Але є суттєва різниця в тому, як експерти з банків

різних груп оцінюють об’єктивну та суб’єктивну складові. В групах найбільших та невеликих банків частка суб’єктивної складової значно перевищує об’єктивну – в першому випадку в 1,5 раза, а в другому – в 2 рази.

Разом із тим у групах великих та середніх банках об’єктивна складова більша. Пояснення цьому факту наступне. У великих системних банків є значна кількість філій, великий обсяг операцій, вони оперують різними фінансовими інструментами. Тому виникнення збитків за операційними ризиками суттєво залежить від правильності організації внутрішніх процедур, організації систем внутрішнього контролю, рівня менеджменту тощо. Для банків із групи невеликих, на перший план виходить інший ефект – прояв одного операційного ризику може призвести до спотворення ефективної діяльності банку, тому вага правильності рішення зростає. Частки об’єктивної та суб’єктивної складових наведено в табл. 1.4.

Таблиця 1.4

Складові операційних ризиків в банківській системі України

Групи банків	Об’єктивна складова	Субєктивна складова
Банківська система України вцілому	48%	52%
Найбільші банки	38%	62%
Великі банки	56%	44%
Середні банки	57%	43%
Невеликі банки	33%	67%

Джерело: [9].

Характеристику типів вимірюваних операційних наведено у табл. 1.5. нижче.

Таблиця 1.5

Типи вимірюваних операційних ризиків

Типи вимірюваних операційних втрат	Опис
1	2
Зменшення вартості активів (Write-Down)	Безпосереднє зменшення вартості активів в результаті крадіжки, шахрайства, несанкціонованих або кредитних / ринкових збитків у результаті операційного характеру
Втрата ресурсів (Loss of Recourse)	Платежі та списання кошти відносно неправильних контрагентів, які не були повернені
Компенсації (Restitution)	Платежі (включаючи відсотки) клієнтам як компенсацію
Юридичні зобов’язання (Legal Liability)	Платежі (включаючи відсотки) клієнтам як компенсацію. Витрати, пов'язані із судовими розглядами й інші юридичні платежі

Продовження табл. 1.5

1	2
Втарта або пошкодження активів (Loss of or Damage to Assets)	Безпосередня втрата вартості фізичних активів у результаті яких-небудь обставин
Регуляторні вимоги та комплайєнс (нормативно-правова відповідність) (Regulatory & Compliance)	Штрафи і інші обов'язкові платежі в результаті порушення нормативних актов.Штрафи за приписами податкових органів та інші втрати, пов'язані з неправильним регулюванням власних податкових платежів та порушеннями правил податкового обліку в результаті помилок операційного характеру
включаючи питання оподаткування	
Податкові втрати (Tax Loss)	

Джерело: складено авторами.

Разом із тим, операційний ризик характеризується значними якісними операційними втратами, зокрема їх класифікацію наведено у таблиці 1.6.

Таблиця 1.6

Типи якісних операційних втрат у банках

Типи якісних операційних втрат	Опис
Service Levels (зниження якості послуг)	Втрата якості наданих послуг і обслуговування і подвльша втрата клієнтів
Foregone Income (недоотримання доходів)	Недоотримання запланованих доходів
Quality (втрата якості)	Втрата якості внутрішніх банківських процесів, які призводять в подальшому до додаткових видатків
Reputation (втрата репутації)	Втрата репутації та подальша втрата клієнтів
Business Interruption (Призупинення діяльності)	Призупинка діяльності в результаті несприятливих обставин, наприклад, технологічного збою або юридичних чи податкових помилок. Поділяється на короткотермінову, довготермінову та остаточну

Джерело: складено авторами.

Операційні ризики, за типом наслідків та частотою прояву можна поділити на 4 групи:

1. Перша характеризується подіями, що виникають з малою частотою та спричиняють невеликі збитки;

2. Друга включає події, що виникають часто та спричиняють невеликі збитки;

3. Третя група характеризується суттєвими збитками, які трапляються з малою ймовірністю.

Події, що трапляються часто та призводять до великих збитків, нами не розглядаються через те, що вони, вочевидь, призводять до банкрутства.

Втрати від подій першої та другої груп мають бути включені до вартості бізнесу, а тому за основні операційні ризики слід прийняти ті. що характеризуються суттєвими втратами з малою ймовірністю виникнення.

Базельський комітет з банківського нагляду в опублікованій новій угоді з капіталу пропонує концепцію резервування коштів проти операційних ризиків. Оцінка, аналіз та моделювання операційних ризиків на основі затвердженої концепції здійснюється лише в трохи більше чверті банків. Більшість банків в групах найкрупніших, великих та середніх розробляють подібну концепцію. У той же час всі банки з вибірки невеликих банків відповіли про відсутність якої-небудь концепції аналізу та моделювання операційних ризиків (див. табл. 1.7).

Таблиця 1.7

Наявність затвердженої концепції аналізу операційних ризиків

Характеристика	Банківська система в цілому	Найбільші банки	Великі банки	Середні банки	Невеликі банки
Існує концепція аналізу, оцінки та моделювання операційних ризиків, затверджена керівним органом банку	27%	33%	43%	17%	0%
На даному етапі банк працює над розробкою концепції аналізу, оцінки та моделювання операційних ризиків	41%	50%	28%	66%	0%
Концепції аналізу, оцінки та моделювання операційних ризиків в банку не існує	32%	17%	28.5%	17%	100%

Джерело: [10].

Отже, можна зробити висновок, що операційний ризик тією чи іншою мірою несуть усі банки, тому що кожний з них може зіткнутися з помилками й збоями в роботі інформаційних систем, персоналу та несприятливимт зовнішніми подіями. Однак не в усіх банках є підрозділ з управління ризиками, і тим більше не в усіх банках на сьогоднішній день є система управління операційними ризиками. Саме це і створює причини для негативного впливу операційного ризику на діяльність українських банків [11].

Операційний ризик зумовлений невизначеністю стану і функціонування внутрішнього середовища. Створення чітко налагодженої системи управління

операційними ризиками у банках є надзвичайно важливим для побудови всебічної системи управління ризиками. Для банків, функціонуючих в умовах ринкових відносин, є свідомо програшною як стратегія абсолютної мінімізації операційного ризику, так і стратегія його абсолютного ігнорування. У першому випадку це обумовлено збільшенням витрат і зниженням конкурентоспроможності банківських продуктів та послуг, а в другому - виникненням реальних загроз для існування банку. У цьому зв'язку виникає задача визначення прийнятного для конкретної банківської установи рівня ризику та управління поточним рівнем ризику в рамках заданих обмежень.

1.2 Місце операційного ризику у діяльності банку згідно Базеля II

Одним з найважливіших міжнародних документів, що регламентує питання операційного ризик - менеджменту у банківській діяльності, є «Угода про міжнародне наближення визначення капіталу та стандартів капіталу переглянута концептуальна основа» (Базель II), прийнята 26 червня 2004 р. Базельським комітетом з банківського нагляду, що встановлює вимоги до достатності банківського капіталу в сучасних умовах високого рівня різноманітних ризиків у банківській діяльності.

Базель II містить три базові аспекти, які присвячені:

- по-перше, вимогам щодо мінімального розміру власного капіталу;
- по-друге, перевіркам з боку органів банківського регулювання;
- по-третє, питанням прозорості та ринкової дисципліни в банках.

Одним із головних нововведеньугоди Базель II є встановлення трьох різних варіантів розрахунку кредитного ризику й трьох варіантів розрахунку банківського операційного ризику. Базельський комітет вважає, що неможливо й небажано виміряти одним мірилом обидва види ризику. Замість цього як щодо кредитного, так і щодо операційного ризику пропонуються три методи підвищення чутливості до ризиків, що дозволяють банкам і наглядовим органам вибрати для себе такий метод (або методи), які, на їхню думку, найбільше підходять для даного етапу розвитку

діяльності банку та інфраструктури ринку в межах обраної банком системи ризик-менеджменту.

Базель II створювалася як угода, що максимально диференціює коефіцієнти достатності капіталу залежно від ризиків конкретних позичальників. Концептуальне нововведення – використання кредитних рейтингів зовнішніх агентств для визначення ступеня ризику, за допомогою яких розраховується підсумковий коефіцієнт достатності капіталу.

Саме кредитні рейтинги позичальників, виставлені незалежними агентствами, дозволяють банкам реалізувати найбільш гнучке управління ризиками завдяки єдиному з наглядовими органами розумінню ризиків кожного позичальника й принципів ризик - менеджменту банку.

Використання кредитних рейтингів не випадкове, адже в останнє десятиліття з розвитком нових ринків, посиленням міжнародних фінансових відносин рейтинги набули надзвичайно великого значення. Вони показали себе як зручний і ефективний елемент інфраструктури інвестиційних відносин і це стало причиною для рішення Базельського комітету з банківського нагляду використати цю інфраструктуру також у кредитних відносинах.

Два інші аспекти або їх ще називають «стовпами» нової угоди – «ринкова дисципліна» і «посилення нагляду» – переслідують фактично ту ж мету – посилення змістовного управління банківськими ризиками – і не тільки кредитним і операційними, але й усіма іншими. Такої мети передбачається досягти за допомогою стимулювання банків використовувати найефективніші методи управління ризиками.

Безумовно, Базель II забезпечив вихід на новий рівень взаємин банків і фінансової влади. І, як часто буває, цей інструмент настільки ж ефективний, як і складний у застосуванні. Саме тому для ефективного процесу управління ризиками важливим чинником є сприятливе середовище, в якому функціонує банк. Базельський комітет виділяє кілька принципів його формування:

1. Спостережна рада має бути обізнаною щодо основних аспектів операційних ризиків банку як окремої категорії ризику, яка повинна управлятися, і він повинен

схвалити і періодично переглядати систему управління операційними ризиками. Система повинна давати для всього банку визначення операційного ризику та викладати принципи того, як операційний ризик повинен бути ідентифікований, оцінений, відстежено і контролюємо / знижений.

Для реалізації даного принципу у банку необхідно визначення ризику та його складу, політики управління ризиками, адекватної організаційної структури; обов'язковим є виділення незалежної служби внутрішнього контролю, визначення ключових процесів для першочергового контролю.

2. Спостережна Рада повинна забезпечити, щоб система управління операційним ризиком була об'єктом внутрішнього аудиту з незалежним, навченим і компетентним штатом. Внутрішній аудит не несе прямої відповідальності за управління операційним ризиком.

3. Правління банку має бути відповідальним за впровадження системи управління операційним ризиком, схваленої Спостережною радою. Ця система повинна бути послідовно впроваджена по всій структурі банку, і персонал на всіх рівнях повинен розуміти всю відповідальність щодо управління операційним ризиком. Правління повинно бути також відповідальним за розробку і впровадження політик, процедур, процесів для управління операційним ризиком у всіх матеріальних продуктах, напрямки діяльності, процесах і системах банку.

Реалізація даного принципу можлива за допомогою наявності кваліфікованого штату, взаємодії штату, який відповідає за управління операційним ризиком, зі штатом, що відповідає за управління кредитним, ринковим та іншими ризиками, а також з тими, хто взаємодіє зі страховими компаніями. Також необхідна система мотивації не стимулююча порушення лімітів і т. п. Особливу увагу за Базель II слід приділяти контролю над якістю документів і практиці обробки транзакцій.

Безпосередній процес моніторингу та управління операційними ризиками, знову ж таки на думку Базельського Комітету, повинен грунтуватися на наступних принципах:

1. Банки повинні ідентифікувати та оцінювати операційний ризик у всіх матеріальних продуктах, напрямках діяльності, процесах і системах.

Банки мають забезпечити виконання процедури оцінки операційних ризиків перед запуском нового продукту, напрямки діяльності, процесу або системи.

Втілення цього принципу в життя передбачає аналіз чинників, що негативно впливають на досягнення цілей банку (організаційна структура банку, особливості діяльності, якість кадрів, плинність кадрів та інші; зміни в банківському секторі і технологіях). Інструментами такого аналізу є: семінари з оцінки сильних і слабких сторін системи управління операційним ризиком банку, карта ризику - співвідношення різних підрозділів і процесів з різними компонентами ризику для виявлення слабких місць і організації превентивних дій, розробка системи індикаторів операційного ризику (база даних про втрати, показник плинності кадрів, використання зовнішньої статистики тощо).

2. Банки повинні впровадити процес регулярного моніторингу профілю і позицій з операційного ризику.

Даний принцип передбачає наявність у банку регулярної звітності, істотної інформації Правлінню та Спостережній раді банку, що підтримує активне управління операційними ризиками. Індикаторами раннього попередження для відображення потенційних джерел операційного ризику можуть бути: швидке зростання, введення нових продуктів, частота і тривалість системних збоїв тощо. Частота моніторингу повинна відображати величину ризику і частоту змін в операційному середовищі.

3. Банки повинні мати політику, процеси і процедури для контролю або зниження матеріального операційного ризику.

Даний принцип передбачає те, що банки повинні періодично переглядати свої обмеження по ризику і стратегії з його керування відповідно до свого загального рівня прийнятного ризику і профілю ризику. На практиці, для всіх типів операційного ризику банк вирішує: або знижувати чи контролювати його, чи нести цей ризик. Для ризиків, які не піддаються управлінню, банк повинен вирішити: або приймати його, або знизити рівень діяльності за відповідним напрямом, або зовсім припинити цю діяльність. Обов'язковою аспектом є поділ обов'язків для уникнення конфлікту інтересів. Для ризиків з низькою ймовірністю, але високими збитками

можливе використання страхування. При цьому зниження ризику не повинно підміняти внутрішній контроль.

4. Банки повинні мати план на випадок надзвичайних ситуацій та у продовження операцій для забезпечення своєї діяльності на безперервній основі і для обмеження втрат у випадку серйозних збоїв у бізнесі.

Практична сторона цього принципу передбачає розгляд різних сценаріїв перерв у діяльності, визначення критичних процесів і чисельності персоналу для перенесення на запасний майданчик, вирішення проблеми переносу і збереження фізичних і електронних даних, необхідних для продовження бізнесу.

5. Резервування капіталу.

Необхідність резервування капіталу під операційний ризик може стати для комерційних банків в Україні реальністю вже в найближчі роки, так як це є однією з рекомендацій Базельського комітету. Базельський Комітет виділяє три підходи до оцінки капіталу під операційний ризик.

- Підхід на базі Основного Індикатора (The Basic Indicator Approach).

Відповідно до даного підходу, капітал під операційний ризик резервується на підставі використання єдиного індикатора як достатньої умови для покриття повного операційного ризику інститутів. Як індикатор запропоновано валовий дохід (за винятком несподіваних доходів), при цьому для кожного банку сума капіталу під операційний ризик дорівнює показнику α (встановлений відсоток), помноженому на розмір валового доходу банку. Поточне значення - α, так само 15%. Підхід на базі основного індикатора легкий у застосуванні і його можні універсально використовувати для всіх банків для формування резерву під операційний ризик. Для забезпечення стимулу просування до більш складного підходу, можливе встановлення α на більш високому рівні. Однак, Базельський Комітет очікує, що банки з міжнародними операціями та істотним операційним ризиком будуть використовувати більш складні підходи і при поточному значенні α.

- Стандартизований підхід (The Standardised Approach).

Стандартизований підхід являє собою подальшу розробку еволюційного спектру підходів до визначення розміру капіталу під операційний ризик. Цей підхід

відрізняється від попереднього тим, що діяльність банку як економічної одиниці розділена на безліч стандартизованих ділових одиниць і ділових ліній. Таким чином, стандартизований підхід більше придатний відобразити чим відрізняються профілі ризику банків, обумовлені їх широкими спектрами ділової активності.

Запропоновані ділові одиниці та ділові лінії стандартизованого підходу відображають зібрані послідовним чином ініціативною групою Базельського Комітету дані про внутрішні втрати.

У межах кожної ділової лінії, резерв капіталу розрахований множенням основного фінансового індикатора на β-фактор. β-фактор служить грубим наближенням для виявлення причинно-наслідкового зв'зку між втратами внаслідок операційного ризику в бізнесі для даних ділових ліній і основними фінансовими індикаторами, що представляють діяльність банків за цими діловими лініями. Наприклад, для ділової лінії роздрібних брокерських послуг резерв капіталу був би розрахований таким чином: K = β * Валовий дохід, де K - вимога капіталу для лінії роздрібних брокерських послуг, β-фактор капіталу, який буде застосований для даної ділової лінії (кожен ділова лінія має різний β-фактор), і валовий дохід - індикатор для цієї бізнес-лінії.

Повний резерв капіталу розраховується як просте сумування резервів капіталу для кожної з ділових ліній.

При стандартизованому підході діяльність банку поділяється на вісім бізнес-ліній:

- корпоративні фінанси (corporate finance);
- торговельні операції (trading & sales);
- роздрібні банківські операції (retail banking);
- комерційні банківські операції (commercial banking);
- розрахунково-касові операції (payment & settlement);
- агентські і депозитарні послуги (agency services);
- управління активами (asset management);
- роздрібні брокерські послуги (retail brokerage).

Валовий дохід служить загальним показником масштабу операцій і, отже, очікуваного масштабу операційних ризиків у рамках кожній із бізнес-ліній.

Щоб отримати право на застосування стандартизованого підходу, банк повинен довести органам нагляду, що, як мінімум:

- його рада директорів і старший менеджмент активно беруть участь у нагляді за механізмом управління операційними ризиками;
- він має концептуально надійну і адекватно реалізовану систему управління операційними ризиками;
- він має достатні ресурси для використання підходу в основних бізнес-лініях, а також в галузі контролю та аудиту.

При цьому органи нагляду мають право встановити попередній період, в ході якого зможуть здійснювати моніторинг застосування банком стандартизованого підходу, перш ніж він одержить право на його практичне використання з метою розрахунку регулятивного капіталу.

Також банк повинен розробити конкретні стратегії і мати документовані критерії розподілу валового доходу за поточними бізнес-лініях і видів діяльності в цілях стандартизованого підходу. По мірі появи нових або зміни існуючих видів діяльності критерії повинні перевірятися і корегуватися.

Перевагою даного підходу є врахування специфіки діяльності банку, а відповідно і окремих обсягів наданих послуг з різним діловим лініях при розрахунку резерву капіталу під операційний ризик.

- Підхід вдосконаленого вимірювання (Advanced Measurement Approach).

Підхід вдосконаленого вимірювання забезпечує свободу вибору банку з приводу використання даних про внутрішні втрати. Однак існують кількісні та якісні критерії, за допомогою яких буде оцінюватися підхід, що використовується кожним конкретним банком. Наприклад, наглядові органи вимагатимуть від банків розраховувати нормативи з регулятивного капіталу у вигляді суми очікуваних збитків (ОУ) і непередбачених збитків (НУ), якщо тільки банк не зуміє довести, що його внутрішні методи роботи в достатній мірі враховують ОУ. Тобто, для того, щоб розраховувати свої мінімальні вимоги щодо регулятивного капіталу лише на основі

непередбачуваних збитків, банк повинен переконати свій національний наглядовий орган у тому, що оцінив свою схильність до очікуваних збитків і відзвітував по ній. Також банк повинен довести, що застосовуваний ним підхід враховує так звані «хвостові втрати», тобто великі втрати з низькою ймовірністю. У рамках підходу вдосконаленого вимірювання банку буде дозволено визнавати, що страхування послаблює ризик. Визнання зниження операційного ризику завдяки страхуванню буде обмежено 20% від загальної суми резервування капіталу під операційний ризик.

Серед інструментів страхування (крім поширених серед українських комерційних банків полісів майнового страхування і страхування відповідальност), яке може вважатися фактором, що знижують операційний ризик, великий інтерес викликає поліс BBB (Bankers Blanket Bond) - комплексна програма страхування від злочинів і професійної відповідальності фінансових інститутів .

Для використання підходу вдосконаленого вимірювання банк повинен відповідати наступним якісним стандартам, щоб отримати дозвіл на використання зазначеного підходу для розрахунку капіталу під операційні ризики:

1. Банк повинен мати незалежний підрозділ операційного ризик-менеджменту (функцію), що відповідає за розробку та впровадження механізму управління операційними ризиками. Цей підрозділ проводить розробку і здійснення:

- корпоративної політики, кодифікацію і розробку процедур управління та контролю за операційними ризиками;
- корпоративної методології оцінки операційних ризиків;
- системи звітності про операційні ризики;
- виявлення, оцінки, моніторингу та контролю / зниження операційних ризиків.

2. Внутрішньобанківська система оцінки операційних ризиків має бути тісно інтегрована з поточними процесами управління ризиками в банку, а її результати - складати невід'ємну частину процесу моніторингу і контролю структури операційних ризиків банку.

Наприклад, ця інформація повинна грати суттєву роль при складанні звітів про ризики, управлінських звітів, внутрішньому розподілі капіталу і аналізі ризиків. Банк повинен мати методики розподілу капіталу під операційні ризики основних бізнес-ліній і стимулювання поліпшення корпоративного управління операційним ризиком.

3. Звітність про операційні ризики та збитки повинна регулярно представлятися менеджменту бізнес-підрозділів, старшому менеджменту і раді директорів.

Банк повинен мати процедуру прийняття заходів відповідно до інформації, що міститься в управлінських звітах.

4. Банківська система управління операційними ризиками повинна бути добре документована.

Банк повинен мати механізм дотримання внутрішніх стратегій, процедур контролю та управління операційними ризиками, включаючи заходи на випадок їх недотримання.

5. Внутрішні або зовнішні аудитори повинні регулярно перевіряти процеси управління і систем оцінок операційних ризиків.

Перевіряється діяльність як бізнес-підрозділів, так і самостійного підрозділу з управління операційним ризиком.

Згідно вимог Базеля II внутрішні дані про збитки повинні бути релевантними, тобто чітко прив'язані до поточної ділової діяльності банку, технологічних процесів та процедур управління ризиками. Банк повинен мати документовані процедури оцінки поточної релевантністю історичних даних про збитки, включаючи опис ситуацій, в яких можуть застосовуватися скасування професійних суджень, масштабування або інші коригування, ступінь використання подібних методів, а також особи, уповноважені приймати подібні рішення. При цьому самостійно генеруються оцінки операційних ризиків, які використовуються з метою регулятивного капіталу, повинні бути засновані, як мінімум, на п'ятирічному періоді спостережень внутрішніх даних про збитки, незалежно від використання внутрішні дані про збитки безпосередньо для розробки показника збитків або для його

перевірки. При первісному переході на підхід вдосконалюваного вимірювання допустимо трирічний період.

Базельський Комітет встановив, що банк, який використовує підхід вдосконаюваного вимірювання, повинен бути в змозі продемонструвати, що його підхід враховує потенційно значущі випадки екстремальних збитків. Незалежно від підходу, який використовується, банк повинен продемонструвати, що його показник операційного ризику підтримує стандарт надійності, порівнянних із стандартом IRB-підходу до кредитного ризику (тобто є зіставним з періодом володіння в один рік і 99, 9% - м одностороннім інтервалом впевненості).

Використання зовнішніх баз даних для оцінки екстремальних подій при оцінці рівня операційних ризиків Базельський Комітет допускає використання зовнішніх комерційних баз даних за конкретними фактами реалізації окремих факторів ризику з оцінкою понесених при цьому втрат:

- база компанії NetRisk, заснованої на даних американського банку Bankers Trust (з 1993р.), консорціуму MORE, інших великих банків і фірми PricewaterhouseCoopers;
- інтерактивна база даних Operational Riskdata eXchange Association (ORX) (Zurich) за 10 років. Дані цих баз використовує Базельський Комітет для розрахунку рекомендованих ставок резервування за операційним ризикам.

Власні бази ведуть найбільші IT і аудиторсько-консалтингові компанії, які пропонують свої послуги для складання каталогу операцій банку і його ранжирування за рівнем потенційно притаманних їм категорій операційного ризику.

Одним із найбільш дискусійних моментів Базеля II є запровадження вимоги до утримання банками капіталу на покриття операційного ризику. Ця ідея, вперше була оприлюднена Базельським комітетом у середині 1990 – х років, викликала неоднозначну реакцію банківської спільноти.

Необхідність врахування операційного ризику при оцінці капіталу зумовили гучні банкрутства кількох банків у 1980 – 1990х роках, що постраждали внаслідок проблем із системами внутрішнього контролю та корпоративного управління [12].

Отже, серед основних принципів побудови ефективної системи операційного ризик – менеджменту Базельський Комітет в Угоді Базель II визначив наступні.

Принцип 1. Рада директорів банку повинна бути поінформована про основні аспекти операційного ризику банку як окремої категорії ризику, яка повинна управлятися. Рада повинна затверджувати і періодично переглядати систему управління операційними ризиками банку. Система повинна надати визначення операційного ризику для банку і повинна викладати принципи ідентифікації, оцінки, моніторингу, контролю / пом'якшення:

- внутрішнього шахрайства;
- зовнішнього шахрайства;
- порушення умов праці (втрати через випадки порушення умов праці співробітників, порушення їхнього здоров'я або правил безпеки);
- бізнес практики (втрати через невиконання професійних обов'язків) о шкода, завдана фізичній майну
- нездатності проведення операцій, здійснення бізнесу та збої в системах
- порушення в управлінні керівництвом і процесами.

Принцип 2. Рада директорів банку повинна забезпечити, щоб система управління операційним ризиком була об'єктом внутрішнього аудиту, з незалежним, професійним і компетентним штатом. Внутрішній аудит не несе прямої відповідальності за управління операційним ризиком.

Принцип 3. Вище керівництво банку повинно бути відповідальним за реалізацію завдань системи управління операційним ризиком, схваленої Радою директорів банку. Система повинна бути послідовною, впроваджена по всій структурі банку. Персонал усіх рівнів зобов'язаний розуміти свою відповідальність щодо управління операційним ризиком. Вище керівництво повинно бути також відповідальне за розробку та впровадження політик, процедур, процесів для управління операційним ризиком у всіх істотних продуктах, напрямки діяльності, процесах і системах банку.

Принцип 4. Банки повинні ідентифікувати та оцінювати операційний ризик у всіх істотних продуктах, напрямках діяльності, процесах і системах. Банки мають забезпечити виконання процедури оцінки опреаційного ризику перед введенням нового продукту, напрямків діяльності, процесів або систем.

Принцип 5. Банки повинні впроваджувати процес регулярного моніторингу сукупності параметрів операційного ризику. Також повинен бути забезпечений процес регулярної подачі істотної інформації вищому керівництву банку і Раді директорів банку, що в свою чергу призводить до активного управління операційним ризиком.

Принцип 6. Банки повинні мати політику, процеси і процедури для контролю і / або зниження матеріального операційного ризику. Банки повинні періодично переглядати свої обмеження по ризику і стратегії з управління. Банки повинні регулювати параметри операційних ризику згідно відповідним стратегіям, відповідно до загальної схильності до ризику та його параметрів.

Принцип 7. Банки повинні мати план дій на випадок надзвичайної ситуацій для забезпечення своєї діяльності на безперервній основі і для обмеження втрат у випадку серйозних збоїв у проведенні операцій.

Принцип 8. Банківський нагляд повинен вимагати від усіх банків, незалежно від їх розміру, наявність ефективної системи для визначення, оцінки, моніторингу та управління / зниження матеріального операційного ризику, як частину загального управління ризиками у банку.

Принцип 9. Банківський нагляд повинен проводити, прямо або опосередковано, регулярну незалежну оцінку політик, процедур, і практики банку, пов'язаної з операційними ризиками. Нагляд повинен бути впевнений, що відповідні механізми ефективні.

Принцип 10. Банки зобов'язані публічно розкривати відомості достатні для того, щоб учасники ринку могли дати оцінку підходу банку до управління операційним ризиком.

1.3 Складові операційного ризику

У науковій літературі немає однозначної позиції щодо класифікації операційних ризиків, але більшість учених розділяє операційний ризик на наступні чотири категорії:

- ризик персоналу;
- ризик систем і технологій;
- ризик бізнес – процесів;
- ризик зовнішнього середовища функціонування банку.

Класифікатор операційного ризику повинен мати форму, яка найбільш проста і допоможе мінімізувати цей ризик. Операційні ризики є динамічними і постійно мінливими в залежності від стратегії, бізнес-процесів і технологій, конкурентного середовища тощо. Операційні ризики є ризиками ендогенного характеру, і, отже, різні для кожного суб'єкту господарювання чи фінансової установи. Вони залежать від технологій, процесів, управління персоналом і організаційної культури. Існує необхідність збирати конкретні дані для суб'єкту господарювання чи фінансової установи, оскільки використання загально-статистичних даних може бути не зовсім доречно.

Визначення поняття «операційний ризик» запропоноване Базельською угодою, дає підстави розуміти, що по суті, - це ризик появи пограбувань, шахрайства, стихійних лих, помилок персоналу, помилок трансакцій тощо. У це визначення також входять юридичний ризик, стратегічний ризик та ризик репутації (хоча Базельська угода й не включає останній) [13].

Безперечно, що всі ризики - взаємозалежні.

Основними видами операційних ризиків є:

- технологічний ризик збоїв обладнання;
- технологічний ризик збоїв програмного забезпечення та інформаційних технологій;
- методичний ризик помилкової методології здійснення того чи іншого процесу;

- організаційний ризик невірної (помилковою) організаційної структури банку;
- ризик персоналу;
- правовий ризик в частині невідповідності документів банку з чинним законодавством, нормативними документами регулюючих органів;
- ризик зовнішніх джерел впливу на об'єкти, активи, процеси і технології банку;
- ризики помилок управління і неправильних рішень;
- ризики виникнення несприятливих подій через неефективних процедур внутрішнього контролю;
- ризики операційних збоїв і помилок інформаційного взаємини до контрагентами / користувачами.

Ризик неадекватних процедур внутрішнього контролю виявляється на наступних факторах:

- неповноти процедур контролю та авторизації поточних операцій;
- неадекватна система обліку та реквізитів звітності;
- неадекватність структури звітної інформації;
- неадекватна система контролю за прийнятими ризиками;
- ігнорування принципу розмежування конфлікту інтересів.

Прикладом такого ризику є ситуація, коли співробітники нью-йоркського відділення французького банку БіЕнПі Паріба (BNP Paribas) Едвард Кенел і Майкл Коноллі, що працюють у відділі облігацій, користувалися службовим становищем, щоб спершу продати за заниженою ціною цінні папери власним фірмам, а потім реалізовували їх на свою користь за ринкових котирувань.

Працювала й інша схема, коли покупцям через ці фірми продавалися високо ризиковані активи близьких до банкрутства компаній за цінами, що не враховує цих ризиків.

Кенел і Коноллі відразу після арешту повернули 8 млн. доларів США з привласнених 12.2 млн. доларів США. Почали вони свій проект у червні 2001 року, коли ними були засновані дві нью-йоркські «інвестиційні» компанії Хідра Кепітал

(Hydra Capital) і Бреф Ессоciейтс (Brel Associates). Можливість здійснення всіх махінацій виявилося можливим завдяки тому, що всі операції проводилися через Федеральний резервний банк Сан-Франциско. Через те що цей банк не зберігає рапорти і звіти, що надходять з банків Нью-Йорка. Виявити шахрайство допомогла аудиторська перевірка в лютому 2004 р. [14].

Часто з операційним ризиком пов’язують ризик репутації – ушкодження репутації та втрати існуючого і майбутнього бізнесу внаслідок операційного інциденту після надходження інформації про інцидент зовнішнім зацікавленим особам (наприклад, пресі, аналітикам, клієнтам).

Ризик репутації є ризиком другого порядку, оскільки він є похідним від операційного інциденту, а не власне інцидентом; крім того, його наявність залежить від того, чи вийшла інформація за межі суб’єкту господарювання.

Потенційний обсяг ризику репутації важко оцінити кількісно, оскільки він трапляється зрідка, а фінансові наслідки набувають форми втрати бізнесу та клієнтів. Одним із шляхів до вимірювання цього ризику є аналіз вартості суб’єкту господарювання на фондовому ринку одразу ж після інциденту та його порівняння зі змінами ціни на акції конкурентів.

Ризик репутації впливає на спроможність банку встановлювати нові відносини з контрагентами, надавати нові послуги або підтримувати існуючі відносини. Цей ризик може привести банк (або його керівників) до фінансових втрат, зменшення клієнтської бази та до притягнення до адміністративної, цивільної чи кримінальної відповідальності.

На сьогоднішній день, операційні ризики найбільш доцільно класифікувати за такими складовими:

1) ***ризик персоналу*** – ризик втрат, пов'язаний із можливими помилками співробітників, шахрайством, недостатньою кваліфікацією персоналу, можливістю несприятливих змін у трудовому законодавстві тощо;

Даний вид ризиків неможливо уникнути, адже завжди є загроза помилок персоналу та зловживань. З метою мінімізації цього ризику в банку необхідно

створити систему якісного відбору, підготовки та перепідготовки фахівців та створити умови для мінімізації зловживань працівниками.

Навчання та підвищення кваліфікації співробітників має проводитися не рідше чим раз на рік. Воно обов’язково повинно включати в себе:

а) заходи по організації навчання співробітників залежно від їх посадових обов'язків;

б) ознайомлення співробітників з фактами операційних ризиків і законодавством україни ;

в) ознайомлення співробітників з нормативними документами банку з питань операційних ризиків з метою роз'яснення співробітникам банку їхніх дій.

Для підвищення власної кваліфікації - співробітники спеціалізованих відділів з організації та управління операційним ризиком повинні брати участь у семінарах і конференціях які освітлюють теми операційних ризиків.

Суттєвими чинниками ефективного управління ризиками у банках є високий професійний рівень та належна ділова репутація керівництва і персоналу. З метою зменшення ризиків персоналу, в банках необхідно розробити і запровадити вимоги до працівників банків та заходи внутрішнього контролю, які забезпечували б належне дотримання вимог законодавства, виконання договірних та інших зобов’язань, дотримання відповідної ділової поведінки.

Працівники банківських установ, які безпосередньо обслуговують клієнтів мають усвідомлювати свою відповідальність, бути обізнаними з внутрішніми процедурами банку.

Керівникам банківських установ та працівникам служби безпеки необхідно звертати увагу на працівників, які:

- раптово почали вести інший (більш розкішний) спосіб життя та не беруть відпусток;
- досягли за короткий термін різкого, неочікуваного зростання обсягів продажу;
- відмовляються від зміни посадових обов’язків, наприклад, підвищення по службі.

Вищевказані ознаки можуть свідчити про те, що згадані працівники можуть нести додаткову загрозу для збільшення обсягів операційного ризику [15].

Отже, для мінімізації ризику персоналу необхідне:

- постійне підвищення стандартів обслуговування і регулярний моніторинг якості обслуговування клієнтів;
- розробка системи підтримки фронтофісу через call-центр;
- впровадження системи протидії шахрайству;
- розподіл прав доступу в інформаційних системах та дотримання правил інформаційної безпеки;
- впровадження ефективної системи мотивації персоналу;
- аналіз хронометражу надання послуг клієнту (порівняння нормативного значення з фактичним);
- створення «єдиного вікна обслуговування» для співробітників фронт-офісу (у випадку, якщо банк використовує кілька різнорідних інформаційних систем);
- постійний аналіз показників з управління персоналом (плинність кадрів, кількість навчених співробітників тощо).

2) ***ризик процесу*** – ризик втрат, пов'язаний із помилками в процесах проведення операцій і розрахунків за ними, їхнього обліку, звітності, ціноутворення тощо;

Ризик процесу є одним із найбільш небезпечних операційних ризиків, адже його ігнорування або недостатня увага до цього виду ризику може призвести до значних фінансових та не фінансових втрат банку. Для мінімізації цього виду ризику необхідно постійно вдосконалювати процеси проведення операції та переглядати їх на предмет підвищеної ризикованості та збоїв.

Отже, з метою зменшення рівня ризику процесу в банках необхідне:

- впровадження процесного підходу (структурування бізнесу на процеси, опис процесів, визначення власників процесів, нейтралізація «зон безвідповідальності», своєчасна актуалізація внутрішньої нормативної документації тощо);

- формування електронної бази бізнес-процесів, які підтримуються в актуальному стані;
- впровадження системи моніторингу показників діяльності на щоденній основі (застосування ключових індикаторів ризику в рамках загальної системи моніторингу показників банку);
- аналіз організаційної структури банку;
- впровадження системи розробки (від ідеї до введення в дію) додаткових процесів і нових продуктів;
- впровадження системи визначення пріоритетності автоматизації процесів (з урахуванням ризиків);
- створення єдиного сховища даних і формування на його основі ERP-системи, системи бізнес-аналізу (Business Intelligence, BI)
- посилення внутрішнього контролю бізнес-процеси.

3) ***ризик технологій*** – ризик втрат, який обумовлений недосконалістю технологій, що використовуються, тощо;

Ризик технологій можна мінімізувати шляхом постійного моніторингу та подальшого впровадження нових, більш ефективних та якісних банківських технологій. Банку необхідно визначити програму оновлення технологій та неухильно її дотримуватися.

З метою зменшення ризику технологій у комерційних банках необхідно:

- вести оперативний облік інформаційних активів (інформаційні системи, обладнання, канали зв'язку);
- формувати плани відновлення ІТ-сервісу;
- впроваджувати системи оперативної заміни обладнання, системи резервування каналів зв'язку, системи Help-Desk, віртуалізації серверів;
- впровадження проектного підходу до діяльності підрозділу, який відповідає за доопрацювання використовуваного програмного забезпечення і розробку нового;

- впровадження сервісного підходу до діяльності підрозділу, який відповідає за обслуговування IT-сервісів (інформаційних систем) (IT Service Management, ITSM);
- чіткий поділ функцій між відділами, що займаються розробкою програмного забезпечення та обслуговуванням інформаційних систем.

4) ***ризики середовища*** – ризики втрат, пов'язані з не фінансовими змінами в середовищі, в якому діє суб'єкт господарювання, – змінами в законодавстві, політичними змінами, змінами системи оподатковування тощо;

Для мінімізації цього виду ризику необхідно створювати більш гнучку систему управління у банку, яка мінімізує зовнішні впливи на його діяльність та визначати декілька сценаріїв поведінки зовнішнього середовища, які будуть прийнятні для банку під час здійснення банківської діяльності. Також необхідно диверсифікувати зовнішні впливи на банк шляхом прогнозування.

Основними заходами для зменшення ризику зовнішнього середовища у комерційному банку мають стати наступні:

- комплексне страхування бізнесу;
- впровадження системи забезпечення безперервності діяльності та / або відновлення діяльності банку у випадку виникнення непередбачених обставин;
- підвищення фізичної безпеки об'єктів банку;
- підвищення інформаційної безпеки банку;
- підвищення організаційної безпеки банку.

Представлені вище проекти можуть бути як взаємодоповнюючими, так і взаємовиключними.

5) ***ризики фізичного втручання*** – ризики втрат, пов'язані з безпосереднім фізичним втручанням у діяльність суб'єкти господарювання: стихійними лихами, пожежами, пограбуваннями, катастрофами, терористичними актами, землетруси, цунамі тощо.

Ризики зовнішнього втручання майже неможливо передбачити і з огляду на це вони є досить небезпечними.

Яскравим прикладом ризику зовнішнього втручання стали терористичні акти в США 11 вересня 2001 року, внаслідок яких 85 млн.доларів США прямих збитків зазнав лише банк Нью-Йорка.

Ряд зарубіжних фінансових інститутів використовує класифікацію операційних ризиків (ОР), запропоновану Бенкер Траст (Banker Trust), яка складається з наступних категорій:

- ***ризик персоналу*** - всі ризики, які пов'язані зі співробітниками компанії, зокрема їх несанкціоновані дії, недостатня компетентність, залежність від окремих фахівців і т.п.;
- ***технологічний ризик*** - ризик, викликаний збоями і відмовами інформаційних систем, програм або баз даних, систем передачі інформації та іншого устаткування, необхідного для діяльності банку;
- ***ризик фізичної шкоди*** - ризик, який настає в результаті природних катастроф та інших факторів, які можуть завдати шкоди основного обладнання, систем, технологій і ресурсів банку. Такий ризик зазвичай мінімізується шляхом страхування майна.;
- ***ризик взаємин*** - ризик, який настає в результаті виникаючих відносин при здійсненні бізнес - процесів, таких як труднощі при взаємодії з клієнтами і недостатність внутрішнього контролю;
- ***зовнішній ризик*** - ризик настає у результаті злочинних дій сторонніх організацій, фізичних осіб, а також в результаті змін вимог регулюючих органів.

Управління цими ризиками включає в себе чотири основні функції:

- визначення схильності до ризику та вибір «профілю ризику» (стратегії) банку за видами бізнесу та регіонам;
- управління профілем ризику на рівні окремих напрямків бізнесу;
- створення інформаційної системи підтримки прийняття рішень для керівництва, що дозволяє контролювати хід діяльності;

- впровадження системи оцінки результатів діяльності відповідальних осіб, яка створювала б дієві стимули до відмови від неприйнятного і неприбуткового ризику.

У більшості українських банках існує наступна система класифікації операційних ризиків:

- **ризик пов'язаний з діями працівників і безпекою робочого місця** – всі ризики, які пов'язані з працівниками банку, зокрема, їх несанкціоновані дії, недостатня компетентність, залежність банку від окремих фахівців ,травми які виникають на робочому місці в наслідок халатності, або недотримання умов безпеки праці;
- **ризик пов'язаний з роботою систем і технологій** – ризик, пов'язаний з перебоями і відмовами інформаційних систем, програм або баз даних, систем передачі інформації та обладнання, необхідного для діяльності банку;
- **ризик помилки у банківських процесах –** ризик неузгоджених, або хибних бізнес процесів, методологічних помилок або неузгодженості документів, відсутність повної нормативної бази, недостатність внутрішнього контролю, неузгодженість дій при здійсненні операцій, тощо
- **ризик пов'язаний з зовнішніми чинниками** – ризик втрат пов'язаний з діями третіх осіб , включаючи зовнішнє шахрайство, а також ризик який виникає в наслідок природних катастроф, та інших факторів, які можуть нанести збитки основному устаткуванню, системам, технологіям і ресурсам банку.

1.4 Методологічні основи управління операційним ризиком в комерційному банку

Основною методологічною сутністю управління операційним ризиком є орієнтація на запобігання негативних наслідків, які можуть відбутися у процесі

поточної діяльності та на контроль за бізнес процесами, за їх відповідністю вимогами безпеки банківської діяльності.

Методологія управління операційним ризиком базується на основі визначення категорії «операційний ризик» як ризику прямих або непрямих збитків, які є наслідком неадекватних або неправильно функціонуючих внутрішніх процесів, персоналу, систем та змін зовнішнього середовища.

Методологічна основа управління операційним ризиком у банку проявляється із того що даний вид ризику поділяється на ризик операційних помилок (внутрішній тип ризику) та операційний стратегічний ризик (зовнішній тип ризику).

Якщо причиною настання внутрішніх операційних ризиків є людський, процесний або технологічний фактор, то причиною настання зовнішніх ризиків є політичні, природні, податкові, регулятивні, соціальні фактори та конкуренція на ринку [11].

Належна практика управління операційним ризиком, що є прийнятною для західної економічної традиції, складається з таких 10 аспектів:

Аспект 1. Структура корпоративного управління банку визначає її «апетит до ризику». Система ризик менеджменту має охоплювати усі елементи ризику і забезпечувати як оцінку, так і управління ризиком.

Основним інструментом управління операційним ризиком має стати адекватна для кожного банку та середовища, в якому він працює, політика управління ризиками.

Аспект 2. Управління ризиком і його кількісна оцінка мають складатися з таких компонентів як:

- планування неперервності банківської діяльності ;
- аутсорсинг;
- юридичні аспекти;
- питання дотримання законодавства;
- інформування зацікавлених осіб;
- злиття та поглинання.

Аспект 3. Банк повинен мати чітку стандартизовану систему управління ризиками, що ґрунтується на конкретних задачах з управління операційним ризиком.

Інструментом такої системи мають стати:

- політика управління ризиком;
- документи нижчого рівня;
- регламенти операцій.

Аспект 4. Для належного управління операційним ризиком необхідно мати:

- чітко визначених осіб, відповідальних за операційні ризики;
- чіткі ліміти наданих повноважень;
- конкретних осіб, відповідальних за дотримання вимог законодавства, внутрішніх регламентів та правил, які регулюють питання управління операційними ризиками у банку;
- періодичні незалежні перевірки.

Аспект 5. Програма управління операційними ризиками повинна пройти «дослідну експлуатацію», тобто стати невід'ємною частиною комерційної діяльності банку в цілому, при цьому:

- жоден із напрямків діяльності не повинен бути вільним від дотримання політики і правил;
- необхідно використовувати інформацію, що отримується за допомогою зворотного зв'язку з бізнес – підрозділами для забезпечення безперебійної та ефективної роботи.

Аспект 6. Управління операційним ризиком не має стати самостійним напрямом роботи банку, а бути процесом, що є взаємоузгодженим із іншими процедурами і дає інформацію про:

- природу ризиків;
- кількісний вимір ризику;
- напрями управління ризиком.

Аспект 7. Процес управління операційним ризиком має підкріплюватися надійною, достовірною, повною та своєчасною звітністю.

Аспект 8. При оцінці наслідків збитків від операційного ризику мають бути враховані усі відповідні елементи, зокрема:

- зусилля на ліквідацію наслідків;
- втрачений час;
- вплив на залежні бізнес – процеси;
- компенсаційні виплати.

Аспект 9. Система оцінки результатів управління операційним ризиком та система винагороди, що використовується, має відображати загальну культуру управління та сприяти дотриманню прийнятного рівня ризику.

Аспект 10. При управлінні операційним ризиком кожен співробітник банку або його представник має вважатися ризик – менеджером.

В той же час керівники найвищого рівня повинні розуміти, що на них покладено обов'язки із управління ризиками та відповідальність за їх виконання.

Методологія управління операційним ризиком відображена на рис. 1.3.

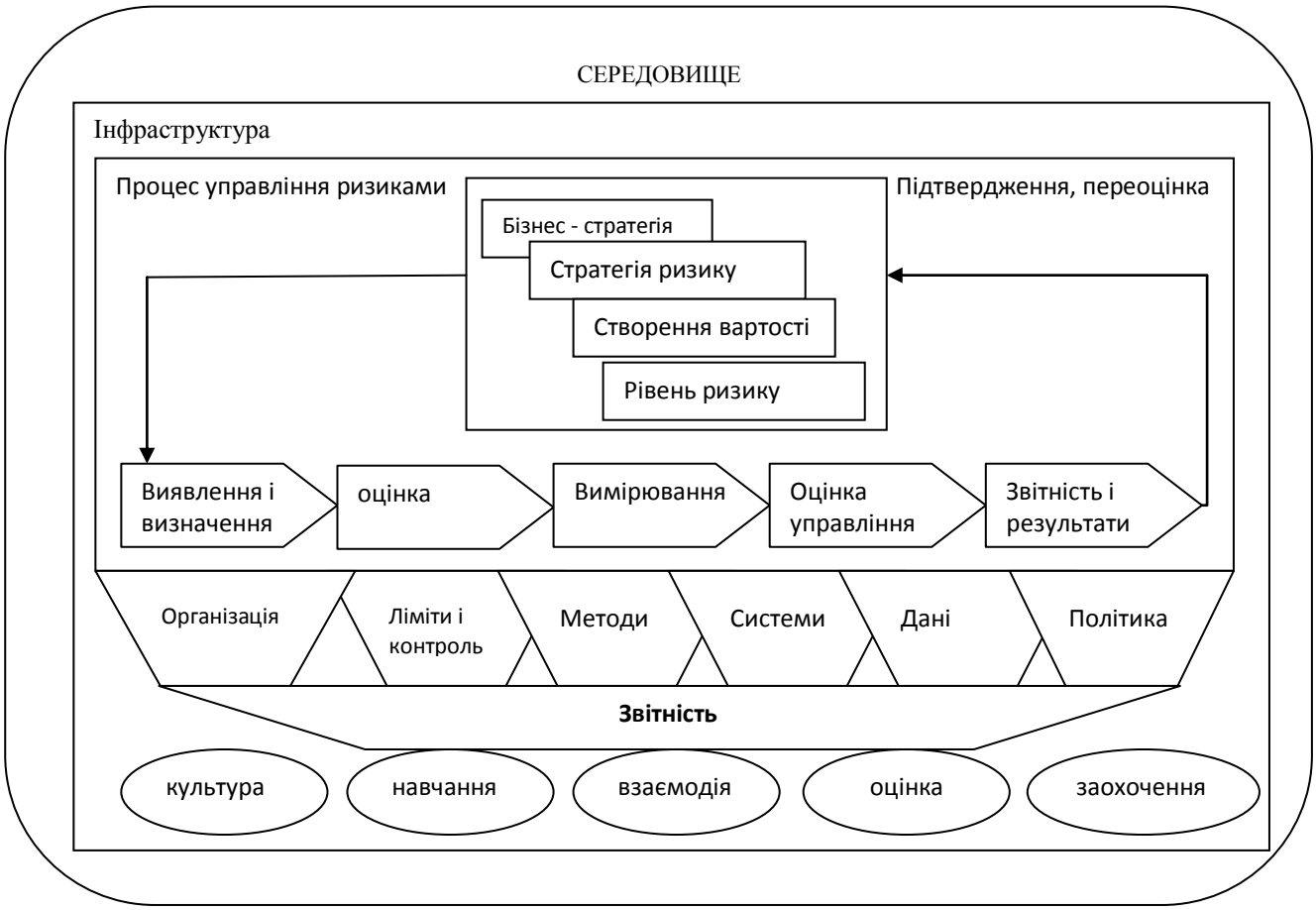


Рис. 1.3 Методологія управління операційним ризиком у банку

Як видно із цієї схеми, логіка методології управління операційним ризиком у комерційному банку базується на взаємозалежності ряду факторів зовнішнього та внутрішнього середовища. Процес управління операційним ризиком має базуватися на бізнес – стратегії банку, стратегії ризику, створенні вартості та рівні ризику.

Головними стадіями процесу управління ризиком є визначення і виявлення ризиків, їх оцінка, вимірювання, оцінка управління ним та звітність і результати управління.

Побудова ефективного процесу управління ризиками є неможливою без наявності взаємоповязаної системи організації такого управління та наявності єдиної політики управління операційним ризиком.

Ефективність системи управління операційним ризиком значною мірою залежить також від таких факторів, як культура банку, навчання працівників, взаємодія у підрозділах, оцінка якості управління та належної системи заохочення та стимулювання працівників.

Взаємозвязок різних факторів при формуванні ефективної системи управління операційним ризиком відображено на рис 1.4.

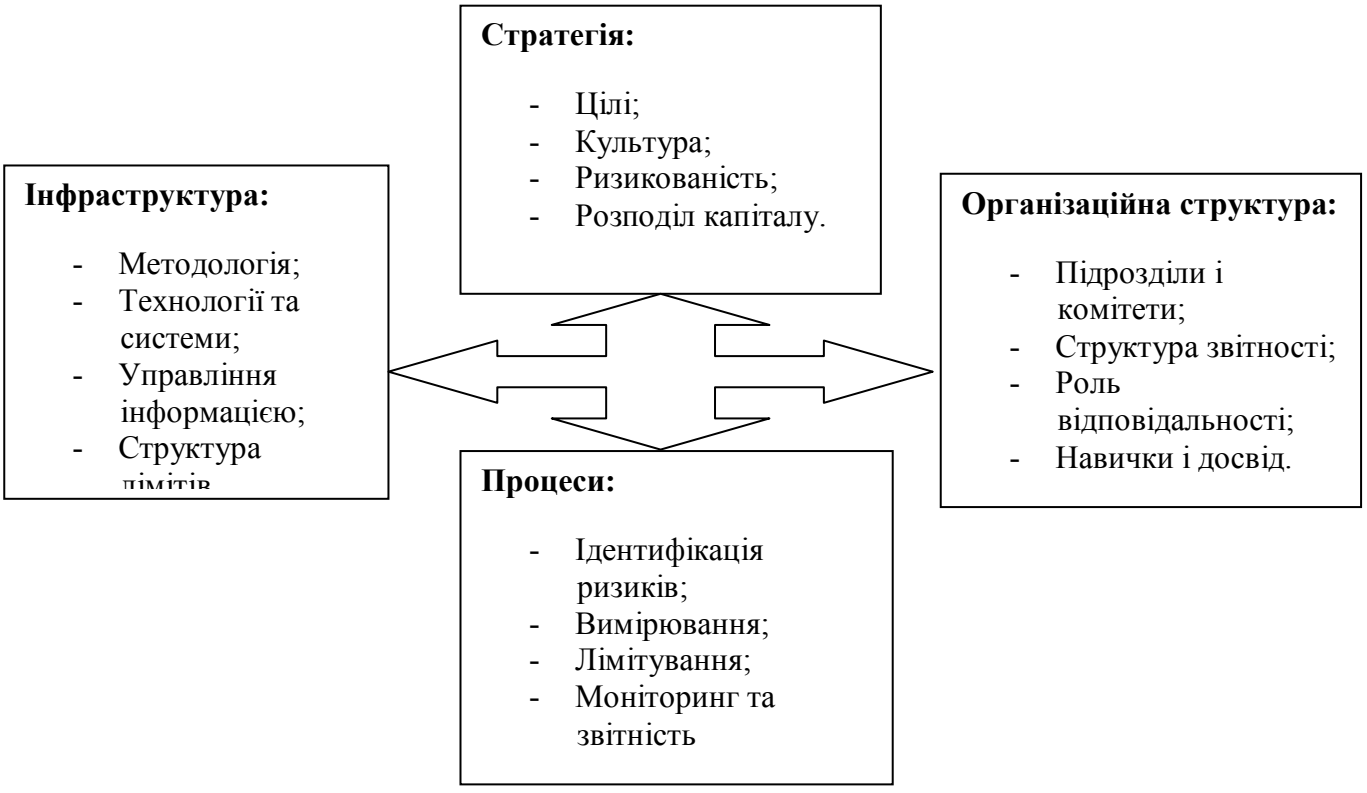


Рис.1.4 Методологія аналізу системи управління ризиками

Ефективна система управління операційним ризиком повинна пройти декілька етапів еволюції. Зокрема це видно з даних рис.1.5.

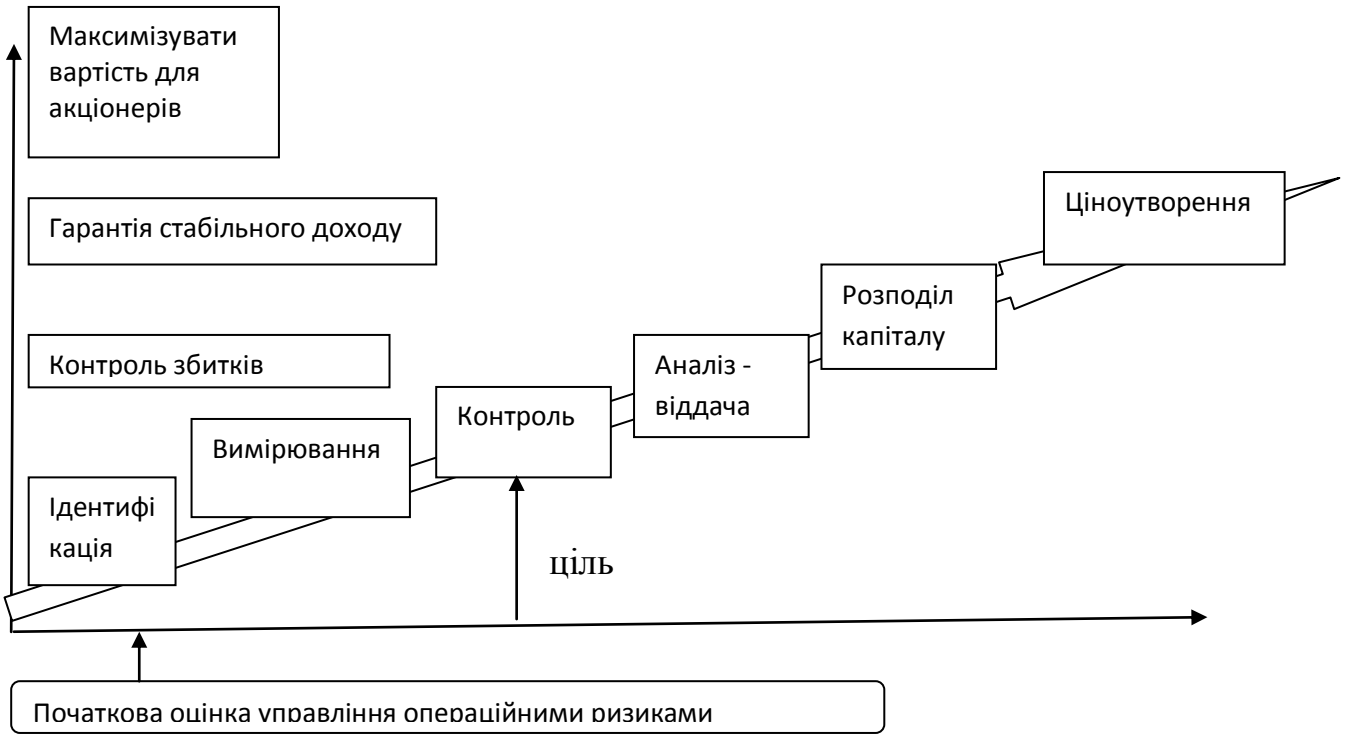


Рис.1.5 Еволюція системи управління операційним ризиком

Як видно із поданої схеми, система управління операційним ризиком може ускладнюватись в процесі розвитку. І залежно від досягнутого рівня складності такої ситеми, виникає потреба у відповідних інструментах управління.

У банківській справі основними інструментами управління банківських ризиків є:

- мінімальний розмір капіталу для новостворюваних банків;
- вимоги до складу й нормативи достатності капіталу;
- стандарти організації й діяльності служб внутрішнього контролю й управління ризиками;
- вимоги до розкриття інформації про фінансовий стан і загальний ризик банку;
- нормативні вимоги до методик кількісної оцінки ризику тощо.

На рівні банків поряд із зовнішніми використовуються 6 основних механізмів управління фінансовими ризиками [16]: стратегія уникнення ризику, лімітування, страхування, диверсифікація, управління активами і пасивами, хеджування.

Водночас, управління операційним ризиком потребує мінімізації ризиків з урахуванням впливу зовнішнього середовища й специфіки діяльності банка покликана саме система управління ризиками, наявність якої є обов'язковою умовою успішної стратегічної діяльності банківської установи. Наявність такої системи часто дозволяє уникати значних втрат.

Згідно з нормативними документами Національного банку України управління ризиками – це процес, за допомогою якого банк виявляє (ідентифікує) ризики, проводить оцінку їх величини, здійснює їх моніторинг і контролює свої ризикові позиції, а також враховує взаємозв'язки між різними категоріями (видами) ризиків.

Комплекс дій з ризик-менеджменту має на меті забезпечити досягнення таких цілей:

- ризики мають бути зрозумілими та усвідомлюватися банком та його керівництвом;
- ризики мають бути в межах рівнів толерантності, встановлених спостережною радою;
- рішення з прийняття ризику мають відповідати стратегічним завданням діяльності банку;
- рішення з прийняття ризику мають бути конкретними і чіткими;
- очікувана дохідність має компенсувати прийнятий ризик;
- розподіл капіталу має відповідати розмірам ризиків, на які наражається банк;
- стимули для досягнення високих результатів діяльності мають узгоджуватися з рівнем толерантності до ризику.

З точки зору сучасного ризик-менеджменту, банківська діяльність зводиться до прийняття певного обсягу ризику й отримання за це відповідної компенсації (економічної вигоди).

Одним з актуальних питань сучасного банківського ризик-менеджменту в світі є питання про наявність системи інтегральної оцінки ризику. Дослідження в

українських банках вказує на суттєве відставання в організації ефективних систем ризик-менеджменту.

Так, переважна більшість банків (80%) станом на 2008 рік використовує системи ризик-менеджменту, за яких ризики оцінюються окремо за кожною категорією. Експерти цих банків вказують на відсутність потреби в інтегральній оцінці ризиків банку. В кращому випадку вони планують впровадження інтегральної системи оцінки ризиків у майбутньому. Причиною даної ситуації є неповне розуміння функцій відділів ризик-менеджменту, частково обумовлене невисоким рівнем розвиненості фінансової системи в цілому [11].

Дослідження, проведене у 2005 році компанією Ернст енд Янг (Ernst & Young), як провідних практиків в галузі управління ризиком показало, що 59% головних виконавчих директорів та фінансових директорів провідних банків світу визнали, що вони не мають комплексного бачення процесу управління своїми ключовими ризиками. Що стосується організаційної структури, то більшість повідних компаній світу мають не менш ніж 10 відділів, що виконують різні функції ризик-менеджменту незалежно один від одного. Спостережні ради та аудитори піддаються більшому контролю з приводу нагляду за управлінням ризиками.

Сьогодні, управління ризиком зводиться до трьох ключових питань, на які треба відповісти:

- Чи ми приймаємо той ризик, який варто приймати?
- Чи ми приймаємо той обсяг ризику, який варто приймати?
- Чи адекватно ми керуємо нашим ризиком?

Відповідь на питання «Чи ми приймаємо той ризик, який варто приймати?» передбачає визначення наступних відповідей:

- Як пов'язані ті ризики, які ми приймаємо, з нашими стратегіями та цілями?
- Чи ми знаємо значні ризики, які приймаємо?
- Чи ті ризики, які ми приймаємо, пов'язані з тією діяльністю, яка створює вартість?
- Чи ті ризики, які ми приймаємо, дають нам конкурентні переваги?

Відповідь на питання «Чи ми приймаємо той обсяг ризику, який варто приймати?» передбачає оцінку таких факторів:

- Чи ми отримуємо дохід, який відповідає загальному рівню ризику?
- Стимулює наша організаційна культура належний рівень прийняття ризику чи навпаки?
- Чи було піддано нашу готовність приймати ризик кількісній оцінці як у загальному обсязі, так і в розрізі окремих випадків?
- Чи відповідає фактичний рівень ризику нашій готовності приймати ризик?

Для відповіді на питання «Чи адекватно ми керуємо нашим ризиком?» потрібно проаналізувати наступне:

- Чи узгоджено наш процес управління ризиком з процесом ухвалення стратегічних рішень та існуючими показниками ефективності?
- Чи є процес управління ризиком скоординованим та єдиним в усій компанії? Чи всі використовують одне й те саме визначення ризику?
- Чи маємо ми випадки браку та/або дублювання в тому, що стосується ризиків?
- Чи є наш процес управління ризиком ефективним з точки зору витрат?

У своїй праці «Управління ризиком у XXI сторіччі» відомий економіст Т. Стюарт стверджує, що «управління ризиком – це усунення ризиків». Виходячи з даної позиції можна припустити, що ризик, по суті має позитивні сторони, адже він неодмінно пов'язаний із прибутком, а в питаннях управління ризиком головне – не усувати його, а управляти ним.

Однок, існування ризику не обов'язково є причиною для занепокоєння. Ризики вважаються виправданими, якщо вони є зрозумілими, контрольованими, такими, які можна виміряти, і що відповідають здатності банку швидко реагувати на негативні обставини. Невиправданий ризик може випливати із навмисних або ненавмисних дій. Якщо ризики є невиправданими, ризик-менеджери мають взаємодіяти із керівництвом і спостережною радою банку, спонукаючи їх до пом'якшення або усунення цих невиправданих ризиків. Заходи, які в такому разі має здійснити банк, включають зменшення сум під ризиком, збільшення капіталу або зміцнення процесів управління ризиками. Саме тому, важливо визначити, на що робити ставку, а чого варто взагалі уникати.

ІІ. УПРАВЛІННЯ ОПЕРАЦІЙНИМ РИЗИКОМ У КОМЕРЦІЙНОМУ БАНКУ

2.1 Внутрішня система управління операційним ризиком

В даний час існує багато методів управління операційним ризиком у банку. Але їх основним недоліком є складність в застосуванні в реальних українських умовах. Як правило, в документах Базельского комітету з банківського нагляду основний акцент робиться на резервуванні капіталу під операційний ризик. Але мало хто задається питанням що сліпе копіювання при побудові системи операційних ризиків, мало підходить для України з огляду на особливості ведення банківського бізнесу, законодавство та стан розвитку банківської ситеми України.

Також не можна забувати що операційні ризики - це той вид діяльності, що практично не регулюється чинним законодавством України. Часто навіть досвідчені менеджери українських банків плутаються в поняттях, починаючи з визначення операційного ризику (він же операційно-технологічний, згідно нормативних актів Національного банку України) та терміну «комплаєнс[2]».

Операційний ризик-менеджмент, на думку Р.Чепмана, дає такі переваги в бізнесі:

- покращення можливостей для досягнення бізнес-цілей;
- дає можливість керівникам суб’єкта господарювання зосередитись на доходній діяльності;
- мінімізація повсякденних втрат;
- забезпечення більш надійної системи управління ризиками у суб’єкті господарювання;
- сприяння у створенні системи, яка б дозволила зрозуміти зв'язок між різними класами ризиків, та, відповідно, їх моделювати.

[2] Від англ. compliance – можна перекласти як нормативно-правова відповідність. Більше того, в системі комплайєнсу часто значне місце відводять протидії легалізації коштів, отриманих злочинним шляхом, та фінансування тероризму.

Відомо, що управління в теорії менеджменту розглядається як функція. У той же час зауважимо, що управління ризиками представляє собою безперервний процес, який базується на ідентифікації ризиків, їх оцінці, прийнятті рішень та моніторингу. Більше того, ми вважаємо, що управління - це системний процес, тобто управління операційними ризиками представляє собою певну систему з відповідним набором елементів.

У сучасному мінливому середовищі, в умовах світової економічної та фінансової кризи для ведення бізнесу необхідний новий підхід до управління операційними ризиками. Зокрема, керівники банків повинні приділяти більше уваги управлінню ризиками для стратегічної переваги. Взаємодія між традиційною практикою ризик-менеджменту та операційним менеджментом не відповідає сьогоденню, оскільки управління ризиками носило здебільшого оборонний характер, зосередивши основну увагу на небезпеці ризику, а не на потенціалі зростання при правильному підході до прийняття ризиків.

Оскільки темпи змін продовжують прискорюватися, кризові явища в світовій економіці загострюються, тому багато суб'єктів господарювання почали розуміти, що вони більше не можуть дозволити собі приймати виключно оборонну позицію щодо ризику. Хоча схеми контролю є першим необхідним кроком в управлінні ризиками. В даний час багато суб'єктів господарювання повинні управляти ризиком для отримання стратегічної переваги, підвищення задоволення потреб клієнтів і збільшення акціонерної вартості.

Темпи змін є однією з найбільш важливих проблем, що стоять перед керівництвом суб'єктів господарювання у XXI столітті. Зміна і ризик вже давно вважаються нероздільними категоріями. У більшості людей існує вроджена неприязнь до змін. Серед двигунів змін, які підсилили схильність суб'єктів господарювання до операційних ризиків в більшості секторів промисловості, можна виділити такі: глобалізація, світова економічна та фінансова кризи, зростання електронного бізнесу, конкуренція, збільшення регулювання, зростаюче усвідомлення неможливості страхування певних ризиків, збільшення кількості судових процесів.

Типова програма управління операційними ризиками, що зосереджена на наданні допомоги організації в набутті операційної цілісності та в досягненні цілей, як правило, охоплює широкий спектр діяльності, у тому числі:

- визначення сфери операційного ризик-менеджменту;
- розробка і впровадження необхідних функцій і обов'язків, звітності;
- визначення категорій операційних ризиків, їх пріоритетності та відображення даних ризиків поряд з бізнес-процесами для вивчення їх впливу;
- робота по закріпленню кожного ризику за конкретним підрозділом ланки бізнесу (центрами відповідальності);
- надання допомоги підрозділам ланки бізнесу щодо виявлення операційних ризиків та впровадження необхідного контролю;
- впровадження необхідних заходів, методів та інструментів.

Одним із ефективних способів вивчення операційних ризиків є аналіз ймовірних наслідків збоїв у тих чи інших процесах, зокрема:

- прямі фінансові втрати, які виникають в результаті невиконання зобов'язань (наприклад, штрафи або реституційні витрати);
- прямі фінансові втрати, зумовлені відсутністю доходів (наприклад, втрати від продаж, плата за трансакції, комісійні);
- заходи впливу, що передбачені законодавством та нормативними документами, починаючи від попередження до відкликання ліцензій;
- інші втрати, що можуть виникати, наприклад, у зв'язку з негативною інформацією, зупинкою торгівельної діяльності, затримками в певних процесах, неякісними товарами або послугами.

Побудова профілю операційних ризиків, тобто цілісної картини операційних ризиків, яка базується на різноманітних джерелах їх виникнення, є одним із результатів ефективного операційного ризик-менеджменту, що дає чітке уявлення про ризики, які стоять перед суб’єктом господарювання .

Сучасні складні системи управління операційними ризиками вимагають застосування прогностичних моделей ризику, що дадуть можливість керівникам

суб’єктів господарювання отримувати важливу інформацію для прийняття стратегічних рішень. Так, моделювання ризику, пов’язаного з поточними операціями у фінансовій сфері, розпочалося з банків. Найважливішою передумовою моделювання ризиків є наявність статистичних даних про об'єкт моделювання, що для операційних ризиків є серйозною проблемою. Пояснюється це малою частотою прояву значної частини операційних ризиків. Так, наприклад, зовнішнє шахрайство може в середньому зустрічатися 1-2 рази на рік. Внаслідок цього, створення статистичної бази за випадками зовнішнього шахрайства у конкретному банку вимагатиме досить тривалого періоду часу. Побудова ж статистичної бази в рамках всієї банківської системи чи її частини є проблематичною задачею через приховування банками подібних випадків. Окрім цього, обґрунтування висновків із статистичної бази, створеної на основі даних з усієї банківської системи, може бути не завжди коректним для окремого банку.

Сьогодні у світі приділяється значна увага питанню створення високоякісної бази даних щодо операційних втрат у фінансовій сфері. Зокрема, у 2002 році засновано провідний світовий консорціумом по збору статистичних даних щодо операційних втрат у фінансовій сфері The Operational Riskdata eXchange Association (ORX). Головною метою ORX є створення платформи високої якості для безпечного та анонімного обміну даних про втрати, пов’язані з операційним ризиком. В даний час консорціум нараховує 51 членів. Протягом останніх чотирьох років ORX зібрано дані по 102 500 випадках операційних втрат, кожен з яких більше за 20 тис. євро, на загальну суму 34,4 млрд. євро.

Потреба в обміні даних щодо операційних втрат існує не тільки у фінансовій сфері, оскільки операційні ризики є проблемою всіх суб’єктів господарювання. На жаль, в Україні майже відсутнє розуміння важливості створення подібних баз даних, що підтверджують результати низки експертних досліджень. Відповідно створення ефективної системи управління операційними ризиками унеможливлюється, внаслідок чого важливі ризики залишаються некерованими або неконтрольованими.

В розділі V ми зробили спробу викласти основи щодо створення та управління відповідними базами даних, що дасть змогу фахівцям у галузі управління

операційними ризиками в банках отримати відповіні знання для створення адекватних інструментів вимірюваного та управління даного виду ризику.

Одним з основних видів ризику суб'єкту господарювання незалежно від сфери діяльності, є операційний ризик, зумовлений невизначеністю стану і функціонування внутрішнього середовища. Хоча, на сьогодні перед банками стоїть завдання модернізації не тільки виробничої та технологічної бази, але й систем управління, що наочно продемонструвала остання світова фінансова криза. Створення чітко налагодженої системи управління операційними ризиками є надзвичайно важливим для здійснення ефективного керування суб'єктом господарювання в умовах несприятливого зовнішнього середовища та економічної невизначеності. Впровадження такої системи на рівні банків може стати суттєвим фактором стабільності їх розвитку у середньо- і довгостроковій перспективах та підвищення їх конкурентоспроможності на внутрішньому та світовому ринках.

Для суб'єктів господарювання, функціонуючих в умовах ринкових відносин, є свідомо програшним як стратегія абсолютної мінімізації операційного ризику, так і стратегія його абсолютного ігнорування. У першому випадку це обумовлено збільшенням витрат і зниженням конкурентоспроможності, а в другому - виникненням реальних загроз для існування на ринку. З цього приводу виникає задача визначення прийнятного для кожного окремого банку рівня ризику та управління поточним рівнем ризику в рамках заданих обмежень.

Вважаємо за потрібне зазначити, що викладені підходи щодо теоретичних основ управління операційними ризиками вимагають подальших досліджень в цьому напрямку з метою їх поглиблення, зокрема щодо розробок моделей управління операційними ризиками та їх впровадження, зокрема у практику комерційних банків [17].

Спробуємо дати відповідь на запитання як уникнути найбільш поширених помилок при роботі з таким видом ризику як операційний.

Найпершим кроком повинно стати визначення цілей, які переслідує керівництво банку при створення підрозділу, який займаєтиметься операційними ризиками. Єдино правильний варіант в цьому питанні - пряме підпорядкування

підрозділу операційних ризиків Спостережній Раді банку. Однак сьогодні практика роботи показує, що подібний стан речей вкрай рідко трапляється в українських банках. У кращому випадку підрозділ операційних ризиків прямо підпорядкувується Голові Правління банку, в гіршому - відділ у складі іншого структурного підрозділу займається операційними ризиками. В останньому випадку не потрібно намагатися побудувати нормальну систему роботи з операційними ризиками. Такий стан справ може свідчити про те, що керівництво банку не зацікавлене в розвитку цього напрямку і підвищені реальної ефективності.

Специфіка операційних ризиків дозволяє при правильній побудові системи аналізу знаходити помилки скрізь, і в ситуації, коли підрозділ підпорядковується не Спостережній раді, можливість виправити або вплинути на них практично зводиться до нуля.

Другим кроком у побудові внутрішньої системи управління операційними ризиками має стати аналіз дійсної ситуації в банках. Правильний підхід зводиться до того, що головним завданням підрозділу по роботі з операційними ризиками має стати:

- збір та класифікація інформації про вже наявні факти операційного ризику в цілому по банку;
- аналіз отриманої інформації, вимірювання розміру операційного ризику;
- надання інформації керівництву з зазначенням найбільш проблемних ділянок;
- побудова системи обліку контролю операційних ризиків;
- розробка заходів щодо зниження (обмеження) операційного ризику (з залученням вузькопрофільних фахівців та з урахуванням причин виникнення кожного виду ризику), розробка рекомендацій для керівництва банку;
- контроль за дотриманням встановлених заходів щодо зниження (обмеження) операційного ризику, ведення статистики, бази даних операційних ризиків.

Після збору, класифікації, аналізу інформації необхідно здійснити:

- визначення напрямів роботи;
- створення системи та вироблення рекомендацій щодо зниження рівня операційного ризику;
- контроль роботи системи ведення статистики операційних ризиків.

Дуже часто неправильним кроком стає те, що кожним видом операційного ризику займаються окремо. Для цього в банку мають бути спеціальні підрозділи, які відповідають за вид операційного ризику, який виникає в процесі їх роботи.

Основними питаннями, на які необхідно відповісти, що б розібратися в існуючій ситуації щодо управління операційними ризиками у конкретному банку мають стати:

- Чи є нормативна документація банку, що містить принципи управління операційним ризиком?
- Чи є орган (комітет) у складі органів управління банку та / або спеціальний підрозділ (співробітник) з управління операційним ризиком?
- Який порядок інформування органів управління і співробітників банку щодо рівня і методів управління операційним ризиком?
- Чи проводиться аналіз (оцінка) можливих витрат на створення (вдосконалення) системи управління операційним ризиком і вигоди від їх впровадження?
- Чи проводиться цілеспрямоване виділення коштів на організацію (вдосконалення) управління операційним ризиком?
- Які цілі і завдання поставлені перед підрозділами (службовцями), що здійснюють управління операційним ризиком?
- Які способи (засоби) підтримки процесу управління операційним ризиком застосовуються в банку?
- Який порядок здійснення функцій управління операційним ризиком застосовується у банку?
- Який порядок збору інформації про збитки, пов'язаних з операційним ризиком, застосовується у банку?

- Які заходи контролю і за мінімізації (зниження) операційного ризику застосовуються (розглядаються)?

Якщо банк починає роботу з операційними ризиками з нуля, необхідність у цих питаннях відповідно частково відпадає і систему управління операційними ризиками потрібно будувати з самого початку.

Наступним кроком у створенні ефективної системи управління операційними ризиками має стати збір і класифікація інформації про вже наявні факти операційного ризику в банку.

Під збором інформації, мається на увазі збір вже відомих інцидентів. З огляду на специфіку операційних ризиків, в термінології треба використовувати саме інцидент, і враховувати кількість інцидентів, які відбулися.

Інциденти операційних ризиків - факт настання події операційного ризику або ряду подій операційного ризику. Прикладом інциденту операційного ризику може бути збій автоматизованої банківської системи або розкрадання, здійснене певним співробітником. Кожен інцидент має ряд відмінних рис, таких як: дата виявлення, суб’єктів, тип події, напрям діяльності тощо.

Інцідетни бувають двох видів: з прямим фінансовим збитком та інциденти без прямих фінансових втрат. Збиток від операційного ризику визначається як негативний фінансовий вплив, пов'язаний з виникненням інциденту, що наступив.

Як приклади інцидентів операційного ризику з прямим збитком можна розглядати фінансовий вплив, який включає збиток чи знецінення активів, зміна пасивів і всі сплачені витрати, пов'язані з операційним інцидентом (внутрішні або зовнішні витрати на здійснення перевірки тощо), який відбувся, але не включає альтернативні витрати, витрати або доходи, пов'язані з інвестиційними програмами та понесені з метою запобігання супутнім їм збитків від операційних ризиків.

Збитки від основної діяльності банку виражаються в зниженні або втрати частини вартості активів, зовнішніх витратах (судові витрати з питань права, плата за послуги експертів, які здійснюють аналіз / перевірку подій), регулятивні дії (штрафи, пеня, виключення ліцензії), втрати по компенсації (компенсація третім

сторонам), втрати в результаті помилок у реквізитах платежів (неналежного виконання).

Наступним питанням є інцидент беззбитковості операційного ризику, який є інцидентом операційного ризику, в результаті якого банк не зазнав збитків у зв'язку з наявністю певнихсприятливих обставин.

Майбутні події, такі як загроза бомбового атаки, які можуть бути представлені у вигляді економічних збитків (евакуація, порушення нормального ходу роботи тощо.) і не можуть бути безпосередньо представлені в бухгалтерській звітності, теж вважаються інцидентами беззбитковості операційного ризику.

Іншим прикладом інциденту беззбитковості операційного ризику може бути помилка з боку банку в разі невірно відправлених коштів і їх повернення (кошти повернені на рахунок) беззбитковості без несення банком збитків, за винятком внутрішніх витрат на розслідування і повернення коштів.

Для збору та аналізу інформації про вже наявні інциденти операційного ризику необхідно знати які форми звітності існують у банку:

- форми звітів для подачі в НБУ;
- форми звітів (внутрішньобанківські) між підрозділами.

Одним із завдань управління операційними ризиками є організувати роботу таким чином, що б в процесі роботи самого підрозділу було задіяно найменшу кількість людей, але ефективність роботи при цьому була максимальною. При цьому необхідно, щоб кожен працівник банку опосередковано долучався до операційного ризик менеджменту.Створювати в банку підрозділ з великим штатом людей, є само по собі операційним ризиком. Не можна забувати що підрозділ з управління операційним ризиком є супутнім підрозділом. А витрати на управління ризиком не повинні перевищувати суму збитку від самого ризику. Знання та використання форм вже існуючих звітів, дозволить зменшити навантаження на структурні підрозділи, які за родом діяльності повинні будуть надавати інформацію в підрозділ операційного ризику.

Грунтуючись на рекомендаціях Базельського комітету з банківського нагляду та з огляду на досвід західних країн щодо формування банківської системи

управління операційним ризиком. Внутрішня система управління операційним ризиком та контролю - це не просто процедура або політика, яка виконується в певний момент, а постійно здійснюваний процес на всіх рівнях банку.

Правління банку і старші посадові особи несуть відповідальність за формування відповідних традицій в цілях сприяння виконанню заходів внутрішнього контролю, а також за моніторинг його ефективності на безперервній основі.

Основна задача системи управління операційними ризиками - ідентифікація всіх внутрішніх процесів і операцій банку, які можуть бути піддані виявленим джерел (факторів ризиків шахрайства), і оцінка даних ризиків.

Однак у цьому процесі повинен брати участь кожен співробітник банку. Дуже важливо відразу донести до свідомості всіх співробітників, що здійснення внутрішнього контролю не є функцією окремого підрозділу, а є частиною функціональних обов'язків кожного співробітника.

Сучасний банк повинен мати незалежний підрозділ, що відповідає за розробку та впровадження механізму управління операційними ризиками. Цей підрозділ здійснює корпоративну кодифікацію політики і процедур управління при проведенні контролю операційних ризиків; розробку та впровадження системи звітності про операційні ризики; розробку стратегії виявлення, оцінки, моніторингу та контролю операційних ризиків. Таким підрозділом, може бути один з підрозділів банківської безпеки. Функції і завдання його наступні:

1. Виявлення і усунення зовнішніх і внутрішніх загроз (потенційні або реально існуючі впливу, що призводять до морального або матеріальних збитків), які сприяють нанесенню банку, його співробітникам, акціонерам і клієнтам матеріальних збитків, заважають його нормальному функціонуванню та розвитку;

2. Розробка та реалізація заходів оперативного реагування на зовнішні і внутрішні загрози та негативні впливи, які виникали по відношенню до банку (персоналу, матеріальних ресурсів, фінансів, інформації). Заходи оперативного реагування можуть бути:

- правові - внутрішньобанківські нормативні документи, що регламентують функціонування системи безпеки банку;
- організаційні - створення 3-х рівневої системи внутрішнього контролю банку;
- інженерно-технічні - впровадження технічних засобів захисту інформаційних ресурсів, систем регулювання доступу, відео контролю за об'єктами банку, комплексне застосування технічних засобів охорони, виявлення, спостереження, збору та обробки інформації.

Негативні впливи можуть проявлятися у вигляді:

- економічних порушень - недобросовісна конкуренція, зрив ділових відносин та переговорів;
- фінансових порушень - розкрадання фінансів, шахрайство;
- фізичних порушень - знищення (пошкодження) об'єктів Банку;
- психічного тиску - хуліганські витівки, погрози і шантаж, тиск з боку правоохоронних органів, порушення кримінальних справ по відношенню до співробітників Банку;
- інформаційного впливу - несанкціонований доступ, обмеження доступу до інформації та інші.

Внутрішньобанківська система управління операційним ризиком банку має спиратися на такі етапи:

- ідентифікація та оцінка категорій та факторів ризиків;
- складання каталогу процесів і операцій банку;
- ідентифікація прояви окремих категорій та факторів ризиків та оцінка їх рівня на процесах і операціях;
- збір даних з операційних втрат і подій;
- виявлення критичних зон концентрації ризику на групах операцій або процесах;
- розробка та реалізація заходів з обмеження та / або нейтралізації виявлених критичних зон ризику (страхування, реінженірінг бізнес-процесів, підвищення надійності окремих елементів процесів і технологій);

- моніторинг і контроль виявлених факторів операційного ризику на окремих процесах і операціях;
- розробка плану організаційних змін з метою зниження ризиків бізнес-процесів, що включають оптимізацію документообігу, інформаційних потоків, розподілу функцій, повноважень і відповідальності.

Базовими елементами інтегрованої системи управління операційними ризиками мають бути:

1. Система внутрішнього контролю;
2. Система операційного ризик-менеджменту;
3. Процедури контролю;
4. Організаційна система розмежування функцій і повноважень;
5. Інформаційні системи.

Отже, із сказаного можна зробити наступні висновки. Сьогодні сприйняття та розуміння операційних ризиків в українських банках відрізняється від прийнятого в західній практиці. Якщо в західній практиці основна проблематика пов’язана з адекватною організацією бізнес - процесів в банку, запобіганню несанкціонованих торгів, використанням якісних моделей тощо, то в українській практиці на перший план виходять проблеми, пов’язані з функціонування інформаційних систем.

Пояснюється така ситуація як об’єктивними причинами, так і недостатнім рівнем розуміння сутності операційних ризиків.

Серед об’єктивних причин можна виділити відносно високу вагу витрат на інформаційні технології в загальній структурі витрат, неефективне їх впровадження, застарілі канали зв’язку, надмірна залежність від внутрішніх спеціалістів в даній області. Іншою особливістю є відсутність єдиної концепції щодо управління операційними ризиками в банках. Покриття збитків за ними здійснюється певною мірою в „ручному” режимі, в залежності від окремого випадку. Накопичення статистичних даних та їх аналіз здійснюються лише в 9% банків. Більше третини банків вважають, що це непотрібно взагалі. Особливо це стосується банків з групи невеликих.

З огляду на це, можна сформулювати наступні пропозиції. Національному банку України доцільно розглянути питання про формування банками резерву для покриття операційних ризиків. Для цього на першому кроці провести комплексне дослідження статистичних даних про відношення втрат від операційних ризиків до валового доходу. На основі такого дослідження може бути встановлений рівень резервування. Резерв має бути спрямований на покриття збитків за операційними ризиками, що характеризуються малою ймовірністю виникнення та високою величиною збитків.

Враховуючи необхідність стимулювання банків приділяти більше уваги проблематиці операційних ризиків, встановити в якості нормативу резервування два підходи - один фіксований розмір резерву (наприклад. 8% від обсягу валового доходу), другий - базується на власній моделі розрахунку резерву, але не менш 4% від валового доходу. Такий підхід буде сприяти розвитку в банках системи власних моделей операційних ризиків. встановлений рівень резервування.

Банкам з групи найкрупніших, необхідно використовувати стандартний підхід оцінки операційних ризиків, який базується на диференційованому підході до напрямків діяльності. Банкам цієї групи необхідно мати структурний підрозділ з аналізу та управління операційними ризиками.

Банкам з групи середніх та невеликих необхідно використовувати підхід на основі базового індикатора, враховуючи відносно малу кількість операцій.

Сьогодні банкам потрібно розробити та затвердити керівним органом концепції аналізу, оцінки, моделювання та управління операційними ризиками та розвивати комплексні системи спостережень та збору статистичних даних про втрати від операційних ризиків. Системи мають включати сфери прояву операційних ризиків, частоту виникнення та розмір збитків [10].

2.2 Організаційно – функціональна структура управління операційним ризиком

Операційний ризик тісно пов’язаний із іншими видами ризиків, зокрема операційний ризик здатний привести до значних прямим і непрямим втрат для банку та може служити причиною виникнення ринкового та кредитного ризиків (табл.) Виходячи із цього, при побудові організаційно – функціональної системи управління операційним ризиком необхідно врахувати комплексність загально банківської системи ризик – менеджменту.

Таблиця 2.1

Зв'язок між ринковим, кредитним та операційним ризиком

Операційний ризик	Ринковий ризик	Кредитний ризик
Неправильне уведення даних по договору	Збиткова торгівельна позиція	Неправильний розмір кредиту
Недостовірна ринкова інформація	Неправильна оцінка теперішньої вартості	Неправильна величина резерву, некоректна оцінка кредитного портфелю
Відсутність контролю за лімітами	Перевищення лімітів	Перевищення лімітів
Некоректні підтвердження	Помилкове хеджування	Неправильний розмір кредиту чи резервів
Відсутність контролю за подіями	Пропущені строки за подіями	Пропущені платежів
Затримка зі звітами	Торгівля «всліпу»	Несанкціонована видача кредитів

Етапи створення організаційно – функціональної системи управління операційними ризиками є наступними:

1. Етап виявлення джерел (видів) ризику на процесах:
   - декомпозиція кожного процесу банку на складові його операції;
   - складання технологічної карти документообігу процесу;
   - збір даних про несприятливі події та втрати;
   - ідентифікація на кожній операції можливих проявів окремих джерел (видів) ризику.

2. Етап створення організаційної системи виявлення, вимірювання і управління операційними ризиками.

3. Етап створення методології та технології вимірювання операційних ризиків.

4. Створення методологічних основ прийняття ризику або розробка інструментів імунізації та заходів зниження ризику на окремих процесах або операціях.

5. Калькуляція вартості реалізації інструментів імунізації ризику.

6. Підтвердження або корекція бюджету плану організаційних заходів та інструментів імунізації (страхування).

7. Реалізація планів імунізації ризику.

Очевидно, що наріжним каменем інтегрованого ризик-менеджменту є кількісна оцінка сукупного ризику банку, а також його декомпозиція по окремих видах ризику, портфеля та напрямки бізнесу.

Організаційно це завдання вирішується шляхом створення спеціального допоміжного підрозділу з оцінки та контролю за ризиками, в основні функції якого можуть входити:

- розробка політики з управління ризиками на підприємстві, включаючи вимоги до звітності для керівників функціональних підрозділів і вищого керівництва;
- координація щоденного процесу управління ризиками за допомогою встановлення лімітів, розміщення капіталу і санкціонування операцій;
- оцінка сукупних ризиків компанії на основі єдиного і послідовного підходу і відстеження фінансових ринків і інших подій в економічному житті, які можуть вплинути на розмір прийнятих ризиків;
- розробка, тестування і санкціонування застосування методів і моделей оцінки ризиків, особливо що використовуються для ціноутворення фінансових інструментів і продуктів;
- створення і ведення баз даних, необхідних для цілей ризик-менеджменту;
- взаємодія зі службами внутрішнього контролю з метою забезпечення дотримання вимог законодавства, регулюючих органів, а також внутрішніх положень та процедур;

- доведення результатів оцінки та управління ризиками до керівництва банку, а також підготовка інформації для регулюючих органів, інвесторів і рейтингових агентств.

Політика операційного ризик – менеджменту у банку відображена на рис.2.1.

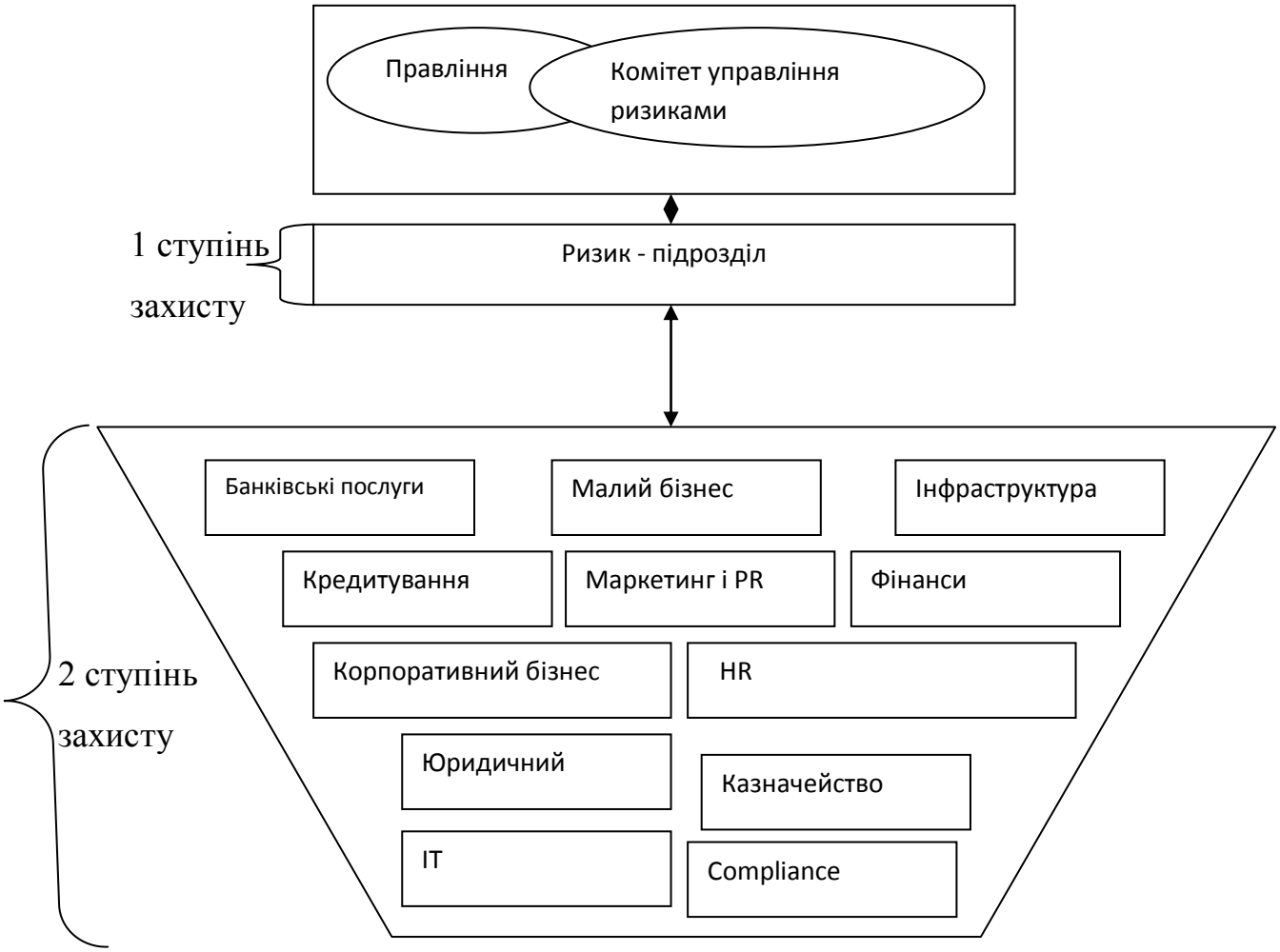


Рис.2.1 Політика операційного ризик – менеджменту

Отже, можна зробити висновок, що для побудови ефективної системи управління операційним ризиком необхідно:

На рівні Правління і Комітету з управління ризиками:

1. Встановити цілі та стратегію їх досягнення для розвитку політики управління операційним ризиком.
2. Переглянути ризик профілів і відповідні заходи в цій області.
3. Здійснювати управління/ контроль за ступенем стратегічної значимості інцидентів.

4. Оглянути і контролювати відповідні заходи в області політики.

5. Ідентифікувати цілі та розробити стратегічні заходи з управління операційним ризиком.

6. Проаналізувати звітності ризик підрозділів і виробити відповідні рекомендації.

7. Встановити цілі та стратегію - для обговорення на робочих нарадах по управлінню ризиками.

На рівні ризик підрозділу:

1. Розробити політику операційного ризик – менеджменту.

2. Зробити таку політику гнучкою через:

- зміни в ризик профілі;
- зміни в стратегії;
- зміни регулюючих органів;
- технологічні зміни.

3. Відстежувати відповідності всередині організації.

4. Періодично переглядати ризик профілю і політики.

5. Розробити і проводити робочі наради з питань управління ризиками.

6. Аналізувати діяльність робочих груп, використовувати результати такої роботи на практиці.

7. Виявляти тенденції у ризик контролі.

8. Відстежувати дії, необхідні для проведення самооцінки ефективності системи.

9. Розробляти базову структуру звітності.

10. Отримувати, накопичувати та аналізувати звітність.

11. Розробляти, впроваджувати та пропагувати зміни в політиці.

12. Оцінювати індикатори ризику відповідно до наявних даних.

На рівні окремого підрозділу:

1. Здійснювати політику з управління операційним ризиком «на місцях».

2. Удосконалювати політик в міру необхідності.

3. Надавати практичні поради для змін в політиці управління ризиком та стратегії.

4. Гарантувати відповідність.

5. Забезпечити експертів необхідною інформацією щодо ризиків в частині їх предметних областей.

6. Визначати та інформувати про істотні інциденти та реагувати на них.

7. Контролювати здійснення політики та стратегії на рівні підрозділу.

8. Забезпечити постійне подання необхідної інформації для ризик підрозділу.

9.Ідентифікувати ризики у поточній роботі.

10. Брати участь у робочих групах по управлінню ризиками.

11. Впроваджувати та надавати звітність за досягнутими результатами, відповідно оцінити:

- критичні фактори успіху;
- прихильність топ - менеджменту до проведення необхідних змін, наявність спільного бачення;
- розуміння один одного, за допомогою єдиного процесу;
- здійснення комунікації та тренінгів;
- застосування hr механізмів для досягнення відповідних цілей;
- постійний моніторинг процесу ризик - менеджменту.

Типова організаційна структура системи управління операційним ризиком банку включає наступні ланки:

- Наглядова Рада – колегіальний орган, що визначає та затверджує стратегію банку щодо управління операційним ризиком, контролює етапи впровадження та її виконання;
- Правління банку – забезпечує ухвалення внутрішніх документів, що визначають правила і процедури управління операційним ризиком, встановлення порядку взаємодії і надання звітності; Правління Банку здійснює контроль за діяльністю підрозділу з управління операційним ризиком і оцінює ефективність управління операційних ризиків як в цілому по Банку, так і на постійній основі переглядає існуючі внутрішні процеси і

процедури, використовувані інформаційно-технологічні системи з метою виявлення неврахованих раніше операційних ризиків.

- Підрозділ операційних ризиків – структурний підрозділ що забезпечує, розробку та впровадження нормативної бази щодо управління та оцінки операційного ризику, кількісну оцінку, або вимірювання ризику порівняльним методом, формує пропозиції щодо управління ризиковими позиціями, проводить постійний моніторинг ризикових позицій, та інформаційно забезпечує роботу Правління банку в частині управління о ризиком банку; Відділ операційних ризиків не рідше двох разів на рік надає керівництву Банку звіт про основні напрями концентрації операційних ризиків, причини їх виникнення і заходи, прийняті для зниження можливих операційних збитків
- Всі підрозділи банку що задіяні в операційній роботі – поточний контроль відповідності здійснених операцій встановленим внутрішніми та зовнішніми нормативно-правовими актами процедур та процесів, формування інформаційної бази встановлених помилок.

Усі керівники структурних підрозділів банку повинні нести відповідальність за виявлення операційних ризиків. Враховуючи те, що ОР мають відношення до всієї банківської мережі, відповідальність за цей процес лежить також на керівниках РУ. Виконавчі одиниці - всі структурні підрозділи Банку і окремі співробітники.

В середині структурного підрозділу, призначається виконавча одиниця, яка буде співпрацювати з Відділом управління організацій операційним ризиком в частині збору даних про операційні ризики.

Відповідальність виконавчих одиниць полягає в зборі інформації про випадки операційних ризиків які призводять до втрат (інформаційних втрат) обробляються в електронному вигляді. Особи, винні у виникненні операційних ризиків (збитків), повинні нести відповідальність відповідно до чинного законодавства.

2.3 Методи управління операційним ризиком

Процес управління операційним ризиком банку охоплює всі структурні щаблі та рівні – від Правління Банку до рівня, на якому безпосередньо приймається ризик, тому методи виявлення операційного ризику складаються з аналізу всіх умов функціонування банку, з метою виявлення де, коли і як, може виникнути операційний ризик. А знання потенційних небезпек, та ступінь їх значимості, дозволяють здійснювати управління ризиком.

Управління операційним ризиком – це процес, за допомогою якого банк виявляє (ідентифікує) операційний ризик, проводить оцінку його величини, здійснює його моніторинг і контролює свої позиції, а також враховує взаємозв'язки операційного ризику з іншими видами ризиків.

Методи управління операційними ризиками включають наступні функції:

Ідентифікація - вимірювання та оцінювання величини ризику, виявлення найбільш критичних ризиків, частоти виникнення (кількість прояву ризику за певний період), та можливість їх виникнення. Ідентифікація передбачає детальний опис основних видів операційних ризиків та форм їх прояву, згрупованих за певною ознакою факторів ризику та причинами виникнення притаманних саме банку.

З метою виявлення індивідуальних ризиків проводиться анкетування структурних підрозділів банку у термін не частіше ніж раз на рік. На основі анкетування та інших даних складається каталог операційних ризиків банку.

Моніторинг - дозволяє здійснювати поточний контроль, спостереження, нагляд за операційними ризиками, подіями, пов’язаними з їх реалізацією безпосередньо в ході операційної роботи. Моніторинг передбачає постійне, систематичне і послідовне відстеження та попередження операційних ризиків.

Моніторинг операційного ризику проводиться як на рівні структурних підрозділів, так і в цілому по банку.

Поточний моніторинг ризиків – це внутрішній оперативний поточний контроль та ризиками, які властиві напряму діяльності підрозділу, що здійснює операційний моніторинг. Постійний моніторинг сприяє оперативному виявленню та вжиттю заходів щодо мінімізації наслідків операційних ризиків.

Відділ з організації та управління операційними ризиками повинен здійснювати загальний моніторинг, в цілому по банку, на основі звітності яка надається структурними підрозділами.

Для створення власної інформаційної аналітичної бази, аналізу та управління операційними ризиками створюється система звітності. Форма звітності та терміни подачі встановлюється індивідуально для кожного підрозділу. Форми звітів та термін подачі для кожного структурного підрозділу є індивідуальними.

Також проводиться моніторинг, шляхом регулярного вивчення системи показників (зокрема статистичних, фінансових) діяльності банку.

В цілях моніторингу операційного ризику створюється система індикаторів рівня операційного ризику — показників або параметрів, які пов'язані з рівнем операційного ризику.

Для кожного індикатора встановлюються ліміти (критичні значення), що дозволять забезпечити виявлення значущих для банку операційних ризиків і розробити своєчасну адекватну дію на них.

Для створення власної інформаційної аналітичної бази, аналізу та управління операційними ризиками створюється система звітності.

При наявності інформації за попередні періоди, підрозділ операційних ризиків відстежує функціонування системи контролю, а не самі банківські процеси.

На основі накопичених даних банк розраховує індикатори операційної діяльності та визначає процедури контролю.

Для кожного виду операційного ризику, процедури контролю як зовнішні так і внутрішні встановлюються індивідуально.

Контроль операційних ризиків - це комплекс регулярних поточних заходів, спрямованих на попередження, фіксацію та усунення недоліків та порушень у сфері моніторингу ризиків, а також на виявлення негативних тенденцій для ініціювання заходів протидії.

Банку як можливість реального контролю операційного ризику необхідно вибрати розділення кожного процесу банку на його елементарні операції, складання

технологічної карти документообігу процесу, ідентифікація і оцінка по кожній операції можливих проявів ризику.

Система контролю операційного ризику банку має містити, як мінімум, такі компоненти:

- політику та положення щодо контролю операційного ризику з метою його мінімізації, які мають бути розглянуті та затверджені спостережною радою або правлінням банку, відповідно до принципів корпоративного управління. Така політика та положення мають підлягати періодичному перегляду.
- процедури і засоби контролю операційного ризику, що притаманні операціям банку, в тому числі:
- процедури та засоби контролю за дотриманням облікової політики банку та вимог нормативно-правових актів Національного банку щодо методів оцінки активів та складання звітності;
- процедури та засоби контролю за функціонуванням інформаційних систем банку та забезпечення безперебійної діяльності, зокрема процеси дублювання і відновлення інформації, а також резервні системи на випадок втрати доступу або знищення важливої інформації або технологій;
- інформаційну систему управління (набір форм звітності, схему документообігу тощо) для спостережної ради, правління або профільних колегіальних органів банку щодо моніторингу уразливості всіх видів діяльності банку до операційно-технологічного ризику;
- програму управління персоналом, котра охоплює:

1) постійний, ефективний процесс залучення і утримання достатньої кількості кваліфікованого персоналу, що відповідає потребам банку та зовнішнім обставинам, з метою виконання завдань його діяльності і реалізації стратегії та бізнес-планів;

2) чітко визначені і продумані рівні повноважень з прийняття рішень;

3) чітке доведення до персоналу його обов'язків;

4) контроль за діяльністю персоналу;

5) розроблення і впровадження процесу навчання з метою підвищення кваліфікації працівників;

6) технологічні схеми (карти) продуктів та послуг банку, що підтримуються в постійно актуальному стані;

7) процедури забезпечення потреб банку в інфраструктурі (зокрема в програмному, аппаратному та іншому забезпеченні), у відповідності до його обсягів та складності поточної та запланованої діяльності. Такі процедури мають передбачати санкціонування, тестування та документування всіх операційно-технологічних систем банку перед початком їх експлуатації, а також механізми їх актуалізації, в тому числі перевірку чинності ліцензійних угод;

8) процес періодичного тестування встановлених процедур та технологій здійснення операцій, в тому числі процедур фізичної та інформаційної безпеки, з метою контролю за дотриманням цих процедур і технологій та збору інформації щодо їх можливого вдосконалення у разі їх неефективності.

Крім того для належного контролю за операційним ризиком рекомендується:

- забезпечити надійне позаофісне зберігання всіх важливих резервних документів і файлів банку;
- у разі використання банком послуг аутсорсингу, забезпечити чітку регламентацію наступних питань:

1. обставин, за яких можуть використовуватись послуги аутсорсингу та переліку операцій, до яких можуть бути залучені сторонні особи;

2. процедур та критеріїв вибору постачальників послуг;

3. моніторингу якості роботи і ризиків, пов'язаних з використанням сторонніх постачальних послуг [18].

Найбільш реальною можливістю контролю операційного ризику є поділ кожного процесу банку на складові його елементарні операції, складання технологічної карти документообігу процесу, ідентифікація та оцінка на кожній операції можливих проявів конкретних категорій джерел ризику.

При цьому, внутрішній контроль повинен бути основним інструментом управління операційним ризиком. Його призначення полягає в тому, щоб служити інструментом превентивних дій, а не констатувати факти минулих подій.

Спочатку, внутрішній контроль призначався для запобігання шахрайства, несанкціонованих дій та зумисних помилок персоналу. Зараз його сфера застосування розширилася, в тому числі завдяки тому, що внутрішній контроль є ефективним способом запобігання інших видів операційного ризику.

Першим, базовим принципом успішної побудови та функціонування системи внутрішнього контролю є постійна участь кожного співробітника банку в процесі контролю у поєднанні з багаторівневої системи контролю.

Другою умовою є організація не вибіркового, а постійного, тобто суцільного контролю.

Третьою умовою роботи системи контролю є можливість кожного співробітника (незалежно від рангу) інформування служби внутрішнього контролю про відхилення від правил, помічених у ході проведення діяльності.

Четвертою умовою є незалежність у своїй діяльності служби внутрішнього контролю і можливості ініціювання заходів впливу щодо посадових осіб та зупинки будь-яких операцій при виявленні порушень.

На відміну від методик оцінки та мінімізації кредитних і ринкових ризиків методики управління операційним ризиком почали розробляти порівняно недавно. У Базельській угоді від 1988 р. операційний ризик за фіксували як побічний продукт кредитного та ринкового ризиків і віднесли до категорії «інші» в сім'ї ризиків. В Угоді «Базель-2» операційний ризик розглянуто окремо, наведено визначення, методи його оцінки, причини виникнення. Базельський Комітет вважає, що операційний ризик є важливим ризиком, із яким стикаються банки, і що банкам потрібно тримати певну суму капіталу на випадок пов'язаних із ним збитків.

Підходи до оцінки операційних ризиків протягом останнього часу стрімко розвиваються, але відстають за ступенем точності від методів вимірювання кредитних і ринкових ризиків. Оцінка операційного ризику допускає оцінку ймовірності настання подій або обставин, що призводять до операційних збитків, і

оцінку розміру потенційних збитків. Методи, засновані на застосуванні статистичного аналізу розподілів фактичних збитків, дають змогу прогнозувати потенційні операційні збитки, орієнтуючись на розміри операційних збитків, у даній кредитній організації в минулому. Статистичні методи і моделі активно використовують у випадку, якщо ймовірність настання конкретного виду операційного ризику достатньо велика, а його поширення на ринку – масове.

У цьому випадку можна використовувати кореляційні моделі, в яких функцією буде ймовірність настання операційного ризику, а змінними – чинники, що формують операційний ризик (наприклад, кількість операцій, яка прямо визначає частоту помилок персоналу).

Суть бально-вагового методу полягає в оцінці операційного ризику в зіставленні зі заходами по його мінімізації. На основі експертного аналізу вибирають інформативні для потреб управління операційним ризиком показники і визначають їх значущість (вагові коефіцієнти). Потім вибрані показники зводять у таблиці (оцінні карти) і оцінюють із використанням різних шкал. Отримані результати обробляють із урахуванням вагових коефіцієнтів і зіставляють за напрямками діяльності кредитної організації, окремих видів банківських та інших операцій. Застосування бально-вагового методу разом із оцінкою операційного ризику дає змогу виявити слабкі й сильні сторони в управлінні операційним ризиком.

У рамках методу моделювання (сценарного аналізу) на основі експертного аналізу для напрямів діяльності банку, окремих видів банківських та інших операцій визначають можливі сценарії виникнення події або обставин, що призводять до операційних збитків, і розробляють модель розподілу частоти виникнення та розмірів збитків, яку потім використовують для оцінки операційного ризику. Моніторинг втрат від настання операційного ризику охоплює аналіз кожного випадку, опис природи і причин, що призвели в конкретній ситуації до реалізації операційного ризику. Для виявлення напрямків, найбільш схильних до операційного ризику, рекомендований проводити післяопераційний розподіл процесів і технологій на їх елементарні складові, для кожної з яких емпірично або статистично

визначають ступінь впливу на нього того або іншого джерела ризику. Згаданий розподіл об’єктів операційного ризику на елементарні операції називається декомпозицією операційного ризику за операціями, що становлять каталог операційних ризиків. Каталог дає змогу виявити найуразливіший підрозділ банку.

Складання каталогу операційних ризиків – основне завдання при побудові адекватної системи управління згаданим ризиком. Його можуть складати або підрозділи банку – у вигляді так званої технологічної карти здійснюваних операцій, або можна доручити зовнішній консультаційній фірмі. Після складання каталогу виявляють ті процеси й окремі операції, на яких найбільшою мірою концентруються конкретні чинники ризику.

Потім розробляють заходи щодо зменшення і обмеження виявлених ризиків.

Що стосується математичних методик, то для управління операційним ризиком розробити їх важко. По-перше, катастрофічні події, що можуть завдати істотних збитків організації, трапляються вкрай рідко, і, відповідно, перебувають за межами розумних довірчих інтервалів, у хвості статистичного розподілу ймовірності втрат.

По-друге, важко встановити ймовірність настання ризику, ступінь впливу окремих чинників на ризик. Тому управління операційними ризиками зводять до аналізу подій, що відбулись, і запобігання ризику до настання події. Щоденний моніторинг операційного ризику має охоплювати виявлення операційних втрат, самостійну оцінку ризику підрозділами та відстежування ключових індикаторів ризику.

Сьогодні неможливо оцінити рівень операційного ризику в банку без історії операційних втрат. Спершу слід розробити систему збору даних, навчити персонал ідентифікувати операційний ризик, грамотно встановити рівень відбору, щоби не засмічувати базу даних. Потім можна частково відновити операційні події через бухгалтерію банку або на основі опитування співробітників. Операційні втрати слід розділяти за групами чинників ризику, а також за підрозділами банку і банківськими продуктами.

Природно, що база даних, із якою можна працювати, сформується через кілька років, але в міру її нагромадження слід аналізувати масив даних і вживати заходів

для поліпшення одержуваної інформації. Велике значення в контролі над операційними ризиками має моніторинг ключових індикаторів ризику. Ключовий індикатор ризику – показник, що істотно впливає на рівень конкретного ризику. Фахівці вважають, що серед безлічі діючих випадкових чинників є такі, які багато в чому визначають ймовірність настання несприятливої події і потенційний розмір збитку. Якщо відстежувати такі показники, можна з більшою або меншою впевненістю також виявляти рівень ризику і прогнозувати збитки.

Індикатори, за якими можна судити про діяльність банку і про рівень операційного ризику, розділяють на три групи:

індикатори поточної діяльності (відображають найзначущіші аспекти діяльності компанії);

індикатори ефективності контролю (показують кількість помилок, яким запобігли завдяки системі внутрішнього контролю);

індикатори ризику (будують шляхом зіставлення індикаторів поточної діяльності й ефективності контролю).

Звичайно індикатори формують для тих частин процесу бізнесу, порушення яких може привести до втрат для банку. Наприклад, для інвестиційних підрозділів банку хорошими показниками є обсяг та кількість затримки постачань цінних паперів як від банку до контраґентів, так і від контраґентів до банку.

Для повної ідентифікації ризиків необхідні експертні опитування. Результати анкетування служать основою розрахунку залишкового рівня ризику. Облік фактичних втрат, аналіз індикаторів ризику і сценарних аналізів на основі експертних опитувань не будуть максимально ефективними при управлінні операційним ризиком без можливості зіставлення даних. Тому слід формувати загальну картину, або карту операційного ризику [9].

Основний метод управління операційними ризиками полягає в створенні ефективних процедур контролю, які в сукупності складають єдину систему внутрішнього контролю. Процедури внутрішнього контролю є обов'язковим елементом при здійсненні всіх бізнес-процесів, що дозволяє зменшити ймовірність і наслідки реалізації операційного ризику.

Методи управління операційним ризиком можна класифікувати наступним чином:

1.Аудиторські перевірки дозволяють визначити невідповідності існуючої практики вимогам регулюючих органів і законодавства. Крім того, визначаються найбільш слабкі місця з погляду контролю шляхом порівняння наявних бізнес-процесів з «найкращою практикою». При цьому, внутрішню оцінку і аналіз проводять всі підрозділи з метою самостійного визначення можливих операційних ризиків. Така оцінка частково суб'єктивна, але ґрунтується на зацікавленості підрозділів і окремих співробітників в грамотного виконання своїх обов'язків.

Індикатори поточної діяльності відображають найбільш значущі аспекти діяльності банку, по яких можливо судити про його поточний фінансовий стан.

Індикатори ефективності контролю показую кількість помилок, які запобігли завдяки системі внутрішнього контролю.

Індикатори ризику - є випереджальними показниками і будуються розрахунковим або аналітичним шляхом зіставлення індикаторів поточної діяльності і ефективності контролю. Зіставляючи інформацію про зміни обсягу операцій, плинності кадрів, кількості помилок введення даних, частки видалених та виправних операцій оцінюється рівень операційного ризику для банку. Тим самим, створюються кількісні моделі для аналізу і прогнозування ситуації у сфері операційних ризиків

Індикатори діяльності представлені трьома основними групами показників, за якими можна робити висновок про діяльність банку та наявні операційні ризики.

Усі перераховані індикатори використовуються з метою моніторингу за операційною діяльністю. Управління операційним ризиком ґрунтується на припущенні, що при появі негативних сигналів від таких індикаторів, зростає імовірність подій, які пов'язані з операційним ризиком. Відповідно, департамент з управління фінансовими ризиками може запобігти такій небезпеці, посиливши контроль за ситуацією.

На основі накопичених даних банк розраховує індикатори операційної діяльності.

Причинно-наслідкові моделі дозволяють пояснити походження і оцінити втрати при здійсненні бізнес-процесів за допомогою методів теорії вірогідності. Основою такого підходу є те, що причини і наслідки пов’язані умовною вірогідності.

Для того, щоб оцінити свою схильність ризику дуже суттєвих подій, банк використовує метод аналізу сценаріїв або стрес-тестування. Він дає уявлення про те, яку суму збитків отримає банк у разі, якщо події розвиватимуться за запропонованими сценаріями.

Цей підхід спирається на знання досвідчених керівників бізнесу і експертів у сфері управління ризиками. Наприклад, ці експертні оцінки можна виразити у вигляді параметрів статистичного розподілу збитків.

Крім того, сценарний аналіз використовується для оцінки впливу відхилень від кореляційних припущень, включених в схему оцінки операційного ризику банку, зокрема, для оцінки потенційних збитків, що виникають внаслідок декількох одночасних випадків збитків, пов’язаних з операційним ризиком. Згодом такі оцінки підтверджуються і перевіряються шляхом порівняння з фактичними цифрами збитків, щоб пересвідчитися в їх обґрунтованості.

Розподіл вірогідності збитків. Математичний підхід до аналізу втрат в результаті операційних ризиків.

Співробітники Національного банку України у своїй діяльності з нагляду для оцінки рівня управління операційним ризиком також використовують цілий набір факторів, зокрема перспективним є використання таких показників:

1) Існування адекватної, ефективної, доведеної виконавцям внутрішньої нормативної бази (положень, процедур тощо) щодо управління операційно-технологічним ризиком, затвердженої відповідними органами банку виходячи з принципів корпоративного управління, а також відповідної практики виконання її вимог.

2) Кількість і складність обробки операцій у порівнянні з рівнем розвитку та потужністю операційних і контрольних систем, враховуючи попередні результати роботи цих систем, їх поточний стан та перспективи подальшого удосконалення.

3) Ймовірність технологічних та операційних збоїв, перевищення повноважень персоналом, недоліки у попередньому аналізі операцій під час прийняття рішень, а також відсутність (у тому числі тимчасове) моніторингу або реєстрації операцій з клієнтами або контрагентами.

4) Наявність і дотримання банком технологічних карт здійснення операцій.

5) Наявність, кількість, причини і характер порушень процедур адміністративного і облікового контролю.

6) Потенційна можливість фінансових збитків внаслідок:

- помилки виконавців або шахрайства;
- низької операційної конкурентоспроможності банку;
- неадекватності наявних інформаційних систем;
- неповної інформації щодо контрагента або операції;
- операційних та технологічних збоїв.

7) Історія і характер скарг та звернень клієнтів у банк у зв'язку з недоліками роботи операційних систем і реакція на них банку;

8) Обсяги і адекватність засобів контролю за банківським програмним забезпеченням і його супроводом та іншими послугами, які здійснюються із залученням третіх осіб (outourcing);

9) Адекватність стратегії щодо інформаційних технологій, стратегія щодо інформаційних технологій має відповідати поточним та передбачуваним вимогам щодо діяльності банку і враховувати структуру технічних засобів, телекомунікаційних засобів, програмного забезпечення, даних і мереж, а також цілісність інформаційної бази даних;

10) Існування процесу для:

- визначення інформаційних потреб для ефективного управління банком;
- визначення архітектури інформаційних систем для обробки операцій та надання продуктів і послуг;
- забезпечення достовірності та збереження інформації (наприклад, створення, обробка, збереження і надання даних). Це включає планування

заходів забезпечення безперервної діяльності; - забезпечення своєчасної підготовки та використання управлінської інформації.

11) Рівень кваліфікації та навичок менеджерів і працівників.

12) Існування належних механізмів контролю для моніторингу точності інформації, належних облікових підходів і дотримання положень або законів.

Як видно з вищесказаного, Національний банк України серйозно ставиться до проблеми операційного ризику, і для оцінки його рівня в банку висуває великий обсяг критеріїв оцінки.

На підставі оцінки адекватності вищезгаданих чинників, а також спеціальних матриць оцінки співробітники банківського нагляду зможуть не тільки оцінити величину операційного ризику та якість управління ним, а й дати оцінку тенденції рівня операційного ризику в майбутніх періодах.

Отже із сказаного можна зробити наступні висновки:

- неможливо виявити операційний ризик без постійного дослідження всередині банку;
- неможливо здійснювати аналіз адекватно до поданої інформації;
- не можна робити висновки про стан операційного ризику без урахування думки кваліфікованих співробітників, які знають специфіку процесів бізнесу
- складно проводити аналіз без змоги мати загальне уявлення про картину ризиків в банку.

При здійсненні управління операційними ризиками необхідно врахувати, що:

- теоретичні причини операційного ризику відомі. Необхідно виявляти й усувати причини операційних втрат конкретного банку;
- ефективні технології роботи кредитної організації можливо розробити тільки виявивши недоліки діючих систем і процесів, які і призводять до операційних втрат;
- управління операційним ризиком має бути систематичною і комплексною діяльністю.

2.3.1 Ідентифікація ризиків та створення каталогу операційних ризиків

Незважаючи на широку увагу до операційних ризиків банку, на сьогоднішній день не існує єдиної точки зору щодо їх ідентифікації. Проаналізуємо основні підходи до ідентифікації операційних ризиків.

Перший підхід відбито у назві та полягає в тому, що під цим терміном розуміють ризики, які виникають в процесі здійснення операцій фінансовим інститутом (банком).

Такий підхід включає помилки персоналу, недотримання процедур виконання операцій, збої комп'ютерних систем. Разом з тим. такий підхід не включає навмисного порушення систем внутрішнього контролю (наприклад, свідомого порушення лімітів та резервів співробітниками банку), внутрішнє та зовнішнє шахрайства. Окрім цього, в такий підхід не вкладається ризик, пов'язаний з неадекватною організацію самих процедур виконання операцій та. більш широко, організацією бізнес-процесів у банку (наприклад, надання одному підрозділу одночасно повноважень прийняття рішень та контролю за ними). Також в дане означення не вкладається ризик, пов'язаний з використанням неадекватних моделей оцінки ризику (ринкового та кредитного).

Другий поширений підхід полягає у розбитті ризиків банку на фінансові та нефінансові, та визначенні операційних ризиків як „нефінансові". Під фінансовими ризиками розуміють ризики, що виникають при виконанні банками функцій фінансових посередників. До них відносять ринковий, кредитний, ризик ліквідності, ризик невідповідності активів та зобов'язань, а також страховий ризик. На відміну від фінансових, нефінансові ризики не є притаманними виключно фінансовим посередникам, а є загальними для багатьох компаній. Нефінансові ризики класифікують на три категорії: ризики внутрішніх подій, ризики зовнішніх подій та бізнес-ризики. Перші характеризуються шахрайствами, відсутністю належного внутрішнього контролю, збоями інформаційних систем, помилками та порушеннями правового характеру. Ризики зовнішніх подій пов'язані з такими подіями як катастрофи, терористичні акти, землетруси, цунамі тощо. Прикладом можуть слугувати прямі збитки банків від терористичної атаки на Нью-Йорк 11 вересня

2001 року (лише банк Нью-Йорка мав прямі збитки $85 млн.). Бізнес-ризики включають в себе збитки від нереалізованих конкурентних переваг, неправильного вибору стратегії розвитку та місця на ринку, втрати від регуляторних змін, від змін в попиті тощо.

Другий підхід не зовсім адекватно відбиває сутність операційних ризиків. Так, бізнес-ризики породжують втрати, які спричинені звичайними економічними подіями, а тому мають бути предметом аналізу бізнес-діяльності банку в цілому, а не ризик-менеджерів. Окрім цього, необхідно відокремити безпосередні втрати, пов'язані з певною подією, від побічних втрат. Наприклад, як уже згадувалося,окрім $85 млн. прямих збитків банку Нью-Йорка, були побічні збитки через спотворення економічної діяльності на декілька днів (зокрема, біржа не працювала 4 дні).

Третій підхід до ідентифікації операційних ризиків полягає в тому, що в якості операційних ризиків приймаються ризики, що виникають через неадекватну побудову внутрішніх процесів в банку: обумовлені внутрішнім та зовнішнім шахрайством, технологічними збоями та не передбачуваними подіями (пожежі, аварії тощо). Такий підхід представлено, зокрема, в Енциклопедії фінансового ризик-менеджменту (виданої в Росії у 2003 році), де наведено наступне визначення: Операційний ризик - це ризик прямих та побічних збитків в результаті невірної побудови бізнес-процесів. неефективності процедур внутрішнього контролю, технологічних збоїв, несанкціонованих дій персоналу або зовнішніх впливів". Дане визначення здається найбільш ґрунтовним, та узагальнює підходи, які базуються на перелічені сфери виникнення операційних ризиків, які широко представлені в західній літературі з банківської практики.

Наслідки небажаного операційного ризику можуть призвести до фінансових збитків через помилку, невчасне виконання робіт або шахрайство або стати причиною того, що інтереси банку постраждають у якийсь інший спосіб, наприклад, дилери, кредитні працівники або інші працівники банку перевищать свої повноваження або порушення етичних норм або із занадто високим ризиком.

Найважливішою передумовою моделювання є наявність статистичних даних про об'єкт моделювання, що для операційних ризиків є серйозною проблемою.

Пояснюється це малою частотою прояву значної частини операційних ризиків. Наприклад, за даними експертного дослідження, зовнішнє шахрайство зустрічається в середньому 1-2 рази на рік. Внаслідок цього, створення статистичної бази за випадками шахрайства у конкретному банку вимагатиме досить тривалого періоду часу. Побудова ж статистичної бази в рамках всієї банківської системи чи її частини може бути проблематичною задачею через можливе приховування банками подібних випадків. Окрім цього, обґрунтування висновків із статистичної бази, створеної на основі даних з усієї банківської системи, може бути не завжди коректним для окремого банку.

На жаль, в українських банках до вказаної проблеми додається відсутність розуміння важливості створення подібних баз даних. Це підтверджують результати експертного дослідження. В цілому у банківській системі України більше третини банків вважають за непотрібне запровадження системи накопичення даних про втрати від операційних ризиків. У групі середніх та невеликих банків ця величина перевищує дві третини. Більше того, в жодному з банків з цих груп, які попали у вибірку дослідження, не запроваджена комплексна система спостереження та аналізу втрат від операційних ризиків. Найбільш розвинутими в цьому відношенні є найкрупніші банки. Результати дослідження подальшою сшвоесідою для уточнення відповідей.

Таблиця 2.1

Наявність системи спостережень за операційними ризиками в банках України

Показник	Банківська система в цілому	Найбільші банки	Великі банки	Середні банки	Невеликі банки
Існує комплексна система накопичення та аналізу даних про втрати від операційних ризиків	9,1%	20%	14,3%	0%	0%
Існує система накопичення даних про втрати від операційних ризиків за окремими напрямками,комплексного аналізу не здійснюється	45,5%	60%	57,1%	33%	0%
Актуальної потреби у системі накопичення даних про втрати від операційних ризиків немає	36,4%	20%	14,3%	67%	67%
Власні варіанти відповідей	9,1%	0%	14,3%	0%	33%

Джерело: [10]

Вцілому, ідентифікація операційних ризиків здійснюється за 2 напрямками:

- ідентифікація всіх факторів окремих видів (джерел) ризику;
- розкладання процесів і продуктів банку на складові їхні елементарні операції (технологічна карта процесу);
- оцінка рівня впливу кожного фактору ризику на окремі операції процесу (послідовно по технологічній карті) і складання каталогу операційних ризиків банку.
- інструментами ідентифікації та вимірювання операційних ризиків є:
  - ✓ самооцінка ризику (risk self assessment - rsa);
  - ✓ інші процедури схвалення ризику (other risk approval process - orap);
  - ✓ аналіз бази даних з операційних втрат (corporate loss database);
- ключові ризик індикатори (key risk indicators - kri's)
- процедури контролю ключових операційних ризиків key operational risk controls (korcs).

Всі інструменти включають розробку за результатами вимірювання активних планів попередження (імунізації) ризику. Зокрема вони поділяються на кількісні та якісні. Кількісні інструменти:

- бази даних про втрати;
- об'ємні індикатори;
- ключові індикатори;
- статистичний аналіз.

Якісні інструменти включають:

- самооцінку ризику;
- звіти експертів;
- звіти аудиторів.

Оцінка імовірності здійснення несприятливого події на даному об'єкті ризику через реалізацію конкретного джерела ризику. Приклад: гіпотеза про функції розподілу ймовірності даної випадкової величини (джерела ризику) на множині об'єктів ризику, наприклад - на безлічі транзакцій через платіжну систему;

Статистична оцінка результату несприятливого події як статистична оцінка (математичне очікування) розміру можливих втрат за типами втрат, які можуть виникнути на даному об'єкті ризику.

Статистична оцінка можливих відхилень (дисперсія) із заданим рівнем довірчої ймовірності від оцінки можливих втрат.

Складання каталогу ризиків може бути проведено:

- власними силами;
- залученими зовнішніми аудиторами та консультантами.

При здійсненні роботи власними силами виникають ризики помилок та перекручень, пов'язані:

- з фактором відсутності незалежності та об'єктивності співробітників банку та їх можливу залежності від думки окремого керівника;
- з відсутністю достатньої кваліфікації для декомпозиції окремих процесів банку на складові їх операції, і оцінки тривають них рівня окремих категорій операційного ризику.

Каталог операційних ризиків це - двомірна таблиця у якої,

- за і-м рядками розташовуються об'єкти ризику:
- докладний перелік операцій і технологій, що становлять процеси банку, види активів і майна;
- за j-м стовпцями розташовуються джерела і окремі фактори ризику.

На перетині рядків і стовпців розташовуються якісні або числові оцінки рівня виявлених для даних операцій джерела ризику.

Оцінки агрегуються («підсумовуються»):

- за рядками (тобто операціям і процесам);
- за стовпцями (тобто за джерелами або категорій ризиків.

Приклад каталогу операцыних ризиків наведенов таблицы нижче.

Таблиця 2.2

Каталог операційних ризиків

	процеси\операції	ризик збоїв обладнання	ризик збоївПО	методичний ризик	організаційний ризик	ризик персоналу	правовий ризик	ризик зовнішніх джерел
i=	j=	1	2	3	4	5	6	7
1	**РКО юридичних осіб**	**4**	**5**	**2**	**4**	**7**	**5**	**6**
1.1.	прийом платежів	1	2	1	2	6	1	1
1.2	ввод до АБС	2	4	1	3	7	1	1
1.3	поточний контроль	1	3	1	4	5	1	1
1.4	формування виписки	2	2	1	2	2	1	1
1.5	формув. реєстру платежів РКЦ	2	2	1	2	2	1	1
1.6	відправка платежів РКЦ	3	2	1	2	2	2	4
1.7	клієнт-банк	4	5	2	3	2	5	6
4	**процесинг пластикових карт**	**3**	**5**	**3**	**4**	**6**	**3**	**6**
4.1.	виготовлення пл. карти	2	1	1	2	6	1	1
4.2	авторизація пл. карти	2	3	1	3	5	3	2
4.3	авторизація рахунку	1	4	1	4	4	3	5
4.4	перевірка залишку на рахунку	2	4	3	2	3	2	5
4.5	авторизація платежу	1	4	1	4	5	1	6
4.6	формування виписки	2	2	1	2	2	2	3
4.7	міжбанківський кліринг	3	5	2	3	4	2	1
4.8	поточний контроль	1	2	2	3	3	2	1
4.9	поповнення спецкартсчета	1	2	1	3	2	2	1

2.3.2 Моніторинг операційних ризиків

Безпосередній процес моніторингу та управління операційними ризиками, знову ж таки на думку Базельського Комітету, повинен ґрунтуватися на наступних принципах:

- банки повинні ідентифікувати та оцінювати операційний ризик у всіх матеріальних продуктах, напрямки діяльності, процесах і системах;
- банки мають забезпечити виконання процедури оцінки операційних ризиків перед запуском нового продукту, напрямки діяльності, процесу або системи.

Втілення цього принципу в життя має на увазі собою аналіз чинників, що можуть негативно впливати на досягнення цілей банку (організаційна структура

банку, особливості діяльності, якість кадрів, плинність кадрів та інші; зміни в банківському секторі і технологіях). Інструментами такого аналізу є:

- семінари з оцінки сильних і слабких сторін системи управління операційним ризиком банку;
- карта ризику - співвідношення різних підрозділів і процесів з різними компонентами ризику для виявлення слабких місць і організації превентивних дій, розробка системи індикаторів операційного ризику (база даних про втрати, показник плинності кадрів, використання зовнішньої статистики тощо).

Сьогодні банки повинні впровадити процес регулярного моніторингу профілю і позицій операційного ризику. Повинна бути регулярна звітність істотної інформації Правлінню та Спостережній раді банку, що підтримує активне управління операційними ризиками.

Індикаторами раннього попередження для відображення потенційних джерел операційного ризику можуть бути: швидке зростання, введення нових продуктів, частота і тривалість системних збоїв та ін.

Частота моніторингу повинна відображати величину ризику і частоту змін в операційному середовищі.

З огляду на сучасні умови, банки повинні мати політику, процеси і процедури для контролю і або зниження матеріального операційного ризику. Також банки повинні періодично переглядати свої обмеження по ризику і стратегії з його керуванню відповідно до свого загальному рівню прийнятного ризику і профілем ризику.

На практиці, для всіх типів операційного ризику банк вирішує: або знижувати / контролювати його, чи нести цей ризик. Для ризиків, які не піддаються управлінню, банк повинен вирішити: або приймати його, або знизити рівень діяльності за відповідним напрямом, або зовсім припинити цю діяльність. Обов'язковою аспектом є поділ обов'язків для уникнення конфлікту інтересів. Для ризиків з низькою ймовірністю, але високими збитками можливе використання страхування. При цьому зниження ризику не повинно підміняти внутрішнім контролем.

Основною метою моніторингу моніторингу будь – яких ризиків є зіставлення відповідних активних заходів, і спостереження за реалізацією запланованих заходів. У разі індивідуальних ризиків, в яких розміри втрат досягають значної суми, необхідно також вести спостереження за пороговими величинами ключових індикаторів робочих характеристик, і ключових індикаторів ризиків.

Результатом моніторингу операційних ризиків мають бути звіти, які грунтуються на зіставленні усієї наявної інформації про ризик, а також як у випадках збитків і індикаторах ризиків. Такі звіти використовуються для надання інформації для членів правління, старшого менеджменту, операційного ризик-менеджера і додаткових адресатів.

Основна мета моніторингу - перегляд всіх процесів управління операційними ризиками щодо відповідності, функціональності і результативності.

Моніторинг операційного ризику проводять із встановленою періодичністю шляхом спостереження, тобто операційного ризику (групі операційних ризиків) присвоюється статус: «усунутий», «мінімізований», «прийнято», «переданий стороннім організаціям», «в роботі».

Необхідно фіксувати, яким чином був мінімізований той чи інший операційний ризик. Існує кілька варіантів проведення моніторингу. На підставі аналізу індикаторів операційного ризику. Відзначимо, що в деяких випадках впровадження облікової системи ключових індикаторів ризику вимагає значних витрат, при цьому отриманий ефект залишається «непрозорим» у грошовому вираженні. На підставі звітів керівника робочої групи про хід виконання того чи іншого проекту. На підставі повторного виявлення операційних ризиків. На підставі даних системи адміністративного контролю (результати виконання завдань, зафіксованих у письмовій або електронній формі у контрольних картках). Адміністративний контроль дозволяє знижувати ймовірність затягування робіт з мінімізації ОР і часто допомагає поліпшити якість та ефективність виконання рішень. На думку авторів, найбільш складним моментом у моніторингу процесу мінімізації операційного ризику є визначення якості виконуваних робіт. Це питання можна вирішити шляхом підвищення компетентності ризик-менеджерів у тій чи іншій професійній галузі, а

також за допомогою сторонніх експертів (дорогий варіант рішення) або шляхом проведення опитування внутрішніх споживачів послуг. Система управління операційними ризиками може бути представлена наступними звітами:

- звіти, рекомендовані Нацыональним банком України;
- звіт про операційні ризики, виявлених за певний період (і імовірності їх реалізації). Більшість внутрішніх замовників цікавить не математичний розрахунок ймовірності реалізації ризику (особливо в умовах кризи), а конкретні заходи щодо його запобігання; звіт за ключовими індикаторами ризик; звіт про технологічний відміну (перевазі / відставанні) від лідируючих кредитних організацій в частині операційного ризику;
- звіт про операційні ризики корпоративного рівня та рівня бізнес-одиниць ;
- карта ризиків.

З метою моніторингу операційного ризику застосовується система індикаторів рівня операційного ризику (фіксування подій), тобто показників, які пов'язані з рівнем операційного ризику, прийнятого кредитною організацією.

При визначенні індикатора ризику формулюється гіпотеза про існування в банку об'єктивного вимірного кількісного показника ризику, який характеризує певну групу втрат. В якості індикаторів рівня операційного ризику можуть бути використані:

- відомості про кількість зірваних або незавершених банківських операцій та інших угод, збільшення їх частоти чи обсягів;
- плинності кадрів;
- частота допускаються помилок і порушень;

Для кожного індикатора рекомендується встановити ліміти (порогові значення), що дозволить забезпечити виявлення значущих для кредитної організації операційних ризиків і своєчасне адекватне вплив на них.

2.4 Корпоративне управління та оцінка ділової репутації власників банку як частина управління операційним ризиком

Згідно з документом Базельського комітету з банківського нагляду «Удосконалення корпоративного управління в кредитних організаціях», корпоративне управління в банківських організаціях - це управління їх діяльністю, що здійснюється радами директорів і менеджерами вищої ланки та визначає методи, за допомогою яких банки:

- визначають цілі свого бізнесу, серед яких і створення вартості для власників банків; проводять щоденні фінансові операції;

- враховують у своїй роботі позиції зацікавлених сторін (співробітників, клієнтів, громадськості, регулюючих органів і держави).

Сьогодні проблема розвитку корпоративного управління у банках зумовлена тим, що на перший план у банківському бізнесі виходить управління ризиками: воно стає найважливішим елементом системи внутрішнього контролю. Як відомо, Базельський комітет з банківського нагляду виділяє 12 категорій банківського ризику: системний, стратегічний, кредитний, кредитний, ринковий, процентний, ризик ліквідності, валютний, операційний, правовий, репутаційний, ризик дотримання.

Складність ситуації з управлінням ризиками в банках країн з ринками, що формуються, пояснюється, насамперед, низьким рівнем корпоративного управління: серйозними конфліктами інтересів і їхнім неефективним вирішенням у рамках нерозвинутої системи правозастосування, неадекватним відношенням рад директорів до проблеми управління ризиками в рамках системи внутрішнього контролю (поверхневим розумінням суті питання і слабким наглядом за роботою менеджерів, які забезпечують функціонування відповідних служб), недоліками в розкритті інформації, нечисленністю національних фірм, здатних провести кваліфікований і незалежний зовнішній аудит. Іншими словами, ефективне управління банківськими ризиками і належне корпоративне управління в банках - дві сторони однієї медалі.

Тісний взаємозв'язок цих сторін виявляється і у впливі якості корпоративного управління в банку на оцінку ризику, що надають банку потенційні інвестори. З погляду останніх, неефективне корпоративне управління в банку означає посилення притаманних йому кредитного, операційного і репутаційного ризиків і тому призводить до зниження вартості його цінних паперів.

Зростання операційного ризику в банку зі слабким корпоративним управлінням пов'язано з відсутністю або незадовільним функціонуванням системи внутрішнього контролю, комітету з аудиту, служби внутрішнього аудиту.

Добре відомо, що репутація фінансової установи істотно залежить від репутації тих осіб, які користуються її послугами. Щоб не мати справи з компаніями, які одержали чи можуть одержати скандальну популярність, банк повинен приділяти значну увагу стану корпоративного управління у своїх контрагентів. Звичайно, не можна очікувати подібного відношення від банку, що не вважає за необхідне поліпшувати власну систему корпоративного управління, тому інвестор підвищує оцінку репутаційного ризику.

Сьогодні вітчизняним банкам необхідно кардинально поліпшити якість «двосторонньої медалі» (управління ризиками - корпоративне управління). При досягненні цього, частина з них зможе вистояти в конкурентній боротьбі і залишитися самостійними організаціями, а інші одержать максимальну ціну за свої акції при продажі бізнесу закордонним покупцям.

Підвищення рівня корпоративного управління дозволяє банкам вирішити проблему "поганих" кредитів і зміцнити довіру потенційних контрагентів (вкладників, позичальників, клієнтів по валютних і фондових операціях). В наслідок цього розподіл кредитних ресурсів між нефінансовими компаніями стає більш раціональним, що дає можливість економіці країни вийти на траєкторію стійкого зростання. Від створення належної системи корпоративного управління в банківському секторі виграють усі зацікавлені сторони:

- банки підвищать ефективність своєї діяльності;
- банківська система в цілому залучить нових вкладників, позичальників, інвесторів та інших контрагентів;

- акціонери банків одержать впевненість у забезпеченні захисту і підвищенні прибутковості своїх інвестицій;
- держава зможе розраховувати на підтримку банківського сектора у своїх зусиллях щодо зміцнення конкурентноздатності національної економіки і боротьби із шахрайством та корупцією;
- суспільство в цілому скористається плодами збільшення суспільного багатства.

Відповідно до документів Базельського комітету, ефективна система корпоративного управління в сучасному конкурентноздатному банку ґрунтується на низці принципів, суть яких полягає в наявності:

- цінностей корпоративної культури, зафіксованих у кодексі корпоративної поведінки й інших стандартів ділової етики, а також системи, що забезпечує прихильність цим цінностям на практиці;
- чітко сформульованої стратегії розвитку, відповідно до якої оцінюються результати роботи усього банку й окремих осіб;
- чіткого розподілу прав (у тому числі певної ієрархії прав у сфері прийняття рішень) і обов'язків;
- ефективного механізму взаємодії і співробітництва між радою директорів, топ-менеджментом і аудиторами;
- надійної системи внутрішнього контролю (включаючи оцінку ефективності даної системи, проведену службою внутрішнього аудиту і зовнішнім аудитором) і служби управління ризиками (що діє незалежно від бізнес-напрямків і бізнес-одиниць);
- постійного моніторингу ризиків у певних галузях банківського бізнесу, що характеризуються високою імовірністю виникнення конфліктів інтересів (ці галузі охоплюють, по-перше, взаємодію банку з позичальниками - афільованими і пов'язаними особами, акціонерами і менеджерами вищої ланки, і, по-друге, діяльність осіб, які здійснюють істотні угоди, наприклад операції провідних трейдерів банку на фондовому ринку);

- сукупності фінансових і кар'єрних стимулів, що створюють умови для належної роботи менеджерів та інших співробітників;
- системи інформаційних потоків, що забезпечує внутрішні потреби організації і необхідний для зовнішніх контрагентів рівень прозорості банку.

Для банківського бізнесу надзвичайно важливо, щоб структури корпоративного управління функціонували на основі принципу «перевіряй та складай баланси»[3]. Система взаємообмежень містить у собі контроль на чотирьох рівнях:

а) рада директорів;

б) спеціально уповноважені особи, які не мають відношення до управління щоденними операціями;

в) підрозділи, що несуть пряму відповідальність за різні сфери діяльності банку;

г) служби управління ризиками і внутрішнім аудитом, що функціонують незалежно від бізнес-напрямків і бізнес-одиниць банку.

Як зазначає Базельський комітет з банківського нагляду варто організувати як мінімум чотири комітети: з аудиту, винагород, призначення, управління ризиками.

Проаналізуємо, як реалізується це правило в десятьох провідних банках США і Європейського союзу (див. табл. 2.3).

Комітетиз аудиту організовані у всіх розглянутих банках - як в американських, так і в європейських. Ситуація з іншими комітетами неоднакова: банки США частіше створюють комітети з винагород і призначень, а банки Євросоюзу - комітети з управління ризиками. Звичайно, відсутність того чи іншого спеціального комітету не означає відсутності діяльності у відповідних сферах: у цьому випадку визначені обов'язки покладаються на інші комітети. Так, у трьох з десяти найбільших американських банків підбір кандидатів на посади менеджерів вищої ланки здійснюється комітетом з корпоративного управління.

У трьох банків Євросоюзу замість окремих комітетів з винагород і призначень створено один комітет, що займається обома зазначеними питаннями. Два

[3] Від англ. - checks and balances.

європейських банки віднесли винагороди і призначення до компетенції інших комітетів, а один банк включив призначення директорів і топ-менеджерів у перелік функцій комітету з корпоративного управління і сприяння голові ради директорів.

Таблиця 2.3

Організація комітетів ради директорів у банках США та Євросоюзу

Комітети СД в американських і європейських банках				
	Наявність спеціальних комітетів у СД, кількість банків			
	Аудит	Винагороди	Управління ризиками	Призначення
Банки США	10	10	7	1
Банки Євросоюзу	10	5	4	5

Що стосується управління ризиками, то при відсутності спеціального комітету за цей напрямок відповідає, як правило, або комітет з аудиту, або об'єднаний комітет з аудиту і управління ризиками (перший варіант використовують п'ять банків Євросоюзу і три банки США, другий - два американських банки). В інших випадках це завдання виконують інші комітети (з фінансів, технологій, якості активів тощо).

Відповідно до розпоряджень Базельського комітету і рекомендацій Глобального форуму з корпоративного управління банки повинні приділяти особливу увагу процесу взаємодії ради директорів із внутрішніми і зовнішніми аудиторами.

Відносини між ними необхідно будувати на базі визнання всіма директорами украй важливої ролі аудиту в системі корпоративного управління. Рада директорів зобов'язана використовувати інформацію, надану внутрішніми і зовнішніми аудиторами, для перевірки інформації, отриманої від топ-менеджерів. Співробітництво ради директорів з аудиторами здійснюється насамперед через комітет ради директорів з аудиту. З метою забезпечення незалежності структур, що діють у сфері аудиту, потрібно дотримуватись наступних правил:

- головою комітету ради директорів з аудиту не слід призначати голову ради директорів;
- голова служби внутрішнього аудиту повинен звітувати перед комітетом ради директорів з аудиту;

- -призначення/перерозподіл співробітників служби внутрішнього аудиту повинні затверджуватися в комітеті ради директорів з аудиту;
- комітет ради директорів з аудиту повинен мати прямий доступ до керівника групи співробітників фірми, що здійснює зовнішній аудит (старшого партнера);
- у договорі з фірмою, що здійснює зовнішній аудит, необхідно передбачити процедуру зміни зазначеного старшого аудитора кожні п'ять-сім років;
- якщо банк користується не тільки аудиторськими, але й консультаційними послугами фірми, що здійснює зовнішній аудит, то консультації повинні бути додатковим, а не основним напрямком ділових взаємин.

Розглянемо основні вимоги до групи виконавчих посадових осіб вищої ланки, системи винагороди і заохочення топ-менеджерів і головних співробітників, системи забезпечення інформаційної прозорості.

Система винагороди і заохочення топ-менеджерів і ключових співробітників повинна відповідати цінностям корпоративної культури, що склалася в банку, а також його цілям, стратегії і створеному в ньому контрольному середовищу (умовам, у яких функціонує система внутрішнього контролю).

Фінансові і кар'єрні стимули варто орієнтувати на підтримку необхідного балансу між виконанням довго- і короткострокових завдань і на недопущення надмірно ризикованих операцій.

Інформаційна прозорість у сфері корпоративного управління необхідна для реалізації принципу підзвітності ради директорів і топ-менеджерів акціонерам банку. Базельський комітет вказує, що банки повинні розкривати інформацію про: раду директорів (чисельність і склад ради директорів, комітети ради директорів і їхній склад, кваліфікацію директорів); менеджерів вищої ланки (обов'язки, підзвітність, кваліфікацію, досвід); організаційну структуру банку (функціональні й операційні підрозділи, бізнес-одиниці); систему матеріального стимулювання членів ради директорів і топ-менеджерів (політика в сфері винагород, дані про премії,

пільги й опціони на придбання акцій); а також сутність і розміри угод з афільованими і пов'язаними фізичними та юридичними особами.

Отже, основними цілями ефективного корпоративного управління у банку є:

- забезпечення збалансованого співвідношення між ризиком та вигодою для захисту інтересів акціонерів та інших зацікавлених осіб;
- належне визначення стратегії управління ризиками, що підвищує динамізм роботи банку.

Основними вигодами від ефективного корпоративного управління та управління операційними ризиками є:

- підвищення ефективності діяльності банку;
- покращення його репутації;
- доступ до міжнародних джерел капіталу;
- здешевлення вартості залученого капіталу;
- збільшення ринкової вартості банку та підвищення інтересу інвесторів до нього.

Основні недоліки у корпоративному управлінні у банку можуть призвести до:

- зловживань;
- втрати довіри та репутації;
- втрати ділових партнерів та клієнтів;
- поглинання;
- банкрутства та ліквідації.

Питання управління операційними ризиками як елементу корпоративного управління є важливим з огляду на те, що виважене ризикування у банку є джерелом значних доходів. В той же час управління ризиками, на відміну від їх уникнення, забезпечує стабільний розвиток та зростання банку.

Провідну роль у корпоративному управлінні та управлінні ризиками грають акціонери, які призначаючи до Спостережної ради досвідчених та кваліфікованих фахівців можуть встановлювати «Належні правила та політики».

З огляду на це, Спостережна рада повинна:

- затверджувати політику управління ризиками;

- направляти правління на правильні рішення щодо ризиків;
- розуміти та впливати на обрану правлінням схильність до ризиків;
- відстежувати стан управління ризиками;
- портфельно розглядати ризики банку.

У той же час Правління повинне:

- розробляти політику управління ризиками;
- впроваджувати стратегічні плани та політику управління ризиками;
- визначати, оцінювати та управляти усіма видами ризиків;
- створити систему негайного інформування про порушення управління ризиками.

Органи нагляду мають забезпечити збільшення довіри суспільства до банків, захист інтересів вкладників та створення конкурентного середовища у банківській системі.

Отже, Спостережна рада має установити стратегії, що управляють поточною діяльністю банку. Вона також має бути лідером в установленні правильного "тону на горі" і ухваленні корпоративних цінностей для себе, правління, а також інших працівників. Цінності мають визнавати особливу важливість своєчасного відвертого обговорення проблем. Наприклад, важливо, щоб ці цінності забороняли корупцію і хабарництво в корпоративній діяльності, як у внутрішніх операціях, так і у зовнішніх операціях.

Рада директорів має забезпечити виконання положень правлінням, що забороняє (або значно обмежує) операції і стосунки, що погіршують якість корпоративного управління, як наприклад:

- конфлікт інтересів;
- надання позик керівникам і працівникам, а також інші форми самокредитування (наприклад, внутрішнє кредитування слід обмежити кредитуванням, що узгоджується з ринковими умовами і певними типами позик, і звіти про кредитування інсайдерів мають надаватися раді, а також підлягати розгляду внутрішніми і зовнішніми аудиторами); а також забезпечення привілейованого ставлення до пов'язаних сторін та

інших привілейованих осіб (наприклад, надання кредитів на високо привілейованих умовах, покриття торговельних збитків, скасування комісійних тощо).

Слід запровадити у практику процеси, що дозволяють раді здійснювати моніторинг за виконання цих положень і забезпечити, щоб відповідний рівень керівництва інформувався про будь-які відхилення від цього.

Визначення і запровадження чіткого розмежування сфер відповідальності і підзвітності в межах установи.

Ефективна рада директорів чітко визначає повноваження і основні сфери відповідальності як для себе, так і для правління. Вона також визнає, що невизначені рівні підзвітності або плутані, множинні сфери відповідальності • можуть погіршити проблему через повільне або розпливчасте реагування. Вище керівництво відповідає за створення ієрархії підзвітності для персоналу, проте воно має знати про те, що вони зрештою несуть відповідальність перед радою за діяльність банку.

Забезпечення належної кваліфікації членів ради директорів, що відповідає їх посадам, основного розуміння ними своєї ролі в корпоративному управління і захисту їх від неприйнятного тиску з боку керівництва або зовнішніх сторін.

Рада директорів несе відповідальність за операції і фінансову надійність банку. Рада директорів має отримувати своєчасно достатню інформацію для того, щоб судити про діяльність керівництва. Ефективна. кількість членів ради має бути здатна використовувати своє судження, незалежно від поглядів керівництва, великих акціонерів або уряду. Включення у раду кваліфікованих директорів, що не є членами правління, або і відокремленість наглядацької ради або ради аудиторів від правління може підвищити незалежність і об'єктивність. Більше того, такі члени можуть привнести нову перспективу з боку інших сфер бізнесу, що може поліпшити стратегічний напрямок, що надається керівництву, як, наприклад, більш глибоке розуміння місцевих умов. Кваліфіковані зовнішні директори можуть також стати важливим джерелом керівного досвіду у часи корпоративного струсу. Рада, директорів має періодично оцінювати власну діяльність, визначати, де існують слабкі сторони і там, де це можливо, вживати виправних заходів.

Рада директорів посилює корпоративне управління банку, коли вона:

- розуміє свою наглядацьку роль і „обов'язок вірності" банку і його акціонерам;
- слугує як система взаємного контролю у щоденних справах банківського керівництва;
- відчуває себе уповноваженою ставити питання перед керівництвом і може наполягати на
- отриманні прямих пояснень від керівництва;
- рекомендує здорову практику, що накопичена в інших ситуаціях;
- надає неупереджені поради;
- не є перевантаженою;
- уникає конфлікт інтересів в діяльності або зобов'язаннях з іншими організаціями;
- зустрічається регулярно з вищим керівництвом І внутрішнім аудитом для того, щоб розробити і
- ухвалити положення, установити канали комунікації, а також контролювати прогрес на шляху до досягнення корпоративних цілей;
- ухиляється від прийняття рішень, коли члени ради нездатні надавати об'єктивні поради;
- не приймає участі в щоденному управлінні банку [19].

В сучасних умовах ефективне управління операційним ризиком можливе виключно при наявності загальної культури управління ризиками:

Така культура повинна передбачати:

- чіткі правила;
- чіткі обов’язки;
- широко розповсюджене розуміння ризику.

З метою формування культури управління операційними ризиками Базельський комітет з банківського нагляду опублікував документ «Належна практика управління і контролю над операційними ризиками» [20].

Структура корпоративного управління створює підґрунтя для будь – якої діяльності, яка супроводжує ризик, в результаті чого формується профіль ризику.

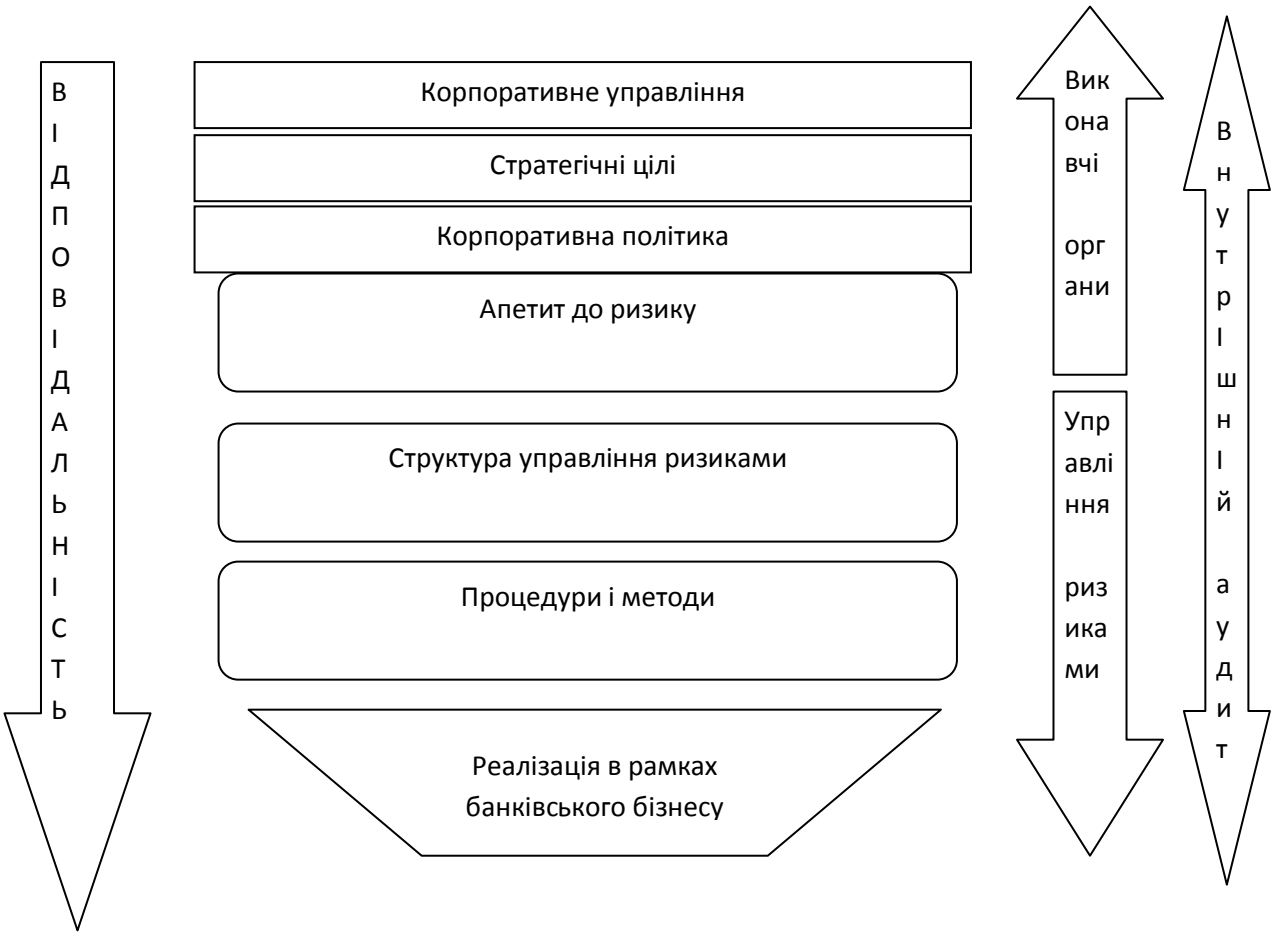


Рис. 2.1. Структура корпоративного управління
Джерело: [19].

Правління є ключовим компонентом корпоративного управління.

В той час як рада директорів забезпечує систему взаємного контролю для вищого керівництва, аналогічним чином, вищі керівники мають брати на себе наглядацьку роль щодо керівників середньої ланки в певних сферах бізнесу і операціях. Навіть в дуже маленьких банках, ключові керівні рішення мають прийматися більше ніж однією особою („принцип чотирьох очей"). Слід уникати ситуацій з керівництвом, що включають:

- вищих керівників, які занадто щільно залучені до прийняття рішень щодо різних сфер бізнесу;
- вищих керівників, яким доручено сферу керівництва, коли вони не мають необхідних попередніх знань або вміння для цього;

- вищих керівників, які не бажають здійснювати контроль за успішними ключовими працівниками (такими як торговці) через страх втратити їх.

Правління складається з основної групи керівників, відповідальних за банк.

Ця група має включати такі особи, як головний фінансовий директор, керівники відділів і головний аудитор. Ці особи мають мати необхідні вміння для керівництва бізнесом під їх наглядом, а також належний контроль за ключовими особами в цих сферах.

Ефективне використання результатів робота внутрішніх і зовнішніх аудиторів, визнання важливої контрольної функції, що вони виконують.

Роль аудиторів є надзвичайно важливою для процесу корпоративного управління. Ефективність ради і вищого керівництва можна посилити шляхом: 1) визнання важливості аудиторського процесу і доведення до відома банківських працівників важливості цього; 2) прийняття заходів, що посилюють незалежність і статус аудиторів; 3) вчасного і ефективного використання висновків аудиторів; 4) забезпечення незалежності головного аудитора через підзвітність раді або аудиторському комітету ради; 5) залучення зовнішніх аудиторів до визначення ефективності системи внутрішнього контролю, а також 6) висування вимоги вчасного виправлення керівництвом проблем, що виявлені аудиторами [19].

Виходячи із сутності корпоративного управління як способу, у який акціонери банку, Спостережна рада та Правління впливають на те, як банки:

- визначають корпоративні цілі;
- проводять щоденну операційну діяльність;
- враховують інтереси зацікавлених осіб;
- захищають інтереси владників;
- приводять корпоративну діяльність та поведінку у відповідність із наявними очікуваннями суспільства.

Основними цілями ефективного корпоративного управління у банку є:

- забезпечення збалансованого співвідношення між ризиком та вигодою для захисту інтересів акціонерів та інших зацікавлених осіб;

- належне визначення стратегії управління ризиками, що підвищує динамізм роботи банку.

Основними вигодами від ефективного корпоративного управління та управління операційними ризиками є:

- підвищення ефективності діяльності банку;
- покращення його репутації;
- доступ до міжнародних джерел капіталу;
- здешевлення вартості залученого капіталу;
- збільшення ринкової вартості банку та підвищення інтересу інвесторів до нього.

Недоліки у корпоративному управлінні у банку можуть призвести:

- зловживань;
- втрати довіри та репутації;
- втрати ділових партнерів та клієнтів;
- поглинання;
- банкрутства та ліквідації.

Питання управління операційними ризиками як елементу корпоративного управління є важливим з огляду на те, що виважене ризи кування у банку є джерелом значних доходів. В той же час управління ризиками, на відміну від їх уникнення, забезпечує стабільний розвиток та зростання банку.

Провідну роль у корпоративному управлінні та управлінні грають акціонери, які призначаючи до Спостережної ради досвідчених та кваліфікованих фахівців можуть встановлювати «Належні правила та політики».

Спостережна рада повинна:

- затверджувати політику управління ризиками;
- направляти правління на правильні рішення щодо ризиків;
- розуміти та впливати на обрану правлінням схильність до ризиків;
- відстежувати стан управління ризиками;
- портфельно розглядати ризики банку.

У той же час Правління повинне:

- розробляти політику управління ризиками;
- впроваджувати стратегічні плани та політику управління ризиками;
- визначати, оцінювати та управляти усіма видами ризиків;
- створити систему негайного інформування про порушення управління ризиками.

Органи нагляду мають забезпечити збільшення довіри суспільства до банків, захист інтересів вкладників та створення конкурентного середовища у банківській системі.

Стосовно питання управління операційними ризиками згідно Базель ІІ є вимога до розкриття інформації, яка вимагає розміщення на інтернет сторінці банку:

- стратегії та методології управління ризиками;
- ранжування ризиків за їх впливом;
- обовязки та відповідальність органів банку з управління ризиками;
- внутрішні процедури та контролю;
- стратегічне управління операційним ризиком та плани запровадження вимог Базель ІІ.

Отже, як засвідчив зарубіжний і вітчизняний досвід, організація ефективного корпоративного управління покликана захистити інтереси акціонерів і засновників фінансово-кредитної установи, вкладників та кредиторів банку і дозволяє наглядовим органам більше довіряти внутрішнім організаційно-економічним процесам. Запровадження корпоративного управління в банківській сфері України стає надзвичайно важливим в умовах вступу нашої країни до СОТ та виходу на ринок іноземних банків, у результаті чого суттєво змінюються умови конкуренції на ринку банківських послуг.

Запровадження ефективного корпоративного управління дозволяє забезпечити раціональне використання фінансових ресурсів, збалансовані взаємовідносини широкого кола учасників бізнесових проектів, включаючи засновників фінансово-кредитних установ, акціонерів і менеджерів, а також підтримувати довіру населення до політики уряду і корпорацій.

Враховуючи надзвичайну роль фінансово-кредитної сфери для економіки країни, слід зазначити, що система корпоративного управління має більш важливе значення для банківських установ, ніж для інших підприємств. Це пов'язано з тим, що банки є ключовою ланкою економіки, вони чутливіші до потенційних ускладнень у випадку неефективного управління, залежать від системи захисту коштів вкладників і клієнтів та їх довіри; а також це зумовлено взаємозв'язком і взаємозалежністю банків з іншими секторами та підприємствами економіки.

Окрім того, забезпечення ефективного корпоративного управління на рівні як окремого банку, так і банківської системи в цілому є запорукою високого рівня довіри громадськості до економіки в цілому.

Розвиток економіки стимулює розвиток банківської системи, а розвиток банків забезпечує поступовий розвиток економіки. І чим швидшими темпами буде розвиватися економічний комплекс держави, тим вищим повинен бути рівень концентрації банківського капіталу, щоб стабільно забезпечувати потреби суб'єктів господарювання у фінансових ресурсах. Основними напрямами підвищення рівня концентрації банківського капіталу є забезпечення капіталізації банківських установ із використанням широкого кола джерел фінансування, а також розвиток процесів консолідації банків шляхом їх об'єднання, злиття та поглинання.

Основними критеріями оцінки ефективності запровадження корпоративного управління в банківських установах є поєднання чотирьох елементів:

1) структури власності та рівня впливу на банк з боку власників (засновників), які визначають прозорість власності та рівень її концентрації в окремих власників;

2) системи прав фінансово зацікавлених осіб та можливості реалізації керівництвом банківської установи на основі надання акціонерам прав в управлінні через збори акціонерів або участь в інших керівних органах, що дозволило б певним чином контролювати фінансову діяльність;

3) фінансової прозорості та відкритості інформації про установу для всіх фінансово зацікавлених учасників ринку і власників капіталу;

4) формування оптимальної структури та запровадження раціональних методів організації роботи наглядової ради та ради директорів, діяльність яких базується,

зазвичай, на створенні та функціонуванні спеціальних комітетів, метою діяльності яких є консультування вищого керівництва.

Групою фахівців під керівництвом П.Кумза було розроблено загальну характеристику ознак високого рівня організації системи корпоративного управління, а проведені дослідження засвідчили: при підвищенні рівня корпоративного управління компанії можуть розраховувати на додатковий 10-12-відсотковий приріст своєї капіталізації, а також суттєвепокращення інших фінансових показників. Так, прозорість фінансових результатів діяльності дозволяє банку встановлювати чіткі орієнтири розвитку, формувати високий рівень відповідальності по всій вертикалі управління. Існування комітету з аудиту створює умови для контролю за діяльністю фінансового директора, допомагає визначити методи управління ризиками, адекватні ситуації на ринку, а також розробити стратегію бізнесу відповідно до змін у зовнішньому середовищі.

Вітчизняна практика засвідчила, що у запровадженні ефективної практики корпоративного управління найбільше повинні бути зацікавлені органи банківського нагляду, які розробляють стратегії своєї діяльності залежно від величини банківських установ та притаманних їм ризиків.

Організація ефективного корпоративного управління вимагає створення належних і міцних юридичних, регуляторних та інституційних засад. На цілісність ринку та загальні економічні показники може вплинути ціла низка різноманітних чинників, від загальної макроекономічної ситуації та законодавчої бази до системи бухгалтерського обліку та аудиту. Разом з тим слід зазначити, що ці фактори часто перебувають поза сферою впливу банківського нагляду, але фахівці банківського нагляду повинні бути обізнані з юридичними та інституційними перешкодами ефективному корпоративному управлінню і на основі цього вживати заходів для забезпечення стабільної і прозорої діяльності фінансово-кредитних установ.

Слід також відмітити, що виключно важливого значення реалізація принципів корпоративного управління набуває після висунення додаткових вимог до переглянутих міжнародних засад достатності банківського капіталу (Друга базельська угода, або Базель II), відповідно до яких вище керівництво банку

зобов’язане враховувати ризики, властиві банку, і забезпечити, щоб рівень капіталу адекватно відображав ці ризики.

Що стосується оцінки ділової репутації власників банку в аспекті корпоративного управління та операційного ризик – менеджменту важливо відзначити, що по суті якість оцінки ділової репутації власників банку прямо взаємозалежна із рівнем операційного ризику.

Діяльність будь-якого банку значною мірою залежить від ділової репутації його керівників та самої фінансової установи. Водночас репутація пов'язана зі значною кількістю ризиків на різних рівнях організації банку. Тому банки повинні постійно страхуватися від цих ризиків і дбати про свій імідж та ділову репутацію співробітників.

Досвід економічно розвинутих європейських країн свідчить, що на сьогодні немає жодного документа чи критерію, який би встановлював та описував підходи до визначення ділової репутації. Тому в дослідженні пропонуємо розглянути можливі методологічні підходи щодо оцінки ділової репутації керівників банків.

Змогу оцінити рівень ділової репутації власників банку і визначити рівень ризику репутації можуть дати анкети, а саме:

— анкета на оцінку ділової репутації особи власника істотної участі (резидента) для юридичної (крім банків) особи;

— анкета на оцінку ділової репутації особи власника істотної участі (резидента) для фізичної особи;

— анкета на оцінку ділової репутації особи члена правління банку;

— анкета на оцінку ділової репутації особи, відповідальної за фінансовий моніторинг.

Ділову репутацію власників можна визначити в першу чергу на основі такої інформації: наявність освіти, відсутність правопорушень адміністративного та карного кодексу України, наявність довідок із податкової інспекції, наявність публікацій про кандидата у засобах масової інформації [13].

ІІІ. МОДЕЛЮВАННЯ КІЛЬКІСНОЇ ОЦІНКИ РІВНЯ ОПЕРАЦІЙНОГО РИЗИКУ

3. Методологічні підходи до обчислення ймовірностей помилок в операційній системі банку

3.1 Практика знаходження рішень в умовах невизначеності

Як відомо, будь-який суб'єкт господарювання функціонує в умовах інформаційної асиметрії, тобто він не може на 100% володіти повним обсягом інформації щодо майбутнього економічного розвитку, інтесивності впливу тих чи інших ринкових сил або дій інших учасників ринку тощо. Саме тому завжи має місце певний ризик – непевність щодо результатів, які очікується отримати в перспективі. І хоча такий ризик не можна повністю уникнути, прте його можна виміряти та врахувати при прийнятті низки управлінських рішень, що в значній мірі дозволить мінімізувати можливі втрати. Безперечно, ризики властиві й банківському бізнесу.

Проте, якщо менеджмент банківської установи володіє інформацією, що дозволяє адекватно вимірювати різного роду ризики, тоді існує можливість сформувати ефективну систему протидії несприятливим ситуаціям. В той же час, за умови неоднозначної ідентифікації дестабілізуючих, факторів особа, що приймає рішення, повинна негайно реагувати на зміну внутрішнього та зовнішнього середовища, оскільки ігнорування невизначених ризиків може призвести до значними за обсягами та рівнем впливу витрат.

Ми неодноразово ототожнювали категорії «ризик» та «непевність». І, безперечно, з нашого боку було б значнним упущенням не надати тлумачення останньому визначенню.

Так, сучасній економічній літературі зустрічаються такі підходи до інтерпретації даної категорії:

- по-перше, як неповнота та неточність інформації про умови реалізації прийнятого рішення [21];
- по-друге, як неясність (відсутність точного знання) відносно майбутніх станів усіх прогнозних параметрів фінансової моделі;
- по-третє, як нечіткість класифікації окремих сторін поточного фінансового стану господарюючого суб'єкта чи стану ринку цінних паперів [22] тощо.

На основі аналізу наведених вище визначень категорії «невизначеність», а також дослідженні літературних джерел [21, 22, 23], можна стверджувати, що невизначеність в діяльності комерційного банку може бути зумовлена такими причинами:

- кон'юнктурою зовнішнього середовища;
- поведінкою контрагентів та конкурентів;
- змінністю соціально-економічних та науково-технічних процесів;
- браком часу для прийняття управлінських рішень;
- неповнотою та асиметрією інформації;
- неоднозначністю інформації, виникнення якої пов'язано з тим, що деяка інформація може інтерпретуватися різними способами;
- неадекватністю інформації, обумовленої застосуванням даних, що не відповідають реальній ситуації (можливими причинами є суб'єктивні помилки: неправдиві данні, дезінформація, невірно запрограмовані обчислювальні операції, тощо);
- ненадійністю прогнозних оцінок функціонування досліджуваних об'єктів та кон'юнктури ринку;
- похибками розрахунків, що виникають в наслідок недотримання вимог правильності та точності критеріїв кількісного представлення даних;

- помилками, проявом яких є випадкові коливання даних щодо їх середнього значення (причиною можуть бути: збої системи збереження та передавання даних, вплив сторонніх факторів) тощо.

Для більш глибокого аналізу категорії «невизначеність» доцільно також розглянути підхід, згідно з яким вона інтерпретується, як складна динамічна система, елементи якої є взаємообумовленими, виконують визначені функції та забезпечують формування нових властивостей не характерних кожній зі складових. Так, системоутворюючими елементами категорії «невизначеність» виступають:

- невизначеність елементів проблеми;
- цільова невизначеність;
- невизначеність середовища.

Розглядаючи кожну зі складових категорії «невизначеність» більш детально, слід сказати, що невизначеність елементів проблеми характеризується неповнотою та недостатністю інформації відносно досліджуваної проблеми, вирішення якої вимагає прийняття управлінського рішення. В свою чергу, цільова невизначеність – нечітке усвідомлення і відповідно неточне подальше формування особою, що приймає рішення, цілей дослідження, обумовлених в більшості випадків суперечливим характером критеріїв ефективності розглянутих альтернатив. Третій елемент системи – невизначеність середовища – це неможливість чіткої ідентифікації можливих наслідків реалізації розроблених альтернатив управлінського рішення. Причиною виникнення даної ситуації вважається невідомість майбутнього розвитку зовнішнього середовища.

Отже, «невизначеність» може розглядатися як недостатність адекватної інформації для прийняття рішення, що, в свою чергу, стає проблемою, оскільки може зашкодити прийняттю найкращого рішення і навіть стати причиною хибних кроків.Тут варто, на наш погляд, навести висловлювання А.Тайманса, консультанта Агентства з передачі фінансових технологій (ЕйТіТіЕф (ATTF), Люксембург), який під час одного з семінарів зазначив: «банкіри — це старі вівці». «Вівці» — оскільки їм притаманне ведення бізнесу за принципом «сліпо наслідуй конкурента і намагайся бути будь-що кращим за нього», а старі — оскільки «уроки історії ніколи

не засвоюються». Спробуємо пояснити як «старі вівці» пов’язані з невизначеністю. Скажімо, що відбудеться, якщо в засобах масової інформації зявится інформація, що акціонерна компанія «А» - на межі банкрутства? Ціна її акцій впаде, а водночас більшість тих, хто мав її акції у своїх портфелях, продадуть їх за безцінь. Проте, інформація виявиться неправдивою – наприклад, це прикра помикла тих, хто дуже бажав отримати контрольний пакет акцій компанії «А» зі знижкою. Але, подивимось на цю ситуацію з іншого боку: учасники ринку діяли в умоваж інформаційної аситемрії – тобто вони мали лише частину даних, які до того ж були неадекватно інтерпретовані. Тому вони, сприаючись на інформацію, що невдовзі компанія «А» збанкрутує, приймають рішеня отримати хоча б частну інвестованих коштів. Більше того, «стадна» поведінка решти учасників ринку, які також продають свої акції, зміцнює їх упевненість у правильності рішення. Врезультаті – «старі вівці», що діяль в умовах непевності, зазнали втрат.

Безперечно, позбутися непевності – неможливо, але можливо розрахувати її ступінь і скоригувати рішення, зменшивши якнайбільше або уникнувши втрат. Хоча тут також є низка складностей.

Зокрема, ефективне рішення, знайдене в реальному часі, часто вважається більш прийнятним, ніж найкраще рішення, для обчислення якого потрібна велика кількість часу. Так, затримка при прийнятті рішення внаслідок збору додаткових даних та їх аналізу може також призвести до суттєвих фінансових втрат.

Отже, ми розібралися з категорією «невизначеність», але, як ви пам’ятаєте, йшлося про прийняття рішень в умовах невизначеності. Таким чином, ми також повинні проаналізувати, що ж означає категорія «рішення».

Внаслідок проведеного аналізу останніх публікацій [21], [24], категорію «рішення» слід розглядати як можливість найбільш ефективного розв’язання комплексу фінансових, науково-технічних, проектно-конструкторських, технологічних і організаційно-управлінських завдань для забезпечення створення продукції чи надання послуг необхідного науково-технічного рівня, об’єму і в завдані строки в умовах діючих ресурсних обмежень та їх прогнозу на період виконання проекту.

В свою чергу, пропонуємо розглянути узагальнений алгоритм прийняття рішення, який, на нашу думку, можна розглядати як процес, що складається з наступної послідовності етапів:

- постановка задачі і діагностика проблеми;
- формування мети вирішення проблеми;
- розробка альтернатив досягнення мети;
- опис можливих станів зовнішнього середовища,
- оцінка імовірностей настання визначених станів зовнішнього середовища,
- виявлення можливих результатів (наслідків) реалізації кожної з альтернатив,
- оцінка результатів реалізації альтернатив у кожному стані зовнішнього середовища,
- вибір критеріїв для оцінки альтернатив у кожному стані зовнішнього середовища,
- розрахунок значень критеріїв ефективності прийняття рішення у кожному стані зовнішнього середовища,
- оцінка очікуваного ефекту реалізації кожної альтернативи,
- порівняння альтернатив за величиною очікуваного ефекту та вибір найкращої альтернативи,
- прийняття рішення, тобто затвердження плану виходу з проблемної ситуації.

Також необхідно зазначити, що проаналізуваши теоретичні аспекти та найпоширеніші науково-методологічні підходи до прийняття ефективних управлінських рішень, зокрема у банківській діяльності, можна виокремити такі основні принципи даного процесу:

- значно підвищити ефективність прийняття рішень в умовах невизначеності і ризику дозволяє застосування *апостеріорних імовірностей* (підхід на основі використання теореми Байєса корегування гіпотези) як оптимального критерію, що обумовлене можливістю врахування як накопиченого досвіду менеджменту банку, так і

оперативної інформації щодо характеристики можливих альтернатив вибору;

- врахувати нечіткість як вхідної інформації, так і результативних характеристик, а також формалізувати опосередкованість впливу визначальних факторів прийнятого управлінського рішення, дозволяє застосування *теорії нечіткої логіки*, що обумовлене можливістю кількісної характеристики неявно або неточно заданих величин.

Підбиваючи підсумок вищевикладеного, ми можемо зазначити, що ***ризик прийняття неефективних рішень*** виникає в ситуації, коли існує можливість вибору декількох варіантів і немає впевненості, що прийняте рішення - найефективніше, тобто виникає інформаційна невизначеність.

3.2 Математичні методи і моделі прийняття рішень в умовах невизначеності

Якщо ви звернули увагу, то у попередньому розділі ми стверджували, що унукнути непевності (власне кажучи, ризику) – неможливо, проте можливо та необхідно її (його) вимірювати. Для цього нам знадобляться математичні формули. На перший погляд ці формули можуть видатися зарозумілими та складними, проте не варто їх лякатись - в даному випадку вони, як ліки – можуть спричинити певний дискомфорт, але в результаті принуть значну користь.

Повертаючись до прийняння рішень, зазначимо, що кількісно та якісно оцінити можливі альтернативи при прийнятті управлінських рішень можливо за допомогою економіко-математичних методів і моделей, серед яких найбільш вживаними є:

- моделі математичної економії (виробничі функції та міжгалузеві баланси);
- моделі математичного програмування;
- моделі теорії ігор;
- статистичні, ймовірнісні та імітаційні моделі.

При цьому нагадаємо, що дана робота присвячена дослідженню операційного ризику комерційних банків, тому нам знадобляться лише певні економіко-математичні методи і моделі, які є найбільш розповсюдженими саме в банківській діяльності, здебільшого у сефрі ризик-менеджменту. Їх можна представити за допомогою наступної схеми (рис. 1) [2121].

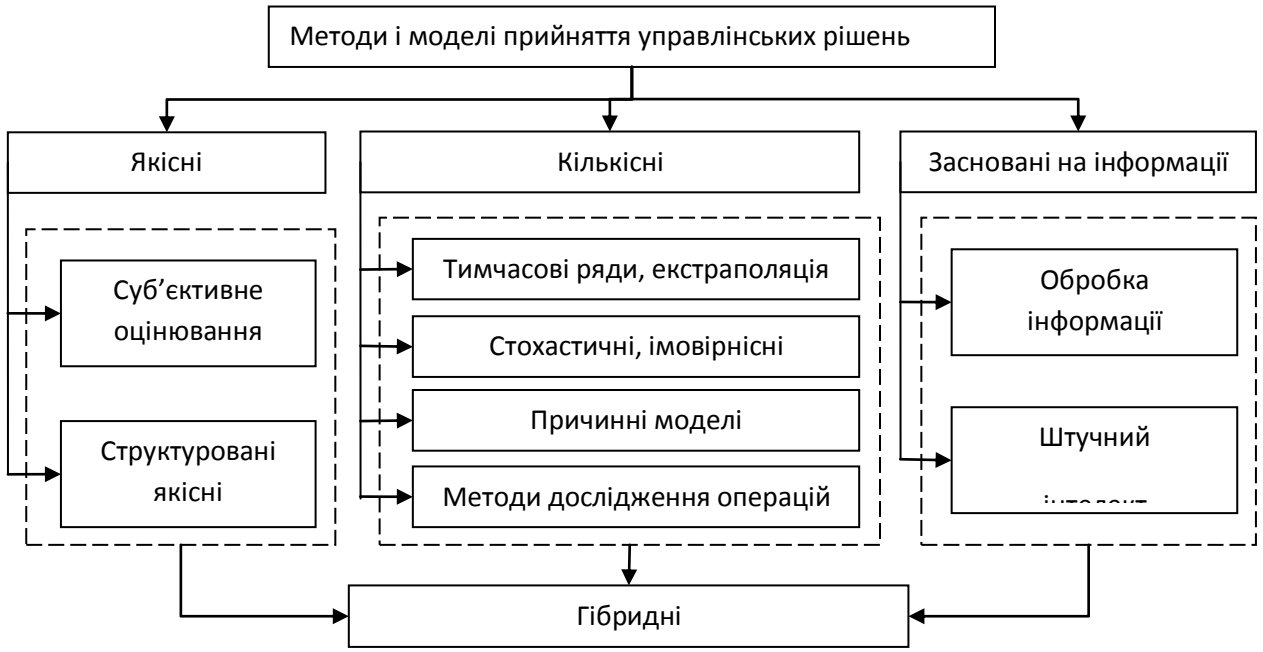


Рис. 3.1 Економіко-математичні методи і моделі, які використовуються при прийнятті рішень в банківському ризик-менеджменті.

Необхідно зазначити, що найчастіше у ризик-менеджменті банків використовуються кількісні методи, які в свою чергу забезпечують надання якісної характеристики діяльності банку шляхом використання якісних та гібридних методів. При цьому методи, засновані на інформації, характеризуються вищим рівнем суб'єктивності одержаних результатів.

Проте, давайте знову згажаємо про «непевність» та «старих овець». У випадках, коли для прийняття рішень потрібно використовувати інформацію, що є невоною, викривленою чи може містити помилки, строгі міркування[4] стають непридатними. Тому на практиці при прийнятті рішень в умовах невизначеності важливо мати змогу формувати міркування, що мають характер нестрогих.

[4] Строгими міркуваннями називають міркування, що спирається виключно на точні факти та точні висновки, які виходять із цих фактів.

В основу системного процесу формування нестрогих міркувань покладена теорія ймовірності, в якій робиться спроба усунення частини (або усіх) помилок та забезпечення прийнятного логічного висновку. ***Такий процес має назву нечіткої логіки.*** На сьогоднішній день розроблена значна кількість теорій ймовірності, що успішно використовуються в нечіткій логіці. До них відносяться:

- теорії, засновані на класичному визначенні ймовірності і на байєсовській ймовірності;
- теорія Хартлі, заснована на класичному визначенні множин;
- теорія Шеннона, заснована на понятті вірогідності;
- теорія Демпстера-Шефера;
- марківські моделі;
- теорія нечітких множин Заде;
- теорія Вальда;
- теорія прийняття рішень в умовах багатокритеріальності.

Найбільш відомими вважаються теорії, засновані на класичному визначенні ймовірності та на апостеріорній імовірності.

Виходячи з вище перерахованих теорій кількісної оцінки ймовірності ми пропонуємо розглянути методологічний підхід, який в умовах невизначеності, на наш погляд, є найбільш прийнятним для прийняття управлінських рішень для комерційного банку. Тепер слід сконцентруватись – адже надалі ми пропонуємо вам ті самі «ліки», про які ми вже згадували. Зі свого боку, спробуємо якомого детальніше викласти матеріал, щоб кожен читаж отримав дієвий інструмент оцінки операційних ризиків комерційного банку.

Оскільки в теорії прийняття рішень вибір найкращого варіанту відбувається з декількох можливих альтернатив, то ефективність прийнятого рішення визначається якістю врахованих даних. Якщо рішення приймається в умовах ризику, то вартість альтернативних рішень описується ймовірнісними розподілами, що обумовлює ***необхідність використання байєсівського аналізу***.

Для початку при визначенні операційного ризику комерційного банку та подальшому прийнятті управлінських рішень пропонуємо застосувати системну оптимізацію, яку можна представити у вигляді:

- послідовності процедур відносно формування моделі вихідного завдання;
- переведення сформованої моделі в область задач математичного програмування;
- рішення завдання математичного програмування в багатокритеріальній постановці [2424].

Але при прийнятті рішень дуже рідко вдається отримати необхідну інформацію відносно об’єкта та зовнішнє середовище в повному обсязі. Навіть якщо відомі системи рівнянь, що описують поведінку системи, часто виявляється, що відсутні даних про величини певних параметрів. В подальшому виявляється, що прийнята при проектуванні модель суттєво відрізняється від реального об’єкту, що значно зменшує ефективність розробленої системи управління при прийнятті рішень.

Таким чином, дуже важливою є можливість уточнення побудованої моделі оптимізації на основі спостережень, отриманих в умовах функціонування об’єкту, що можна реалізути використовуючи Байєсовський підхід.

Оскільки при прийнятті рішень в умовах ризику вартість альтернативних рішень описується ймовірнісними розподілами, то рішення, що приймається, засновується на використанні критерію очікуваного значення, у відповідності з яким альтернативні рішення порівнюються з точки зору максимізації очікуваного прибутку або мінімізації очікуваних витрат. Розподіл імовірностей, що використовуються при формуванні критерію очікуваного значення, відбуваються із накопиченої раніше інформації. У деяких випадках виявляється можливим перерахувати ці ймовірності після отримання інформації відносно нових спостережень або експериментів. Отримані при цьому ймовірності називають *апостеріорними або байєсівськими* на відміну від *апріорних*, отриманих із вихідної інформації.

Таким чином, пропнуємо вам розглянути математичну модель, побудовану на основі Баєсівського підходу, яка, на наш погляд, надасть можливість формалізувати досягнення оптимального рівня операційного ризику комерційного банку.

Нехай процес прийняття рішень включає:

1. $H_j, j = 1 \div n$ станів природи (можливі реалізації яких є випадковими подіями);

2. $B_i, i = 1 \div k$ альтернатив;

3. $P\{B_i\}$ - апріорні йімовірності;

4. $P\{H_j \mid B_i\}$ - умовні ймовірності подій (ймовірність події H_i за умови, що вже відбулася подія B_i).

Тепер розрахуємо ймовірність сумісної появи подій $P\{B_i, H_j\}$ для всіх i, j за формулою:

$$P\{B_i, H_j\} = P\{H_j \mid B_i\} P\{B_i\} \tag{3.1}$$

Надалі проведемо розрахунок абсолютних ймовірностей $P\{H_j\}$ для всіх j за формулою:

$$P\{H_j\} = \sum_i P\{B_i, H_j\} \tag{3.2}$$

Визначаємо апостеріорні ймовірності $P\{B_i \mid H_j\}$ за формулою:

$$P\{B_i \mid H_j\} = \frac{P\{B_i, H_j\}}{P\{H_j\}} \tag{3.3}$$

Виходячи з вищенаведених співвідношень, можна оцінити вартість альтернативних рішень - в нашому випадку – це рівні операційного ризику банку, що виникатимуть в результаті відповідних управлінських рішень). Нехай a_{ij} -

вартість прийняття рішення B_i за станів середовища H_j, де $j = 1 \div n, i = 1 \div k$. Тоді, очікувана вартість прийняття рішення (тобто, очікуваний рівень операційного ризику банку) B_i розраховується за формулою:

$$MV_i = \sum_i P\{B_i \mid H_j\} a_{ij} \qquad (3.4)$$

Теоретично, найкращим рішенням буде виступати те, якому відповідає $MV_i^* = \max_i \{MV_i\}$ або $MV_i^* = \min_i \{MV_i\}$, в залежності від того, яке стоїть завдання: чи максимізувати прибуток, чи мінімізувати можливі втрати. Щодо операційного ризику комерційного банку – то, безперечно він потребує максимально можливого зменшення, але детальніше про це трохи згодом.

Але в реальних економічних умовах при прийнятті будь-яких рішень необхідно враховувати низку обмежень, наприклад, вирішувати задачі планування, проектування, розподілу та регулювання ресурсів (трудових, фінансових) з урахуванням усіх обмежень (технічних, бюджетних, часових тощо). Це стосується й операційного ризику комерційного банку – при визначенні його рівня та прийнятті подальших управлінських рішень щодо його зменшення чи недопущення зростання, необхідно буде врахувати скажімо, якість та обсяг вихідних даних, особливості та потенціал персоналу, сегменти ринку, де банк займає найліпші позиції, структуру клієнтської бази та низку інших особливостей, притаманних тому чи іншому банку.

Для того, аби врахувати відповідні обмеження при визначенні оптимального рішення, доцільно використати метод Байєса-Лапласа:

$$P_{БЛ}\{\nu_j\} = \sum_i a_{ij} P\{B_i\} \qquad (3.5)$$

Згідно з цим методом, найкращим рішенням буде те, що відповідає одній з умов: $MV_i^* = \max_i \left[P_{БЛ}\{\nu_j\}\right]$ або $MV_i^* = \min_i \left[P_{БЛ}\{\nu_j\}\right]$, що знову ж таки залежить від того, яке стоїть завдання.

При цьому, використання методу Байєса-Лапласа можливе за наступних умов:

- імовірності ситуацій $P\{B_i\}, i = 1 \div k$ відомі й їх можна вважати постійними на період реалізації проекту;
- рішення по проектуванню подібних систем приймається і реалізується часто;
- ризик від неправильного прийнятого рішення не призводить до серйозних наслідків.

Більше того, розглянутий вище метод дає нам змогу провести формалізацію процесу прийняття рішення (в нашому випадку – процесу визначення рівнів операційного ризику комерційного банку) в умовах невизначеності та ризику шляхом застосування низки математичних моделей: зокрема моделей, що базуються на критеріях Байєса, Вальда, «оптимізму» та багатокритеріальному підході. Порівнявши отримані результати, ми зможемо обрати той підхід, що є найбільш адекватним для проведення оцінки операційного ризику комерційного банку.

Узагальнити існуючи підходи до формування моделей прийняття рішень в умовах невизначеності в цілому та математичних моделей, які базуються на критеріях Байєса, Вальда та «оптимізму», зокрема, надає можливість форма представлення вихідної інформації. Так, інформаційна база побудови даних моделей визначається у вигляді базової моделі прийняття рішень, яку називають таблицею витрат (див. табл.3.1).

Таблиця 3.1

Базова модель прийняття рішень в умовах невизначеності та ризику

Альтернатива	Стан зовнішнього середовища					Очікуваний ефект
	Стан S_1 Імовірність P_1	…	Стан S_j Імовірність P_j	…	Стан S_m Імовірність P_m	
A_1	Y_{11}	…	Y_{1j}	…	Y_{1m}	K_1
…	…	…	…	…	…	…
A_i	Y_{i1}	…	Y_{ij}	…	Y_{im}	K_i
…	…	…	…	…	…	…
A_n	Y_{n1}	…	Y_{nj}	…	Y_{nm}	K_n

Примітка: $A = \{A_i\}$ - множина альтернатив; $S = \{S_j\}$ - множина можливих станів зовнішнього середовища; P_j - ймовірність настання j-го стану середовища; Y_{ij} - наслідки i-тої альтернативи у випадку настання j-го стану середовища; K_i - очікуваний ефект від вибору i-тої альтернативи, розрахований з урахуванням наслідків даної альтернативи в кожному з імовірних станів зовнішнього середовища.

Проаналізувавши дані таблиці 3.1, можна зробити висновок, що в умовах невизначеності або ризику не можливо однозначно визначити найкращу альтернативу при вирішенні поставленої задачі в цілому. Це обумовлено тим, що в межах кожного із визначених станів зовнішнього середовища можна обрати найкращу альтернативу, але, як наслідок, не можна однозначно сформувати методологічний підхід до ідентифікації оптимального рішення. Тим не менше, в сучасній економічній літературі наводяться моделі (базуються на критеріях Байєса, Вальда та «оптимізму»), які дозволяють опосередковано подолати невизначеність в даному випадку. Розглянемо дані економіко-математичні моделі.

3.3 Модель прийняття рішення, яка базується на використанні критерію Байєса

В загальному вигляді математична формалізація задачі прийняття рішення в умовах невизначеності в рамках даного підходу має наступний вигляд:

$$A_B = \max_i K_i,$$
$$K_i = \sum_j Y_{ij} \cdot P_j \qquad 3.6)$$

де A_B - альтернатива, оптимальна за критерієм Байєса;

K_i - очікуваний ефект від вибору i-тої альтернативи, розрахований з урахуванням наслідків даної альтернативи в кожному зі станів зовнішнього середовища;

Y_{ij} - наслідки i-тої альтернативи у випадку настання j-го стану зовнішнього середовища;

P_j - ймовірність настання j-го стану зовнішнього середовища.

Модель (3.6) можна інтерпретувати наступним чином: серед розглянутих альтернатив найкращою, тобто оптимальною, вважається та альтернатива, реалізація якої забезпечує найбільше очікуване значення ефективності.

3.4 Модель прийняття рішення, яка базується на використанні критерію Вальда

Даний клас моделей прийняття рішень в умовах невизначеності або ризику відноситься до підходу, основою якого виступає застосування критерію «песимізму». Так, математичну модель в даному напрямку дослідження, можна представити так:

$$A_P = \max_i K_i,$$
$$K_i = \min_j Y_{ij} \qquad 3.7)$$

де A_P - альтернатива, оптимальна за критерієм песимізму;

Y_{ij} - наслідки i-тої альтернативи у випадку настання j-го стану зовнішнього середовища.

В свою чергу, формулу (3.7) можна інтерпретувати як характеристику такої оптимальної альтернативи прийняття управлінського рішення, реалізація якої забезпечує досягнення максимального гарантованого критерію ефективності, тобто найкращий результат такої альтернативи є найкращими з найгірших результатів усіх альтернатив.

Протилежним до описаного вище підходу є підхід, згідно з яким вибір оптимальної альтернативи базується на застосуванні критерію оптимізму.

3.5 Модель прийняття рішення, яка базується на використанні критерію оптимізму

Математично постановку задачі прийняття оптимального управлінського рішення на сонові застосування критерію оптимізму можна представити так:

$$A_O = \max_i K_i,$$
$$K_i = \max_j Y_{ij} \qquad 3.8)$$

де A_O - альтернатива, оптимальна за критерієм оптимізму;

Y_{ij} - наслідки i-тої альтернативи у випадку настання j-го стану зовнішнього середовища.

Сутність моделі (3.8) полягає в наступному: оптимальною вважається та альтернатива, яка забезпечує досягнення «ідеального» можливого розв'язку поставленої задачі, тобто найкращий результат якої є найвищим з найкращих результатів усіх альтернатив.

Порівнюючи наведені математичні моделі, які використовуються в умовах невизначеності або ризику для прийняття ефективного управлінського рішення, необхідно зазначити таке:

- критерій Байєса доречно використовувати в тих випадках, коли прийняття рішення визначається як послідовність повторюваних ситуацій вибору, кожна з яких характеризується певною ймовірнісною величиною. Цей підхід є найкращим тоді, коли значна кількість реалізацій виграшного варіанту забезпечує поступове уникнення ризику і стабілізації критерію ефективності прийняття рішення;
- критерій «песимізму» доречно використовувати за умови крайньої обережності. В межах даного підходу вибір найкращої альтернативи прийняття управлінського рішення обумовлює досягнення найгіршого, але гарантованого результату;
- критерій «оптимізму» придатний для тих випадків, коли вартість прийняття ризику визначається як відносно низька характеристика на

відміну від вартості наявних ресурсів. В рамках побудови математичної моделі на базі даного критерію, вибір оптимальної альтернативи прийняття рішення забезпечується максимізацією можливих результатів, навіть, якщо вони є недостатньо прийнятними.

Викладені вище підходи і побудовані на їх основі економіко-математичні моделі, які базуються на критеріях Байєса, Вальда та «оптимізму», враховують вибір значення лише одного результативного критерію при виборі ефективного управлінського рішення, тобто вони не дозволяють врахувати одночасно низку обмежень. Таке обмеження вказаних моделей може значно погіршувати отримані результати і навіть призводити до неадекватності, зокрема при визначенні рівня операційного ризику комерційного банку. Саме тому надалі доцільно розглянути підхід, який дозволяє уникнути зазначеної невідповідності, шляхом врахування умови багатокритеріальності.

3.6 Моделі прийняття рішень в умовах багатокритеріальності

Формалізація моделі прийняття ефективного рішення на основі врахування умови багатокритеріальності передбачає акумуляцію вхідної інформації у вигляді таблиці 3.2, яка є базовою моделлю. Особливість даного підходу полягає в тому, що він враховує цільову невизначеність та надає можливість використовувати методи її подолання з мінімальними витратами.

Таблиця 3.2

Базова модель прийняття рішень в умовах багатокритеріальності

Альтернатива	Критерій					Очікуваний ефект
	Критерій D_1 Оцінка V_1	…	Критерій D_r Оцінка V_r	…	Критерій D_g Оцінка V_g	
A_1	F_{11}	…	F_{1r}	…	F_{1g}	K_1
…	…	…	…	…	…	…
A_i	F_{i1}	…	F_{ir}	…	F_{ig}	K_i
…	…	…	…	…	…	…
A_p	F_{p1}	…	F_{pr}	…	F_{pg}	K_p

Примітка: $A=\{A_i\}$ - множина альтернатив; $D=\{D_r\}$ - множина можливих станів зовнішнього середовища; K_i - підсумкова оцінка i-тої альтернативи, яка враховує її оцінки за кожним з критеріїв; V_r - оцінка важливості r-того критерію з погляду досягнення загальної мети; F_{ir} - оцінка переваги i-тої альтернативи за r-тим критерієм.

Математична модель прийняття рішення в умовах багатокритеральності, побудована на основі даних таблиці 2 та на визначенні сумарного критерію ефективності, описується такою формулою:

$$A_{CE}=\max_i K_i,$$
$$K_i=\sum_r F_{ir}\cdot V_r \qquad 3.9)$$

де A_{CE} - альтернатива, оптимальна за критерієм сумарної ефективності;

K_i - значення сумарної ефективності для i-тої альтернативи;

F_{ir} - оцінка переваги i-тої альтернативи за r-тим критерієм;

V_r - оцінка важливості r-того критерію з погляду досягнення загальної мети.

Сутність даної математичної моделі, формалізованої у вигляді формули (3.9), полягає в тому, що оптимальний вибір найкращої альтернативи визначається критерієм найбільшої величини значення сумарної ефективності.

3.7 Методологічні підходи до прийняття рішень на основі застосування ймовірнісного підходу

Одним з найстарших і найважливіших інструментів для розв'язання задач щодо прийняття рішень в умовах невизначенності є визначення ймовірності. Імовірність – це кількісний спосіб урахування невизначеності. Класична ймовірність бере початок із теорії, яка була вперше запропонована Б. Паскалем і П. де Ферма в 1654 році. З того часу була проведена велика робота в області вивчення ймовірності, а теоретичні здобутки знайшли широке застосування в науці, техніці, бізнесі, економіці та інших галузях.

Класичну ймовірність називають також апріорною ймовірністю і її визначення відноситься до ідеальних систем. Термін «апріорна» означає ймовірність, що визначається «до подій», без урахування багатьох чинників, які мають місце в реальному світі. Поняття апріорної ймовірності розповсюджується на події, що відбуваються в ідеальних системах, несхильних до старіння або впливу інших систем. В ідеальній системі поява будь-якої з подій відбувається однаково, завдяки чому їх аналіз стає набагато простішим.

Фундаментальна формула класичної імовірність (P) має такий вигляд:

$$P = \frac{W}{N} \tag{3.10}$$

У цій формулі W – кількість очікуваних подій, а N – загальна кількість подій з рівними ймовірностями, які є можливими результатами експерименту або випробування. Наприклад, імовірність випадання будь-якої грані шестигранної гральної кістки дорівнює 1/6, а витягання будь-якої карти з колоди, що містить 52 різні карти – 1/52.

Загальна теорія ймовірності базується на трьох основних аксіомах.

Аксіома 1. Областю визначення ймовірності події (E) є дійсні числа від 0 до 1. Від'ємні значення ймовірності не допускаються. Достовірній події привласнюється ймовірність 1, а неможливій події – ймовірність 0:

$$0 \le P(E) \le 1 \tag{3.11}$$

Аксіома 2. У даній аксіомі стверджується, що сума ймовірностей всіх подій, незалежних одна від одної, що називаються взаємовиключними подіями, дорівнює 1:

$$\sum P(E_i) = 1 \tag{3.12}$$

Аксіома 3. Якщо події Е1 і Е2 не можуть виникати одночасно (тобто є взаємовиключними подіями), то ймовірність виникнення тієї або іншої події дорівнює сумі ймовірностей цих подій:

$$P(E_1 \cup E_2) = P(E_1) + P(E_2) \qquad (3.13)$$

Наведені аксіоми дозволили закласти фундамент теорії ймовірності, проте в них не розглядається імовірність подій, що відбуваються в реальних – неідеальних системах.

Методи обчислення апостеріорних ймовірностей

На відміну від апріорного підходу, в реальних системах, для визначення ймовірності деякої події Р(Е), застосовується спосіб визначення експериментальної ймовірності *як ліміту розподілу частот*:

$$P(E) = \lim_{N \to \infty} \frac{f(E)}{N} \qquad (3.14)$$

У цій формулі f(E) позначає частоту появи деякої події серед N-ї кількості спостережень загальних результатів. Імовірність такого типу називається також *апостеріорною ймовірністю*, тобто ймовірністю, що визначається «після подій». В основу визначення апостеріорної ймовірності покладене вимірювання частоти, з якою виникає деяка подія під час проведення великої кількості випробувань. Наприклад, розрахунок апостеріорної ймовірності дозволяє визначити соціальний тип кредитоспроможного клієнта банку на основі емпіричного досвіду.

Події, що не відносяться до взаємовиключних, можуть впливати одна на одну. Такі події відносяться до класу складних. Імовірність складних подій може бути обчислена шляхом аналізу відповідних їм вибіркових просторів. Ці вибіркові простори можуть бути представлені за допомогою діаграм Венна, як показано на рис. 3.2

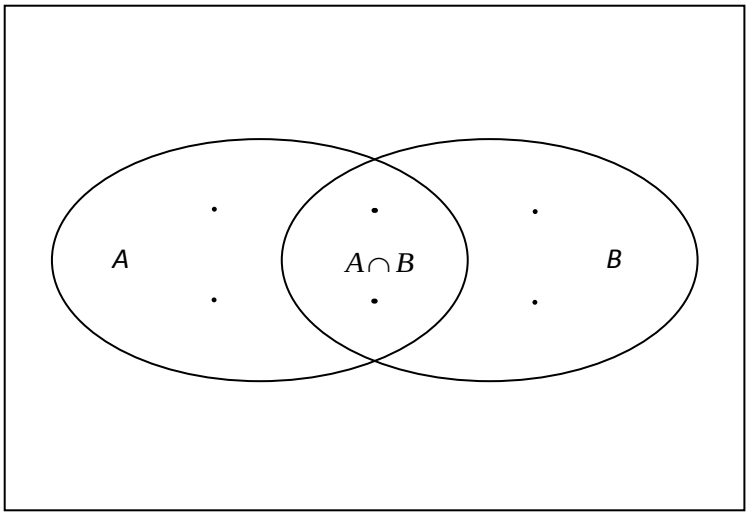


Рис 3.2. Вибірковий простір для двох не взаємовиключних подій

Імовірність виникнення події А, яка визначається з урахуванням того, що відбулася подія В, називається *умовною ймовірністю* і позначається: Р(А |В). Умовна ймовірність визначається наступним чином:

$$P(A \mid B) = \frac{P(A \cap B)}{P(B)} \qquad (3.15)$$

У цій формулі ймовірність Р(В) не повинна дорівнювати нулю, і представляє собою апріорну ймовірність, що визначається до того, як стане відома інша додаткова інформація. Апріорну ймовірність, що застосовується у зв'язку з використанням умовної ймовірності, іноді називають *абсолютною ймовірністю*.

Існує задача, яка є по суті протилежною задачі обчислення умовної ймовірності. Вона полягає у визначенні зворотної ймовірності, яка показує ймовірність попередньої події з урахуванням тих подій, що відбулись у подальшому. На практиці з імовірністю такого типу доводиться зустрічатися досить часто, наприклад, при проведенні медичної діагностики або діагностики

устаткування, при якій виявляються певні симптоми, а задача полягає в тому, щоб знайти ймовірну причину.

Для вирішення цієї задачі застосовується теорема Байєса, названа на честь британського математика XVIII століття Томаса Байєса. Байєсівськая теорія, в наші дні, широко використовується для аналізу дерев рішень в економіці та суспільних науках. Загальна форма теореми Байєса може бути записана в термінах подій (E) та гіпотез (H), у наступному вигляді:

$$P(H \mid E) = \frac{P(E \mid H)P(H)}{P(E)} \qquad (3.16)$$

При визначенні ймовірності події застосовується також ще один тип імовірності, що має назву *суб'єктивної ймовірності*. Поняття суб'єктивної ймовірності поширюються на події, які не є відтворними, і не мають історичної основи, за допомогою якої можна було б здійснювати екстраполяцію. Проте оцінка суб'єктивної імовірності, зроблена експертом, краща, порівняно з повною відсутністю оцінки.

Суб'єктивна ймовірність, фактично, представляє собою переконання або думку, виражену у вигляді ймовірності, а не об'єктивне значення імовірності, засноване на аксіомах та емпіричних вимірюваннях. Переконання та думки експертів виконують важливу роль в процесі знаходження рішень в умовах невизначеності. Саме тому використання байєсовського аналізу є ефективним та перспективним методом прийняття рішень в умовах ризику [25, 26, 27].

Сутність Баєсівського аналізу полягає в одержанні інформації про певний об’єкт та її відповідності певному комплексу нормативів, адекватних поточним економічним реаліям, і розрахунку щодо такої інформації ймовірності стабільного стану об’ єкта.

Запропонована методика імовірнісної оцінки відповідності поточним економічним реаліям здійснюється у 3 етапи. Перший етап – визначення чисельних характеристик оцінки діяльності об’єкта. На наступному етапі заповнюється

таблиця допустимість значень характеристик. Якщо відповідна характеристика лежить у межах допустимих значень, ставиться 1, в іншому випадку 0. На заключному етапі за байєсовським аналізом визначається ризик ризику того, що діяльність об'єкта не відповідатиме необхідними вимогам.

Вихідними статистичними даними для реалізації методики повинні стати значення деякого набору числових характеристик діяльності об' єкта, що умовно поділяються на «ризикові» й «неризикові». Позначимо їх відповідно - $H1, H2$.

Визначальною рисою пропонованої методики є її економічна прозорість, тобто обґрунтованість економічних причин виставлення тієї або іншої оцінки відповідному об'єкту. Даний факт досягається за рахунок специфічного виду інформації, на основі якої відбувається оцінка. По суті, стан кожного об' єкта характеризується набором бінарних величин (ознак), що приймають значення «так» / «ні» («так» - у випадку влучення відповідної характеристики в межі припустимих значень і «ні» – у противному випадку). Так, значення «так» вказують на позитивне, а значення «ні» – на негативні аспекти функціонування об'єкта. Таким чином, вдається одержати єдину числову (імовірнісну) оцінку ефективності діяльності об'єкта.

Після виявлення емпіричних нормативів, кожен об'єкт буде характеризуватись набором бінарних характеристик $B = (B_1, B_2, ..., B_n)$, де B_i приймають значення 1, якщо відповідний норматив виконується, і 0 – у противному випадку. Такі ряди з нулів й одиниць є закодованою інформацією про ефективність діяльності об'єкта, а отже, можна визначити імовірність ($p_B(H1)$) того, що ризик невідповідності діяльності об'єкта певним вимогам є високим, за умови наявності про нього інформації B. Так, відповідно до формули Байєса буде виконуватися співвідношення:

$$P_B(H1) = \frac{P(H1)\cdot P_{H1}(B)}{P(B)} = \frac{P(H1)\cdot p_{H1}(B)}{\sum_{i=1}^{2} P(Hi)\cdot P_{Hi}(B)} = \frac{P(H1)\cdot P_{H1}(B)}{p(H1)\cdot p_{H1}(B) + p(H2)\cdot p_{H2}(B)} =$$

$$= \frac{1}{1+\frac{P(H2)\cdot P_{H2}(B)}{P(H1)\cdot P_{H1}(B)}} \qquad (3.17)$$

Відповідно ймовірність ($p_B(H2)$) того, що діяльність проаналізованого об'єкта є неефективною за умови наявності про неї інформації B.

Імовірності $P(H1)$, $P(H2)$ у байєсівському підході прийнято називати апріорними, їх значення необхідно визначити до початку проведення аналізу. Імовірність $P(H1) = y$ - це ймовірність того, що діяльність досліджуваного об'єкта, при відсутності про нього апостеріорної інформації, є ефективною. Відповідно, імовірність $P(H2)$ - це імовірність того, що для досліджуваного об'єкта, при повній відсутності про нього апостеріорної інформації, операційна діяльність є неефективною. Імовірність $p_{H1}(B)$ - це ймовірність того, що для апріорі ефективного об'єкта буде отримана інформація B. Відповідно, імовірність $p_{H2}(B)$ - це імовірність того, що для апріорі неефективного об'єкта буде отримана інформація B. Виявляється, що при прийнятті припущення про незалежність бінарних характеристик, можна скористатися формулою добутку імовірностей, згідно з якою:

$$\frac{P(H2)\cdot p_{H2}(B)}{P(H1)\cdot p_{H1}(B)} = \frac{P(H2)}{P(H1)}\cdot\frac{\prod_{i=1}^{n} P_{H2}(Bi)}{\prod_{i=1}^{n} P_{H1}(Bi)} = \frac{P(H2)}{P(H1)}\cdot\prod_{i=1}^{n}\frac{P_{H2}(Bi)}{P_{H1}(Bi)} =$$

$$= \frac{P(H2)}{P(H1)}\prod_{i=1}^{n}\left(\frac{b_i}{g_i}\right)^{Bi}\left(\frac{1-b_i}{1-g_i}\right)^{1-Bi} = \frac{1-y}{y}\prod_{i=1}^{n}\left(\frac{1-b_i}{1-g_i}\right)\left(\frac{g_i(1-b_i)}{b_i(1-g_i)}\right)^{Bi} \qquad (3.18)$$

де b_i - імовірність події $B_i = 1$, для «ризикових» об'єктів, а g_i - для «не ризикових».

Таким чином, загальну формулу (3.17), що зв'язує величину імовірнісні оцінки ефективності діяльності об'єкта з наявною інформацією, вдається привести до досить простого виду:

$$P_B(H1) = \frac{1}{1+\frac{1-y}{y}\prod_{i=1}^{n}\left(\frac{1-b_i}{1-g_i}\right)\left(\frac{g_i(1-b_i)}{b_i(1-g_i)}\right)^{Bi}} \qquad (3.19)$$

Отже, розглянувши широкий спектр існуючих підходів для визначення та управління ризиками, ми дійшли висновку, що метод визначення ймовірності на основі Байєсівського аналізу є найбільш придатним для коригування управлінських рішень та, зокрема для оцінки та управління операційним ризиком комерційного

банку, оскільки саме він передбачає аналіз різних факторів ризику та дозволяє виділити певні інциденти операційного ризику (наприклад, ризик, пов’язаний з діями працівників та безпекою робочого місця; ризик систем і технологій; ризик пов’язаний з зовнішніми чинниками; ризик помилки у банківських процесах (ризик взаємовідносин)), а також здійснювати інтервальну оцінку очікуваних втрат в залежності від рівнів ризику та швидкості його зміни. Отже, вказаний підхід ми використали для створення математичної моделі визначення рівнів операційного ризику в комерційному банку. Більше того, вашій увазі буде запропоновано два варіанти такої моделі: перша – для використання при здійсненні регулювання та нагляду Національним банком України (далі – Національний банк); друга – безпосередньо для використання власне комерційним банком для визначення і управління власним операційним ризиком. Варто відмітити, що методика, яка детально буде розглянута в наступному розділі, створювалась на основі реалій, що характерні для банківського ринку України.

IV. МАТЕМАТИЧНА МОДЕЛЬ ВИЗНАЧЕННЯ РІВНІВ ОПЕРАЦІЙНОГО РИЗИКУ КОМЕРЦІЙНОГО БАНКУ

4.1 Теоретичні засади математичної моделі кількісної оцінки операційного ризику комерційних банків

Стійкість функціонування комерційного банку дуже часто порушується у зв’язку з виникненням додаткових витрат, пов’язаних з ліквідацією або попередженням зовнішніх та внутрішніх дестабілізуючих факторів. Відповідно, порушення умов ефективної та прибуткової діяльності банків є наслідком впливу такої економічної категорії як ризик, що пов'язаний з подоланням невизначеності та конфліктності в процесі прийняття управлінських рішень.

Поряд з ризиками, що обумовлюють виникнення витрат, *які підлягають чіткій ідентифікації,* існують ризики, наслідком дії яких виступає *формування нечітко визначених витратних потоків*. Так, до останньої групи ризиків відноситься й операційний ризик.

Причинами значних втрат, які виникають *в результаті реалізації операційних ризиків* в банківській сфері, можуть виступати, зокрема:

- шахрайства в банківській сфері;
- зловживання службовими обов’язками;
- відмови систем;
- порушення технологій здійснення банківських операцій.

При цьому ефективність управління операційними ризиками комерційного банку досягається шляхом прийняття обґрунтованих рішень щодо їх визначення та мінімізації, основою яких виступає кількісна оцінка рівня даних ризиків.

Проводячи аналіз існуючих методик кількісної оцінки банківських ризиків в цілому, та операційного ризику, зокрема, можна виділити наступні: статистичний метод, метод експертних оцінок, аналітичний метод оцінювання ризику, рейтинговий метод оцінювання ризику, нормативний метод, метод аналізу доцільності витрат (метод оцінки фінансової стійкості), метод аналізу чутливості (критичних значень), метод аналізу ризику за допомогою дерева рішень, метод

використання аналогів тощо. Проте, не зважаючи на комплекс переваг вищенаведених методів, вони не надають можливості:

- визначити витрати зумовлені опосередкованим впливом операційного ризику;
- провести аналіз складових елементів (інцидентів) операційного ризику як кожного окремо, так і у їх взаємозв'язку та взаємообумовленості;
- забезпечити можливість прийняття гнучких управлінських рішень на основі отриманих результатів.

Таким чином, для визначення конкретного рівня операційного ризику комерційног банку, на наш погляд, необхідно побудувати математичну модель, яка буде складатись з таких етапів:

1. Формування комплексної системи показників – ідентифікаторів як операційного ризику в цілому, так прямих і опосередкованих наслідків його впливу.

2. Проведення експрес-оцінки щодо визначення рівня операційного ризику.

3. Для банків з критичним та високим рівнями операційного ризику додаткове проведення більш глибокого, детального та структурного аналізу – реалізації комплексного підходу оцінки даної категорії ризику (даний етап присутній тільки при визначенні операційного ризику Національним банком).

4. Застосування теорії нечіткої логіки з метою визначення структури кожного показника в залежності від надання інцидентам операційного ризику бінарних характеристик.

5. Оцінка операційного ризику в розрізі кожного з інцидентів.

6. Розрахунок інтегральної характеристики (кількісної оцінки) операційного ризику шляхом застосування ймовірнісного (Баєсівського) підходу.

7. Надання якісної характеристики рівня операційного ризику відповідного комерційного банку.

Для формалізації, більш чіткого розуміння та наочного представлення вищенаведених етапів методики визначення кількісної оцінки ступеня операційного ризику банківських установ запропоновано вищенаведену послідовність етапів представити у вигляді наступних схем (рис. 4.1 та 4.2).

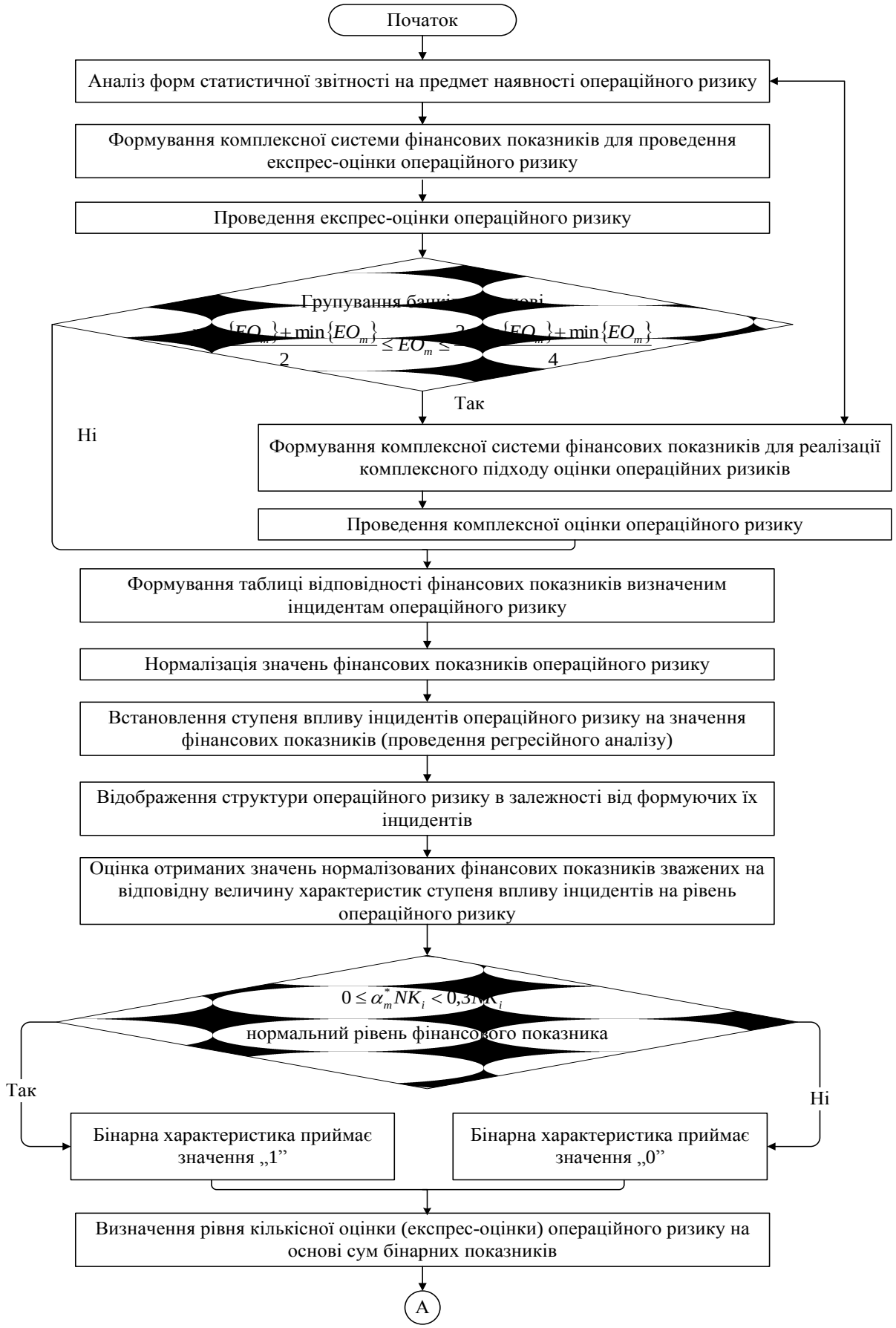


Рис. 4.1 Послідовність етапів методики визначення кількісної оцінки ступеня операційного ризику банківських установ.

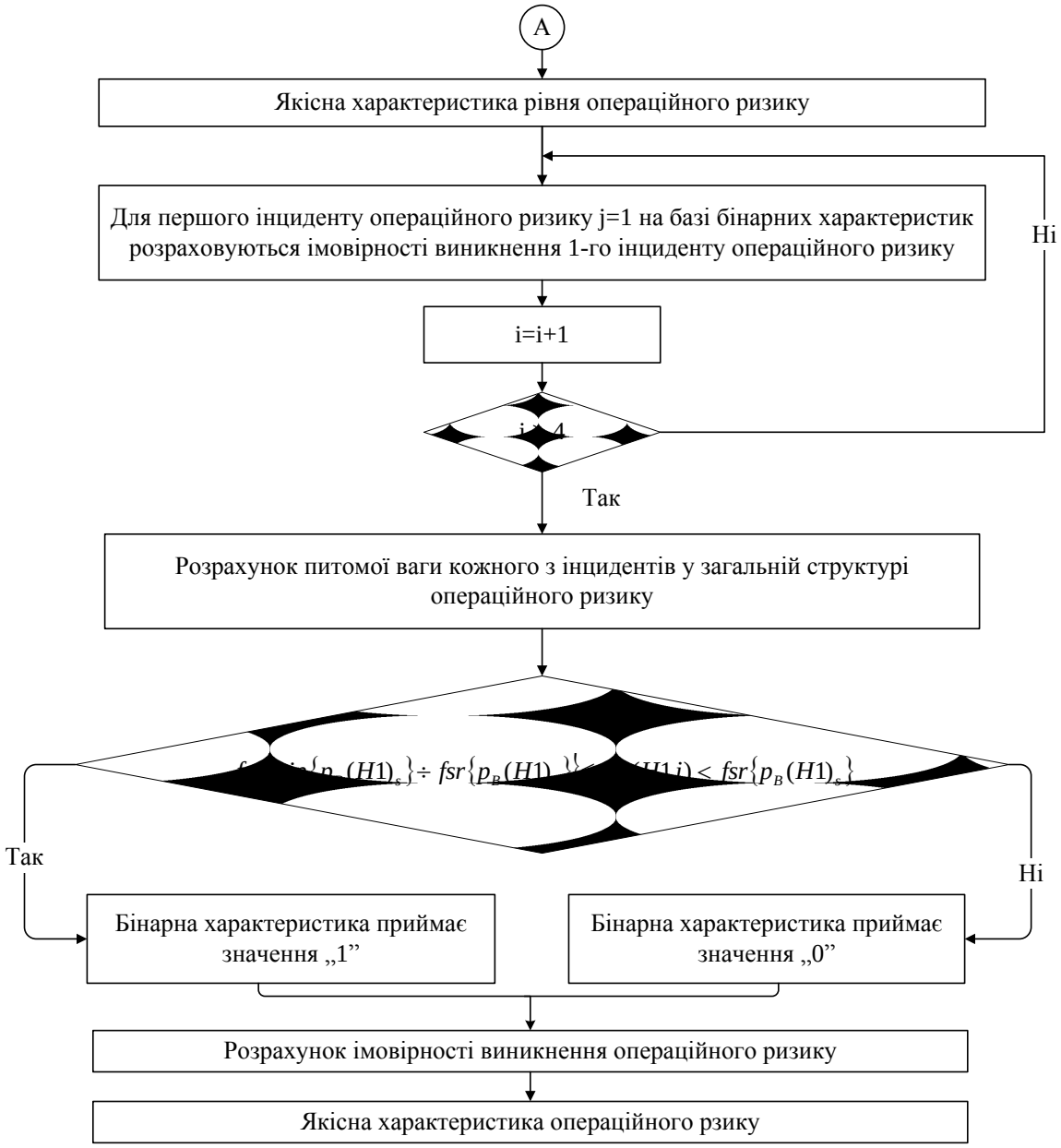


Рис. 4.2. Послідовність реалізації методики визначення рівня операційного ризику комерційного банку

Таким чином, можна стверджувати, що основою методики визначення операційного ризику комерційного банку виступає комбінація нечітко-множинного та імовірнісного (Баєсівського) підходів. Крім того, необхідно зазначити, що інформаційною базою реалізації математичної моделі кількісної оцінки операційного ризику для Національного банку є таблиці відповідності показників визначеним інцидентам операційного ризику (окремо в межах експрес підходу та комплексного підходу).

Дана специфіка оцінки рівня операційного ризику банківських установ вимагає детального аналізу і дослідження окремо нечітко-множинного та ймовірнісного підходів.

Переходячи до аналізу етапів проведення нечітко-множинного підходу, спочатку розглянемо послідовність формування інформаційної бази математичної моделі кількісної оцінки рівня операційного ризику комерційного банку (реалізація яких проводиться в межах перших трьох етапів загальної методики).

Реалізація першого етапу запропонованої методики має ряд особливостей, пов'язаних з набором показників, які використовуються в якості ідентифікаторів можливих наслідків настання даної категорії ризику. Це залежить від цілей, які прийнято визначальними при дослідженні певного напрямку процесу формалізації запропонованої математичної моделі.

В свою чергу, результатом формування комплексної системи показників – ідентифікаторів як операційного ризику в цілому, так прямих і опосередкованих наслідків його впливу, зокрема виступає побудова таблиці відповідності показників визначеним інцидентам операційного ризику (в нашому випадку - ризик, пов'язаний з діями працівників та безпекою робочого місця; ризик систем і технологій; ризик пов'язаний з зовнішніми чинниками; ризик помилки у банківських процесах (ризик взаємовідносин)). В рамках даного підходу необхідно зазначити, що відповідність показників визначеним інцидентам операційного ризику інтерпретується як встановлення бінарних характеристик в межах тих інцидентів, які є визначальними для кожного розглянутого показника.

Другим етапом методики є визначення кількісної оцінки операційного ризику банку виступає проведення експрес-оцінки даного ризику. Ми пропонуємо в якості експрес-оцінки визначити суму бінарних характеристик за всіма показниками та в рамках чотирьох виділених інцидентів:

$$ЕО_m = \sum_{i=1}^{n} \sum_{j=1}^{4} Кбін_{ijm} \qquad (4.1)$$

де EO_m - експрес-оцінка m-го комерційного банку ступеня його операційного ризику;

n – кількість показників – індикаторів прямих та опосередкованих наслідків виявленого операційного ризику;

$Кбін_{ijm}$ - бінарна характеристика в розрізі i-го ($i = 1 \div n$) показника, j-го ($j = 1 \div 4$) інциденту m-го комерційного банку ступеня його операційного ризику.

За результатами розрахованої експрес-оцінки пропонується визначати попередній рівень загрози реалізацій операційного ризику таким чином:

- якщо отримана експрес-оцінка належить проміжку від $\min\{EO_m\}$ до $\frac{\max\{EO_m\} - 3\min\{EO_m\}}{2}$, то рівень загрози є нормальним;
- якщо належить проміжку від $\frac{\max\{EO_m\} - 3\min\{EO_m\}}{2} \le EO_m \le \frac{\max\{EO_m\} + \min\{EO_m\}}{2}$ - допустимий рівень загрози;
- у випадку відповідності проміжку $\frac{\max\{EO_m\} + \min\{EO_m\}}{2} \le EO_m \le \frac{3\max\{EO_m\} + \min\{EO_m\}}{4}$ - високий рівень загрози,
- для проміжку від рівня $\frac{3\max\{EO_m\} + \min\{EO_m\}}{4}$ до $\max\{EO_m\}$ - критичний рівень загрози.

При проведенні оцінки Національнотнимм банком, що здійснюється одночасно для певної сукупності банків, логічним продовженням реалізації експрес-підходу до оцінки відповідності показників визначеним інцидентам операційного ризику виступає реалізація *третього етапу* - додаткового проведення більш глибокого, детального та структурного аналізу – комплексного підходу оцінки операційного ризику. Сутність даного підходу полягає у розрахунку зважених показників на рівень відповідності певним інцидентам операційного ризику, при чому ваги визначаються на основі причинних факторів.

Результатом застосування другого і третього етапів запропонованого методичного підходу оцінки операційного ризику в розрізі кожного конкретного

банку виступає таблиця відповідності показників визначеним інцидентам операційного ризику (див. табл.4.1).

Таблиця 4.1

Таблиця відповідності показників визначеним інцидентам операційного ризику

№	Показник	Інцидент ризику (бінарна характеристика)			
		ризик, пов'язаний з діями працівників та безпекою робочого місця $j=1$	ризик систем і технол огій $j=2$	ризик помилки у банківських процесах (ризик взаємовідноси н) $j=3$	ризик пов'язан ий з зовнішні ми чинника ми $j=4$
А	Б	1	2	3	4
	Назва показника	*Бінарна характеристика*			

Сутність та вид структурних складових (показників) даної таблиці, в розрізі кожного банку, обумовлений підходом, який виступає основою її формування. Так, для банків, які отримали за результати експрес-оцінки задовільні результати, тобто рівень загрози реалізації операційного ризику є нормальним або допустимим, їх показники та бінарні характеристики визначаються за експрес-оцінкою. В іншому випадку, тобто при визнанні банків за експрес-оцінкою достатньо ризиковими (відповідно критичний і високий рівні загрози), таблиця відповідності показників визначеним інцидентам операційного ризику заповнюється за результатами застосування комплексного підходу оцінки даної категорії ризику.

Проведені вище розрахунки виступають основою оцінки операційного ризику *в розрізі кожного з інцидент*ів – що й є основою *п'ятого етапу*.

Так, *для визначення оцінки ступеня операційного ризику комерційного банку* пропонується сформувати групу показників $K_{ij}, i=1\div n, j=1\div m$, кожен із яких у певній мірі характеризує той чи інший j-й інцидент (причину) виникнення операційного ризику.

Кожен з розглянутих показників може характеризувати як один окремий інцидент, так і частково декілька інцидентів виникнення операційного ризику. Це

пов’язано з тим, що деякі показники відображають одночасно властивості різних інцидентів причому з різою мірою впливаючи на них.

Для отримання кількісної характеристики операційного ризику на основі показників, які відображають як однозначний, так і не однозначний вплив різних інцидентів пропонується наступна методика.

На основі того, що показники, яки характеризують рівень операційного ризику, відображають різні аспекти функціонування банку і відповідно є різнорідними, необхідно привести їх у співставний вигляд (визначити нормалізоване значення).

Для цього пропонується використати наступну формулу (формула 4.2):

$$NK_i = \frac{K_i}{\overline{K_i}} \qquad (4.2)$$

де $NK_i i = 1 \div n$ - нормалізоване значення i-го показника кількісної оцінки ступеня операційного ризику;

K_i - абсолютне значення i-го показника кількісної оцінки ступеня операційного ризику;

$\overline{K_i}$ - середнє значення i-го показника за визначеною статистичною інформацію (при дослідженні структури) або за визначений проміжок (при дослідженні динаміки).

Вищенаведений підхід нормалізації значення i-го показника кількісної оцінки ступеня операційного ризику дає можливість надати показникам співставний вигляд в залежності від мети аналізу: дослідження структури або динаміки розвитку операційного ризику. Крім того, даний підхід дає можливість провести нормалізацію показників не враховуючи напрямок їх впливу, що особливо важливо за умови значної кількості показників.

В межах того, що показники, які відображують основні властивості операційних ризиків, можуть як однозначно, так і неоднозначно характеризувати певну групу інцидентів ризику, виникає необхідність їх поділу на три групи:

- показники, які відображають властивості лише однієї групи інцидентів операційного ризику;
- показники, які у певних співвідношеннях відображують дві групи інцидентів ризику;
- показники, які характеризують три або чотири інциденти операційного ризику.

Таким чином, постає необхідність встановлення ступеня впливу кожного інциденту на операційний ризик банку. Так, з метою визначення числових значень характеристик ступеня впливу певного інциденту на рівень показника операційного ризику проведемо наступний аналіз (формула 4.3). Варто зазначити, що показники операційного ризику відображають кожний інцидент ризику у відповідних співвідношеннях. Для проведення даного аналізу представимо групи інцидентів операційного ризику в якості фіктивних змінних, тобто змінних, які приймають значення «1» у випадку можливості їх опису відповідним показником, або «0» в іншому випадку.

$$K_i = \beta_0 + \beta_1 F_{1i} + \beta_2 F_{2i} + \beta_3 F_{3i} + \beta_4 F_{4i} + \varepsilon \qquad (4.3)$$

де K_i - абсолютне значення i-го показника кількісної оцінки ступеня операційного ризику;

$F_{ij}, j = 1 \div 4$ - фіктивна змінна характеристики i-го показника j-го інциденту операційного ризику;

$\beta_m, m = 0 \div 4$ - сталі величини;

ε - похибка (відхилення фактичного і теоретичного рівнів відповідного i-го показника кількісної оцінки ступеня операційного ризику).

Визначити числові значення характеристик ступеня впливу певного інциденту на рівень показника операційного ризику до j-х інцидентів на основі рівняння (2) виявляється неможливим. Тому, щоб визначити на скільки відсотків кожен з

інцидентів пояснює виникнення операційного ризику за відповідним показником (формула 4.4):

$$K_i = \alpha_1 F_{1i} + \alpha_2 F_{2i} + \alpha_3 F_{3i} + \alpha_4 F_{4i} + \varepsilon \qquad (4.4)$$

де K_i - абсолютне значення i-го показника кількісної оцінки ступеня операційного ризику;

$F_{ji}, j = 1 \div 4$ - фіктивна змінна характеристики i-го показника j-го інциденту операційного ризику;

$\alpha_m, m = 1 \div 4$ - сталі величини, які відображають значення характеристик ступеня впливу певного інциденту на рівень показника операційного ризику до j-х інцидентів;

ε - похибка (відхилення фактичного і теоретичного рівнів відповідного i-го показника кількісної оцінки ступеня операційного ризику).

Коефіцієнти $\alpha_m, m = 1 \div 4$ рівняння (3) знаходяться за наступною формулою (4.5):

$$\alpha_m = \beta_m \frac{\sigma_{F_j}}{\sigma_{K_i}} \qquad (4.5)$$

де K_i - абсолютне значення i-го показника кількісної оцінки ступеня операційного ризику;

σ_{F_j}, σ_{K_i} - середні квадратичні відхилення факторних і результативної ознак відповідно, які визначаються за формулами (4.6) і (4.7):

$$\sigma_{F_j} = \sqrt{\overline{F_j^2} - \overline{F_j}^2}, \qquad (4.6)$$

$$\sigma_{K_i} = \sqrt{\overline{K_i^2} - \overline{K_i}^2}. \qquad (4.7)$$

В результаті того, що метою дослідження є встановлення абсолютного значення ступеня впливу інцидентів на показники операційного ризику, то отримані значення, в разі невідповідності знаків, беруться по модулю. На основі скорегованих числових характеристик (α_m^*) розраховується відносний показник структури (формула 4.8), який відображає питому вагу впливу інцидентів на рівень операційного ризику.

$$\alpha_m^* = \frac{\alpha_m}{\sum_{m=1}^{4} \alpha_m}, \qquad (4.8)$$

Знайдені числові значення характеристик ступеня впливу певного інциденту на рівень кожного з показників кількісної оцінки ступеня операційного ризику відповідним пояснюючим ознакам, а також абсолютні значення самих показників зведемо у таблицю 4.2.

Таблиця 4.2

Показники, які відображують основні властивості операційних ризиків, та значення характеристик ступеня впливу певного інциденту на рівень показника операційного ризику

№	Показник ($K_i, i = 1 \div n$)	Значення характеристик ступеня впливу певного інциденту на рівень показника операційного ризику			
		ризик, пов'язаний з діями працівників та безпекою робочого місця $j=1$	ризик систем і технологій $j=2$	ризик помилки у банківських процесах (ризик взаємовідносин) $j=3$	ризик пов'язаний з зовнішніми чинниками $j=4$
А	Б	1	2	3	4
	I група				
1	K_1	α_{111}	α_{112}	α_{113}	α_{114}
2	K_2	α_{121}	α_{122}	α_{123}	α_{124}
…	…				
l	K_l	α_{1l1}	α_{1l2}	α_{1l3}	α_{1l4}
	II група				
l+1	K_{l+1}	α_{2l+11}	α_{2l+12}	α_{2l+13}	α_{2l+14}
l+2	K_{l+2}	α_{2l+21}	α_{2l+22}	α_{2l+23}	α_{2l+24}
…	…				
…	…				
k	K_k	α_{2k1}	α_{2k2}	α_{2k3}	α_{2k4}

Продовження табл. 4.2

А	Б	1	2	3	4
	ІІІ група				
k+1	K_{k+1}	α_{3k+11}	α_{3k+12}	α_{3k+13}	α_{3k+14}
k+2	K_{k+2}	α_{3k+21}	α_{3k+22}	α_{3k+23}	α_{3k+24}
…	…				
n	K_n	α_{3n1}	α_{3n2}	α_{3n3}	α_{3n4}

Використовуючи дані таблиці 4.2 та формулу (4.2) розрахуємо значення нормалізованих показників кількісної оцінки ступеня операційного ризику зважених на характеристики впливу певного інциденту на рівень показника операційного ризику (див. табл. 4.3).

Таблиця 4.3

Відображення структури операційного ризику в залежності від формуючих їх інцидентів

№	Значення нормалізованого показника зваженого на характеристику впливу певного інциденту на рівень показника операційного ризику			
	ризик, пов'язаний з діями працівників та безпекою робочого місця $j=1$	ризик систем і технологій $j=2$	ризик помилки у банківських процесах (ризик взаємовідносин) $j=3$	ризик пов'язаний з зовнішніми чинниками $j=4$
А	1	2	3	4
	І група			
1	$\alpha_1 NK_1$	$\alpha_2 NK_1$	$\alpha_3 NK_1$	$\alpha_4 NK_1$
2	$\alpha_1 NK_2$	$\alpha_2 NK_2$	$\alpha_3 NK_2$	$\alpha_4 NK_2$
…	…	…	…	…
l	$\alpha_1 NK_l$	$\alpha_2 NK_l$	$\alpha_3 NK_l$	$\alpha_4 NK_l$
	…	…	…	…
	ІІ група			
l+1	$\alpha_1 NK_{l+1}$	$\alpha_2 NK_{l+1}$	$\alpha_3 NK_{l+1}$	$\alpha_4 NK_{l+1}$
l+2	$\alpha_1 NK_{l+2}$	$\alpha_2 NK_{l+2}$	$\alpha_3 NK_{l+2}$	$\alpha_4 NK_{l+2}$
…				
k	$\alpha_1 NK_k$	$\alpha_2 NK_k$	$\alpha_3 NK_k$	$\alpha_4 NK_k$
	…	…	…	…
	ІІІ група			
k+1	$\alpha_1 NK_{k+1}$	$\alpha_2 NK_{k+1}$	$\alpha_3 NK_{k+1}$	$\alpha_4 NK_{k+1}$
k+2	$\alpha_1 NK_{k+2}$	$\alpha_2 NK_{k+2}$	$\alpha_3 NK_{k+2}$	$\alpha_4 NK_{k+2}$
…	…	…	…	…
n	$\alpha_1 NK_n$	$\alpha_2 NK_n$	$\alpha_3 NK_n$	$\alpha_4 NK_n$

Таким чином, вище приведений алгоритм є *першим кроком п'ятого етапу* загальної методики визначення кількісної оцінки ступеня операційного ризику, на

якому було визначено набір показників діяльності банків, що можуть сигналізувати про потенційне виникнення операційного ризику, та приведення їх до співставного вигляду з урахуванням формуючих їх факторів.

На другому кроці відбувається оцінка допустимих (граничних) значень для виявлених нормалізованих показників, зважених на відповідне значення характеристик ступеня впливу певного інциденту на рівень кожного з показників кількісної оцінки ступеня операційного ризику (формування «коридору» допустимих значень нормалізованих показників). Для цього визначимо оптимістичний і песимістичний варіанти нормованих показників кількісної оцінки ступеня операційного ризику банку, враховуючи, що кожен показник може приймати будь-яке значення з діапазону $0 \div NK_i$, де $i = 1 \div n$. Це пояснюється тим, що для оптимістичного варіанту характеристика ступеня впливу певного інциденту приймає значення «0», тобто ризик відсутній, а для песимістичного варіанту - значення «1», тобто операційний ризик не лише присутній, але й приймає максимально можливе значення.

На основі отриманого діапазону допустимих значень нормалізованих показників визначається рівні кількісної оцінки ступеня операційного ризику банку за кожним показником:

- якщо $0 \le \alpha_m^* NK_i < 0{,}3NK_i$, нормальний рівень;
- якщо $0{,}3NK_i \le \alpha_m^* NK_i < 0{,}5NK_i$, підвищений рівень;
- якщо $0{,}5NK_i \le \alpha_m^* NK_i < 0{,}7NK_i$, високий рівень;
- якщо $0{,}7NK_i \le \alpha_m^* NK_i \le NK_i$, критичний рівень.

Враховуючи приведену вище класифікацію, можна зробити висновок, що допустимим (граничним) рівнем для виявлених нормалізованих показників, зважених на відповідне значення характеристик ступеня впливу певного інциденту, виступає діапазон $0 \le \alpha_m^* NK_i < 0{,}3NK_i$.

На третьому кроці п'ятого етапу методики проводиться визначення кількісної оцінки ступеня операційного ризику банку шляхом формування бінарних показників, які, в своїй більшості, залежать від отриманих раніше граничних

величин: якщо значення нормалізованого показника, зваженого на відповідне значення характеристик ступеня впливу певного інциденту, належить до «коридору» допустимих значень, відповідний бінарний показник приймає значення «0», а в протилежному випадку – «1».

Для визначення бінарних характеристик за нормалізваними показниками $NK_i i = 1 \div n$ скористаємось наступною формулою (4.9):

$$NKbin_i \begin{cases} = 1; \alpha_m^* \overline{NK_m} \geq \alpha_m^* NK_i, \\ = 0; \alpha_m^* NK_i > \alpha_m^* \overline{NK_m} \end{cases}, \tag{4.9}$$

де $NKbin_i$ - бінарні характеристики по кожному показнику кількісної оцінки ступеня операційного ризику банку відповідно до інцидентів даного ризику;

$NK_i, i = 1 \div n$ - нормалізоване значення i-го показника кількісної оцінки ступеня операційного ризику;

$\alpha_m^*, m = 1 \div 4$ - скорегований характеристика ступеня впливу певного інциденту на рівень операційного ризику;

$\overline{NK_m}$ - середнє значення за всіма нормалізованими показниками m-го інциденту ризику. Проведені розрахунки зобразимо у таблиці 4.4.

На останньому *четвертому кроці* – розраховується сума бінарних показників для кожного j-го фактору ризику, які отримали значення «1», тобто експрес-оцінка операційного ризику за j-м фактором ризику (формула 4.10):

$$EO_j = \sum_{i=1}^{n} NKbin_{ij}, \tag{4.10}$$

де EO_j - експрес-оцінка операційного ризику за j-м фактором ризику;

$NKbin_{ij}$ - бінарні характеристики по кожному показнику кількісної оцінки ступеня операційного ризику банку відповідно до інцидентів даного ризику.

Таблиця 4.4

Бінарні характеристики за показниками кількісної оцінки ступеня операційного ризику банку

№	Значення бінарної характеристики зваженого на характеристику впливу певного інциденту на рівень показника операційного ризику			
	ризик, пов'язаний з діями працівників та безпекою робочого місця $j=1$	ризик систем і технологій $j=2$	ризик помилки у банківських процесах (ризик взаємовідносин) $j=3$	ризик пов'язаний з зовнішніми чинниками $j=4$
A	1	2	3	4
	I група			
1	$NKbin_{11}$	$NKbin_{12}$	$NKbin_{13}$	$NKbin_{14}$
2	$NKbin_{21}$	$NKbin_{22}$	$NKbin_{23}$	$NKbin_{24}$
…	…	…	…	…
l	$NKbin_{l1}$	$NKbin_{l2}$	$NKbin_{l3}$	$NKbin_{l4}$
	…	…	…	…
	II група			
l+1	$NKbin_{l+11}$	$NKbin_{l+12}$	$NKbin_{l+13}$	$NKbin_{l+14}$
l+2	$NKbin_{l+21}$	$NKbin_{l+22}$	$NKbin_{l+23}$	$NKbin_{l+24}$
…				
k	$NKbin_{k1}$	$NKbin_{k2}$	$NKbin_{k3}$	$NKbin_{k4}$
	…	…	…	…
	III група			
k+1	$NKbin_{k+11}$	$NKbin_{k+12}$	$NKbin_{k+13}$	$NKbin_{k+14}$
k+2	$NKbin_{k+21}$	$NKbin_{k+22}$	$NKbin_{k+23}$	$NKbin_{k+24}$
…	…	…	…	…
n	$NKbin_{n1}$	$NKbin_{n2}$	$NKbin_{n3}$	$NKbin_{n4}$

На основі розрахованої суми бінарних показників для кожного j-го інциденту ризику визначається загальна сума бінарних показників, яка і виступає експрес-оцінкою операційного ризику банку (формула 4.11):

$$EO = \sum_{j=1}^{4} \sum_{i=1}^{n} NKbin_{ij}\,, \tag{4.11}$$

де EO - експрес-оцінка операційного ризику банку;

$NKbin_{ij}$ - бінарні характеристики по кожному показнику кількісної оцінки ступеня операційного ризику банку відповідно до інцидентів даного ризику.

На основі отриманих сум бінарних показників (EO), яка виступає кількісною експрес-оцінкою ступеня операційного ризику визначається якісна оцінка рівня даного ризику:

- якщо $0 \le EO < n/3$, нормальний рівень ризику;

- якщо $n/3 \le EO < 2n/3$, підвищений рівень ризику;

- якщо $2n/3 \le EO \le n$, високий рівень ризику.

В зв'язку з тим, що кількісна експрес-оцінка в цілому так, і за інцидентами операційного ризику зокрема, надає можливість визначити тільки «потенційно» проблемні банківські установити. Таким чином, виникає необхідність уточнення результатів проведеного експрес-аналізу та визначення більш точного рівня кількісної оцінки операційного ризику комерційного банку. Практичній реалізації зазначених аспектів сприятиме розробка інтегрального підходу до оцінки операційного ризику шляхом застосування Баєсівського аналізу, що є шостим етапом загальної математичної моделі операційного ризику для Національного банку України.

Шостий етап. В межах імовірнісної оцінки проведення аналізу якісної характеристики операційного ризику комерційного банку відбувається на основі кількісної характеристики її ступеня, яка визначається на основі отриманих бінарних показників та Байєсовського (імовірнісного) підходу, котрий передбачає корегування поточного рівня операційного ризику з урахуванням його значення за попередній період та уточнюючих показників поточного періоду. Кількісну характеристику ступеня операційного ризику запропоновано визначати як імовірність настання даного виду ризику, тобто імовірність ($p_{OR}(H1)$) виникнення операційного ризику (подія $H1$) за умови наявності інформації $OR = (OR_1, OR_2, OR_3, OR_4)$ в розрізі 4-х інцидентів, де $OR_k, k = 1 \div 4$ приймають значення 0, якщо відповідний норматив виконується (імовірність виникнення відповідного фактору ризику знаходиться у допустимих межах), і 1 – у протилежному випадку. Основою визначення складових $OR = (OR_1, OR_2, OR_3, OR_4)$ виступають імовірності ($p_K(H1j)$) виникнення j-го інциденту операційного ризику (подія $H1j$) за умови наявності

інформації $K=(K_1,K_2,...,K_n)$, де $K_k, k=1\div n$ приймають значення 0, якщо відповідний норматив виконується, і 1 – у протилежному випадку.

Розглянемо послідовність визначення йімовірності ($p_{OR}(H1)$) виникнення операційного ризику (подія $H1$) за умови наявності інформації $OR=(OR_1,OR_2,OR_3,OR_4)$.

На основі отриманих бінарних показників трьох груп для кожного j-го інциденту ризику відповідно до формули Байєса (основа імовірнісного підходу), визначимо йімовірність ($p_K(H1j)$) виникнення j-го інциденту операційного ризику (подія $H1j$) за умови наявності інформації $K=(K_1,K_2,...,K_n)$ таким чином (формула (4.12)):

$$p_K(H1j)=\frac{1}{1+e^{\{\lambda_{0j}+L\}}} \qquad (4.12)$$

$$L=\sum_{i=1}^{n}\lambda_i NKbin_{ij}$$

$$\lambda_{ij}=\ln\left(\frac{b_{ij}(1-g_{ij})}{g_{ij}(1-b_{ij})}\right), i=1,...,n \qquad (4.13)$$

$$\lambda_{0j}=\ln\left(\frac{p(H2j)}{p(H1j)}\right)+\sum_{i=1}^{n}\ln\left(\frac{1-b_{ij}}{1-g_{ij}}\right)$$

де $p_K(H1j)$ – імовірність виникнення j-го інциденту операційного ризику за умови наявності інформації $K=(K_1,K_2,...,K_n)$;

L – інтегральний показник (зважена сума) бінарних характеристик $NKбін_{ij}$ (наявна інформація про стан банку виходячи зі значень аналітичних показників);

$P(H1j)$ – імовірність гіпотези $H1j$;

$H1j$ – висунута гіпотеза, що виникне j-й інциденту операційного ризику;

$P(H2j)$ – імовірність протилежної гіпотези;

$NK=\{NKbin_{ij}\}$ – бінарна компонента множини характеристик діяльності банку;

b_{ij} – імовірність події $NK=\{NKbin_{ij}\}$ для банку у розрізі j-го інциденту операційного ризику,

g_{ij} – імовірність протилежної події.

Для визначення кількісної оцінки ступеня операційного ризику за j-м інцидентом спочатку розрахуємо значення b_{ij}- імовірність події $NK\text{бін}_{ij}=0$, та g_{ij}- імовірність події $NKbin_{ij}=1$ за всіма n показниками за формулами:

$$g_{ij}=\frac{\sum_{i} NKbin_{ij}}{n},$$
$$b_{ij}=1-g_{ij} \qquad (4.14)$$

Після визначення b_{ij} - імовірність події $NKbin_{ij}=0$, та g_{ij}- імовірність події $NK\text{бін}_{ij}=1$ для кожного інциденту операційного ризику за всіма n показниками розрахуємо параметри λ_{ij} та λ_{0j} за формулами (4.13), після чого визначимо значення L - інтегрального показника (зваженої суми) бінарних характеристик $NK=\{NKbin_{ij}\}$ і підставимо в загальну формулу (4.12), що показує величину оцінки ризику.

На основі отриманої ймовірнісної (кількісної) оцінки операційного ризику ($p_K(H1j)$) за кожним j-м інцидентом визначається якісна характеристика рівня ризику:

- якщо $0\le p_K(H1j)<fsr\{\min_s\{p_B(H1)_s\}\div fsr\{p_B(H1)_s\}\}$, нормальний рівень ризику (де $fsr\{\ \}$ - середнє значення зазначених показників за сукупністю s банків);

- якщо $fsr\{\min_s\{p_B(H1)_s\}\div fsr\{p_B(H1)_s\}\}\le p_K(H1j)<fsr\{p_B(H1)_s\}$, підвищений рівень ризику;

- якщо $fsr\{p_B(H1)_s\}\le p_K(H1j)<fsr\left\{fsr\{p_B(H1)_s\}\div\max_s\{p_B(H1)_s\}\right\}$, високий рівень ризику;

- якщо $fsr\left\{fsr\{p_B(H1)_s\}\div\max_s\{p_B(H1)_s\}\right\}\le p_K(H1j)\le 1$, критичний рівень ризику.

Використовуючи проведені вище розрахунки, визначимо алгоритм знаходження кількісної оцінки ступеня операційного ризику банку як ймовірності виникнення операційного ризику за умови наявності інформації $B=(p_K(H11),p_K(H12),p_K(H13),p_K(H14))$, яка визначається на основі аналітичних

показників характеристики діяльності відповідного банку $K=(K_1,K_2,...,K_n)$ (див. таблицю 4):

1. Розрахунок імовірностей $p_K(H1j)$ виникнення j-го інциденту операційного ризику за умови наявності інформації $K=(K_1,K_2,...,K_n)$.
2. Знаходження питомої ваги кожного з інцидентів у загальній структурі операційного ризику. $S(p_K(H1j))=\frac{p_K(H1j)}{\sum_{j=1}^{4} p_K(H1j)}\times 100\%$
3. Визначення гранично допустимого коридору імовірнісної (кількісної) оцінки операційного ризику за кожним j-м інцидентом - $0\le p_K(H1j)<0{,}3$, що визначає нормальний рівень ризику.
4. Перехід від імовірнісних показників $p_K(H1j)$ до бінарних показників $NKбін_j$ за j інцидентами операційного ризику: $NKбін_j$ приймає значення «1» у випадку влучення показника $p_K(H1j)$ у гранично допустимі межі або значення «0» в іншому випадку.
5. Визначення g_j- імовірності події $NKбін_j=1$ $(g_{ij}=\frac{\sum_i NKbin_{ij}}{n})$ та b_j- імовірності події $NKbin_{ij}=0$ $(b_{ij}=1-g_{ij})$ за j інцидентами операційного ризику.
6. Розрахунок імовірності виникнення операційного ризику (кількісної оцінки ступеня операційного ризику) $p_B(H1)$ за формулою (14).
7. Ідентифікація якісної оцінки рівня операційного ризику банку на основі визначеної кількісної оцінки його ступеня.

Таблиця 4.5

Показники алгоритму визначення кількісної оцінки ступеня операційного ризику

№	Інциденти операційного ризику			
	ризик, пов'язаний з діями працівників та безпекою робочого місця $j=1$	ризик систем і технологій $j=2$	ризик помилки у банківських процесах (ризик взаємовідносин) $j=3$	ризик пов'язаний з зовнішніми чинниками $j=4$
A	1	2	3	4
Імовірність виникнення j-го інциденту операційного ризику	$p_K(H11)$	$p_K(H12)$	$p_K(H13)$	$p_K(H14)$
Питома вага кожного з інцидентів у загальній структурі операційного ризику	$S(p_K(H1j)) = \frac{p_K(H1j)}{\sum_{j=1}^{4} p_K(H1j)}$ 100%	$S(p_K(H1j)) = \frac{p_K(H1j)}{\sum_{j=1}^{4} p_K(H1j)}$ 100%	$S(p_K(H1j)) = \frac{p_K(H1j)}{\sum_{j=1}^{4} p_K(H1j)}$ 100%	$S(p_K(H1j)) = \frac{p_K(H1j)}{\sum_{j=1}^{4} p_K(H1j)}$ 100%
Гранично допустимий коридор імовірнісної (кількісної) оцінки операційного ризику за кожним j-м інцидентом (за сукупністю s банків)	$0 \le p_K(H1j) < fsr\left\{\min_s \{p_B(H1)_s\} \div fsr\{p_B(H1)_s\}\right\}$			
Бінарні показники за j інцидентами операційного ризику	$NKbin_1$	$NKbin_2$	$NKbin_3$	$NKbin_4$
Імовірність виникнення операційного ризику (кількісна оцінку ступеня операційного ризику)	$p_B(H1)$			

На основі отриманих бінарних показників $NKбін_j$ за j інцидентами ризику відповідно до формули Байєса, яка є основою імовірнісного підходу, визначимо імовірність ($p_B(H1)$) виникнення операційного ризику (подія $H1$) за умови наявності інформації $B=\left(p_K(H11), p_K(H12), p_K(H13), p_K(H14)\right)$ наступним чином (формула (4.15)):

$$L = \sum_{j=1}^{4} \lambda_j NKbin_j \qquad (4.15)$$

$$\lambda_j = \ln\left(\frac{b_j(1-g_j)}{g_j(1-b_j)}\right),\ j = 1,...,4$$

$$\lambda_{0j} = \ln\left(\frac{p(H2)}{p(H1)}\right) + \sum_{j=1}^{4} \ln\left(\frac{1-b_j}{1-g_j}\right)$$

де $p_B(H1)$ - імовірність виникнення операційного ризику за умови наявності інформації $B = \left(p_K(H11), p_K(H12), p_K(H13), p_K(H14)\right)$;

L - інтегральний показник (зважена сума) бінарних характеристик $NKбін_j$ (наявна інформація про стан банку виходячи зі значень аналітичних показників);

$P(H1)$ - імовірність гіпотези $H1$;

$H1$ - висунута гіпотеза щодо виникнення операційного ризику;

$P(H2)$ - імовірність протилежної гіпотези;

$NK = \{NKbin_j\}$ - бінарна компонента множини характеристик діяльності банку;

b_j - імовірність події $NK = \{NKbin_j\}$ для банку у розрізі j-го і операційного ризику,

g_j - імовірність протилежної події.

Логічним продовженням комплексу вище проведених розрахунків виступає реалізація *сьомого етапу* загальної методики визначення рівня операційного ризику банківської установи, сутність якого полягає в надання якісної характеристики рівня даного ризику.

Так, на основі отриманої імовірнісної (кількісної) оцінки операційного ризику ($p_B(H1)$) визначається якісна характеристика рівня ризику:

- якщо $0 \le p_B(H1) < fsr\left\{\min_s\{p_B(H1)_s\} \div fsr\{p_B(H1)_s\}\right\}$, нормальний рівень ризику (де $fsr\{\ \}$ - середнє значення зазначених показників за сукупністю s банків);

- якщо $fsr\left\{\min_s\{p_B(H1)_s\} \div fsr\{p_B(H1)_s\}\right\} \le p_B(H1) < fsr\{p_B(H1)_s\}$, підвищений рівень ризику;

- якщо $fsr\{p_B(H1)_s\} \le p_B(H1) < fsr\left\{fsr\{p_B(H1)_s\} \div \max_s\{p_B(H1)_s\}\right\}$, високий рівень ризику;

- якщо $fsr\left\{ fsr\{p_B(H1)_s\} \div \max_s \{p_B(H1)_s\} \right\} \le p_B(H1) \le 1$, критичний рівень ризику.

Таким чином, можна зробити висновок, що реалізація математичної моделі операційного ризику надає можливість:

- сформувати визначену кількісну характеристику операційного ризику на основі нечітко сформованих величин, які виступають ідентифікаторами даного виду ризику;
- оперативно ідентифікувати операційний ризик в банківській установі (експрес підхід) та провести детальний аналіз формуючих його інцидентів (імовірнісний підхід);
- визначити характер операційного ризику комерційного банку в розрізі аналізу частки інцидентів, які його формують;
- виявити співставність рівнів операційного ризику в межах розглянутої сукупності банківських установ на основі надання якісної характеристики даної категорії ризику.

4.2 Практична реалізація математичної моделі визначення рівнів операційного ризику комерційних банків Національним банком України при здійсненні регулювання і нагляду

Одним із важливим завдань регулятора ринку банківських послуг, функції якого в Україні покладено на Національний банк, є визначення рівня операційного ризику комерційних банків з метою адекватного реагування та недопущення нанесення шкоди вкладникам та кредиторам банків.

Що означає операційний ризик для нагляду з боку центрального банку? В нормальній ситуації має місце забезпечення в комерційних банках ризик-менеджмент, який фокусується на уникненні/зменшенні ризику. В такому випадку здебільшого наголос ставиться на превентивному контролі, який покликаний не допускати реалізації (кристалізації) ризику. Проте, в разі загострення кризових явищ

здійснюється кризовий менеджмент, який фокусується на максимізації надходжень від управління активами та пасивами банку.

Саме тому Національному банку України необхідно володіти дієвими інструментами оцінки та управління операційними ризиками банками. При цьому такі інструменти можуть поділятися на ті, що використовуються камерально (тобто в безвиїзному порядку) та безпосередньо в ході здійснення інспекційних перевірок банків. Одразу зазначимо, що далі піде мова про саме про безвиїзний нагляд, оскільки саме в такому випадку наявність універсального інструменту дозволяє робити неупереджені висновки щодо рівнів відповідних ризиків в банку.

Оскільки питання щодо теорії банківських ризиків та місця операційного ризику в цій системі розглядалось в попередніх розділах, розпочнемо розгляд питання визначення операційного ризику в Національному банку України з концепції апетиту та толерантності до ризику, яка включає:

- по-перше, *концепцію ризику і доходу*: бажання банку прийняти ризик для отримання доходу (при цьому, відповідно, для отримання доходу через прийняття ринкового та кредитного ризику необхідно прийняти певний рівень операційного ризику);

- по-друге, визначення *апетиту до ризику*: та максимальна межа щодо ризику, яку банк готовий досягти в процесі ведення своєї діяльності (одразу зауважимо, що стосовно операційного ризику, як правило, вживають термін «*толерантність до ризику*» замість «апетит до ризику», оскільки він іноді повинен прийматися «вимушено»).

До основних аспектів визначення апетиту (толерантності) до ризику відносяться:

- рівень очікуваних і неочікуваних втрат, які вважаються прийнятними для банку;
- галузеві стандарти, кодекси професійної поведінки та етики, приклади найкращої практики тощо;
- переваги та очікування акціонерів;
- очікувані результати функціонування (наприклад, прибуток на капітал);

- волатильність доходу, прийнята для банку;
- обсяг капіталу, який банк готовий визнати ризиковим капіталом;
- культура організації;
- досвід менеджменту з врахуванням уміння управляти ризиком і контролювати ризик;
- довгострокові стратегічні пріоритети тощо.

Загально прийнятою є думка, що визначення апетиту до ризику може базуватися на кількісних індикаторах лише для фінансових ризиків: для ринкового ризику – на показниках ризикової вартості (Value-at-Risk), для кредитного ризику – на ймовірності дефолту, ступені відшкодування після дефолту тощо. Одночасно більшість дослідників та практиків підтримують точку зору, що операційний ризик не підлягає кількісному вимірювання, в зв'язку з чим визначають такі особливості визначення апетиту (толерантності) до ризику стосовно операційного ризику:

- менш розвинута база вимірювання в порівнянні з фінансовими ризиками;
- відсутність єдиного виміру операційного ризику (такого, як VaR[5]);
- наявність низки непорівнюваних типів операційного ризику.

Тут слід зазначити, що ми не погоджуємось із зазначеними постулатами щодо толерантності до операційного ризику і спробуємо це довести трохи згодом. Більше того, надалі буде зроблена спроба запропонувати алгоритми, що дозволяють порівнювати різноманітні параметри, та побудувати математичні моделі оцінки операційного ризику в Національному банку України та в комерційних банках.

При здійсненні оцінки ризиків, зокрема операційного, одним з наріжних залишається питання, як необхідно їх ідентифікувати і класифікувати ризики.

В такому випадку необхідно, щоб існувала узгодженість щодо, зокрема щодо визначення категорій ризику та визначення ймовірностей і впливу ризиків. Основним проблемним питанням для визначення рівнів операційного ризиків комерційних банків Національним банком України в безвиїзному порядку є нестача статистичних даних щодо інцидентів. Більше того, ця проблема стоїть і перед

[5] VaR – (англ.value at risk) – вартість під ризиком.

комерційними банками, оскільки не існує загальних нормативно-правових вимог щодо збору відповідних даних.

Для побудови економіко-математичної моделі, яка дозволить розрахувати рівень операційного ризику кожного українського банку при здійсненні безвиїзного нагляду фахівцями Національного банку України необхідно визначити низку індикативних показників на основі тієї інформації, що є загальною щодо всіх банків та є в наявності у Національного банку України. Основним джерелом такої інформації є статистична звітність банків.

З метою отримання відповідних даних від територіальних управлінь і установ НБУ, банків, та підприємств (що мають рахунки в іноземних банках), для складання грошової і банківської статистики, статистики платіжного балансу і з міжнародної інвестиційної позиції, та для забезпечення виконання НБУ регулятивних та наглядових функцій відповідно до законодавства України розроблено Правила організації статистичної звітності, що подається до Національного банку України, затверджені постановою Правління Національного банку України від 19.03.2003 № 124 (далі – Правила) [5]. Правила визначають зразки форм статистичної звітності, перелік та порядок їх заповнення, періодичність їх складання, терміни та способи подання даних до НБУ.

Проаналізувавши наявні форми статистичної звітності, можна зробити висновок, що основними формами, які можна використати для визначення базових індикативних показників операційного ризику комерційних банків є такі:

- форма №200 «Звіт про фінансові операції, що підлягають фінансовому моніторингу»;
- форма №363 «Звіт про цінні папери, емітовані банком, іншу заборгованість, похідні фінансові інструменти, доходи та витрати банку (за класифікаціями контрагентів і рахунків)»;
- форма №381 «Довідка про залучені кошти та їх залишки на кореспондентському рахунку»;
- форма №401 «Дані про операції, які здійснені із застосуванням платіжних карток, емітованих для клієнтів банку»;

- форма №402 «Дані про операції, які здійснені із застосуванням платіжних карток через власну інфраструктуру банку»;
- форма №403 «Дані про кількість емітованих (розповсюджених) платіжних карток для клієнтів банку та технічні засоби, що використовуються під час здійснення операцій з їх застосуванням»;
- форма №404 «Дані про збитки банку, держателів платіжних карток і торговців через незаконні дії/сумнівні операції з платіжними картками»;
- форма №406 «Звіт про кількість програмно-технічних комплексів самообслуговування (ПТКС), що належать банку на праві власності або інших речових правах, та обсяги переказів коштів, які здійснюються за їх допомогою»;
- форма №407 «Звіт про кількість програмно-технічних комплексів самообслуговування (ПТКС), що належать суб'єктам господарювання, які уклали агентські договори з банком, та обсяги переказів коштів, що здійснюються за їх допомогою»
- форма №410 «Звіт про кількість клієнтів банків та кількість відкритих клієнтами рахунків»;
- форма №606 «Звіт про формування банками резерву за простроченими та сумнівними до отримання нарахованими доходами»;
- форма №682 «Звіт про застосування Національним банком України до банків заходів впливу».

Надалі пропонуємо короткий огляд перерахованих статистичних форм з метою розкриття їх інформаційного наповнення.

Форма №200 «Звіт про фінансові операції, що підлягають фінансовому моніторингу» передбачає надання банками відомостей за звітний місяць про кількість:

- фінансових операцій, унесених до реєстру фінансових операцій, що підлягають фінансовому моніторингу;
- надісланих уповноваженому органу - Державному комітету фінансового моніторингу України повідомлень про фінансові операції, що підлягають

обов'язковому та внутрішньому фінансовому моніторингу (згрупованих за кодами ознак), повідомлень про фінансові операції, щодо яких у банку були мотивовані підозри, що вони можуть бути пов'язані з тероризмом, повідомлень про фінансові операції, у проведенні яких клієнту було відмовлено, та повідомлень про закриття рахунку клієнта;

- фінансових операцій, за якими банком прийнято рішення не надсилати файла-повідомлення;
- фінансових операцій, за якими від Державного комітету фінансового моніторингу України надходили файли-повідомлення про відмову від узяття їх на облік;
- надісланих Державним комітетом фінансового моніторингу України файлів-запитів та наданих банком файлів-додатків.

Форма №200 складається за такими типами клієнтів банку:

1 тип - юридична особа (без урахування фінансових установ - кореспондентів);

2 тип - фізична особа - суб'єкт підприємницької діяльності;

3 тип - фізична особа;

4 тип - фінансова установа - кореспондент.

Форма №363 «Звіт про цінні папери, емітовані банком, іншу заборгованість, похідні фінансові інструменти, доходи та витрати банку (за класифікаціями контрагентів і рахунків)» передбачає надання банками даних про цінні папери, емітовані банками, залишки коштів за іншою заборгованістю в розрізі секторів економіки, резидентності, кодів валют і початкових строків погашення, а також процентні доходи та витрати, дохід у вигляді дивідендів, отримані та сплачені штрафи, пені у розрізі секторів економіки.

Форма №381 «Довідка про залучені кошти та їх залишки на кореспондентському рахунку» передбачає надання відповідних даних, включаючи кількість випадків недорезервування коштів під час контролю за щоденними залишками.

Форма №401 «Дані про операції, які здійснені із застосуванням платіжних карток, емітованих для клієнтів банку» введена в дію з метою контролю за

діяльністю банків, пов'язаною з емісією та еквайрингом платіжних карток. Звіт подається банками - принциповими та асоційованими членами платіжних систем з урахуванням операцій, які здійснені платіжними картками, розповсюдженими іншими банками за агентськими угодами. Дані повідомляються в розрізі платіжних систем (груп платіжних систем) за фізичними та юридичними особами (у цій формі юридичні особи - це також фізичні особи - підприємці та представництва юридичних осіб - нерезидентів). Звіт складається на підставі даних, наданих банку процесинговими центрами, та власної інформації, отриманої з автоматизованих карткових систем банку (модулів емісії та еквайрингу платіжних карток, автоматизованої карткової системи Національної системи масових електронних платежів тощо).

Форма №402 «Дані про операції, які здійснені із застосуванням платіжних карток через власну інфраструктуру банку» подається банками - принциповими та асоційованими членами платіжних систем з урахуванням операцій, які здійснені платіжними картками, розповсюдженими іншими банками за агентськими угодами. Звіт складається на підставі даних, поданих банку процесинговими центрами, та власної інформації, отриманої з автоматизованих карткових систем банку (модулів емісії та еквайрингу платіжних карток, автоматизованої карткової системи Національної системи масових електронних платежів тощо).

Форма №403 «Дані про кількість емітованих (розповсюджених) платіжних карток для клієнтів банку та технічні засоби, що використовуються під час здійснення операцій з їх застосуванням» подається банками - принциповими та асоційованими членами платіжних систем з урахуванням даних за банками, що працюють з ними за агентськими угодами. У звіті надається інформація про кількість емітованих (розповсюджених) платіжних карток для клієнтів банку та технічні засоби, що використовуються під час здійснення операцій з їх застосуванням, які обслуговуються банком на підставі відповідних договорів з торговцями, а також про власні технічні засоби банку в розрізі платіжних систем (груп платіжних систем). Якщо емітовані банком платіжні картки містять логотипи двох і більше платіжних систем, то в звіті дані за такими картками відображаються

за тією платіжною системою, ідентифікатор емітента якої нанесено на картку. Звіт складається на підставі даних, наданих банку процесинговими центрами, і власної інформації, отриманої з автоматизованих карткових систем банку (модулів емісії та еквайрингу платіжних карток, автоматизованої карткової системи Національної системи масових електронних платежів тощо).

Форма №404 «Дані про збитки банку, держателів платіжних карток і торговців через незаконні дії/сумнівні операції з платіжними картками» подається банками - юридичними особами, які є принциповими та асоційованими членами платіжних систем. У звіті надається інформація в розрізі платіжних систем (груп платіжних систем) про кількість випадків і суми збитків банку, держателів платіжних карток і торговців, яких обслуговує банк відповідно до договору, через незаконні дії/сумнівні операції з платіжними картками (далі - збитки через незаконні дії з картками).

Форма №406 «Звіт про кількість програмно-технічних комплексів самообслуговування (ПТКС), що належать банку на праві власності або інших речових правах, та обсяги переказів коштів, які здійснюються за їх допомогою» подається банками - юридичними особами з урахуванням операцій, які здійснені за допомогою програмно-технічних комплексів самообслуговування (далі - ПТКС), у розрізі областей. Звіт складається на підставі даних, поданих банку процесинговими центрами, та власної інформації, отриманої з автоматизованих систем банку. У звітності не зазначаються показники щодо кількості ПТКС і сум переказів коштів через них під час здійснення: операцій з видачі готівки; торговельних операцій з продажу попередньо оплачених послуг [(карток поповнення рахунків мобільного зв'язку (ваучерів)] і продажу товарів (кави, напоїв тощо), здійснених за допомогою ПТКС (у тому числі платіжних терміналів, які розташовані в пунктах продажу товарів та інших торгових точках).

Форма №407 «Звіт про кількість програмно-технічних комплексів самообслуговування (ПТКС), що належать суб'єктам господарювання, які уклали агентські договори з банком, та обсяги переказів коштів, що здійснюються за їх допомогою» подається банками - юридичними особами, які уклали агентські

договори з суб'єктами господарювання з урахуванням операцій, що здійснені за допомогою програмно-технічних комплексів самообслуговування (далі - ПТКС), у розрізі областей. Звіт складається на підставі даних, поданих процесинговими центрами, і власної інформації, отриманої з автоматизованих систем. У звітності не зазначаються показники щодо кількості ПТКС і сум переказів коштів через них під час здійснення: операцій з видачі готівки; та торговельних операцій з продажу попередньо оплачених послуг [(карток поповнення рахунків мобільного зв'язку (ваучерів)] і продажу товарів (кави, напоїв тощо), здійснених за допомогою ПТКС (у тому числі платіжних терміналів, які розташовані в пунктах продажу товарів та інших торгових точках).

Форма №410 «Звіт про кількість клієнтів банків та кількість відкритих клієнтами рахунків» містить інформацію про кількість клієнтів - юридичних та фізичних осіб (резидентів та нерезидентів), що відкрили поточні та/або вкладні (депозитні) рахунки на відповідних балансових рахунках у банках України, та кількість відкритих ними рахунків. Звіт складається за такими видами клієнтів банку:

1 вид - бюджетні установи;

2 вид - суб'єкти господарювання - небанківські фінансові установи;

3 вид - інші суб'єкти господарювання, у тому числі юридичні особи, які мають рахунки для обліку коштів бюджету та державних цільових фондів, та фізичні особи-підприємці;

4 вид - фізичні особи - приватні нотаріуси та адвокати;

5 вид - інші фізичні особи.

Форма №606 «Звіт про формування банками резерву за простроченими та сумнівними до отримання нарахованими доходами» впроваджена для здійснення контролю за формуванням банками спеціального резерву під прострочені та сумнівні до отримання нараховані доходи за активними операціями та розроблена відповідно до вимог нормативно-правових актів Національного банку України, оскільки банки зобов'язані формувати резерв незалежно від їх фінансового стану на

всю суму прострочених понад 31 день і сумнівних щодо отримання нарахованих доходів, що обліковуються за відповідними балансовими рахунками.

Форма №682 «Звіт про застосування Національним банком України до банків заходів впливу» розроблено з метою контролю за рівнем ризиковості в діяльності банків, дотриманням ними вимог законодавства України, у тому числі нормативно-правових актів Національного банку України, а також своєчасністю і ефективністю застосування заходів впливу. Звіт містить інформацію про застосовані до банків заходи впливу за допущені порушення і складається з двох частин. У першій частині (Інформація за поточний рік) міститься інформація про застосовані заходи впливу за порушення, допущені в поточному році. У другій частині (Інформація за минулі роки за невиконаними заходами впливу) надається інформація про заходи впливу, що застосовані в минулі роки, виконання яких здійснюється в поточному році.

Тепер пропонуємо розглянути ті показники, що на наш погляд, є індикаторами операційного ризику комерційного банку.

Відразу слід зазначити, що всі показники можна класифікувати в залежності від виду банківських операцій на такі, що пов’язані з:

- обслуговуванням клієнтів, та
- з діяльністю банку та його власними операціями.

Також можна виділити групи показників, що характеризують окремі види банківських послуг, оскільки вони є найбільш ризиковими щодо операційного ризику, наприклад, операції банку з платіжними картками та дистанційне обслуговування клієнтів тощо.

Розпочнемо з показників, пов’язаних з обслуговуванням клієнтів банку.

K_1 - *кількість банкоматів, кількість платіжних терміналів та імпринтерів.* Дані показники характеризують наскільки інтенсивно банк використовує відповідні пристрої, обслуговування яких пов’язане з підвищенням операційного ризику через:

- помилки чи необачність персоналу, який міг не вірно здійснити налаштування пристроїв, не забезпечити відповідну кількість готівки у банкоматі або не точно визначити її небохіний обсяг для завантаження тощо;

- помилки в самих пристроях або їх програмному забезпеченні, системах захисту тощо;
- а також різноманітні зовнішні ризики: збої в електромережі, природні лиха, шахрайство, зломи, вандалізм тощо.

Відмітимо важливу роль групи показників, що характеризують збитки банку від різного роду шахрайств з платіжними картками є надзвичайно важливою при визначенні рівня операційного ризику банку.

Так, за даними Національного банку України кількість шахрайських операцій з використанням платіжних карток в Україні в 2009 році зросла порівняно з 2008 роком у 6,5 разів, сягнувши 39,338 тис. операцій. Сума збитків за такими операціями також зросла на 6,12 млн грн. та становила близько 12,97 млн грн. Збитків від карткових шахраїв в 2009 році зазнали 44 українські банки [3].

Таким чином для оцінки операційного ризику банку доцільно розрахувати такі показники щодо збитків через шахрайські операції з платіжними кратками.

K_2 - *збитки через незаконні дії / сумнівні операції з платіжними кратками* безпосередньо свідчить про певний рівень матеріальних втрат банку від нелегітимних дій з платіжними картками.

Варто також врахувати, що існують різноманітні шляхи отримання шахраями коштів за допомогою платіжних краток:

- підробка карток;
- отримання інформації для ідентифікації та авторизації проведення трансакцій по рахунку шахрайським шляхом (наприклад, прохання надати відомості для отримання виграшу у псевдолотереї);
- інсайдерські маніпуляції та використання інформації, що стає відомою під час виконання службових обов'язків;
- злам інформаційної системи банку;
- викрадення картки тощо.

Отже, існує низка методів отримання несанкціонованого доступу до коштів клієнтів банку за допомогою сумнівних дій з платіжними картками. Тому, варто визначити, які саме дії спричинили найбільші збитки банку, спричинивши зростання

операційного ризику в цілому. Для цього пропонуємо розрахувати показники K_3-K_7.

K_3 - *частка збитків за підробленими платіжними картками до загальної суми збитків через незаконні дії / сумнівні операції з платіжними картками.* На наш погляд, окрему увагу слід звернути на збитки, завдані банку через підробні платіжні картки, оскільки даний факт може також свідчити, зокрема про низький рівень захисту картки саме даного банку.

K_4 - *частка збитків за втраченими / викраденими платіжними картками до загальної суми збитків через незаконні дії / сумнівні операції з платіжними картками.* Даний показник є важливим для розрахунку рівня операційного ризику, проте він має свою особливість, адже є цілком незалежним і непідвладним діям банку (його персоналу), а залежить від клієнтів. Проте, врахування подій такого роду і є одним з наріжних каменів визначення операційного ризику.

K_5- *частка збитків за операціями без пред'явлення картки до загальної суми збитків через незаконні дії / сумнівні операції з платіжними картками.* Це стосується в першу чергу операцій через мережу Інтернет, телефоном тощо. Невипадково питання дистанційного обслуговування клієнтів та їх належної ідентифікації викликає постійні дискусії у колі професійних учасників банківського бізнесу – адже йдеться про забезпечення клієнтів інноваційними послугами, що можуть зробити обслуговування клієнтів значно зручнішим особливо в умовах постійного браку часу, та одночасне забезпечення високих стандартів безпеки.

Яскравим прикладом інноваційного продукту, що забезпечує дистанційне обслуговування клієнтів, сьогодні є безконтактні банківські картки. Безконтактні смарт-картки, що передають інформацію з радіочастотного каналу, вже вийшли на оперативний простір і активно використаються в багатьох комерційних проектах по всьому світу [1]. Також їх називають картками з дуальним інтерфейсом, оскільки вони дозволяють розплачуватися як традиційним способом, вставляючи картку в термінал (через контактний мікрочіп або магнітну смугу), так і безконтактним — через радіоканал. Усередині картки знаходиться антена, що посилає радіочастотний

сигнал на термінал, і в такий спосіб швидко й надійно здійснюється передача платіжної інформації на зчитувальний пристрій, підключений до касового апарата торговельної точки. Для здійснення платежу картку не потрібно передавати касирові й навіть діставати її з гаманця, а досить просто тримати гаманець із карткою, що знаходиться в ньому, на відстані приблизно 4 см від зчитувального пристрою. Тобто, в момент оплати безконтактною картою відбуваються лише аутентифікація клієнта й списання коштів. На картці заздалегідь встановлюється офлайновий ліміт (сума, яку можна витратити, не зв'язуючись із банком), у межах якого й дозволяється проводити трансакції. Авторизація, тобто перевірка наявності грошей на рахунку, не проводиться, як не підписується й чек. Це безсумнівний ризик як для банку, так і для клієнта, тому банкіри обмежують разові «безконтактні» платежі невеликими сумами. Наприклад, за карткою Віза Вейв (Visa Wave), що у лютому 2005 року була запущена в комерційну експлуатацію в Малайзії, платежі до 25 дол. США дозволяється проводити безконтактно — без авторизації, без чека й перевірки підпису.

Крім того, в Японії та Південній Кореї чіп з дуальним інтерфейсом вмонтовано в мобільний телефон. Безконтактна частина чіпа працює через радіоканал, а контактна — через інфрачервоний порт мобільного телефону. Він направляється на інфрачервоний порт ПОС-термінала, встановлюється псевдоконтактне з'єднання й відбувається трансакція. Вищенаведений приклад — яскрава ілюстрація реалізації нових технологій у картка ому бізнесі, які, в свою чергу, потребують відповідних методів та захисту та управління новими ризиками, що вони породжують.

K_6 - *частка збитків за картками, які були емітентом поштою і не отримані держателем, до загальної до загальної суми збитків через незаконні дії / сумнівні операції з платіжними картками.* Даний показник також пов’язаний з ризиком, що виникає коли банк запроваджує різні методи поліпшення обслуговування клієнтів і змушений їх нести за умов загострення конкурентної боротьби на ринку.

$К_7$ - частка збитків за операціями з використанням особистих даних клієнта (держателя картки) для відкриття банківського рахунку чи отримання доступу до рахунку за підробленими або викраденими документами до загальної до загальної суми збитків через незаконні дії / сумнівні операції з платіжними картками. Даний показник заслуговує на окрему увагу, оскільки засвідчує надійність системи безпеки банку, рівень підготовки персоналу та його порядність, а також надійність інформаційних систем.

Наприклад, нещодавно поширення набуло шахрайство з платіжними картками за допомогою спеціального пристрою «скіммера», що встановлювався зловмисниками у банкоматах та дозволяв зчитувати персональні дані власника картки для подальшого її злому. Крім того, експерти стверджують [4], що для виготовлення дублікату картки з магнітною полосою необхідно мінімум обладнання та близько 30 хвилин часу.

Підсумовуючи сказане щодо шахрайських дій з платіжними картками хотілося б звернути увагу на те, що досить часто такі події можуть не тільки спричинити певні матеріальні збитки банку, а й суттєво вплинути на його репутацію, зокрема зруйнувати уявлення клієнтів про нього, як про надійний банк.

Крім того, для оцінки операційного ризику, пов'язаного з банківськими операціями за платіжними картками, на наш погляд, варто визначити також наступні показники.

$К_8$- сума фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (операції з отримання готівки - операції, які здійснені із застосуванням платіжних карток, емітованих для клієнтів банку).

$К_9$ - *к*ількість фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (операції з отримання готівки - операції, які здійснені із застосуванням платіжних карток, емітованих для клієнтів банку).

K_{10}- сума фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (безготівкові платежі - операції, які здійснені із застосуванням платіжних карток, емітованих для клієнтів банку).

K_{11} – кількість фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (безготівкові платежі - операції, які здійснені із застосуванням платіжних карток, емітованих для клієнтів банку).

K_{12}– сума фінансові операції за внутрішньодержавними платіжними системами та міжнародними платіжними системами (операції з отримання готівки - операції, які здійснені із застосуванням платіжних карток через власну інфраструктуру банку)

K_{13}– кількість фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (операції з отримання готівки - операції, які здійснені із застосуванням платіжних карток через власну інфраструктуру банку).

K_{14}– сума фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (безготівкові платежі - операції, які здійснені із застосуванням платіжних карток через власну інфраструктуру банку)

K_{15} - кількість фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (безготівкові платежі - операції, які здійснені із застосуванням платіжних карток через власну інфраструктуру банку).

Розрахунок показників K_8 – K_{15} допоможе встановити інтенсивність фінансових операцій за платіжними картками, яка впливає на ймовірність здійснення не лише шахрайських операцій, а, в першу чергу, різного роду помилок, починаючи від недоліках у бізнес-процесах, та закінчуючи необачністю персоналу. Тобто, чим вища інтенсивність та обсяги таких операцій, тим вищим буде й операційний ризик банку.

Розглядаючи два наступні показники, зауважимо, що коли мова йде про операційний ризик, то дуже часто виділяють два важливі фактори, що зумовлюють

підвищення його рівня: по-перше, шахрайства, а, по-друге, аутсорсинг. Про перший фактор ми вже згадували, а от другий – потребує нашої уваги. Саме при залученні фахівців зі сторонніх організацій пов'язане з ризиком шахрайств з їх боку, витоком інформації, помилками через недосконале розуміння певних бізнес-процесів та недостатній рівень кваліфікації для виконання досить специфічних завдань тощо. При цьому, коли банк укладає угоди з суб'єктами господарювання агентські договори на використання програмно-технічних комплексів самообслуговування (ПТКС), то він також наражається на відповідні ризики, незважаючи на те, що аутсорсинг в такому випадку здійснює суб'єкт господарювання. Яскравим прикладом, в даному випадку може слугувати випадок, що стався з українськими користувачами терміналів I-Box на початку 2010 року, коли тисячі громадян не отримали на свої рахунки гроші, сплачені через термінали «Айбокс» (I-Box) через, масштабний збій в роботі терміналів. Кошти клієнтам були повернуті лише за тиждень. Таким чином, необхідно, на наш погляд, розрахувати:

K_{16}- *частку кількості ПТКС, що належать суб'єктам господарювання, які уклали агентські договори з банком до загальної кількості ПТКС та* K_{17} - *середній рівень суми переказів коштів через ПТКС за звітне півріччя - співвідношення загальної суми переказів коштів через ПТКС за звітне півріччя до загальної кількості ПТКС.*

Крім того, сучасні засоби, що використовуються для дистанційного обслуговування клієнтів банку містять також низку факторів операційних ризиків, що поєднують і можливі шахрайській дії, і можливі помилки чи збої у програмному забезпечення та налаштуванні обладнання. Саме тому наступні показники є вкрай важливими для оцінки рівня операційного ризику банку:

K_{18} - *Кількість клієнтів, які використовують систему дистанційного обслуговування рахунків*

K_{19} - *Частка клієнтів, які використовують систему дистанційного обслуговування від загальної кількості клієнтів банку, %*

$К_{20}$ - *Кількість поточних та/або вкладних (депозитних) рахунків, обслуговування яких здійснюється дистанційно*.

При цьому, на наш погляд, варто звернути на два наступні показники (К кількість недіючих рахунків клієнтів та К - сума залишку коштів за недіючими рахунками), оскільки все частіше зустрічають шахрайства серед співробітників банку, коли останні списують на свою користь кошти з так званих «сплячих» рахунків.

$К_{21}$ - *Кількість недіючих рахунків клієнтів*

$К_{22}$ - *Сума залишку коштів за недіючими рахунками.*

Більше того, існує низка ІТ – інструментів, які використовуються не тільки інсайдерами банку, а й шахраями поза межами банку. Так, у 2005-2006 роках в Росії та Україні діяла організована злочинна група, яка викрадала кошти з особистих банківських рахунків французів. Шахраї викрали понад 1 млн. євро за допомогою «сплячих вірусів». У результаті однієї з таких операцій тільки один клієнт банку втратив 40 тис. євро. Злочинці, уразивши комп'ютери жертв вірусами, одержували контроль над банківським рахунком і могли спустошити його за кілька секунд. Вірус впроваджувався через електронну пошту або інтернет-сайти й перебував у неактивному стані доти, поки користувач не перевіряв свій банківський рахунок. Як тільки це відбувалося, вірус активізувався й записував пароль і банківські коди, які потім пересилав зловмисникам. Злочинці перевіряли, є чи в жертви гроші в банку, після чого переводили кошти третім особам («дропам»), які за невелику комісію в 5-10% погоджувалися переводити через їхні рахунки гроші. Але іноді такі перекази здійснювались через рахунки «дропів» без їх відома, в результаті чого фактичне з’ясування джерел походження коштів є неможливим [6].

Ми розглянули низку показників, які можуть виступати характеристиками операційного ризику в банку з огляду на обслуговування клієнтів, проте, не слід забувати про власне банківські операції та ризики, пов’язані з його власною діяльністю. Основними джерелами збитків банку тут можуть бути декілька:

- шахрайські дії інсайдерів (наприклад, інсайдерські торгівля);

- та порушення певних регуляторних вимог, що спричиняють накладення на банк штрафів та пені або можуть стати причиною обмеження певних пунктів ліцензій а банківську діяльність або навіть її повне відкликання тощо. І хоча дуже важко оцінити та спрогнозувати можливі шахрайства з боку інсайдерів, проте давня статистична звітність банків дає змогу здійснити певні розрахунки щодо можливих наслідків через порушення банком окремих регулятивних вимог. Пропонуємо розрахувати наступні показники.

K_{23} - *кількість випадків недорезервування коштів під час контролю за щоденними залишками*. Даний показник може свідчити про штрафи чи пені банку за недотримання певних вимог щодо резервування. При цьому причинами таких порушень можуть бути: дії персоналу (його помилки) або прогалини у побудові бізнес-процесів банку тощо.

K_{24} - *кількість порушень, виявлених Національним банком України.*

K_{25} - *сплачено банком штрафів за виявлені Національним банком України порушення.* Ці два показники говорять самі за себе, адже безпосередньо свідчать про випадки недотримання встановлених норм та вимог.

K_{26} – *сума заборгованості за простроченими та сумнівними до отримання нарахованими доходами за операціями на міжбанківському ринку.*

K_{27} – *сума заборгованості за простроченими та сумнівними до отримання нарахованими доходами за кредитними операціями з клієнтами.*

K_{28} – *сума заборгованості за простроченими та сумнівними до отримання нарахованими доходами за операціями з цінними паперами.*

K_{29} - *сума заборгованості за простроченими та сумнівними до отримання нарахованими доходами за іншими операціями.*

Попри всі вищезазначені показники, які в основному характеризують фінансові результати роботи банку, ми б хотіли звернути увагу на такий напрямок банківської діяльності, як фінансовий моніторинг.

Власне фінансовий моніторинг – молодий напрямок не лише в банківській діяльності, пов’язаний з протидією відмивання коштів, отриманих злочинним

шляхом, та фінансування тероризму. Більше того, аналіз ризиків «легалізації коштів» свідчить про його тісний зв'язок з усіма банківськими ризиками, зокрема з операційним ризиком [1]. Саме тому необхідно врахувати наступні показники:

$К_{30}$ - *кількість фінансових операцій, щодо яких надходили файли про відмову від взяття на облік. Даний показник може свідчити про недостатню компетентність персоналу банку, халатність до виконання своїх обов'язків, а також про помилки у програмному забезпеченні*.

$К_{31}$ - *кількість фінансових операцій, які були анульовані після надання інформації до ДКФМУ*[6]. *Анулювання внесених до реєстру фінансових операцій в більшості випадках відбувається через їх помилкове внесення до реєстру, наприклад, за хибною ознакою. Тому даний критерій допоможе оцінити рівень ризику, що виникає через помилки персоналу*.

Безперечно, лишається ще багато аспектів банківської діяльності, які вливають на формування рівня операційного ризику банку, проте обмеженість даних зумовлена встановленими формами статистичної звітності. Хоча, слід також зазначити і позитивну сторону – адже банки несуть відповідальність за подання

При визначення показників, що характеризують операційний ризик в комерційному банку, слід врахувати, які саме інциденти впливають на їх формування в якості відповідних індикаторів. На наш погляд до основних інцидентів операційного ризику комерційного банку відносяться:

- ризик, пов'язаний з діями працівників та безпекою робочого місця;
- ризик систем і технологій;
- ризик помилки у банківських процесах (ризик взаємовідносин);
- ризик пов'язаний з зовнішніми чинниками.

Отже, визначивши базові індикативні показники для оцінки операційного ризику в комерційному банку на основі статистичної звітності банків, слід встановити які саме з чотирьох основних інцидентів ризику притаманні кожному з них. Для цього пропонуємо розглянути табл. 4.6 (детально див. додаток А.1).

[6] ДКФМУ – Державний комітет фінансового моніторингу України.

Таблиця 4.6

Таблиця відповідності показників визначеним банківським установам в рамках оцінки операційного ризику

№	Показник	Банківська установа			
		А	Б	В	Г
А	Б	1	2	3	4
I. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів					
К1	Кількість банкоматів, кількість платіжних терміналів та інших електронних пристроїв, кількість імпринтерів	5 765	4 846	3 216	3
К2	Збитки через незаконні дії/сумнівні операції з платіжними картками	2 625	951	5 195	0
…	…	…	…	…	…
К21	Кількість недіючих рахунків клієнтів	2 920	24 141	3 711	34
К22	Сума залишку коштів за недіючими рахунками	2 052,38	1 185,92	14 857,34	12,95
II. Операційний ризик, пов'язаний з власною діяльністю банку					
К23	Кількість випадків недорезервування коштів під час контролю за щоденними залишками	0	0	6	0
К24	Кількість порушень, виявлених Національним банком України	18	68	14	28
…	…	…	…	…	…
К30	Кількість фінансових операцій, щодо яких надходили файли про відмову від взяття на облік	14	18	2 349	0
К31	Кількість фінансових операцій, які були анульовані після надання інформації до ДКФМУ	4	33	0	0

На наступному етапі реалізації математичної моделі операційного ризику комерційного банку, необхідно *привести наявну інформацію щодо кожного з чотирьох комерційних банків до порівнюваного вигляду, що здійснюється шляхом нормалізації*. Необхідно зазначити, що нормалізація показників здійснюється окремо для групи показників, пов’язаної з банківським обслуговуванням клієнтів, та окремо для групи показників, які характеризують власну діяльність банку.

Таблиця 4.7

Таблиця відповідності показників визначеним інцидентам операційного ризику

№	Показник	Інцидент ризику (бінарна характеристика)			
		ризик, пов’язаний з діями працівників та безпекою робочого місця	ризик систем і технологій	ризик помилки у банківських процесах (ризик взаємовідносин)	ризик пов’язаний з зовнішніми чинниками
А	Б	1	2	3	4
І. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів					
К1	Кількість банкоматів, кількість платіжних терміналів та інших електронних пристроїв, кількість імпринтерів	0	1	0	1
К2	Збитки через незаконні дії/сумнівні операції з платіжними картками	1	1	1	1
…	…	…	…	…	…
К21	Кількість недіючих рахунків клієнтів	1	0	1	1
К22	Сума залишку коштів за недіючими рахунками	1	0	1	1
ІІ. Операційний ризик, пов'язаний з власною діяльністю банку					
К23	Кількість випадків недорезервування коштів під час контролю за щоденними залишками	1	1	1	1
К24	Кількість порушень, виявлених Національним банком України	1	0	1	0
…	…	…	…	…	…
К30	Кількість фінансових операцій, щодо яких надходили файли про відмову від взяття на облік	1	1	0	0
К31	Кількість фінансових операцій, які були анульовані після надання інформації до ДКФМУ	1	1	0	0

Спочатку, на основі значень показників чотирьох комерційних банків, наведених в додатку(!!!!), розрахуємо середнє значення кожного з показників за формулою середньої арифметичної простої.

На наступному кроці проводиться зважування абсолютного значення кожного показника на рівень середнього, визначеного на попередньому етапі. Для цього перемножуємо значення кожного показника для певного банку на середнє значення цього показника для всіх чотирьох банків. Результати вищенаведених розрахунків наведено в табл. 4.7 (повна таблиця наведена в додатку А, таблиця А.3).

Таблиця 4.7

Нормалізовані значення показників кількісної оцінки операційного ризику банківської установи

№	Показник	Банківська установа			
		А	Б	В	Г
А	Б	1	2	3	4
І. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів					
К1	Кількість банкоматів, кількість платіжних терміналів та інших електронних пристроїв, кількість імпринтерів	1,67	1,40	0,93	0,00
К2	Збитки через незаконні дії/сумнівні операції з платіжними картками	1,20	0,43	2,37	0,00
…	…	…	…	…	…
К21	Кількість недіючих рахунків клієнтів	0,38	3,13	0,48	0,00
К22	Сума залишку коштів за недіючими рахунками	0,45	0,26	3,28	0,00
ІІ. Операційний ризик, пов'язаний з власною діяльністю банку					
К23	Кількість випадків недорезервування коштів під час контролю за щоденними залишками	0,00	0,00	4,00	0,00
К24	Кількість порушень, виявлених Національним банком України	0,56	2,13	0,44	0,88
…	…	…	…	…	…
К30	Кількість фінансових операцій, щодо яких надходили файли про відмову від взяття на облік	0,02	0,03	3,95	0,00
К31	Кількість фінансових операцій, які були анульовані після надання інформації до ДКФМУ	0,43	3,57	0,00	0,00

Отже, ми розрахували нормалізовані значення показників для кожного банку та бінарні характеристики відповідності показників інцидентам операційного

ризику. Тепер ми можемо визначити *ступінь впливу кожного інциденту на операційний ризик банку*.

Проаналізуємо діяльність *першого комерційного банку (банку А)*. Виходячи з цього, зазначені вище характеристики банку А можливо представити у вигляді табл. 4.8 (повна таблиця наведена в додатку А, таблиця А.4).

Таблиця 4.8

Зведена таблиця ознак кількісної оцінки операційного ризику комерційного банку А

№	Показник (нормалізоване значення) (результативна ознака)	Інцидент ризику (факторні ознаки)			
		j=1	*j=2*	*j=3*	*j=4*
А	Б	1	2	3	4
І. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів					
К1	1,67	0	1	0	1
К2	1,20	1	1	1	1
…	…	…	…	…	…
К21	0,38	1	0	1	1
К22	0,45	1	0	1	1
ІІ. Операційний ризик, пов'язаний з власною діяльністю банку					
К23	0,00	1	1	1	1
К24	0,56	1	0	1	0
…	…	…	…	…	…
К30	0,02	1	1	0	0
К31	0,43	1	1	0	0

Надалі проводиться дослідження впливу фіктивних змінних (бінарних характеристик відповідних інцидентів) на значення показників, які є індикаторами даного ризику, яке здійснюється на основі коефіцієнтів рівняння лінійної множинної регресії даної залежності (див. графу 1 таблиці 4.9).

Наведені в табл. 4.9 параметри рівняння регресії відображають, як збільшення чи зменшення відповідних інцидентів операційного ризику (факторних ознак) на 1% вплине на зміну показників (формула 4.16):

Таблиця 4.9

Результати проведення регресійного аналізу встановлення ступеня впливу кожного інциденту на операційний ризик банку А

Інцидент ризику	Коефіцієнти	Стандартна похибка	t -статистика	Нижні 95%	Верхні 95%
А	1	2	3	4	5
Y-перетин	-0,11	0,71	-0,16	-1,58	1,35
Ризик, пов'язаний з діями працівників та безпекою робочого місця	-0,24	0,41	-0,58	-1,09	0,61
Ризик систем і технологій	0,77	0,43	1,80	-0,11	1,65
Ризик помилки у банківських процесах (ризик взаємовідносин)	0,79	0,57	1,39	-0,38	1,97
Ризик пов'язаний з зовнішніми чинниками	0,38	0,43	0,88	-0,51	1,26

$$K = -0{,}11 - 0{,}24F_1 + 0{,}77F_2 + 0{,}79F_3 + 0{,}38F_4 \qquad (4.16)$$

де K – абсолютне значення ідентифікатора операційного ризику;

$F_j, j = 1 \div 4$ – фіктивна змінна характеристики j-го інциденту операційного ризику (приймає значення «1» або «0»).

Для того, щоб визначити, в якій мірі кожен з чотирьох інцидентів впливає на формування відповідного рівня операційного ризику необхідно на основі формули 1 та значень середньоквадратичного відхилення (див. табл. 6, повна таблиця наведена в додатку А, таблиця А.11) розрахувати показник, що характеризуватиме зазначений ступінь впливу. Рівень такого впливу визначається на основі коефіцієнтів стандартизованого рівняння лінійної множинної регресії залежності між інцидентами операційного ризику та показниками, що використовуються для його визначення (ідентифікаторами).

Таблиця 4.10

Проміжні розрахунки для визначення структури змін інцидентів операційного ризику банку А

№	Середнє квадратичне відхилення показників	Середнє квадратичне відхилення			
		F_1	F_2	F_3	F_4
А	1	2	3	4	5
І. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів					
К1	0,24	0,30	0,13	0,76	0,15
К2	0,00	0,20	0,13	0,02	0,15
…	…	…	…	…	…
К21	0,63	0,20	0,42	0,02	0,15
К22	0,52	0,20	0,42	0,02	0,15
ІІ. Операційний ризик, пов'язаний з власною діяльністю банку					
К23	1,38	0,20	0,13	0,02	0,15
К24	0,37	0,20	0,42	0,02	0,38
…	…	…	…	…	…
К30	1,32	0,20	0,13	0,76	0,38
К31	0,55	0,20	0,13	0,76	0,38
Загальний рівень	1,08	0,50	0,48	0,34	0,49

Таким чином, сформувавши комплекс вхідних даних в розрізі параметрів рівняння регресії та середньоквадратичних відхилень факторних і результативної ознак даного рівняння, ми можемо знайти коефіцієнти стандартизованого рівняння регресії. Розрахуємо перший з чотирьох наведених параметрів:

$$\alpha_2 = \beta_2 \frac{\sigma_{F_2}}{\sigma_K} = 0{,}77 \frac{0{,}48}{1{,}08} = 0{,}34 \qquad (4.17)$$

де σ_{F_2}, σ_K – середньоквадратичні відхилення факторних і результативної ознак, відповідно. Розрахунок решти трьох параметрів – здійснюється аналогічно.

Зважаючи на той факт, що визначення ступеня впливу інцидентів на рівень операційного ризику передбачає розрахунок частки кожного з чотирьох інцидентів в їх загальній структурі, необхідно встановити скореговані коефіцієнти стандартизованого рівняння лінійної множинної регресії. На прикладі другого

інциденту (ризик систем і технологій), ми розглянемо процедуру визначення питомої ваги впливу даного інциденту на рівень операційного ризику:

$$\alpha_2^* = \frac{\alpha_2}{\sum_{m=1}^{4} \alpha_m} = \frac{0{,}34}{|-0{,}11| + 0{,}34 + 0{,}25 + 0{,}17} = 0{,}39 . \qquad (4.18)$$

Аналогічно до вищенаведеного співвідношенню (4) розраховується ступінь впливу решти інцидентів операційного ризику (ризик, пов'язаний з діями працівників та безпекою робочого місця, ризик помилки у банківських процесах, ризик пов'язаний з зовнішніми чинниками) на результуючий показник. В розрізі даної методики результуючим показником є масив нормалізованих значень показників кількісної оцінки операційного ризику. Розраховані на попередньому етапі скореговані коефіцієнти стандартизованого рівняння лінійної регресії наведені в табл. 4.11.

Таблиця 4.11

Встановлення ступеня впливу кожного інциденту на операційний ризик банку А (коефіцієнти стандартизованого рівняння лінійної множинної регресії)

Інцидент операційного ризику	Коефіцієнти стандартизованого рівняння лінійної множинної регресії	Абсолютні коефіцієнти стандартизованого рівняння лінійної множинної регресії (взяті по модулю)	Скореговані коефіцієнти стандартизованого рівняння лінійної множинної регресії
А	1	2	3
F1 ризик, пов'язаний з діями працівників та безпекою робочого місця	-0,11	0,11	0,13
F2 ризик систем і технологій	0,34	0,34	0,39
F3 ризик помилки у банківських процесах (ризик взаємовідносин)	0,25	0,25	0,28
F4 ризик пов'язаний	0,17	0,17	0,20

з зовнішніми чинниками			

На основі даних колонки 3 табл. 4.11 стандартизоване рівняння лінійної множинної регресії для банку А, з урахуванням корегування його параметрів, прийматиме наступний вигляд:

$$K = 0{,}13F_1 + 0{,}39F_2 + 0{,}28F_3 + 0{,}20F_4 \qquad (4.19)$$

Проаналізувавши параметри рівняння (5), можна зробити такі висновки щодо основних аспектів рівня впливу інцидентів при здійсненні кількісної оцінки операційного ризику:

- найбільше значення вагового коефіцієнту серед розглянутих інцидентів операційного ризику прослідковується в розрізі ризику систем і технологій. Отже, при збільшенні кожного з інцидентів операційного ризику на 1%, найбільший вплив на зміну кількісної оцінки результуючого показника (біля 39%) справляє саме ризик систем і технологій;
- варіація кількісної оцінки операційного ризику на 61% пояснюється зміною таких трьох інцидентів, як ризик, пов’язаний з діями працівників та безпекою робочого місця, ризик помилки у банківських процесах (ризик взаємовідносин), ризик пов’язаний з зовнішніми чинниками;
- найменшу пріоритетність серед розглянутих інцидентів операційного ризику становить ризик, пов’язаний з діями працівників та безпекою робочого місця. Так, в числовому виразі відповідний ваговий коефіцієнт становить 13%, тобто це може свідчити, що при здійсненні нагляду з питань, пов’язаних з операційним ризиком банків, перевірка саме цього інциденту ризику з боку контролюючих органів може проводитись після детального дослідження інших інцидентів.

На основі визначених вище вагових коефіцієнтів інцидентів операційного ризику необхідно виділити структурні складові для кожного нормалізованого

значення показника, що відповідає чотирьом досліджуваним інцидентам. Для цього здійснюємо зважування значень кожного нормалізованого показника на вагові коефіцієнти інцидентів операційного ризику. Результати відповідних розрахунків наведені в табл. 4.12 (повна таблиця наведена в додатку А, таблиця А.18).

Таблиця 4.12

Відображення структури операційного ризику в залежності від формуючих їх інцидентів ризику для банку А

№ показника	Значення нормалізованого показника	Інциденти операційного ризику			
		ризик, пов'язаний з діями працівників та безпекою робочого місця $j=1$	ризик систем і технологій $j=2$	ризик помилки у банківських процесах (ризик взаємовідносин) $j=3$	ризик пов'язаний з зовнішніми чинниками $j=4$
		Вагові коефіцієнти інцидентів операційного ризику			
		0,13	0,39	0,28	0,20
А	1	2	3	4	5
I. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів					
К1	1,67	0,21	0,65	0,47	0,33
К2	1,20	0,15	0,47	0,34	0,24
…	…	…	…	…	…
К21	0,38	0,05	0,15	0,11	0,07
К22	0,45	0,06	0,18	0,13	0,09
II. Операційний ризик, пов'язаний з власною діяльністю банку					
К23	0,00	0,00	0,00	0,00	0,00
К24	0,56	0,07	0,22	0,16	0,11
…	…	…	…	…	…
К30	0,02	0,00	0,01	0,01	0,00
К31	0,43	0,06	0,17	0,12	0,08
Середнє значення нормалізованих зважених показників на вагові коефіцієнти інцидентів операційного ризику	X	0,18	0,09	0,05	0,02

В подальшому нам необхідно визначити середнє значення нормалізованих зважених показників, наведених в табл. 4.12, обумовленого тим, що розраховані

данні (перетин колонок 2-5 та рядків К1-К31 в табл. 4.12) не дають можливості зробити однозначний висновок щодо рівня операційного ризику банку.

Виходячи з цього, ми маємо змогу розрахувати бінарні показники, порівнявши значення нормалізованого показника, зваженого на характеристику впливу певного інциденту, з середнім рівнем нормалізованих зважених показників. Бінарна характеристика приймає значення «1», за умови перевищення кожного нормалізованого зваженого показника його гранично допустимого (середнього) рівня, і «0» - в протилежному випадку (див. табл. 4.13).

Таблиця 4.13

Бінарні характеристики за показниками кількісної оцінки ступеня операційного ризику для банку А

№ показника	Інциденти операційного ризику				Сума бінарних характеристик
	ризик, пов’язаний з діями працівників та безпекою робочого місця $j=1$	ризик систем і технологій $j=2$	ризик помилки у банківських процесах (ризик взаємовідносин) $j=3$	ризик пов’язаний з зовнішніми чинниками $j=4$	
І. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів					
К1	1	1	1	1	4
К2	1	1	1	1	4
…	…	…	…	…	…
К21	1	0	1	1	3
К22	1	0	1	1	3
ІІ. Операційний ризик, пов'язаний з власною діяльністю банку					
К23	0	0	0	0	0
К24	1	1	1	1	4
…	…	…	…	…	…
К30	0	0	0	0	0
К31	1	0	1	1	3
Разом	-	-	-	-	97

На основі даних табл. 4.13, ми можемо розрахувати суму бінарних характеристик в розрізі інцидентів операційного ризику в межах тридцяти одного показника, дасть нам змогу зробити попередній висновок про *загальний рівень операційного ризику комерційного банку. Це і буде експрес-оцінкою рівня операційного ризику комерційного банку. Так, згідно наших розрахунків рівень*

операційного ризику для банку А за експрес-оцінкою дорівнює 97 одиниць. Використовуючи наведену в табл. 4.14 градацію рівнів операційного ризику, можна зробити висновок, що *банк А має критичний рівню рівень операційного ризику*.

Таблиця 4.14

Класифікатор рівня операційного ризику комерційного банку

Кількісна оцінка		Рівень операційного ризику банку за експрес-оцінкою
Нижня межа	Верхня межа	
0	31	нормальний
32	62	допустимий
63	93	високий
94	124	критичний

Здійснена експрес-оцінка надає основу для проведення більш глибокого та детального аналізу операційного ризику банку А. Тому, на наш погляд, необхідно *дослідити причини формування такого рівня ризику, напрямків визначивши напрямки його негативного впливу на діяльність банку А та встановивши інцидент, який переважним чином його обумовлює*. Такий аналіз проводиться за допомогою Байєсівського підходу, який дозволяє визначити апостеріорну ймовірність виникнення операційного ризику як в цілому для банку(ів), так і в розрізі кожного з інцидентів.

З метою реалізації алгоритму визначення кількісної оцінки ступеня операційного ризику, необхідно представити результати реалізації експрес-оцінки (проведеної на попередньому етапі) у вигляді бінарних характеристик в межах кожного з чотирьох інцидентів (див. табл. 4.15, повна таблиця наведена в додатку А, таблиця А.26).

Таблиця 4.15

Бінарні характеристики показників кількісної оцінки ступеня операційного ризику банку А

Інцидент ризику	I. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів					II. Операційний ризик, пов'язаний з власною діяльністю банку					Сума
	К1	К2	…	К21	К22	К23	К24	…	К30	К31	
F1	1	1	…	1	1	0	1	…	0	1	25
F2	1	1	…	0	0	0	1	…	0	0	22
F3	1	1	…	1	1	0	1	…	0	1	25

F4	1	1	…	1	1	0	1	…	0	1	25

Використовуючи данні, наведені в табл. 4.15, можливо визначити ймовірності прийняття бінарними характеристиками значень «0» або «1» в розрізі j-го (j=1÷4) інциденту за такою формулою:

$$g_2 = \frac{\sum_i NKbin_{i2}}{n} = \frac{22}{31} = 0{,}71, \qquad b_2 = 1 - g_2 = 1 - 0{,}71 = 0{,}29 \tag{4.20}$$

Проведення аналогічного розрахунку в межах інших інцидентів операційного ризику (див. табл. 4.16) дає можливість провести подальші проміжні розрахунки, які *виступатимуть основою для визначення результативних характеристик*, що і слугуватимуть кількісною оцінкою операційного ризику.

Таблиця 4.16

Імовірності прийняття бінарними характеристиками значень «0» або «1» в розрізі від j-го (j=1÷4) інциденту для банку А

Інцидент ризику	b (імовірність прийняття бінарними характеристиками значення «0»)	g (імовірність прийняття бінарними характеристиками значення «1»)
1	0,19	0,81
2	0,29	0,71
3	0,19	0,81
4	0,19	0,81

Проміжні розрахунки щодо другого інциденту операційного ризику для банку А, будуть такими:

$$\lambda_2 = \ln\left(\frac{b_2(1-g_2)}{g_2(1-b_2)}\right) = \ln\left(\frac{0{,}29(1-0{,}71)}{0{,}71(1-0{,}29)}\right) = 0{,}89$$

$$\lambda_0 = \ln\left(\frac{p(H2j)}{p(H1j)}\right) + \sum_{i=1}^{n}\ln\left(\frac{1-b_{ij}}{1-g_{ij}}\right) = \ln\left(\frac{0{,}5}{0{,}5}\right) + \sum_{i=1}^{4}\ln\left(\frac{1-b_i}{1-g_i}\right) = -1{,}79 \tag{4.21}$$

$$L = \frac{\sum_{i=1}^{n}\lambda_2 NKbin_i}{n} = \frac{(-1{,}79)\times 1 + (-1{,}79)\times 1 + \ldots + (-1{,}79)\times 0 + (-1{,}79)\times 0}{31} = -1{,}27$$

Загальні результати визначення ймовірності виникнення кожного з чотирьох інцидентів операційного ризику для банку А приведені нижче в табл. 13 (повна таблиця наведена в додатку А, таблиця А.33).

Таблиця 4.17

Проміжні розрахунки для визначення ймовірності виникнення інциденту операційного ризику банку А

Інцидент ризику	ln(1-b)/(1-g)	λi	I. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів					II. Операційний ризик, пов'язаний з власною діяльністю банку					L (середнє значення масиву L1-L31)	p(s) ймовірність виникнення інциденту операційного ризику
			L1	L2	…	L21	L22	L23	L24	…	L30	L31		
F1	1,43	-2,85	-2,85	-2,85	…	-2,85	-2,85	0,0	-2,85	…	0	-2,85	-2,30	0,71
F2	0,89	-1,79	-1,79	-1,79	…	0,00	0,00	0,0	-1,79	…	0	0,00	-1,27	0,59
F3	1,43	-2,85	-2,85	-2,85	…	-2,85	-2,85	0,0	-2,85	…	0	-2,85	-2,30	0,71
F4	1,43	-2,85	-2,85	-2,85	…	-2,85	-2,85	0,0	-2,85	…	0	-2,85	-2,30	0,71

На основі даних рядка F2 табл. 13 можливо визначити ймовірність виникнення ризику систем і технологій для банку А за такою формулою:

$$p_K(H1_2) = \frac{1}{1+e^{\{\lambda_0+L\}}} = \frac{1}{1+e^{\{-1,79|-1,27\}}} = 0,59 \qquad (4.22)$$

Проведення аналогічних розрахунків щодо решти інцидентів (ризику, пов’язаного з діями працівників та безпекою робочого місця, ризику помилок у банківських процесах та ризику, пов'язаного з зовнішніми чинниками) дає можливість визначити ймовірності кожного з них. Відповідні розрахунки на основі даних табл. 14 (графа 1, рядки F1, F3, F4) свідчать про однаковий рівень ймовірності виникнення відповідних інцидентів операційного ризику, яка становить 0,71. Водночас, на основі отриманої кількісної характеристики складових операційного ризику банку, можна зробити висновок, що загальний рівень операційного ризику банку А є критичним (4 група ризику).

Разом з тим, результати наведених розрахунків не дають можливості однозначно стверджувати про рівнозначність впливу кожного з проаналізованих інцидентів на узагальнюючий показник операційного ризику. Даний недолік можна усунути шляхом визначення зваженої структури операційного ризику за інцидентами, яка відображатиме скореговані значення ймовірності виникнення даних інцидентів в залежності від ступіню їх впливу (вагові коефіцієнти стандартизованого рівняння регресії (формула 4.19)) на величину результативного показника.

Таблиця 4.18

Вхідна інформація для визначення ймовірності виникнення операційного ризику та проведення його структурного аналізу для банку А

Інцидент ризику	p(s) ймовірність виникнення інциденту операційного ризику	Група ризику	Бінарні показники	Структура операційного ризику за інцидентами	Зважена структура операційного ризику за інцидентами
А	1	2	3	4	5
F1	0,71	4	1	26,04	13,65
F2	0,59	2	0	21,87	35,12
F3	0,71	4	1	26,04	30,26
F4	0,71	4	1	26,04	20,97

Свідченням доцільності корегування структури операційного ризику за інцидентами виступають результати дослідження даного ризику на прикладі банку А. Так, отримавши однакові значення ймовірності виникнення першого, третього та четвертого інцидентів (F1, F3, F4) і відповідно їх питомої ваги – 26,04%, ми встановили, що зважена структура інцидентів операційного ризику банку А приймає інший вигляд. Найбільшу частину серед розглянутих трьох елементів займає ризик помилок у банківських процесах (ризик взаємовідносин), який відповідає рівню 30,26%. Сума двох інших інцидентів, а саме ризику, пов’язаного з діями працівників та безпекою робочого місця і ризику, пов’язаного з зовнішніми чинниками, складає 34,62%. Отже, комплексна дія даних двох складових на рівень операційного ризику банку А відповідає, з незначним відхиленням, впливу ризику взаємовідносин.

В той же час, ризик систем і технологій, приймаючи найменше значення ймовірності виникнення – 0,59 одиниць та питомої ваги – 21,87%, в кінцевому підсумку здійснює найбільший вплив на рівень операційного ризику банку А (зважена структура складає 35,12%). Дана тенденція пояснюється найбільшим ступенем впливу даного інциденту (виходячи з формули (4.19) ваговий коефіцієнт дорівнює 0,39 одиниць) на рівень результативного показника. Разом з тим, надаючи якісну характеристику ризику систем та технологій можна стверджувати про його підвищений рівень.

Останнім етапом реалізації математичної моделі оцінки операційного ризику при здійсненні регулювання та нагляду Національним банком України виступає визначення узагальнюючого показника кількісної оцінки ступеня операційного ризику – ймовірнісної оцінки на основі Байєсівського підходу. Так, на основі зазначених вище ймовірностей виникнення чотирьох інцидентів операційного ризику (табл. 4.19, рядок 1) та їх відповідності встановленому гранично допустимому інтервалу (табл. 15, рядок 2) проводиться перехід до бінарних характеристик (табл. 4.19, рядок 3), які виступають інформаційною базою розрахунку ймовірності виникнення операційного ризику для банку А.

Розглянемо послідовність визначення зазначеної числової характеристики (табл. 4.19, рядок 4) на прикладі банку А. Отже, *по-перше*, розраховується ймовірність прийняття бінарним показником в розрізі кожного з інцидентів операційного ризику значення «1» за такою формулою:

$$g_A = \frac{\sum_i NKbin_i}{n} = \frac{3}{4} = 0{,}75, \qquad (4.23)$$

По-друге, проводиться встановлення протилежної події – ймовірності прийняття бінарними характеристиками значення «0» за такою формулою:

$$b_A = 1 - g_A = 1 - 0{,}75 = 0{,}25 \qquad (4.24)$$

По-третє, безпосередньо здійснюється розрахунок імовірності виникнення операційного ризику (кількісної оцінки ступеня операційного ризику) $p_B(H1)$ за формулою (4.25):

$$p_B(H1) = \frac{1}{1+e^{\left\{\ln\frac{1-b_A}{1-g_A}+L\right\}}} = \frac{1}{1+e^{\left\{\ln\frac{1-0,25}{1-0,75}+\left|\frac{(-2,197)\times1+(-2,197)\times0+(-2,197)\times1+(-2,197)\times1}{4}\right|\right\}}} = 0,63 \qquad (4.25)$$

Таблиця 4.19

Показники алгоритму визначення кількісної оцінки ступеня операційного ризику для банку А

№	Показники	Інциденти операційного ризику			
		ризик, пов'язаний з діями працівників та безпекою робочого місця $j=1$	ризик систем і технологій $j=2$	ризик помилки у банківських процесах (ризик взаємовідносин) $j=3$	ризик пов'язаний з зовнішніми чинниками $j=4$
А	В	1	2	3	4
1	Ймовірність виникнення j-го інциденту операційного ризику	0,71	0,59	0,71	0,71
2	Гранично допустимий коридор імовірнісної (кількісної) оцінки операційного ризику за кожним j-м інцидентом (за сукупністю s банків)	$0,00 \le p_K(H1j) < 0,60$			
3	Бінарні показники за j інцидентами операційного ризику	1	0	1	1
4	Імовірність виникнення операційного ризику (кількісна оцінку ступеня операційного ризику)	0,63			

По-четверте, проводиться ідентифікація якісної оцінки рівня операційного ризику банку на основі визначеної кількісної оцінки його ступеня. Так, значенню $p_B(H1)$=0,63 одиниці відповідає високий рівень операційного ризику банку А.

Виходячи з того, що структура операційного ризику представлена в розрізі двох груп факторів:

- операційний ризик, пов'язаний з банківським обслуговуванням клієнтів;
- операційний ризик, пов'язаний з власною діяльністю банку.

Проте, також необхідно визначити обумовленість операційного ризику банку конкретними показниками даних груп. Інструментом реалізації вищенаведеного дослідження виступає факторний аналіз, послідовність проведення якого наведена в табл. 4.20.

Таблиця 4.20

Факторний аналіз структури операційного ризику (на прикладі банку А)

№	Показник	Фактори операційного ризику	
		1 група	2 група
	А	1	2
1	Сума бінарних характеристик відповідності показників інцидентам операційного ризику, од.	74,00	23,00
2	Частка кожної групи факторів операційного ризику (в розрізі бінарних характеристик, які приймають значення «1»), част. од.	0,76	0,24
3	Вагові коефіцієнти груп факторів, част. од.	0,71	0,29
4	Зважена частка на вагові коефіцієнти кожної групи факторів операційного ризику, част. од.	0,54	0,07
5	Питома вага впливу груп факторів на рівень операційного ризику, %	88,72	11,28

На основі дослідження структури кількісної оцінки операційного ризику, в межах формуючих її факторів на прикладі банку А, ми встановили, що для нього визначальною є група, яка обумовлює частину ризику, пов’язаного з банківським обслуговуванням клієнтів, про що свідчить значення її питомої на рівні 88,72%. В той же час, на 11,28% рівень операційного ризику банку А пояснюється впливом ризиків, пов’язаних з його власною діяльністю.

Аналогічно проведеним розрахункам експрес- та ймовірнісної оцінки операційного ризику банку А в цілому та структурного і факторного аналізу інцидентів його ризику нами була здійснюється комплексна оцінка операційного ризику решти трьох досліджуваних комерційних банків (див. табл. 4.21).

Таким чином, порівнюючи отримані результати розрахунку рівнів операційного ризику чотирьох комерційних банків, можна зробити висновок, що існують значні проблеми управління операційною діяльністю у банках А та Б, підтвердженням чого виступає їх кількісна характеристика операційного ризику на рівні 97 од. і 68 од. (експрес-оцінка) та 0,63 част. од. (імовірнісна оцінка) відповідно.

Таблиця 4.21

Комплексна оцінка операційного ризику чотирьох досліджуваних комерційних банків (таблиці, які відображують комплекс проміжних розрахунків в межах банків Б, В, Г, наведені в додатку А, таблиці А.37-А.45)

№	Показник		Банківська установа			
			А	Б	В	Г
А	Б		1	2	3	4
1	Експрес-оцінка (сума бінарних характеристик)	кількісна, од.	97	68	88	22
		якісна	критичний	високий	високий	нормальний
2	Вагові коефіцієнти інцидентів операційного ризику, част. од.	1 інцидент	0,13	0,34	0,27	0,08
		2 інцидент	0,39	0,01	0,44	0,34
		3 інцидент	0,28	0,10	0,03	0,16
		4 інцидент	0,20	0,56	0,26	0,41
3	Імовірність виникнення інциденту операційного ризику, част. од.	1 інцидент	0,71	0,50	0,59	0,14
		2 інцидент	0,59	0,54	0,53	0,10
		3 інцидент	0,71	0,50	0,71	0,10
		4 інцидент	0,71	0,41	0,59	0,10
4	**Імовірність виникнення операційного ризику (кількісна оцінку ступеня операційного ризику) част. од.**	**кількісна, част. од.**	**0,63**	**0,63**	**0,16**	**0,16**
		якісна	**високий**	**високий**	**нормальний**	**нормальний**
5	Зважена структура операційного ризику за інцидентами, %	1 інцидент	13,65	37,95	27,74	10,82
		2 інцидент	35,12	0,61	41,16	33,22
		3 інцидент	30,26	11,05	3,70	15,98
		4 інцидент	20,97	50,38	27,40	39,99
6	Питома вага впливу груп факторів на рівень операційного ризику, %	1 група факторів	88,72	80,79	83,97	77,93
		2 група факторів	11,28	19,21	16,03	22,07

На відміну від зазначених банків, банк Г характеризується нормальним рівнем операційного ризику, як за результатами експрес-оцінки (кількісний показник – 22

од.), так і в межах імовірнісної оцінки (кількісний показник – 0,16 част. од.) прослідковується в банку Г.

Неоднозначна тенденція властива для банку В, оскільки результати, отримані за результатами експрес- та ймовірнісної оцінки його операційного ризику є суперечливими. В ході аналізу за допомогою експрес-оцінки встановлено високий рівень операційного ризику (кількісний показник – 88 од.), на відміну від імовірнісної оцінки, яка свідчить про нормальний рівень операційного ризику (кількісний показник – 0,16 част. од.). На наш погляд, це може свідчити про наявність низки незначних проблем у банку, які, хоч і не несуть значної загрози втрат, втім які не слід ігнорувати.

Крім того, для всіх досліджуваних комерційних банків встановлено низку спільних закономірності:

- в розрізі кожного з банків можна виділити домінантний інцидент, який переважним чином обумовлює виникнення операційного ризику (варіація даного інциденту коливається в межах від 35% до 51%). Так, для банків А і В домінантний інцидент – це ризик систем і технологій, а для банків Б і Г - ризик, пов’язаний з зовнішніми чинниками;
- визначальним фактором операційного ризику для всіх чотирьох комерційних банків виступають ризики, пов’язані з банківським обслуговуванням клієнтів (питома вага впливу груп факторів складає від 78% до 89%).

Отже, проведена практична реалізація математичної моделі оцінки рівня операційного ризику банківських установ дозволяє сформувати аналітичні матеріали, які можуть слугувати основою діагностики рівнів операційного ризику та виступати основою для банків здійснення регулювання та нагляду Національним банком, зокрема в ході безвиїзного нагляду та при підготовці для інспекційних перевірок банків щодо їх організації управління операційним ризиком.

4.3 Математична модель операційного ризику для комерційного банку

Запропонована економіко-математична модель оцінки операційного ризику може бути практично застосована не тільки для дослідження даного виду ризику комерційних банків в рамках здійснення регулювання та нагляду Національним банком, але використовуватисьбезпосередньо банками з метою моніторингу власних операційних ризиків. Виходячи з цього, ми зробили спробу визначити показники, що є актуальними для характеристики операційного ризику банку «з середини» та здійснили розрахунки для на прикладі реальних даних банку А за період 2009 - 2010 рр.

Проводячи дане дослідження на прикладі статистичних даних діяльності банку А, ми виділили наступні етапи її реалізації. Так, вхідні дані, які необхідно визначити на першому етапі практичної реалізації математичної моделі операційного ризику, відображують значення показників функціонування банку А. Згрупувавши відповідні значення показників в розрізі:

- ризиків, пов’язаних з діями працівників та безпекою робочого місця;
- ризиків систем і технологій;
- ризиків помилок у банківських процесах (ризик взаємовідносин);
- ризиків, пов’язаних з зовнішніми чинниками;
- а також ризиків бізнес-середовища.

Дані були зібрані за місяць, квартал і в цілому за рік, що дало можливість знайти середнє значення досліджуваних коефіцієнтів за місяць (див. табл. 4.22). Отримані значення графи 4 табл. 1 виступають основою проведення подальших розрахунків.

Поряд з розрахованими вище кількісними характеристиками операційного ризику необхідно визначити, із яких інцидентів даного виду ризику складається кожен з виділених показників. Для наочного представлення структури показників операційного ризику пропонується використовувати бінарні коефіцієнти. Так, якщо відповідний інцидент характеризує розглянутий показник, бінарний коефіцієнт приймає значення «1», в протилежному випадку – «0». Результати практичної

реалізації даного етапу математичної моделі операційного ризику для комерційного банку А представимо в табл. 4.23.

Таблиця 4.22

Значення показників комерційного банку А в рамках оцінки операційного ризику

№	Показник	Значення показника			
		за місяць	за квартал	за рік	середнє значення за місяць (на основі даних в розрізі року)
А	Б	1	2	3	4
1. Ризик, пов'язаний з діями працівників та безпекою робочого місця					
К1	Несанкціоновані дії	25	50	105	8,75
К2	Крадіжки і шахрайства	36	200	1000	83,33
К3	Зловживання посадовим становищем	50	200	1000	83,33
К4	Відносини з працівниками та організація праці	50	200	1000	83,33
К5	Безпека робочого місця	1	3	8	0,67
К6	Помилки, які виникають при обслуговуванні клієнтів, виконанні робочих функцій	100	500	2500	208,33
К7	Невідповідна, (невдала) практика ведення бізнесу	10	30	100	8,33
К8	Неадекватна система рейтингової оцінки	25	100	500	41,67
К9	Помилки у документації	5	10	25	2,08
2. Ризик систем і технологій					
К10	Ризик систем	10	45	150	12,50
К11	Ризик технологій	3	8	30	2,50
3. Ризик помилки у банківських процесах (ризик взаємовідносин)					
К12	Впровадження даних до системи, виконання, розрахунок і обслуговування операцій	25	100	500	41,67
К13	Моніторинг операцій і звітність по проведеним операціям	2	5	15	1,25
К14	Відсутність (недостатність) системи внутрішнього контролю, помилки керівництва	20	75	300	25,00
К15	Порушення в управлінні рахунками клієнтів	15	45	200	16,67
4. Ризик, пов'язаний з зовнішніми чинниками					
К16	Природні катастрофи та інші випадки викликані зовнішніми чинниками	1	1	1	0,08

К17	Крадіжки і шахрайство (зовнішні)	5	10	25	2,08
К18	Безпека системи	10	35	50	4,17
Ризики бізнес-середовища					
К19	Політичний ризик	1	-	20	1,67
К20	Юридичний ризик	1	-	10	0,83
К21	Пруденційний ризик	2	-	36	3,00
К22	Стратегічний ризик	2	-	20	1,67
К23	Репутаційний ризик	5	-	80	6,67

Таблиця 4.23

Таблиця відповідності показників визначеним інцидентам операційного ризику банку А

№	Показник	Інцидент ризику (бінарна характеристика)			
		ризик, пов'язаний з діями працівників та безпекою робочого місця	ризик, пов'язаний з діями працівників та безпекою робочого місця	ризик, пов'язаний з діями працівникі в та безпекою робочого місця	ризик, пов'язаний з діями працівників та безпекою робочого місця
А	Б	1	2	3	4
К1	Несанкціоновані дії	1	0	0	0
К2	Крадіжки і шахрайства	1	1	1	1
К3	Зловживання посадовим становищем	1	0	0	0
К4	Відносини з працівниками та організація праці	1	0	1	0
К5	Безпека робочого місця	1	0	1	1
К6	Помилки, які виникають при обслуговуванні клієнтів, виконанні робочих функцій	1	1	1	0
К7	Невідповідна, (невдала) практика ведення бізнесу	1	0	1	0
К8	Неадекватна система рейтингової оцінки	1	0	1	1
К9	Помилки у документації	1	0	0	0
К10	Ризик систем	0	1	0	1
К11	Ризик технологій	0	1	0	0
К12	Впровадження даних до системи, виконання, розрахунок і обслуговування операцій	1	1	1	0
К13	Моніторинг операцій і звітність по проведеним операціям	1	1	0	0
К14	Відсутність (недостатність) системи внутрішнього контролю, помилки керівництва	1	0	1	0
К15	Порушення в управлінні рахунками клієнтів	1	1	1	1
К16	Природні катастрофи та інші випадки викликані зовнішніми чинниками	0	0	0	1
К17	Крадіжки і шахрайство (зовнішні)	0	0	0	1
К18	Безпека системи	0	1	0	1
К19	Політичний ризик	1	0	0	1
К20	Юридичний ризик	1	0	0	1

К21	Пруденційний ризик	1	0	1	1
К22	Стратегічний ризик	1	0	1	0
К23	Репутаційний ризик	1	0	1	1

Третім етапом послідовності впровадження математичної моделі виступає проведення регресійного аналізу. Сутність реалізації даного аналізу полягає у побудові рівняння лінійної множинної регресії залежності результативної ознаки від виділених факторних. В даному випадку результативною ознакою є нормалізовані значення показників операційного ризику комерційного банку А (значення, приведені у порівнюваний вигляд), а факторними, в свою чергу, виступають бінарні коефіцієнти відповідності показників визначеним інцидентам операційного ризику (див. табл. 4.24).

Таблиця 4.24

Зведена таблиця ознак кількісної оцінки операційного ризику комерційного банку А

№	Показник (нормалізоване значення) (результативна ознака)	Інцидент ризику (факторні ознаки)			
		j=1	*j=2*	*j=3*	*j=4*
А	Б	1	2	3	4
К1	2,86	1	0	0	0
К2	0,43	1	1	1	1
К3	0,60	1	0	0	0
К4	0,60	1	0	1	0
К5	1,50	1	0	1	1
К6	0,48	1	1	1	0
К7	1,20	1	0	1	0
К8	0,60	1	0	1	1
К9	2,40	1	0	0	0
К10	0,80	0	1	0	1
К11	1,20	0	1	0	0
К12	0,60	1	1	1	0
К13	1,60	1	1	0	0
К14	0,80	1	0	1	0
К15	0,90	1	1	1	1
К16	12,00	0	0	0	1
К17	2,40	0	0	0	1
К18	2,40	0	1	0	1
К19	0,60	1	0	0	1
К20	1,20	1	0	0	1
К21	0,67	1	0	1	1
К22	1,20	1	0	1	0
К23	0,75	1	0	1	1

Використовуючи дані, наведені в таблиці 4, запишемо отримане рівняння у вигляді формули 4.26:

$$K = 9{,}60 + 7{,}08F_1 + 13{,}17F_2 + 10{,}49F_3 - 14{,}62F_4 \qquad (4.26)$$

де K – абсолютне значення ідентифікатора операційного ризику;

$F_j, j = 1 \div 4$ – фіктивна змінна (приймає значення «1» або «0») характеристики j-го інциденту операційного ризику (див. графу 1 табл. 4.25).

Таблиця 4.25

Результати проведення регресійного аналізу встановлення ступеня впливу кожного інциденту на операційний ризик банку А

Інцидент ризику	Коефіцієнти	Стандартна похибка	t -статистика	Нижні 95%	Верхні 95%
А	1	2	3	4	5
Y-перетин	9,60	14,43	0,67	-20,72	39,91
Ризик, пов'язаний з діями працівників та безпекою робочого місця	7,08	14,88	0,48	-24,18	38,35
Ризик систем і технологій	13,17	10,20	1,29	-8,26	34,59
Ризик помилки у банківських процесах (ризик взаємовідносин)	10,49	11,22	0,94	-13,07	34,06
Ризик пов'язаний з зовнішніми чинниками	-14,62	9,76	-1,50	-35,12	5,88

Економічну сутність (з точки зору оцінки операційного ризику комерційного банку А) побудованого рівняння мають коефіцієнти перед змінними управління ($F_j, j = 1 \div 4$). Вони характеризують обумовленість загальної кількісної оцінки операційного ризику відповідними інцидентами. В той же час, недоліком розрахованих параметрів виступає неможливість визначити, яку частину з можливих 100% займає кожен з інцидентів. Вирішити дану проблему пропонується шляхом корегування побудованого рівняння лінійної множинної регресії і в результаті переходу до стандартизованого рівняння, що передбачає наступний етап реалізації математичної моделі операційного ризику. В свою чергу, розробка стандартизованого рівняння залежності загальної кількісної оцінки операційного

ризику від інцидентів пов'язана з проведенням ряду проміжних розрахунків, а саме – визначення середнього квадратичного відхилення показників (див. табл. 4.26).

Отже, стандартизоване рівняння приймає наступний вигляд (див. табл.4.27):

$$K = 0{,}13F_1 + 0{,}29F_2 + 0{,}24F_3 + 0{,}34F_4 \qquad (4.27)$$

Визначення коефіцієнтів даного рівняння, які мають найбільше значення в розрізі дослідження ризиків операційної діяльності комерційних банків, проводиться наступним чином (для прикладу розглянемо розрахунок першого параметру рівняння):

$$\alpha_1 = \beta_1 \frac{\sigma_{F_1}}{\sigma_K} = 7{,}08 \frac{0{,}41}{22{,}94} = 0{,}13 \qquad (4.28)$$

де σ_{F_1}, σ_K – середньоквадратичні відхилення факторних і результативної ознак, відповідно.

Таблиця 4.26

Проміжні розрахунки для визначення структури змін інцидентів операційного ризику банку А

№	Середнє квадратичне відхилення показників	Середнє квадратичне відхилення			
		F_1	F_2	F_3	F_4
А	1	2	3	4	5
К1	55.28	0.05	0.12	0.27	0.27
К2	339.84	0.05	0.43	0.23	0.23
К3	1052.02	0.05	0.12	0.27	0.27
К4	1052.02	0.05	0.12	0.23	0.27
К5	274.41	0.05	0.12	0.23	0.23
К6	6795.49	0.05	0.43	0.23	0.27
К7	57.23	0.05	0.12	0.23	0.27
К8	55.28	0.05	0.12	0.23	0.23
К9	157.88	0.05	0.12	0.27	0.27
К10	57.23	0.61	0.43	0.27	0.23
К11	212.15	0.61	0.43	0.27	0.27
К12	55.28	0.05	0.43	0.23	0.27
К13	242.28	0.05	0.43	0.27	0.27
К14	5.93	0.05	0.12	0.23	0.27
К15	6.58	0.05	0.43	0.23	0.23
К16	274.41	0.61	0.12	0.27	0.23
К17	157.88	0.61	0.12	0.27	0.23
К18	57.23	0.61	0.43	0.27	0.23
К19	274.41	0.05	0.12	0.27	0.23
К20	274.41	0.05	0.12	0.27	0.23
К21	242.28	0.05	0.12	0.23	0.23

К22	242.28	0.05	0.12	0.23	0.27
К23	157.88	0.05	0.12	0.23	0.23
Загальний рівень	22.94	0.41	0.48	0.50	0.50

Результати проведених розрахунків за всіма параметрами рівняння (2) наведемо у графі 1 таблиці 4.27. На основі аналізу отриманих даних зазначимо, що коефіцієнти стандартизованого рівняння приймають як додатні, так і від'ємні значення. З метою надання даним параметрам економічної інтерпретації необхідно на їх основі розрахувати скореговані коефіцієнти (для прикладу розглянемо розрахунок четвертого параметру рівняння):

$$\alpha_4^* = \frac{\alpha_4}{\sum_{m=1}^{4} \alpha_m} = \frac{|-0{,}32|}{0{,}13 + 0{,}27 + 0{,}23 + |-0{,}32|} = 0{,}34. \qquad (4.29)$$

Таблиця 4.27

Встановлення ступеня впливу кожного інциденту на операційний ризик банку А (коефіцієнтів стандартизованого рівняння лінійної множинної регресії)

Інцидент операційного ризику	Коефіцієнти стандартизованого рівняння лінійної множинної регресії	Абсолютні коефіцієнти стандартизованого рівняння лінійної множинної регресії (взяті по модулю)	Скореговані коефіцієнти стандартизованого рівняння лінійної множинної регресії (вагові коефіцієнти інцидентів операційного ризику)
А	1	2	3
F1 ризик, пов'язаний з діями працівників та безпекою робочого місця	0,13	0,13	0,13
F2 ризик систем і технологій	0,27	0,27	0,29
F3 ризик помилки у банківських процесах (ризик взаємовідносин)	0,23	0,23	0,24
F4 ризик, пов'язаний з зовнішніми чинниками	-0,32	0,32	0,34

Проводячи дослідження ступеня впливу кожного інциденту на операційний ризик банку А на основі графи 3 таблиці 4.27 та рівняння (4.27), необхідно зазначити, що досягнутий рівень операційного ризику найбільшим чином обумовлений чинниками зовнішнього середовища, оскільки зміна загального

критерію операційного ризику даного банку на 34% зі 100% можливих. Практично аналогічний вплив (на рівні 29%) на ризиковість операційної діяльності банку А здійснює ризик систем і технологій. В свою чергу, найменше значення в структурі досліджуваного показника мають дві останні групи факторів впливу: ризик, пов'язаний з діями працівників і безпекою робочого місця, та ризик помилки у банківських процесах, які в сукупності складають 37% забезпечення негативних наслідків настання операційного ризику.

Наступним етапом практичної реалізації математичної моделі операційного ризику для комерційного банку А виступає визначення структури операційного ризику в залежності від формуючих його інцидентів. Для цього проводиться розподіл відповідного значення нормалізованого показника оцінки операційного ризику на формуючі його інциденти шляхом зважування даних графи 1 таблиці 7 на вагові коефіцієнти даних інцидентів. З метою отримання можливості економічної інтерпретації визначеної структури операційного ризику результати даного етапу представимо у графах 2 - 5 таблиці 4.28.

Таблиця 4.28

Відображення структури операційного ризику в залежності від формуючих їх інцидентів банку А

№ показника	Значення нормалізованого показника	Інциденти операційного ризику			
		ризик, пов'язаний з діями працівників та безпекою робочого місця $j=1$	ризик систем і технологій $j=2$	ризик помилки у банківських процесах (ризик взаємовідносин) $j=3$	ризик пов'язаний з зовнішніми чинниками $j=4$
		Вагові коефіцієнти інцидентів операційного ризику			
		0,13	0,29	0,24	0,34
А	1	2	3	4	5
К1	25,00	3,36	7,21	6,03	8,40
К2	36,00	4,84	10,39	8,68	12,10
К3	50,00	6,72	14,42	12,06	16,80
К4	50,00	6,72	14,42	12,06	16,80
К5	1,00	0,13	0,29	0,24	0,34
К6	100,00	13,44	28,85	24,11	33,60
К7	10,00	1,34	2,88	2,41	3,36
К8	25,00	3,36	7,21	6,03	8,40
К9	5,00	0,67	1,44	1,21	1,68

K10	10,00	1,34	2,88	2,41	3,36
K11	3,00	0,40	0,87	0,72	1,01
K12	25,00	3,36	7,21	6,03	8,40
K13	2,00	0,27	0,58	0,48	0,67
K14	20,00	2,69	5,77	4,82	6,72
K15	15,00	2,02	4,33	3,62	5,04
K16	1,00	0,13	0,29	0,24	0,34
K17	5,00	0,67	1,44	1,21	1,68
K18	10,00	1,34	2,88	2,41	3,36
K19	1,00	0,13	0,29	0,24	0,34
K20	1,00	0,13	0,29	0,24	0,34

Продовження табл. 4.28

А	1	2	3	4	5
К21	2,00	0,27	0,58	0,48	0,67
К22	2,00	0,27	0,58	0,48	0,67
К23	5,00	0,67	1,44	1,21	1,68
Середнє значення нормалізованих зважених показників на вагові коефіцієнти інцидентів операційного ризику	X	0,32	1,46	1,02	1,98

Аналізуючи вплив інцидентів операційного ризику на його загальний кількісний критерій в розрізі статистичних даних банку А необхідно зазначити, що описане вище дослідження надає можливість провести лише опосередкований аналіз структури даного виду ризику, не дозволяючи отримати якісну характеристику. Подолання даного недоліку проводиться шляхом порівняння отриманих результатів в межах кожного інциденту операційного ризику з середніми (прийнятими за нормативні) значеннями, наведеними в останньому рядку таблиці 4.28. Так, у випадку перевищення відповідної складової нормалізованого значення показника гранично допустимого рівня бінарний коефіцієнт, які характеризує результати даного порівняння, приймає значення «1». Інтерпретацією даного співвідношення виступає наявність підстав стверджувати, що виникнення значного рівня операційного ризику відбувається за рахунок відповідного напрямку діяльності комерційного банку. В іншому випадку бінарний коефіцієнт приймає значення «0», що свідчить про відсутність підстав для необхідності корегування відповідного напрямку діяльності банку (див. табл. 4.29).

Таким чином, використовуючи дані графи 5 табл. 4.29 отримаємо суму бінарних характеристик як в розрізі кожного окремого показника кількісної оцінки операційного ризику, так і в межах банківської установи в цілому. Проводячи даний аналіз на основі даних банку А, необхідно сказати, що загальна сума бінарних коефіцієнтів знаходиться на рівні 55 одиниць. Економічна сутність отриманої

величини полягає в наданні експрес-оцінки досягнутого рівня операційного ризику. Крім того, додатково до визначення кількісної оцінки набуває актуальності проведення якісного аналізу операційної діяльності комерційного банку А.

Таблиця 4.29

Бінарні характеристики за показниками кількісної оцінки ступеня операційного ризику банку А

№ показника	Інциденти операційного ризику				Сума бінарних характеристик
	ризик, пов'язаний з діями працівників та безпекою робочого місця $j=1$	ризик, пов'язаний з діями працівників та безпекою робочого місця $j=1$	ризик, пов'язаний з діями працівників та безпекою робочого місця $j=1$	ризик, пов'язаний з діями працівників та безпекою робочого місця $j=1$	
А	1	2	3	4	5
К1	1	1	1	1	4
К2	1	1	1	1	4
К3	1	1	1	1	4
К4	1	1	1	1	4
К5	0	0	0	0	0
К6	1	1	1	1	4
К7	1	1	1	1	4
К8	1	1	1	1	4
К9	1	0	1	0	2
К10	1	1	1	1	4
К11	1	0	0	0	1
К12	1	1	1	1	4
К13	0	0	0	0	0
К14	1	1	1	1	4
К15	1	1	1	1	4
К16	0	0	0	0	0
К17	1	0	1	0	2
К18	1	1	1	1	4
К19	0	0	0	0	0
К20	0	0	0	0	0
К21	0	0	0	0	0
К22	0	0	0	0	0
К23	1	0	1	0	2
Разом	-	-	-	-	55

Використовуючи градацію рівнів операційного ризику, наведену в табл. 4.30, можна зробити висновок про високий рівень даного показника. Це свідчить про

наявність проблемних складових в процесі функціонування банківської установи і, відповідно, призводить до необхідності її поточного корегування.

Таблиця 4.30

Класифікатор рівня операційного ризику комерційного банку А

Кількісна оцінка		Якісна характеристика
Нижня межа	Верхня межа	
0	23	нормальний
24	46	допустимий
47	70	високий
71	92	критичний

З метою подальшого проведення структурного аналізу операційної діяльності банку А проведемо розрахунок імовірності досягнення відповідного рівня даного виду ризику за умови отримання інформації, що характеризує рівень операційного ризику в розрізі інцидентів, представленої в табл. 4.31.

Таблиця 4.31

Бінарні характеристики показників кількісної оцінки ступеня операційного ризику банку А

Інцидент ризику	1. Ризик, пов'язаний з діями працівників та безпекою робочого місця									2.Ризик систем і технологій	
	К1	К2	К3	К4	К5	К6	К7	К8	К9	К10	К11
F1	1	1	1	1	0	1	1	1	1	1	1
F2	1	1	1	1	0	1	1	1	0	1	0
F3	1	1	1	1	0	1	1	1	1	1	0
F4	1	1	1	1	0	1	1	1	0	1	0

Таблиця 4.31.1

Бінарні характеристики показників кількісної оцінки ступеня операційного ризику банку А

Інцидент ризику	3. Ризик помилки у банківських процесах (ризик взаємовідносин)				4. Ризик пов'язаний з зовнішніми чинниками			Ризики бізнес-середовища					Сума
	К12	К13	К14	К15	К16	К17	К18	К19	К20	К21	К22	К23	
F1	1	0	1	1	0	1	1	0	0	0	0	1	16
F2	1	0	1	1	0	0	1	0	0	0	0	0	12
F3	1	0	1	1	0	1	1	0	0	0	0	1	15
F4	1	0	1	1	0	0	1	0	0	0	0	0	12

Використання імовірнісного (Баєсівського) підходу для надання кількісної характеристики забезпечення рівня операційного ризику банку А відповідними інцидентами передбачає проведення наступних проміжних розрахунків:

- імовірності виникнення проблемних напрямків діяльності (бінарний коефіцієнт приймає значення 1 (див. табл. 4.32, графа 1)) і, як наслідок ($g = 1 - b$), виконання банком А встановлених гранично допустимих величин показників (див. табл. 4.32, графа 2);

Таблиця 4.32

Імовірності прийняття бінарними характеристиками значень «0» або «1» в розрізі від j-го (j=1÷4) інциденту для банку А

Інцидент ризику	b (імовірність прийняття бінарними характеристиками значення «0»)	g (імовірність прийняття бінарними характеристиками значення «1»)
А	1	2
1	0,30	0,70
2	0,48	0,52
3	0,35	0,65
4	0,48	0,52

- зважених бінарних показників величини операційного ризику на значення корегуючого коефіцієнта λ, а також їх середнього значення L (див. табл. 4.33).

Таблиця 4.33

Проміжні розрахунки для визначення імовірності виникнення інциденту операційного ризику банку А

Інцидент ризику	ln(1-b)/(1-g)	λi	1. Ризик, пов'язаний з діями працівників та безпекою робочого місця									2.Ризик систем і технологій	
			К1	К2	К3	К4	К5	К6	К7	К8	К9	К10	К11
F1	0,83	-1,65	-1,65	-1,65	-1,65	-1,65	0,00	-1,65	-1,65	-1,65	-1,65	-1,65	-1,65
F2	0,09	-0,17	-0,17	-0,17	-0,17	-0,17	0,00	-0,17	-0,17	-0,17	0,00	-0,17	0,00
F3	0,63	-1,26	-1,26	-1,26	-1,26	-1,26	0,00	-1,26	-1,26	-1,26	-1,26	-1,26	0,00
F4	0,09	-0,17	-0,17	-0,17	-0,17	-0,17	0,00	-0,17	-0,17	-0,17	0,00	-0,17	0,00

Таблиця 4.33.1

Проміжні розрахунки для визначення імовірності виникнення інциденту операційного ризику банку А

Інцидент ризику	3. Ризик помилки у банківських процесах (ризик взаємовідносин)				4. Ризик пов'язаний з зовнішніми чинниками			Ризики бізнес-середовища					L (середнє значення масиву L1-L31)	p(s) імовірність виникнення інциденту операційного ризику
	K12	K13	K14	K15	K16	K17	K18	K19	K20	K21	K22	K23		
F1	-1,65	0,00	-1,65	-1,65	0,00	-1,65	-1,65	0	0	0	0	-1,65	-1,15	0,58
F2	-0,17	0,00	-0,17	-0,17	0,00	0,00	-0,17	0	0	0	0	0,00	-0,09	0,50
F3	-1,26	0,00	-1,26	-1,26	0,00	-1,26	-1,26	0	0	0	0	-1,26	-0,82	0,55
F4	-0,17	0,00	-0,17	-0,17	0,00	0,00	-0,17	0	0	0	0	0,00	-0,09	0,50

Використовуючи проведені вище розрахунки, постає можливість визначення результативної характеристики кількісної оцінки кожного інциденту операційного ризику – імовірності його виникнення p(s) (графа 1 табл. 4.34). Так, за даними банку А перший та третій інциденти операційного ризику мають найбільшу імовірність настання, а отже їм відповідає 4-та група ризику (див. табл. 4.34, графа 2), і відповідно можна зробити висновок, що ризик, пов'язаний з діями працівників та безпекою робочого місця і ризик помилки у банківських процесах (ризик взаємовідносин) здійснюють найбільший вплив на стійкість функціонування даної банківської установи. На відміну від описаних інцидентів менш впливовими вступають інциденти другої та четвертої груп, оскільки імовірність настання ризику систем і технологій та ризику пов'язаного з зовнішніми чинниками складають відповідно по 0,5 частки одиниці.

Визначення загального рівня операційного ризику банку А базується на знаходженні бінарних показників (див. табл. 4.34, графа 3).

Практичні аспекти реалізації загального алгоритму визначення ступеня оцінки операційного ризику на основі попередньо проведеного аналізу рівня даного ризику в розрізі відповідних інцидентів наведені в табл. 4.35. Так, перший рядок табл. 4.35, який містить результати першого етапу математичної моделі операційного ризику, відображує імовірнісну оцінку виникнення кожного конкретного інциденту.

Таблиця 4.34

Данні для визначення імовірності виникнення операційного ризику та проведення його структурного аналізу банку А

Інцидент ризику	p(s) імовірність виникнення інциденту операційного ризику	Група ризику	Бінарні показники
A	1	2	3
F1	0,58	4	1
F2	0,50	2	0
F3	0,55	4	1
F4	0,50	2	0

На другому етапі методики проводиться перехід від отриманих даних (рядок 1, табл. 4.35) до бінарних характеристик наявності проблемних аспектів в діяльності банку на основі нерівності (рядок 2 табл. 4.35), де розкриваються межі гранично допустимого інтервалу показників операційного ризику (рядок 3 табл. 4.35).

Наступним етапом послідовності розрахунків виступає визначення загального рівня кількісної оцінки операційного ризику на основі застосування Баєсівського підходу (рядок 4 табл. 4.35). Аналізуючи результати розрахунків рівня операційного ризику банку А зазначимо, що ймовірність реалізації даного виду ризику складає 0,5 частки од., характеризуючи високий рівень.

Завершальним етапом реалізації методики кількісної оцінки операційного ризику виступає якісна характеристика отриманого на попередньому етапі показника. Так, з метою подолання негативних наслідків впливу операційних ризиків банку А, в першу чергу, необхідно звернути увагу на ризик, пов’язаний з зовнішніми чинниками, оскільки в зваженій структурі операційного ризику даний інцидент займає найбільшу питому вагу – 32,19%. В свою чергу, найменший вплив (14,91%) на діяльність банку А здійснює ризик, пов’язаний з діями працівників та безпекою робочого місця, не дивлячись на те, що даному інциденту відповідає найбільша імовірність виникнення.

Питома вага ризику систем і технологій та ризику помилки у банківських процесах (ризик взаємовідносин) знаходиться в межах від 25% до 28%, що свідчить про відносно помірний рівень впливу даних інцидентів на кількісну характеристику операційного ризику. Результати вищенаведеного аналізу наведені в табл. 4.36.

Таблиця 4.35

Показники алгоритму визначення кількісної оцінки ступеня операційного ризику банку А

№	Показники	Інциденти операційного ризику			
		ризик, пов'язаний з діями працівників та безпекою робочого місця $j=1$	ризик систем і технологій $j=2$	ризик помилки у банківських процесах (ризик взаємовідносин) $j=3$	ризик пов'язаний з зовнішніми чинниками $j=4$
А	В	1	2	3	4
1	Імовірність виникнення j-го інциденту операційного ризику	0,58	0,50	0,55	0,50
2	Гранично допустимий коридор імовірнісної (кількісної) оцінки операційного ризику за кожним j-м інцидентом (за сукупністю s банків)	$0{,}00 \le p_K(H1j) < 0{,}53$			
3	Бінарні показники за j інцидентами операційного ризику	1	0	1	0
4	Імовірність виникнення операційного ризику (кількісна оцінку ступеня операційного ризику)	0,5			

Таблиця 4.36

Данні для визначення імовірності виникнення операційного ризику та проведення його структурного аналізу для банку А

Інцидент ризику	p(s) імовірність виникнення інциденту операційного ризику	Структура операційного ризику за інцидентами	Зважена структура операційного ризику за інцидентами
А	1	4	5
F1	0,58	27,24	14,91
F2	0,50	23,52	27,64
F3	0,55	25,72	25,26
F4	0,50	23,52	32,19

Таким чином, підводячи підсумок проведеній практичній реалізації математичної моделі операційного ризику на прикладі даних банку А зазначимо, що дана банківська установа має високий рівень операційногоу ризику. Виявлена тенденція, в своїй більшості, пояснюється впливом зовнішнього середовища та наслідків збоїв існуючих систем і технологій.

V. ПРОГРАМНІ ЗАСОБИ ТА БАЗИ ДАНИХ: НЕВІДЄМНА СКЛАДОВА СУЧАСНОГО РИЗИК-МЕНЕДЖМЕНТУ КОМЕРЦІЙНОГО БАНКУ

5.1 Методи штучного інтелекту при оцінці ризиків

Зростання рівнів різноматнітних дуже чамто зумовлено необхідністю ухвалювати рішення за таких умов: неточність, двозначність, невизначеність, нечіткість і необґрунтованість інформації. Необхідність підвищення швидкості і адекватності даного процесу вимагає залучення програмних засобів, які здатні сприяти його здійсненню. Програмні засоби, в основу роботи яких покладена виключно класична логіка – тобто алгоритми рішення відомих задач, не в змозі надавати об'єктивні рекомендації для прийняття рішень в невизначених ситуаціях. Якісне рішення цих задач під силу лише програмним системам, які здатні функціонувати подібно до людського інтелекту, а саме: мати здатність здобувати, адаптувати, модифікувати і поповнювати знання з метою вирішення задач, формалізація яких ускладнена. Такі системи відносяться до категорії штучного інтелекту, що здатні в залежності від поточної ситуації самі розробляти алгоритми рішення новоутворених проблем.

З моменту визнання штучного інтелекту одним із напрямків наукових досліджень (50-і роки XX століття) до наших часів у полі зору розробників інтелектуальних систем знаходились завдання різноманітного спрямування. Поміж ними реальних технологічних успіхів було досягнуто в процесі вирішення таких класів задач: доведення теорем, розпізнавання образів, машинного перекладу, ігрових програм, машинної творчості, експертних систем тощо. Найпоширініше практичне застосування технології штучного інтелекту знайшли у вигляді експертних системи, комерційне впровадження яких почалося з початку 80-х років минулого сторіччя. З того часу експертні системи в значній мірі використовуються в бізнесі, науці, техніці, на виробництві.

За визначенням експертна система – це програмна система, яка оперує зі знаннями в певній предметній області з метою розробки рекомендацій для вирішення проблем. Отже, ключова відмінність методології розробки експертних

систем від програмних систем, які мають алгоритмічну основу, полягає у відокремленні поняття даних від поняття знань. Цю відмінність наглядно ілюструє аналогія з класичним виразом, який оприлюднив Д.Кнут у своїй роботі, присвяченій програмуванню алгоритмічних задач [28]**:**

Програма = Структура даних + Алгоритми.

Стосовно експертних систем цей вираз виглядає таким чином:

Експерта система = Знання + Логічний висновок.

Експертна система, що побудована за таким принципом, може узяти на себе функції, виконання яких вимагає залучення досвіду фахівця, або виконувати роль асистента для особи, що приймає рішення. В будь-якому випадку людина – фахівець певної предметної області, має нагоду отримати результати вищої якості за умови співпраці з експертною системою.

У попередньому розділі ми представили вашій увазі математичну модель визначення рівнів операційного ризику комерційного банку. Моделювання ґрунтується на використанні байєсівського підходу і зводиться до розрахунку імовірності відхилення реальних результатів бізнесу від очікуваних, внаслідок низки порушень та інших чинників. Відхилення результатів відбувається внаслідок існування причинних факторів неявного характеру. Використання теореми Байєса спрямовує рішення зазначеної задачи до визначення вірогідності існування факторів операційного ризику, за наявності відбувшихся подій негативного характеру – інцидентів операційного ризику.

Такий підхід до прогнозування повторення інцидентів операційного ризику має певний проблемний момент. Він пов’язаний з відсутністю однозначної методи встановлення причинно-наслідкового зв’язків між факторами та інцидентами операційного ризику. Способи розрахунку показників оцінки операційного ризику ґрунтуються на суб’єктивних рішеннях експертів стосовно існування цих зв’язків. Оскільки своєчасне впровадження новітніх продуктів у сферу банківського бізнесу в наші часи прийнято вважати запорукою успіху, комплекс показників ризикового аналізу повинен зазнавати постійних змін. Здійснення таких змін вимагає залучення дедалі більших обсягів знань різних за фахом експертів. Зважаючи на наведену

формалізацію призначення експертних систем, неважко дійти висновку стосовно доречності їхнього використання в ролі акумулятора таких знань.

Експертні системи накопичують знання завдяки інженерії знань. Інженерія знань представляє собою процес отримання знань від експертів з метою подальшого представлення знань в експертній системі. Класичний варіант інженерії знань ґрунтується на обширних інтерв'ю з експертами. На початку цього процесу інженер по знаннях встановлює діалог з експертом, щоб виявити його знання. Потім інженер по знаннях представляє знання в явному вигляді для внесення в базу знань. Після цього експерт проводить оцінку експертної системи і передає критичні зауваження інженеру по знаннях. Такий процес повторюється до тих пір, доки експерт не оцінить результати роботи системи як прийнятні.

Найбільш поширеним методом накопичення знань в експертних системах ґрунтується на використанні системи продукційних правил. Продукційними називаються правила, що організовані у вигляді IF-THEN структур. Частина продукційного правила, що розмішена між ключовими словами IF і THEN носить назву – антецедент або ліва частина (LHS – left-hand-side) правила. На практиці застосовуються також назви: умовний елемент та шаблон. Після слова THEN заноситься список дій, які повинні бути виконані відповідно до правила. Ця частина продукційного правила носить назву – консеквент, або права частина (RHS – Right-Hand Side) правила.

Продукційні правила сумісно з інтерпретатором, який управляє їх активізацією залежно від наявності фактів, складають продукційну модель представлення і використовування знань в експертних систем. Такі системи носять назву продукційних. У продукційних системах знання, що представлені у формі множини правил, визначають висновки, які повинні бути зроблені (або не зроблені) у певних ситуаціях.

Застосовуючи методу продукційних правил, з’являється нагода перекласти інтелектуальний тягар з накопичення знань для оцінки операційного ризику банку на спеціалізовану експертну систему. В якості прикладу розглянемо організацію знань стосовно ідентифікації існування факторів операційного ризику на основі

даних з форм статистичної звітності Національного банку. Зокрема, за допомогою звіту про застосування до банків заходів впливу (форма №682) можна сформувати знання стосовно підвищення ймовірності існування факторів операційного ризику в залежності від виду порушень. В продукційній системі ці правила можуть виглядати наступним чином:

IF *порушення нормативів ліквідності* THEN *зловживання посадовим становищем для отримання власної вигоди;*

IF *порушення максимального розміру кредитів, гарантій та поручительств* THEN *невірна оцінка кредитоспроможності клієнта;*

IF *несвоєчасне подання, приховування або перекручення встановленої НБУ звітності про валютні операції* THEN *невиконання своїх безпосередніх обов'язків з метою спрощення роботи;*

IF *недотримання лімітів відкритої валютної позиції* THEN *помилки виконання, розрахунку і обслуговування операцій;*

IF *Порушення банками касової дисципліни* THEN *несанкціоноване надання інформації та консультування клієнта співробітниками;*

IF *Порушення порядку, строків і технології виконання банківських операцій, що встановлені нормативно-правовими актами Національного банку* THEN *збої в роботі комп'ютерного обладнання.*

Метод представлення знань з використанням продукційних правил дозволяє фахівцям з управління операційним ризиком отримати цілком відчутні переваги. По-перше, завдяки такій організації спрощується як представлення знань, так і процес розширення експертної системи по методу розробки крок за кроком. По-друге, такі експертні системи дозволяють легко створювати засоби пояснення за допомогою правил. Засіб пояснення дозволяє стежити за тим, активізація яких правил була застосована, що дає змогу відновити хід міркувань, які привели до певного висновку. По-третє, ця метода має суттєві аналогії з пізнавальним процесом людини. Згідно з результатами досліджень, одержаним Ньюеллом і Саймоном [29], правила є найбільш природним способом моделювання процесу вирішення задач людиною. Крім того, в процесі формалізації знань, якими володіють експерти, їм

досить нескладно пояснити структуру представлення знань на основі достатньо простої схеми правил IF-THEN.

Загальну структуру експертної системи заснованої на правилах можна зобразити у вигляді рис. 5.1.

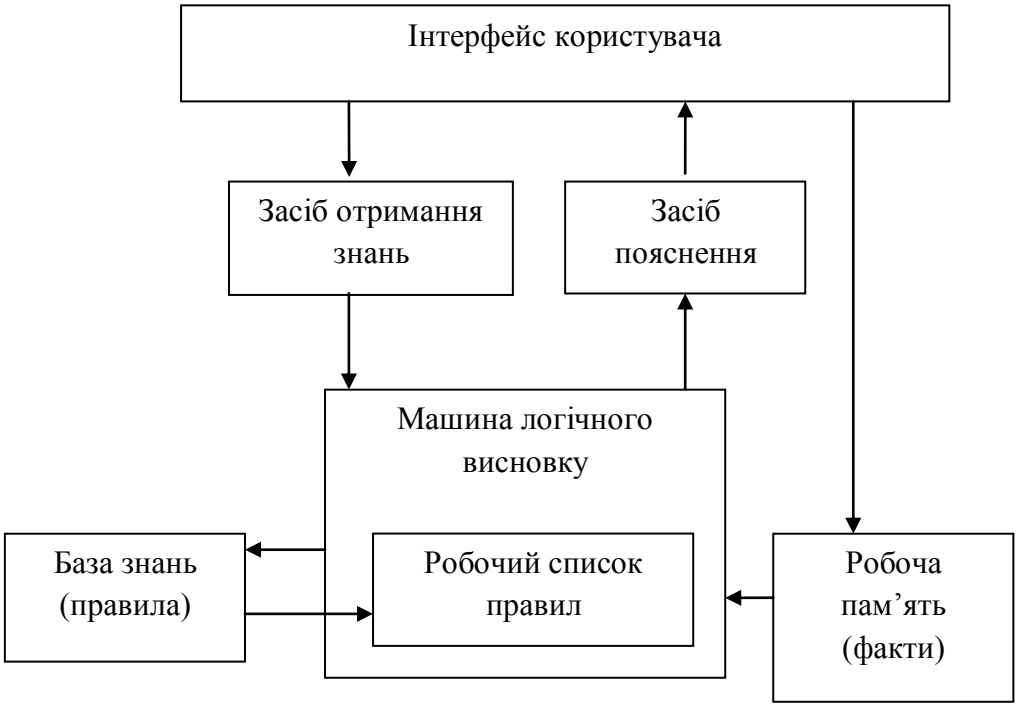


Рис.5.1. Загальна структура експертної системи

Приведена структура наглядно ілюструє основні аспекти реалізації експертних систем, тому розглянемо детально сутність та призначення її компонентів.

Інтерфейс користувача – це механізм, за допомогою якого відбувається спілкування користувача з експертною системою. Залежно від призначення системи інтерфейс користувача може використовувати простий текстовий дисплей або складний растровий дисплей з високою розподільною здатністю. Останні зазвичай застосовуються для задач моделювання, які вирішує експертна система.

Засіб отримання знань являє собою автоматизований спосіб, який дозволяє користувачу вводити знання в систему, не застосовуючи явного кодування знань за допомогою інженера по знаннях. Цей інструментальний засіб в деяких експертних системах здатний навчатися, здійснюючи автоматичне формування правил на підставі прикладів. Для формування правил в машинному навчанні застосовуються

такі методи і алгоритми, як ID3, C4.5, C5.1, штучні генетичні алгоритми і нейронні мережі.

База знань системи вміщує знання, необхідні для вирішення задач в певній проблемній області, в нашому випадку – управлінні операційним ризиком. Базу знань експертної системи, в якій знання закодовані у формі правил, називають продукційною пам’яттю. До складу дій консеквентів правил зазвичай входить додавання або видалення фактів з робочої пам'яті або досягнення результатів. Формат опису цих дій залежить від синтаксису мови програмування експертної системи.

Машина логічного висновку є програмним компонентом, який визначає, які антецеденти правил (якщо такі існують) виконуються згідно фактам. Для цього машина логічного висновку виконує наступні дії:

- ухвалює рішення про те, яким правилам відповідають факти;
- розподіляє по пріоритетам правила, обрані до виконання;
- виконує правило з найвищим пріоритетом.

В якості класичних стратегій рішення задач в експертних системах використовуються два загальні методи логічного висновку: прямий логічний висновок і зворотний логічний висновок. Загальною стратегією вирішення задач, є розбиття їх на фрагменти, які можна легше доводити. При цьому системи з прямим логічним висновком управляються даними або фактами. Вони починають свою роботу з відомих початкових фактів і продовжують роботу, використовуючи правила для формування нових висновків або виконання певних дій.

Системи із зворотним логічним висновком управляються цілями або гіпотезами. Вони починають свою роботу з деякої гіпотези, або мети, яку користувач намагається довести, і продовжують роботу, відшукуючи правила, які дозволять довести істинність гіпотези. До інших методів, що використовуються для виконання конкретизованих завдань, можуть входити: аналіз цілей і засобів, спрощення задачі, перебір з поверненнями, метод «запланувати-виробити-перевірити», ієрархічне планування тощо.

Робоча пам'ять системи призначена для розміщення фактів, що стосуються поточного стану об'єкту досліджень. Факти, що знаходяться в робочій пам'яті, не взаємодіють один з одним, на відміну від правил, що зберігаються в базі знань. Якщо в робочій пам'яті є факт, який відповідає умовній частині правила, машина логічного висновку розміщує це правило в робочому списку правил. У випадку, якщо правило має декілька шаблонів, то для того, щоб правило можна було розмістити в робочому списку правил, всі ці шаблони повинні бути розпізнані як відповідні. В якості умови відповідності деяких шаблонів можна вказати відсутність певних фактів в робочій пам'яті. Машина логічного висновку працює в режимі здійснення циклів «розпізнавання-дія».

Робочий список правил являє собою список правил, створений машиною логічного висновку та розташований по пріоритетах, шаблони яких відповідають фактам, що знаходяться в робочій пам'яті. Правило, всі шаблони якого розпізнані як відповідні, називається активізованим, або реалізованим. У робочому списку правил може бути одночасно присутнім декілька активізованих правил. В цьому випадку машина логічного висновку повинна вибрати залежно від пріоритету одне з правил для запуску дії.

Після завершення виконання всіх правил управління повертається до інтерпретатора команд верхнього рівня, щоб користувач міг видати командному інтерпретатору експертної системи додаткові інструкції. Роль верхнього рівня системи виконує інтерфейс користувача, який по суті є механізмом інтерпретації команд користувача.

Головною особливістю експертної системи є передбачений в ній засіб пояснення, який відображає інформацію про те, як система дійшла певного висновку. В системах, заснована на правилах, не складно організувати пояснення яким чином був отриманий певний висновок, оскільки хронологія активізації правил і вміст робочої пам'яті можна зберігати в стеку. Розвинені засоби пояснення можуть дати користувачу можливість ставити питання на кшталт «що», «якщо» і вивчати альтернативні шляхи формування висновків за принципом гіпотетичних міркувань.

Підсумовуючи викладені положення можна дійти висновку, що в разі організації раціональної взаємодії між особою, яка приймає рішення з мінімізації операційних ризиків та експертною системою можна досягти певних переваг. Мається на увазі переваги в порівнянні з необхідністю взаємодії з експертами для ухвалення прийнятних рішень. Ці переваги наявно проявляються в наступних моментах:

- рівень знань експертної системі, що були скомбіновані шляхом об'єднання знань декількох експертів, ймовірно перевищуватиме рівень знань окремо взятого експерта-людини;
- знання експертної системи зберігаються протягом невизначено довгого часу на відміну від експертів-людей, які можуть піти на пенсію, звільнитися з роботи тощо;
- здатність експертної система детально пояснити свої міркування, які привели до певного висновку, у будь який час і з практично необмеженою кількістю повторень, сприяє підвищенню довіри до ухваленого рішення;
- експертна система гарантує об’єктивний результат в екстремальних ситуаціях, в яких людина-експерт може виявитися нездатним діяти з максимальною ефективністю через дію стресу, втоми, хвороби тощо;
- експертну систему можна використовувати в якості інтелектуальної навчальної програми, для розвинення у нових співробітниках аналітичних навичок завдяки здійснення поступового детального розгляду міркувань системи в процесі рішення задач.

Прийняття рішень в процесі управління операційним ризиком багато в чому залежить від об’єктивності експертних знань. Тому метода формалізації знань експертів та накопичення їх в експертній системі являє, на наш погляд, один з найбільш прийнятних на теперішній час підходів до створення програмного забезпечення підтримки дій в умовах невизначеності. Метод продукційних правил вважається класичним для формалізації інтелекту і може бути успішно застосований в інженерії знань експертів з оцінки операційного ризику комерційного банку. Отже,

створення відповідної інтелектуальної системи є вкрай необіхним для сучасного банку і її побудову доцільно починати саме з накопичення даних. Звичайно, наступні кроки в розвитку системи будуть пов'язані з новими проблемами та методами їх подолання, які в алгоритмічному програмуванні зазвичай не застосовувані. Проте успіх цього процесу здатен покласти початок такому необхідному сьогодні зниженню міри суб'єктивності рішень як в ризик-менеджменті так і в загальній практиці управління банківською діяльністю.

5.2 Методи створення і ведення баз даних для оцінки операційного ризику в комерційному банку

Один з ключових моментів створення експертної системи полягає в організації технологічної структури бази знань, системи її зберігання та доступу до її елементів. Класичним підходом вважається організація бази знань в системах, розроблених за допомогою спеціалізованої мови програмування експертних систем CLIPS. Знання в таких системах мають структуру продукційних правил і зберігаються списком у файлах текстового формату зі специфічним розширенням (.clp). Такий підхід може бути прийнятним для створення баз знань з невеликою кількістю правил. Проте для створення бази знань оцінки операційного ризику банку можливості нарощування інформаційного обсягу в такій системі істотно обмежені внаслідок високої схильності до збільшення надмірності даних.

Термін «надмірність даних» використовується для опису ситуації, коли одні і ті ж дані зберігаються в різних місцях зовнішньої пам'яті (файлах). Надмірність в експертних системах небажана з декількох причин. Перша причина – неоднозначність. Виникає ситуація, коли одне і те саме правило має різні шаблони в різних записах файлів бази знань. Ефективна робота системи вимагає відсутності подібних неоднозначностей. Друга причина – неузгодженість. У випадку, коли використовується паралельний аналіз кожна машина логічного висновку по-різному сприймає список дій одного правила, існує висока ймовірність неузгодженості. Наприклад, якщо в системі, яка працює на одному комп'ютері змінився консеквент

правила – необхідно внести такі самі зміни в файли бази знань на інших комп'ютерах, де працюють машини логічного висновку. Такий процес називається розповсюдженням оновлень і, зазвичай, вимагає значних ресурсних витрат. Третя причина – марна праця. Дублювання існуючих антецедентів і консеквентів правил для урахування нових варіантів їх співвідношень, є марною витратою часу, сил і коштів.

В експертних системах, які використовують базу знань, сформовану як записи продукційних правил в текстових файлах, вірогідність неузгодженості, неоднозначності та марних витрат праці дуже висока. Для експертної системи оцінки операційного ризику, що вимагає використання великої кількості правил, такий підхід - неприпустимий. Цієї проблеми можна уникнути, сформувавши базу знань у вигляді в спеціалізованої програмної системи, що управляє процесом створення, зберіганням і обробки правил – сервера баз даних. Реалізація функцій сервера баз даних покладаються на особовий клас програмного забезпечення – систему управління базою даних (СУБД). По своїй суті, СУБД виконуватиме роль посередника між програмою, що виконує функції машини логічного висновку і даними, які формують правила.

Проблему надмірності даних в структурі продукційних правил бази знань експертної системи оцінки операційного ризику СУБД вирішує завдяки реалізації концепції інтегрованого використання даних. Під концепцією інтегрованого використання даних, мається на увазі виконання наступних положень:

- по-перше, різні користувачі можуть використовувати одні й ті ж дані;
- по-друге, ці дані можуть використовуватися різними користувачами в один і той самий час.

Процес інтегрованого використання даних називається паралельним доступом або паралелізмом (concurrency). Паралелізмом необхідно керувати, інакше дані можна легко пошкодити (наприклад, якщо один користувач змінює елемент правила, який використовується в цей момент машиною логічного висновку). Тому, крім паралелізму СУБД має забезпечувати гарантії безпеки й цілісності бази даних. Користувачі системи повинні мати нагоду захистити базу знань від

несанкціонованого доступу, а також відновити їх у разі будь яких системних збоїв. Централізоване управління безпекою даних – одна з найбільш важливих особливостей СУБД.

В експертній системі, для організації бази знань якої використовується СУБД, дані продовжують фізично зберігатися у файлах. Але, це не текстові файли, доступ до яких можна отримати використовуючи текстовий редактор. Ці файли утворюють загальну множину даних, доступ до вмісту якої можливо отримати виключно через СУБД. Роль СУБД в забезпечені доступу до даних полягає в тому, щоб генерувати запити, що дозволяють використовувати функціональні можливості системи управління файлами комп'ютера, на зовнішній пам'яті якого вони розташовані. СУБД виконує роль додаткового рівня програмного забезпечення, надбудованого над системним програмним забезпеченням.

Та частина інформації з бази даних, яка потрібна певному користувачу, називається представленням (view). СУБД повинна підтримувати можливості різноманітного представлення частин загального обсягу даних. Кожне представлення бази даних – це окрема логічна структура, побудована з фізичних даних, що лежать в її основі. Щоб забезпечити інтерфейс між фізичною пам'яттю бази даних та її різноманітними логічними версіями, СУБД, у свою чергу, повинна поділятись на декілька рівнів.

У будь-якій системі з базою даних є центральний, або, так званий, концептуальний рівень – логічне представлення даних системи. Концептуальний рівень повинен мати наступні характеристики:

- незалежністю від того, як фізично зберігаються дані;
- повнотою, тобто він повинен містити опис усіх даних, що зберігаються в системі.

Концептуальний рівень СУБД складається з усіх об'єктів бази даних, доступних користувачам. Об'єкт бази даних – це її певний логічний елемент. Залежно від типу бази даних її користувачам будуть доступні різні типи об'єктів. Концептуальний рівень СУБД є останнім рівнем представлення даних, що

доступний користувачу. Користувачі навмисно усунені від розгляду питань про те, як насправді зберігаються дані на фізичному рівні.

Сукупність всіх представлень утворюють так званий зовнішній рівень бази даних – інтерфейс між базою даних і її користувачами. Якщо концептуальна схема бази даних модифікується, то всі представлення, які причетні до цієї модифікації, необхідно буде змінити так, щоб вони залишались для своїх користувачів незмінним. Логічна незалежність даних полягає в усуненні користувачів від зміни логічного представлення бази даних.

Існує також інша форма незалежності даних, так звана фізична незалежність даних. Вона полягає в усуненні користувачів від змін, що відбуваються в фізичному сховищі бази даних. Фізичне сховище пересічної бази даних часто піддається оновленням і змінам з метою підвищення продуктивності та оперативного відображення змін, що відбуваються з реальними об’єктами (в нашому випадку – продукційними правилами), данні про які зберігаються в базі даних. На самому нижньому рівні СУБД повинна встановити відповідність між представленням бази даних у вигляді концептуальної схеми та її фізичним представленням. Це відображення називається внутрішнім рівнем системи з базою даних. Він виступає в якості інтерфейсу між СУБД і операційною системою комп'ютера, на якому вона встановлена. Якщо фізичне сховище бази даних змінюється, то СУБД повинна на внутрішньому рівні знов встановити відповідність концептуальної схеми новому фізичному представленню. Сама концептуальна схема повинна залишитися незмінною.

Таким чином, СУБД складається з трьох рівнів: множини відображень концептуального рівня в представлення користувачів, самого концептуального рівня і відображення концептуального рівня у фізичне сховище. Ці три рівні називаються відповідно: зовнішнім, концептуальним і внутрішнім рівнями.

Такий розподіл СУБД на рівні був запропонований як стандарт ANSI/SPARC (1978). Насправді, такий чіткий розподіл на рівні рідко використовується на практиці. Зокрема, з міркувань підвищення продуктивності, СУБД часто не звертається до засобів операційної системи комп'ютера, на якому вона встановлена,

а сама виконує ті операції, які стосуються управління файлами. Слід зазначити, що упродовж еволюції СУБД було розроблена значна кількість моделей практичної реалізації приведених положень. Для визначення найбільш прийнятної з них для організації бази знань системи оцінки операційного ризику розглянемо чотири моделі, які найчастіше використовуються в якості базових підходів до проектування СУБД: ієрархічний, мережевий, реляційний і об'єктно-орієнтований.

У 1968 році компанія IBM запропонувала своїм клієнтам систему управління інформацією (Information Management System, IMS). Це була одна з перших спроб досягти інтегрованого управління файлами на основі баз даних і один з перших прикладів СУБД. Дані в ієрархічній базі були концептуально організовані в набори, які зв'язувалися один з одним відносинами володіння. Ієрархічні бази даних підходять для тих інформаційних систем, які природно ґрунтуються на ієрархічній моделі. Існує ряд високопродуктивних систем, побудованих на основі IMS. Проте більшість систем, неможливо реалізувати у вигляді IMS таким чином, щоб уникнути великої кількості повторень даних.

На початку 70-х років XX сторіччя, Конференцією по мовах і системах даних (Conference On Data Systems Languages, CODASYL) була створена спеціальна робоча група – Database Task Group, метою якої була розробка методичних вказівок з реалізації інтегрованого підходу до управління файлами, заснованого на технології баз даних. Результатом роботи групи стала розробка мережевої моделі, яка є, по суті, модифікацією ієрархічної моделі. У мережевій моделі існують дві основні конструкції: записи і зв'язки. Зв'язок представляє собою набір фізичних покажчиків, які задають відносини володіння між наборами записів. На відміну від ієрархічної моделі, у мережевій моделі немає обмеження, яке вимагає, щоб володіння задавалося тільки в одному напрямку, тому набір записів може брати участь у довільній кількості зв'язків володіння. Використовуючи мережевий підхід, можна шляхом ретельного аналізу даних, усунути надмірність, і використання файлів системи стане інтегрованим. Але така інтеграція досягається за рахунок значної складності в організації доступу до вмісту файлів. Мережеві бази даних характеризуються великою кількістю наборів записів, кожен з яких містить порівняно невеликий обсяг інформації, і багато покажчиків на іншу множину

записів. Навіть написання простих запитів до такої системи даних може вимагати складну навігацію від одного набору записів до інших.

Реляційна модель бази даних була вперше запропонована І.Коддом у 1970 році). Вона позитивно відрізнялася від моделей баз даних, що застосовувались до неї і, як наслідок, у 80-х роках XX сторіччя отримала загальне визнання як найбільш узгоджена й практична модель розробки СУБД. Згідно з реляційною моделлю, дані на концептуальному рівні представляються у вигляді звичайних двовимірних таблиць, що складаються з рядків і стовпців. Рядки таблиць в реляційній теорії називаються кортежами, а стовпці – атрибутами. Кортежі практично відображають ті розуміння, що у попередніх моделях відповідали записам файлів. Атрибути, у свою чергу, відображають характеристики кожного кортежу. У реляційній базі даних зв'язок між даними в різних таблицях здійснюється за допомогою значень визначених атрибутів. Реляційні системи забезпечують більш практичне середовище розробки, ніж попередні підходи. Реляційні структури даних легко розуміти і створювати. Крім того, процеси розробки прикладних програм, що їх використовують, також не відносяться до категорії високої складності. Тому останніми роками переважна більшість виробників сучасних СУБД, у тій чи іншій мирі, використовують реляційну модель. Проте, у реляційної моделі є певні недоліки, які частково можуть бути усунуті завдяки використанню об'єктно-орієнтованої моделі.

Реляційний підхід до реалізації СУБД, найчастіше піддається критиці за те, що він ґрунтується на ідеї пасивної множини даних. У них відсутні засоби, які дозволяють моделювати реальну поведінку даних. Крім того, його семантичні можливості також достатньо обмежені, тому буває важко представляти дійсне значення об’єктів даних. Об'єктно-орієнтована технологія баз даних намагається подолати ці обмеження. Схема об'єктно-орієнтованої бази даних складається з колекції класів. Клас є колекцією об'єктів, причому структура і поведінка об'єктів одного класу однакові. Видима структура об'єкту визначається властивостями його класу. Важливою властивістю об'єктно-орієнтованої бази даних є те, що користувачу не потрібно знати про взаємодію об'єктів. Використовуючи об'єкти і методи, можна зберігати і неодноразово використовувати не тільки структуру

об'єкту бази даних, але і його поведінку. Однак, практичних реалізацій об'єктно-орієнтованих СУБД на даний момент існує порівняно небагато. Незважаючи на спроби стандартизації, що відбуваються останнім часом, визначення поняття «об'єктно-орієнтована база даних» все ще недостатньо чітке в порівнянні із визначенням реляційної моделі. Це призвело до значних відмінностей у способах реалізації об'єктно-орієнтованих баз даних. Тому розробники ІТ систем, яким добре знайома наочна реляційна модель організації даних і пов’язані з нею відносно однорідні програмні продукти, не поспішають переходити до об'єктно-орієнтованих систем.

Підводячи підсумки аналізу моделей реалізації СУБД можна дійти висновку, що перші два з цих підходів (ієрархічний та мережевий) представляють більше історичний ніж практичний інтерес. Останнім часом більшість інформаційних систем включає ті або інші аспекти реляційного підходу, тому реляційні бази даних домінують на ринку інформаційних систем. Тому, реляційна модель реалізації СУБД видається найбільш прийнятною для реалізації бази знань системи оцінки операційного ризику. Для підтвердження розглянемо технологічну структуру реляційної бази даних.

Як було зазначено раніше, у реляційній базі даних всі дані зберігаються у двовимірних таблицях. Для кожного об'єкту, інформації про який планується зберігати в базі даних, створюється окрема таблиця. Усі об'єкти з однаковими характеристиками зберігаються в одній таблиці. Характеристики об'єкту представляються заголовками стовпців, що описуються в заголовку таблиці. Екземпляри конкретного об'єкту представляються рядками таблиці.

Усі реляційні таблиці повинні мати заголовок. Заголовок складається з імені таблиці та імен атрибутів (стовпців), які складають дану таблицю. Кількість атрибутів визначає ступінь таблиці. У реляційній теорії обмеження на кількість атрибутів, що становлять таблицю, не накладаються, але на практиці в СУБД, зазвичай вказується верхня межа для їхньої кількості. Кортежі реляційної таблиці (рядки) утворюють її тіло. Кортеж представляє собою впорядкований список атрибутів певного об’єкту. Кожен атрибут характеризується його положенням у кортежі. Кількість кортежів таблиці визначає її кардинальність. Кортежі таблиці

можуть зберігатися й відображатися в довільній послідовності. У більшості реляційних систем кортежі зберігаються і відображаються в тому порядку, в якому вони заносились до таблиці.

На дані, які можна присвоювати атрибутам, накладаються певні обмеження. Це можуть бути цілі числа або послідовності символів. Область значень, які може приймати атрибут, називається його доменом. На деякому рівні поняття «домен» дуже близьке поняттю типів даних у програмуванні. Як і тип даних, домен не тільки визначає множину значень, що може приймати атрибут, але й задає діапазон допустимих операцій для кожного типу значень (наприклад, складання й віднімання чисел, розбиття і конкатенація символьних строк тощо). При визначенні атрибуту необхідно задати для нього ім'я і домен. З цього моменту кожне значення, що привласнюється атрибуту, повинне відповідати його домену. Домени можуть бути достатньо узагальненими (наприклад, «позитивні цілі числа в діапазоні від 0 до 99999», «строки завдовжки не більше 20 символів») або достатньо конкретними (наприклад, «депозитний рахунок»). Більшість реляційних програмних продуктів забезпечує підтримку загальних доменів у формі базових типів даних. Найрозвиненіші з них пропонують користувачам бази даних засоби, що дозволяють створювати свої власні домени.

Важливим моментом реляційної технології є те, що реляційні домени повинні бути простими, тобто складатися тільки з окремих величин. У кожному кортежі кожному атрибуту можна надати тільки одне значення. Багатозначні домени не допускаються. Якщо атрибут таблиці повинен бути багатозначний, то для його реалізації необхідно створити додаткову таблицю. Багатозначний домен не є атомарним, тобто він може містити значення, які не є простими «атомами». Під «атомами» розуміють об’єкти, які не допускають їх розклад на складові. У реляційній базі даних всі домени повинні бути атомарними.

Базова таблиця представляє собою самий нижній рівень представлення даних, який доступний користувачам бази даних. Усі дані реляційної бази даних зберігаються у вигляді набору базових таблиць. Але одержувати дані і маніпулювати ними можна також за допомогою представлень. Представлення можно трактувати як логічну таблицю, яка прямо або опосередковано одержує дані з

базових таблиць. Представлення може бути просто підмножиною деякої базової таблиці. У представленні можуть знаходитися дані з декількох базових таблиць. Представлення до певної міри можуть трактуватися як базові таблиці: їх можна використовувати як для отримання даних, так і для додавання, видалення і змін значень даних.

При створенні представлення домени атрибутів визначаються базовими таблицями, звідки беруться дані для цього представлення. Створення представлення ґрунтується на визначенні списку базових таблиць, дані яких будуть покладені в його основу. Коли базова таблиця видаляється з бази даних, усі представлення, що походять від неї (повністю або частково, безпосередньо або опосередковано), логічно припиняють своє існування.

Організація фізичного рівня реляційних баз даних ґрунтується на взаємодії базових таблиць СУБД і файлів, в яких данні фізично зберігаються. Запис даних у зовнішню пам'ять і отримання їх звідти утворюють одну із задач операційної системи комп'ютера. Операційна система є набором напівперманентних програм, які забезпечують інтерфейс між прикладними програмами й апаратним забезпеченням комп'ютера. Вона надає програмам такі послуги, як управління пам'яттю й організацією вводу-виводу. Операційна система сприймає СУБД як звичайну прикладну програму, що потребує обслуговування. Основним необхідним для СУБД сервісом, який може запропонувати операційна система, є обробка фізичних файлів.

На практиці не завжди має місце чітке відділення файлової системи від СУБД. Багато операційних систем не надають необхідні для СУБД можливості по управлінню файлами. З іншого боку, деякі СУБД самі ігнорують файлову систему і взаємодіють безпосередньо з програмою управління дисковою пам'яттю. Організація внутрішнього рівня реляційної системи може бути достатньо різноманітною. Наприклад, в одних системах під кожну створювану таблицю виділяється окремий файл системи, в інших файл системи створюється для кожного набору таблиць, що належать окремому користувачу. Важливе те, що всі ці системи виглядають як реляційна база даних для своїх користувачів. Теоретично, вони можуть надавати користувачам однакові можливості. Проте внутрішня організація

реляційних систем впливає на продуктивність інформаційної системи, що їх використовують.

У класичній схемі реляційна СУБД має два рівні взаємодії: один – з користувачем бази даних, а другий – з операційною системою компютера, на зовнішній пам'яті якого зберігаються файли з даними. Користувач може розглядати і використовувати базу даних тільки як набір таблиць. Все інше від користувача приховане. Управління таблицями й блоками даних у табличному просторі відносяться виключно до задач СУБД.

Підсумовуючи викладені положення можна зазначити, що при використанні реляційної бази даних для організації бази знань системи оцінки операційного ризику можна на концептуальному рівні створити структуру таблиць для збереження антецедентів та консеквентів продукційних правил, яка дозволить позбутися надмірності даних. Структури базових таблиць забезпечать контроль за шаблонуванням частин правил. Використовуючи реляційний механізм можна забезпечити оптимальні структури правил у вигляді представлень для передачі в машину логічного висновку. З'являється можливість покласти на плечі СУБД рішення завдань з оптимізації розміщень елементів правил в файлах зовнішньої пам'яті, управління доступу до них та відновлення на випадок аварій в системі. Для цього на ринку реляційних СУБД існує низка продуктів, що позитивно зарекомендувала себе у багатьох автоматизованих інформаційних системах, а саме: ORACLE, MS SQL SERVER, DB2, INFORMIX та інші. Отже, використання реляційної СУБД в експертній системі оцінки операційного ризику являє собою основу для створення надійної, інтегрованої та гнучкої бази знань.

5.3 Основні засади автоматизації процесу оцінки операційного ризику

Автоматизація процесу оцінки операційного ризику комерційного банку полягає у створенні програмної системи, яка оперує із знаннями у відповідній предметній області з метою розрахунку рівня операційного ризику банківських установ. Така програмна система повинна реалізовувати функції машини логічного

висновку, що взаємодіє з базою знань у вигляді реляційної бази даних та інтерфейс користувача з реалізацією засобів ведення бази знань, пояснення результатів, вводу фактів в систему. Оскільки автоматизована система оцінки операційного ризику відноситься до класу експертних систем, процес її створення та інструментальні засоби, що при цьому використовуються, відрізняються від програмних систем іншого спрямування.

Інструментальні засоби розробки програмних систем утворюються поєднанням мови програмування з набором допоміжних програм. Практично всі інструментальні засоби, що використовуються в процесі розробки експертних систем, використовують методологію автоматизації проектування на основі прототипів. По відношенню до програмного забезпечення термін прототип означає працюючу модель програми, яка функціонально еквівалентна підмножині кінцевого продукту. Ідея використання прототипів полягає в розробці на ранній стадії роботи проекту спрощеної версії кінцевої програми, яка була б в змозі послужити доказом продуктивності основних ідей, покладених в основу проекту. Тобто, прототип повинен бути здатний вирішувати одну з характерних задач для заданої області застосування. На основі аналізу досвіду роботи з прототипом розробники можуть уточнити вимоги до основних функціональних характеристик експертної системи. Працездатність прототипу може послужити наочним доказом можливості рішення проблем за допомогою створюваної системи ще до того, як на її розробку будуть витрачені значні засоби.

Процес розробки експертної системи, як правило, складається з послідовності окремих етапів, упродовж яких нарощуються можливості системи, причому кожний з етапів підрозділяється на фази: проектування, реалізації, компоновки та тестування. В результаті, після завершення чергового етапу, утворюється система, яка здатна справлятися з більшими по складності варіантами проблеми. На відміну від експертних систем, при створенні більшості програмних продуктів інших видів, використовується інша модель процесу: спочатку розробляється специфікація продукту, потім виконується планування, проектування компонентів, їх реалізація, компоновка комплексу та тестування кінцевого варіанту. Той факт, що при розробці експертних систем існує можливість спочатку побудувати та всебічно випробувати

прототип, дозволяє уникнути безлічі переробок в процесі створення робочої версії системи. Однак, слід зазначити, технологія послідовного нарощування функціональних можливостей містить в собі проблему інтеграції нових функцій системи з функціями, що були реалізовані в попередніх варіантах. Тому інструментальні засоби розробки експертних систем від початку створювалися на основі модульного представлення знань, з урахуванням необхідності подолання виникаючих при цьому ускладнень.

Слід зазначити, що розробка та впровадження експертної системи оцінки операційного ризику неодмінно стикнеться з проблемами, характерними для процесу створення експертних систем. Систематизація цих проблем дозволить виробити практичні рекомендації для їх успішного подолання. Один з варіантів систематизації цих проблем та способів їх подолання представлений в таблиці 5.1.

Успіх у розробці експертної системи з оцінки операційного ризику багато в чому залежить від вибору інструментальних засобів. Практика вибору інструментальних засобів для побудови експертної системи ґрунтується на зіставленні характеристик проблем, що має вирішувати експертна система та необхідних функціональних можливостей інструментального комплексу.

При цьому рекомендується дотримуватись наступних загальних правил:

- слід вибирати інструмент зі ступенем сервісної насиченості, який не перевищує необхідного рівня для вирішення даної задачі;
- вибір інструментарію повинен визначатися в першу чергу характеристиками задачі, яку вирішуватиме експертна система, а не іншими сторонніми обставинами (наприклад тим, що якийсь інструмент вже є в наявності або знайомий розробннику краще за інших);
- якщо успіх проекту залежить від терміну розробки, то слід вибирати інструментальне середовище з вбудованими засобами формування пояснень та елементів користувальницького інтерфейсу, оскільки їх розробка найбільш трудомістка;
- необхідно постаратися якнайшвидше провести випробування нового інструментального середовища на реальних даних.

Таблиця 5.1

Характерні проблеми, що вникають при розробці експертних систем

№	Сутність проблеми	Причина проблеми	Подолання проблеми
1	Знання, що стосуються предметної області, дуже тісно переплетені з іншими частинами системи.	Складність відокремлення знань предметної області від знань загального застосування.	Покласти в основу організації бази знань сукупність продукційних правил, збережених в реляційній базі даних.
2	База знань, яка сформувалася в процесі опиту експертів, виявляється неповною настільки, що не дозволяє вирішувати потрібні задачі.	Відсутність в базі знань фундаментальних концепцій предметної області, або ці концепції представлені з помилками.	Послідовно нарощувати об'єм бази знань, починаючи з фундаментальних понять – це дозволить ще на ранніх стадіях розробки виявити вказану проблему.
3	Середовище розробки позбавлене вбудованих засобів формування функцій пояснення експертної системи.	Додавання таких функцій у вже спроектовану систему являє собою надскладну задачу.	Слід піклуватися про прозорість експертної системи з перших кроків її розробки
4	Система може містити надмірну кількість дуже специфічних правил, що призводить до уповільнення роботи системи та ускладнює управління нею.	Складність трансформації знань предметної області в набір продукційних правил.	Слід уникати надто специфічних і надто загальних правил – прагнути знайти компроміс між ефективністю правил та їх зрозумілістю.

Процес рішення питання вибору можна представити схематично, як показано на рис. 5.2.

Найважливішим питанням в процесі вибору інструментального середовища є питання стосовно способу визначення характеристик проблеми для вирішування якої призначається експертна система. Ці характеристики можна звести до 4-х основних категорій.

1) *Малий простір рішень, надійні дані та знання*. Передбачається, що кількість альтернатив, які слід брати до уваги при пошуку рішення, є невеликою, всі дані є достовірними та істинність правил не викликає сумнівів. Для вирішення проблем цієї категорії можна скористатися готовими рішеннями, тобто раніше створеною оболонкою на базі експертної системи, що вирішувала аналогічну проблему в іншій предметній області.

Рис. 5.2. Типова схема вибору інструментальних засобів для розробки експертної системи

2) *Ненадійні дані або знання*. Якщо дані або знання ненадійні, то існує небезпека, що дані, які вводяться в систему, не є достовірними, а правила в базі знань не мають однозначності. В цьому випадку в експертній системі потрібно комбінувати інформацію від декількох джерел та використовувати логіку нечітких міркувань.

3) *Великий факторизований простір рішень*. Простір пошуку можна назвати факторизованим, якщо існує можливість розділити його на декілька незалежних підпросторів, які можна обробляти окремо. Причому для різних підпросторів можуть бути використані різні множини правил або окремі підмножини однієї і тієї ж множини правил. Зазвичай таке розбиття виконується на рівні проблеми, тобто велика загальна проблема розбивається на декілька дрібніших. Успіх в досягненні головної мети, таким чином, оцінюється по сукупності успіхів в досягненні незалежних цілей.

4) Великий нефакторизований простір рішень. Простір рішень може виявитися нефакторизованим, якщо задача допускає вироблення рішення будь-якого компоненту тільки в контексті всього проекту. Загальний підхід до роботи у великому просторі пошуку полягає в тому, щоб послідовно розглядати його на різних рівнях абстракції. Тобто, потрібно використовувати варіанти описання простору з різним рівнем урахування деталей. Рішення проблеми таким методом часто називають низхідним уточненням.

З'ясувавши характеристики проблеми для вирішення яких розробляється експертна система, можна визначитися з властивостями простору рішень. Потім вони розглядаються спільно з передбачуваними характеристиками системи: моделі подання знань, напрямком логічного висновку, способу формування пояснень. В результаті виявляються бажані характеристики інструментального середовища, які дозволяють підібрати потрібну модель інструментального середовища. Як показує практика, більшість розробників явно або неявно використовують саме такий підхід при створенні експертних систем.

В процесі вибору інструментального середовища важливе значення мають також наступні аспекти:

- наскільки просте середовище у використанні,
- як швидко розобники експертної системи зможуть оволодіти методикою роботи в цьому середовищі,
- яку підтримку готова надавати фірма-розробник середовища,
- яка буде загальна вартість середовища з урахуванням прямих і непрямих витрат.

В матеріалах, що описують програмні засобі з розробки експертних систем, можна зустріти твердження, що даним інструментом «може успішно користуватися програміст, малознайомий з технологіями штучного інтелекту» або навіть непрограміст. Проте, практика показує, що це не так. Практичне оволодіння типовими інструментальними засобами проектування експертних систем не поступається по складності оволодінню новою мовою програмування.

Як правило, типове середовище розробки експертних систем підтримує чотири режими роботи:

- підготовка та редагування бази знань;
- використовування бази знань для виконання консультацій, тобто прогін програми;
- виявлення та усунення помилок на стадії компіляції;
- виявлення та усунення помилок на стадії виконання.

Як показав досвід, навіть досвідчені програмісти важко засвоюють методику сумісного використовування цих режимів в процесі проектування експертної

системи. Це зв'язано, перш за все, з тим, що стандартна стратегія розробки бази знань передбачає постійне нарощування її об'єму. Тому, інженеру по знаннях доводиться виконувати інтерактивні процедури поповнення бази знань значно частіше, ніж звичному програмісту виконувати розширення функцій програми.

По своєму призначенню та функціональним характеристикам інструментальні засоби, що використовуються в програмуванні експертних систем, можна розділити на наступні категорії:

1) *Оболонки експертних систем*. Системи типу оболонки експертних систем створюються, як правило, на основі експертних систем, які достатньо добре зарекомендувала себе на практиці. В процесі створення оболонки, з системи-прототипу видаляються компоненти, які є специфічними для області її безпосереднього застосування та залишаються ті, що не мають вузької спеціалізації. В загальному сенсі, оболонки експертних систем створюються з метою дозволити непрограмістам скористатися результатами роботи програмістів, що вирішували аналогічні проблеми. Клас цих інструментальних засобів орієнтований на достатньо вузький клас задач, проте, не зважаючи на обмеження, цей тип експертних систем прогресує. Наприклад, оболонка M.4 може функціонувати під управлінням будь-якої з операційних систем персональних комп'ютерів, підключатися до баз даних, включати фрагменти програмного коду на мовах Visual BASIC та Visual C++.

2) *Мови* описання продукційних правил**.** Представляють собою ефективний засіб швидкого створення прототипів експертних систем. Вони дозволяють забезпечити гнучкість процесу розробки, мінімізацію матеріальних витрат та термінів виконання проекту. Одним з найвідоміших представників таких мов є OPS5. Для цієї мови характерний порівняно простий синтаксис та механізм активізації правил. Однак, для мови OPS5 характерною ознакою є труднощі при реалізації деяких типів структур управління ходом виконання. Наприклад, до них можна віднести рекурсивні та ітераційні цикли, оскільки вони вимагають серйозного ускладнення описання процесу обробки правил. Розробники мов, подібних OPS, завжди вимушені шукати компроміс між наочністю засобів мови програмування та ефективністю виконання програмного коду.

3) *Об'єктно-орієнтовані мови*. В цьому контексті, мовами об'єктно-орієнтованого програмування створюється програмне середовище для організації знань в термінах декларативного представлення об'єктів предметної області. Усі дії, пов'язані з процедурною стороною рішення проблем, розподіляється між цими об'єктами, які мають в своєму розпорядженні власні процедури та можуть спілкуватися один з одним за допомогою інтерфейсів передачі повідомлень. Корисним аспектом об'єктно-орієнтованого програмування є можливість інтеграції символічних обчислень в операційне середовище, яке базується на засобах графічного інтерфейсу. Оснащення експертної системи цими засобами дозволяють краще представити користувачу процеси, що відбуваються в системі. До недоліків використовування об'єктно-орієнтованого стилю в програмуванні експертних систем можна віднести складність в організації співвідношення програмних об'єктів з абстрактними поняттями та категоріями предметної області.

4) *Мови логічного програмування*. Типовою мовою логічного програмування експертних систем є PROLOG. Для цього PROLOG володіє достатньо корисними можливостями, а саме: вбудований в PROLOG режим управління приблизно відповідає стратегії зворотного логічного висновку; індексовану базу даних фраз мови PROLOG можна використовувати для представлення правил; рекурсивні структури даних (графи та дерева) можна організувати за допомогою фраз мови PROLOG; універсальний механізм зіставлення мови PROLOG дозволяє виконувати зіставлення даних та шаблонів, що включають змінні; мовні засоби PROLOG дозволять програмісту розробити власний механізм обробки невизначеності. Проте, практика застосування ідей логічного програмування в експертних системах не позбавлена недоліків. Зокрема наявність синтаксичних та семантичних обмежень, що присутні в стандартних версіях PROLOG не були подолані ані в системах MECHO та PLANNER, ані в інших системах, що базуються на аналогічній ідеології.

5) *Середовище програмування з підтримкою декількох парадигм***.** Засоби цієї категорії включають декілька програмних модулів, що дозволяє комбінувати в процесі розробки експертної системи різні стилі програмування, вибираючи

відповідні поєднання різних методів. Причиною їх створення стали результати роботи експертних систем з різними схемами представлення знань та логічного висновку. Виявилося, що кожна з них має свої слабкі сторони. В результаті їх аналізу, логічним чином була сформована ідея об'єднання методик в єдине середовище, в якому переваги одних компенсують недоліки інших. Одним з перших багатофункціональних середовищ штучного інтелекту став відповідний продукт, що має назву LOOPS (Bobrow and Steflk, 1983). В ньому в рамках єдиної архітектури обміну повідомленнями були об'єднані чотири парадигми програмування: процедурно-орієнтоване програмування, програмування, орієнтоване на правила, об'єктно-орієнтоване програмування, програмування, орієнтоване на дані. Основу системи складає об'єктно-орієнтована парадигма. В рамках її модулів можна комбінувати модулі середовища, що підтримують різні стилі програмування. Такий стиль об'єднання парадигм реалізований в мові CLIPS.

6) *Додаткові модулі програмування експертних систем***.** Засоби цієї категорії є автономними програмними модулями, які призначені для виконання специфічних задач в рамках вибраної архітектури експертної системи. Під додатковими модулями розуміються корисні програмні розробки, які можна виконувати разом з основним програмним додатком. Як правило, такі програми реалізують деякі спеціальні функції, підключаючи їх, начебто, з за меж системи. Причому звернення до таких функцій не потребує додаткового програмування в основному додатку.

По мірі збільшення складності проектованої системи відбувається збільшення об'єму бази знань, додавання до розгляду різного роду невизначеностей, включення в роботу системи додаткових режимів. Тому, стратегія проектування вимагає від розробників дедалі більш ретельної попередньої підготовки. Крім того, можна виділити інші характерні причини складності вибору інструментального середовища розробки експертних систем:

- більшість розвинених середовищ розробки надто дорога для того, щоб купувати їх для проведення порівняльного аналізу;

- час, необхідний для освоєння навиків роботи з системою та виявлення її сильних та слабких сторін, надто великий, тому складно проводити порівняння конкуруючих моделей на практиці;
- термінологія, яку застосовують в документації розробники різних систем, істотно відрізняється, тому проводити їх порівняння на основі технічної документації, достатньо важко.

Останнє зауваження справедливе відносно більшості програмних продуктів, що пропонуються на ринку. Коли ж йдеться про програмні засоби, що пов'язані з областю експертних систем, то новизна та незвичність термінології ще більш посилює проблему. Вже давно в середовищі фахівців існує думка, що порівняння конкуруючих систем одного класу можна виконувати тільки після ретельного вивчення їх на практиці.

На завершення слід зазначити, що будь-які інструментальні засоби потребують адекватної методології користування ними. В літературних джерелах, присвячених програмуванню, для виразу рівня адекватності часто застосовується поняття «стиль програмування». Дотримуючись загальноприйнятого стилю програмування можна уникнути небезпеки зробити програмну систему нежиттєздатною ще до закінчення етапу розробки проекту. Тому, доречно буде розглянути загальні рекомендації, які визначають стиль програмування експертної системи оцінки операційного ризику:

1) Задача, яку передбачається вирішувати за допомогою експертної системи, повинна бути повністю під силу експерту-людині.

2) Задача повинна бути чітко сформульована. Краще створити систему, яка зможе надійно вирішувати обмежену задачу, ніж систему, що претендує на вирішення широкого класу задач, проте дає вірне рішення лише час від часу.

3) Починаючи з першої стадії роботи над системою необхідно визначити, як вона буде вдосконалюватися та окреслити межі, яких вона повинна досягти в процесі еволюції.

4) Слід ретельно відпрацювати поведінку системи на наборі окремих випадків та організувати бібліотеку таких випадків. Тобто приклади, які застосовувались на етапі проектування, повинні бути репрезентовані.

5) Потрібно відділити ті знання, які є специфічними для предметної області, від знань, які стосуються загальної методики рішення проблем. Бажано, наскільки це можливо, спростити машину логічного висновку в системі.

6) Необхідно на самих перших стадіях проектування системи розробити однозначні угоди про оформлення програм. Це надасть їй одноманітний вигляд.

7) Бажано поступатися продуктивністю програми, якщо це зробить її зрозумілішою та спростить її супровід. Це необхідно, оскільки в роботі інтерактивної експертної системи велика частина часу йде на діалог з користувачем та звернення до баз знань.

8) Як тільки встане питання про розробку нового прототипу системи, від попереднього необхідно відмовитися. Багато проектів потерпіли невдачу лише тому, що їх автори не змогли позбавитися прихильності до першого варіанту реалізації власних ідей. Звичайно, в процесі розробки нового прототипу потрібно враховувати досвід створення попереднього, але тільки досвід, а не програмний код.

9) Розробка експертної системи, яка буде здатна успішно працювати, вимагає наполегливості і терпіння професійного програміста, залучення до роботи досвідченого експерта у відповідній області та певного рівня примусу з боку керівництва.

Наведений перелік рекомендацій, звичайно, не можна вважати вичерпуючим, зважаючи хоча б на той факт, що інструментальні засоби постійно знаходяться в процесі розвитку. Тим не менше, вони можуть претендувати на звання фундаментальних в процесі створення програмних продуктів класу експертних систем. Програміст, який буде дотримуватись цих рекомендацій, відповідно буде дотримується такого стилю програмування, що дозволить максимізувати вірогідність успіху в розробці експертної системи оцінки операційного ризику комерційного банку.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Дмитров С.О., Медвідь Т.А. Новітня компонента в системі банківських ризиків / Сергій Дмитров, Тетяна Медвідь // Науково-практичний журнал Вісник Національного банку України. — 2010. — №4 (170). — С. 11-14.

2. Заславская О. Бесконтактные карты скоро появятся в наших кошельках [Електронний ресурс] / О. Заславская // газета Финансовые известия. — 23.03.2005. — Режим доступу : http://www.finiz.ru/cfin/tmpl—art_oo/id_art—913767.

3. УНІАН [Електронний ресурс] — Режим доступу : http://economics.unian.net/rus/detail/38859

4. Костюк Д. Мошенничество с карточками и банкоматами [Електронний ресурс] / Дмитрий Костюк. — 20.03.2008. — Режим доступу : http://tristar.com.ua/2/art/moshennichestvo_s_kartochkami_i_s_bankomatami.html

5. Правила організації статистичної звітності, що подається до Національного банку України [Електронний ресурс] : Постанова Правління Національного банку України від 19.03.2003 №124 зі змінами, внесеними 26.05.2010 Постановою Правління Національного банку України №244. - Режим доступа : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=z0406-10.

6. «Типології легалізації злочинних коштів в Україні в 2005-2006 роках», - затверджені наказом Держфінмоніторингу України від [Електронний ресурс] — 22.12.2006. - №265. - Режим доступу : www.sdfm.gov.ua/content/File/Site_docs/26.12.06/.

7. Синебрюхов Л. Великий комбинатор Ник Лисон - гениальный трейдер, разоривший старейший британский банк [Електронний ресурс] / Лев Синебрюхов // Финансовые известия. – Май, 2005. — Режим доступу : http://www.finiz.ru/economic/article923190.

8. Даньків В.Й. Теоретичні основи управління операційними ризиками / В.Й. Даньків // Науковий вісник Ужгородського університету. Економіка. – 2009. – Вип. 27. – С. 158-162.

9. Стубайло Т. Місце операційних ризиків у банках україни / Т. Стубайло // Українська наука: минуле, сучасне, майбутнє : Збірник наукових праць Тернопільський національний економічний університетю. – 2007. – вип. №12. – С. 297- 304.

10. Камінський А., Кияк А. Ідентифікація, аналіз та управління операційними ризиками в українських банках // Вісник НБУ. – 2005. – № 10. – С. 7 – 11.

11. Швець Н.Р. Ризики банківських установ: проблеми, визначення та управління / Н.Р. Швець // Регіональна економіка. – 2008. - №4. – С. 97-103.

12. Кротюк В. Базель ІІ: Розрахунок мінімально необхідної величини капіталу згідно з першою компонентою / В.Кротюк, О.Куценко // Вісник НБУ. - 2006. - №7. – С. 2-7.

13. Дмитрова. О. Методичні рекомендації щодо оцінки ділової репутації керівників банків / О.Дмитрова, К.Гончарова // Вісник Національного банку України. – 2009. – № 6. – С. 37-39.

14. Ольшевская А. Банкиры проворовались [Електронний ресурс] / Анастасия Ольшевская. — 08.12.2004. — Режим доступу : http://www.gazeta.ru/2004/08/12/oa_129924.shtml

15. Наказ Державного комітету фінансового моніторингу України від 22.12.2008 №267 «Методичні рекомендації щодо здійснення страховими установами внутрішнього фінансового моніторингу з використанням критеріїв ризику» [Електронний ресурс] — Режим доступу : http://www.sdfm.gov.ua/print.php?what=art&id=996&cat_id=221&lang=uk

16. Поддєрьогін А. М. Фінансовий менеджмент / А. М. Поддєрьогін — К.: КНЕУ, 2005. — 535 с.

17. Даньків В.Й. Теоретичні основи управління операційними ризиками // Науковий вісник ДВНЗ «УжНУ». Випуск 27. Серія «Економіка» – 2009.

18. Постанова Національного банку України «Про Схвалення Методичних рекомендацій щодо організації та функціонування систем ризик-менеджменту в

банках України» від 02.04.2008 №361 [Електронний ресурс] — Режим доступу : http://www.bank.gov.ua/Bank_Supervision/Risks/index.htm.

19. Базельський комітет з банківського нагляду «Посилення корпоративного управління банківських установ». — [Електронний ресурс] — Режим доступу : www.bank.gov.ua/Bank.../corporate_management.pdf

20. Базельський комітет з банківського нагляду «Належна практика управління і контролю над операційним ризиком». — [Електронний ресурс] — Режим доступу : www.ifc.org/...Practices.../Microsoft+PowerPoint+-+1+-+Op+Risk+Sound+Practices_UKR_final.ppt.pdf.

21. Системи підтримки прийняття рішень [Текст] : навчальний посібник / [О.І.Пушкар, В. М. Гіковатий, О. С. Євсєєв, Л.В.Потрашкова]; За ред. д-ра екон. наук, проф. Пушкаря О.І. – Х. : ВД «ІНЖЕК», 2006. – 304 с.

22. Недосекин А. О. Методологические основы моделирования финансовой деятельности с использованием нечетко-множественных описаний [Текст] : дис. доктора. экон. наук: 08.00.13 - Санкт-Петербург. – 2003. – 280 с.

23. Галіцин В. К. Моделі і методи оцінки інвестиційних проектів [Текст] : монографія / В. К. Галіцин, О. П. Суслов, Ю. О. Кубушко. – К. : КНЕУ, 2005. – 168 с.

24. Чаплінський Ю. П. Системна оптимізація як методологічна основа оцінки реалізує мості інвестиційних проектів [Текст] / Ю. П. Чаплінський, А. О. Ширяєв // Економіко-математичне моделювання соціально-економічних систем. Збірник наукових праць. Вип. 7 / Відп. ред. академік НАН України О.О.Бакаєв. – Київ : Міжнародний науково-навчальний центр інформаційних технологій і систем НАН та МО і Н України, 2003. – 158 с.

25. Буздалин А. В. Содержательный анализ устойчивости банка искусственным интеллектом [Електронний ресурс] / А. В. Буздалин. – Режим доступа : http://www.buzdalin.4u.ru/text/banks/t8/intel.html.

26. Дмитров С. О. Управління операційним ризиком комерційного банку методом байєсовського аналізу [Текст] / С. О. Дмитров, О.В. Меренкова // Проблеми

і перспективи розвитку банківської системи України: збірник наукових праць. Т. 20. – Суми : УАБС НБУ, 2007. – С.131-140.

27. Меренкова О. В. Використання Байєсовського аналізу як методу оцінки надійності комерційних банків. Математичні моделі та інформаційні технології в сучасній економіці [Текст] / О. В. Меренкова, В. В. Колдовський / під редакцією д.е.н., професора А. О. Єпіфанова. – Суми : УАБС НБУ, 2007. – С.132-143.

28. Кнут, Д. Э. Искусство программирования: В 3 т. Т. 1: Основные алгоритмы [Текст] : учебное пособие : пер. с англ / Д. Э. Кнут. - 3-е изд. - М.-СПб.-К. : Вильямс, 2000. - 720 с.

29. Ньюэлл А., Моделирование мышления человека с помощью электронно-вычислительной машины / А. Ньюэлл, Дж. Шоу, Г. Саймон // Хрестоматия по психологии мышления. – М.: 1981. – С.305-327.

Таблиця А.1 – Ідентифікація інцидентів за показниками операційного ризику (для Національного банку)

№	Показник	Інцидент ризику (бінарна характеристика)			
		ризик, пов’язаний з діями працівників та безпекою робочого місця $j=1$	ризик систем і технологій $j=2$	ризик помилки у банківських процесах (ризик взаємовідносин) $j=3$	ризик пов’язаний з зовнішніми чинниками $j=4$
А	Б	1	2	3	4
І. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів					
К1	Кількість банкоматів, кількість платіжних терміналів та інших електронних пристроїв, кількість імпринтерів	0	1	0	1
К2	Збитки через незаконні дії/сумнівні операції з платіжними картками (за платіжними системами - Національна система масових електронних платежів (НСМЕП), Одноемітентні (внутрішньобанківські) платіжні системи, УкрКарт, MasterCard , VISA, Інші банківські платіжні системи , Небанківські платіжні системи (American Express тощо))	1	1	1	1
К3	Частка збитків за підробленими платіжними картками до загальної суми збитків через незаконні дії/сумнівні операції з платіжними картками	0	0	1	1
К4	Частка збитків за втраченими/викраденими платіжними картками до загальної суми збитків через незаконні дії/сумнівні операції з платіжними картками	0	0	0	1
К5	Частка збитків за операціями без пред'явлення картки (операції, які здійснюються через мережу Інтернет, телефон, факс, замовлення поштою тощо) до загальної суми збитків через незаконні дії/сумнівні операції з платіжними картками	1	1	1	1
К6	Частка збитків за картками, які були надіслані емітентом поштою і не отримані держателем до загальної суми збитків через незаконні дії/сумнівні операції з платіжними картками	0	0	1	1
К7	Частка збитків за операціями з використанням особистих даних клієнта (держателя картки) для відкриття банківського рахунку чи отримання доступу до рахунку за підробленими або викраденими документами до загальної суми збитків через незаконні дії/сумнівні операції з платіжними картками	1	0	1	1

Продовження таблиці А.1

А	Б	1	2	3	4
К8	Сума фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (Операції з отримання готівки - операції, які здійснені із застосуванням платіжних карток, емітованих для клієнтів банку)	0	1	1	0
К9	Кількість фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (Операції з отримання готівки - операції, які здійснені із застосуванням платіжних карток, емітованих для клієнтів банку)	0	1	1	0
К10	Сума фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (Безготівкові платежі - операції, які здійснені із застосуванням платіжних карток, емітованих для клієнтів банку)	0	1	1	0
К11	Кількість фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (Безготівкові платежі - операції, які здійснені із застосуванням платіжних карток, емітованих для клієнтів банку)	0	1	1	0
К12	Сума фінансові операції за внутрішньодержавними платіжними системами та міжнародними платіжними системами (Операції з отримання готівки - операції, які здійснені із застосуванням платіжних карток через власну інфраструктуру банку)	0	1	1	0
К13	Кількість фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (Операції з отримання готівки - операції, які здійснені із застосуванням платіжних карток через власну інфраструктуру банку)	0	1	1	0
К14	Сума фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (Безготівкові платежі - операції, які здійснені із застосуванням платіжних карток через власну інфраструктуру банку)	0	1	1	0
К15	Кількість фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (Безготівкові платежі - операції, які здійснені із застосуванням платіжних карток через власну інфраструктуру банку)	0	1	1	0

Продовження таблиціА.1

А	Б	1	2	3	4
К16	Частка кількості програмно-технічних комплексів самообслуговування (ПТКС), що належать суб'єктам господарювання, які уклали агентські договори з банком до загальної кількості ПТКС	0	1	1	1
К17	Середній рівень суми переказів коштів через ПТКС за звітне півріччя - співвідношення загальної суми переказів коштів через ПТКС за звітне півріччя до загальної кількості ПТКС	0	1	1	1
К18	Кількість клієнтів, які використовують систему дистанційного обслуговування рахунків	1	0	1	1
К19	Частка клієнтів, які використовують систему дистанційного обслуговування від загальної кількості клієнтів банку, %	1	0	1	1
К20	Кількість рахунків, обслуговування яких здійснюється дистанційно	1	0	1	1
К21	Кількість недіючих рахунків клієнтів	1	0	1	1
К22	Сума залишку коштів за недіючими рахунками	1	0	1	1
ІІ. Операційний ризик, пов'язаний з власною діяльністю банку					
К23	Кількість випадків недорезервування коштів під час контролю за щоденними залишками	1	1	1	1
К24	Кількість порушень, виявлених Національним банком України	1	0	1	0
К25	Сплачено банком штрафів за виявлені Національним банком України порушення	1	0	1	0
К26	Сума заборгованості за простроченими та сумнівними до отримання нарахованими доходами (за операціями на міжбанківському ринку)	1	1	1	1
К27	Сума заборгованості за простроченими та сумнівними до отримання нарахованими доходами (за кредитними операціями з клієнтами)	1	1	1	1
К28	Сума заборгованості за простроченими та сумнівними до отримання нарахованими доходами (за операціями з цінними паперами)	1	1	1	1
К29	Сума заборгованості за простроченими та сумнівними до отримання нарахованими доходами (за іншими операціями)	1	1	1	1
К30	Кількість фінансових операцій, щодо яких надходили файли про відмову від взяття на облік	1	1	0	0
К31	Кількість фінансових операцій, які були анульовані після надання інформації до ДКФМУ	1	1	0	0

Таблиця А.1 – Таблиця відповідності показників визначеним банківським установам в рамках оцінки операційного ризику

№	Показник	Банківська установа			
		А	Б	В	Г
А	Б	1	2	3	4
І. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів					
К1	Кількість банкоматів, кількість платіжних терміналів та інших електронних пристроїв, кількість імпринтерів	5765	4846	3216	3
К2	Збитки через незаконні дії/сумнівні операції з платіжними картками	2625	951	5195	0
К3	Частка збитків за підробленими платіжними картками до загальної суми збитків через незаконні дії/сумнівні операції з платіжними картками	0,34	0,95	1,00	0,00
К4	Частка збитків за втраченими/викраденими платіжними картками до загальної суми збитків через незаконні дії/сумнівні операції з платіжними картками	0,00	0,05	0,00	0,00
К5	Частка збитків за операціями без пред'явлення картки (операції, які здійснюються через мережу Інтернет, телефон, факс, замовлення поштою тощо) до загальної суми збитків через незаконні дії/сумнівні операції з платіжними картками	0,64	0,00	0,00	0,00
К6	Частка збитків за картками, які були надіслані емітентом поштою і не отримані держателем до загальної суми збитків через незаконні дії/сумнівні операції з платіжними картками	0,00	0,00	0,00	0,00
К7	Частка збитків за операціями з використанням особистих даних клієнта (держателя картки) для відкриття банківського рахунку чи отримання доступу до рахунку за підробленими або викраденими документами до загальної суми збитків через незаконні дії/сумнівні операції з платіжними картками	0,00	0,00	0,00	0,00
К8	Сума фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (Операції з отримання готівки - операції, які здійснені із застосуванням платіжних карток, емітованих для клієнтів банку)	2355220,78	4671933,67	1906378,70	3765464,91
К9	Кількість фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (Операції з отримання готівки - операції, які здійснені із застосуванням платіжних карток, емітованих для клієнтів банку)	3031738,00	8433220,00	3592,00	6232179,00
К10	Сума фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (Безготівкові платежі - операції, які здійснені із застосуванням платіжних карток, емітованих для клієнтів банку)	145167,98	51197,99	162452,13	7,24
К11	Кількість фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (Безготівкові платежі - операції, які здійснені із застосуванням платіжних	432306,00	576748,00	506776,00	61,00

	карток, емітованих для клієнтів банку)				
К12	Сума фінансові операції за внутрішньодержавними платіжними системами та міжнародними платіжними системами (Операції з отримання готівки - операції, які здійснені із застосуванням платіжних карток через власну інфраструктуру банку)	2358913,79	4832625,60	3799784,66	1906228,10
К13	Кількість фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (Операції з отримання готівки - операції, які здійснені із застосуванням платіжних карток через власну інфраструктуру банку)	2986116,00	8556620,00	6246350,00	3542,00
К14	Сума фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (Безготівкові платежі - операції, які здійснені із застосуванням платіжних карток через власну інфраструктуру банку)	307398,24	1335,46	31807,46	0,00
К15	Кількість фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (Безготівкові платежі - операції, які здійснені із застосуванням платіжних карток через власну інфраструктуру банку)	1088241,00	232223,00	97902,00	0,00
К16	Частка кількості програмно-технічних комплексів самообслуговування (ПТКС), що належать суб'єктам господарювання, які уклали агентські договори з банком до загальної кількості ПТКС	1,00	0,00	1,00	0,00
К17	Середній рівень суми переказів коштів через ПТКС за звітне півріччя - співвідношення загальної суми переказів коштів через ПТКС за звітне півріччя до загальної кількості ПТКС	191,46	0,00	168,28	0,00
К18	Кількість клієнтів, які використовують систему дистанційного обслуговування рахунків	58332,00	6114,00	29267,00	611,00
К19	Частка клієнтів, які використовують систему дистанційного обслуговування від загальної кількості клієнтів банку, %	6,10	0,01	1,51	11,88
К20	Кількість рахунків, обслуговування яких здійснюється дистанційно	118991,00	12591,00	62126,00	1053,00
К21	Кількість недіючих рахунків клієнтів	2920	24141	3711	34
К22	Сума залишку коштів за недіючими рахунками	2052,38	1185,92	14857,34	12,95
II. Операційний ризик, пов'язаний з власною діяльністю банку					
К23	Кількість випадків недорезервування коштів під час контролю за щоденними залишками	0	0	6	0
К24	Кількість порушень, виявлених Національним банком України	18	68	14	28
К25	Сплачено банком штрафів за виявлені Національним банком України порушення	5,78	574,61	91,66	5190,21
К26	Сума заборгованості за простроченими та сумнівними до отримання нарахованими доходами (за операціями на міжбанківському ринку)	2123,49	0	6275,77	0
К27	Сума заборгованості за простроченими та сумнівними до отримання нарахованими	333763,8	272821,96	1500132,48	1519,06

	доходами (за кредитними операціями з клієнтами)				
К28	Сума заборгованості за простроченими та сумнівними до отримання нарахованими доходами (за операціями з цінними паперами)	13680,85	3976,73	7286,71	0
К29	Сума заборгованості за простроченими та сумнівними до отримання нарахованими доходами (за іншими операціями)	1134,28	1313,64	4275,27	78,48
К30	Кількість фінансових операцій, щодо яких надходили файли про відмову від взяття на облік	14	18	2349	0
К31	Кількість фінансових операцій, які були анульовані після надання інформації до ДКФМУ	4	33	0	0

Таблиця А.2 – Таблиця відповідності показників визначеним інцидентам операційного ризику

№	Показник	Інцидент ризику (бінарна характеристика)			
		ризик, пов’язаний з діями працівників та безпекою робочого місця	ризик систем і технологій	ризик помилки у банківських процесах (ризик взаємовідносин)	ризик пов’язаний з зовнішніми чинниками
А	Б	1	2	3	4
І. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів					
К1	Кількість банкоматів, кількість платіжних терміналів та інших електронних пристроїв, кількість імпринтерів	0	1	0	1
К2	Збитки через незаконні дії/сумнівні операції з платіжними картками	1	1	1	1
К3	Частка збитків за підробленими платіжними картками до загальної суми збитків через незаконні дії/сумнівні операції з платіжними картками	0	0	1	1
К4	Частка збитків за втраченими/викраденими платіжними картками до загальної суми збитків через незаконні дії/сумнівні операції з платіжними картками	0	0	0	1
К5	Частка збитків за операціями без пред'явлення картки (операції, які здійснюються через мережу Інтернет, телефон, факс, замовлення поштою тощо) до загальної суми збитків через незаконні дії/сумнівні операції з платіжними картками	1	1	1	1
К6	Частка збитків за картками, які були надіслані емітентом поштою і не отримані держателем до загальної суми збитків через незаконні дії/сумнівні операції з платіжними картками	0	0	1	1
К7	Частка збитків за операціями з використанням особистих даних клієнта (держателя картки) для відкриття банківського рахунку чи отримання доступу до рахунку за підробленими або викраденими документами до загальної суми збитків через незаконні дії/сумнівні операції з платіжними картками	1	0	1	1
К8	Сума фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (Операції з отримання готівки - операції, які здійснені із застосуванням платіжних карток, емітованих для клієнтів банку)	0	1	1	0
К9	Кількість фінансових операцій за	0	1	1	0

	внутрішньодержавними платіжними системами та міжнародними платіжними системами (Операції з отримання готівки - операції, які здійснені із застосуванням платіжних карток, емітованих для клієнтів банку)				
К10	Сума фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (Безготівкові платежі - операції, які здійснені із застосуванням платіжних карток, емітованих для клієнтів банку)	0	1	1	0
К11	Кількість фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (Безготівкові платежі - операції, які здійснені із застосуванням платіжних карток, емітованих для клієнтів банку)	0	1	1	0
К12	Сума фінансові операції за внутрішньодержавними платіжними системами та міжнародними платіжними системами (Операції з отримання готівки - операції, які здійснені із застосуванням платіжних карток через власну інфраструктуру банку)	0	1	1	0
К13	Кількість фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (Операції з отримання готівки - операції, які здійснені із застосуванням платіжних карток через власну інфраструктуру банку)	0	1	1	0
К14	Сума фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (Безготівкові платежі - операції, які здійснені із застосуванням платіжних карток через власну інфраструктуру банку)	0	1	1	0
К15	Кількість фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (Безготівкові платежі - операції, які здійснені із застосуванням платіжних карток через власну інфраструктуру банку)	0	1	1	0
К16	Частка кількості програмно-технічних комплексів самообслуговування (ПТКС), що належать суб'єктам господарювання, які уклали агентські договори з банком до загальної кількості ПТКС	0	1	1	1
К17	Середній рівень суми переказів коштів через ПТКС за звітне півріччя - співвідношення загальної суми переказів коштів через ПТКС за звітне півріччя до загальної кількості ПТКС	0	1	1	1
К18	Кількість клієнтів, які використовують систему дистанційного обслуговування рахунків	1	0	1	1
К19	Частка клієнтів, які використовують систему дистанційного обслуговування від загальної кількості клієнтів банку, %	1	0	1	1
К20	Кількість рахунків, обслуговування яких здійснюється дистанційно	1	0	1	1
К21	Кількість недіючих рахунків клієнтів	1	0	1	1
К22	Сума залишку коштів за недіючими рахунками	1	0	1	1
II. Операційний ризик, пов'язаний з власною діяльністю банку					
К23	Кількість випадків недорезервування коштів під час контролю за щоденними залишками	1	1	1	1
К24	Кількість порушень, виявлених Національним банком України	1	0	1	0
К25	Сплачено банком штрафів за виявлені Національним банком України порушення	1	0	1	0
К26	Сума заборгованості за простроченими та сумнівними	1	1	1	1

	до отримання нарахованими доходами (за операціями на міжбанківському ринку)				
К27	Сума заборгованості за простроченими та сумнівними до отримання нарахованими доходами (за кредитними операціями з клієнтами)	1	1	1	1
К28	Сума заборгованості за простроченими та сумнівними до отримання нарахованими доходами (за операціями з цінними паперами)	1	1	1	1
К29	Сума заборгованості за простроченими та сумнівними до отримання нарахованими доходами (за іншими операціями)	1	1	1	1
К30	Кількість фінансових операцій, щодо яких надходили файли про відмову від взяття на облік	1	1	0	0
К31	Кількість фінансових операцій, які були анульовані після надання інформації до ДКФМУ	1	1	0	0

Таблиця А.3 – Нормалізовані значення показників кількісної оцінки операційного ризику банківської установи

№	Показник	Банківська установа			
		А	Б	В	Г
А	Б	1	2	3	4
I. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів					
К1	Кількість банкоматів, кількість платіжних терміналів та інших електронних пристроїв, кількість імпринтерів	1,67	1,40	0,93	0,00
К2	Збитки через незаконні дії/сумнівні операції з платіжними картками	1,20	0,43	2,37	0,00
К3	Частка збитків за підробленими платіжними картками до загальної суми збитків через незаконні дії/сумнівні операції з платіжними картками	0,59	1,66	1,75	0,00
К4	Частка збитків за втраченими/викраденими платіжними картками до загальної суми збитків через незаконні дії/сумнівні операції з платіжними картками	0,00	4,00	0,00	0,00
К5	Частка збитків за операціями без пред'явлення картки (операції, які здійснюються через мережу Інтернет, телефон, факс, замовлення поштою тощо) до загальної суми збитків через незаконні дії/сумнівні операції з платіжними картками	3,98	0,02	0,00	0,00
К6	Частка збитків за картками, які були надіслані емітентом поштою і не отримані держателем до загальної суми збитків через незаконні дії/сумнівні операції з платіжними картками	0,00	0,00	0,00	0,00
К7	Частка збитків за операціями з використанням особистих даних клієнта (держателя картки) для відкриття банківського рахунку чи отримання доступу до рахунку за підробленими або викраденими документами до загальної суми збитків через незаконні дії/сумнівні операції з платіжними картками	0,00	0,00	0,00	0,00
К8	Сума фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (Операції з отримання готівки - операції, які здійснені із застосуванням платіжних карток, емітованих для клієнтів банку)	0,74	1,47	0,60	1,19
К9	Кількість фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (Операції з отримання готівки - операції, які здійснені із застосуванням платіжних карток, емітованих для клієнтів банку)	0,69	1,91	0,00	1,41
К10	Сума фінансових операцій за внутрішньодержавними	1,62	0,57	1,81	0,00

	платіжними системами та міжнародними платіжними системами (Безготівкові платежі - операції, які здійснені із застосуванням платіжних карток, емітованих для клієнтів банку)				
К11	Кількість фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (Безготівкові платежі - операції, які здійснені із застосуванням платіжних карток, емітованих для клієнтів банку)	1,14	1,52	1,34	0,00
К12	Сума фінансові операції за внутрішньодержавними платіжними системами та міжнародними платіжними системами (Операції з отримання готівки - операції, які здійснені із застосуванням платіжних карток через власну інфраструктуру банку)	0,73	1,50	1,18	0,59
К13	Кількість фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (Операції з отримання готівки - операції, які здійснені із застосуванням платіжних карток через власну інфраструктуру банку)	0,67	1,92	1,40	0,00
К14	Сума фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (Безготівкові платежі - операції, які здійснені із застосуванням платіжних карток через власну інфраструктуру банку)	3,61	0,02	0,37	0,00
К15	Кількість фінансових операцій за внутрішньодержавними платіжними системами та міжнародними платіжними системами (Безготівкові платежі - операції, які здійснені із застосуванням платіжних карток через власну інфраструктуру банку)	3,07	0,65	0,28	0,00
К16	Частка кількості програмно-технічних комплексів самообслуговування (ПТКС), що належать суб'єктам господарювання, які уклали агентські договори з банком до загальної кількості ПТКС	2,00	0,00	2,00	0,00
К17	Середній рівень суми переказів коштів через ПТКС за звітне півріччя - співвідношення загальної суми переказів коштів через ПТКС за звітне півріччя до загальної кількості ПТКС	2,13	0,00	1,87	0,00
К18	Кількість клієнтів, які використовують систему дистанційного обслуговування рахунків	2,47	0,26	1,24	0,03
К19	Частка клієнтів, які використовують систему дистанційного обслуговування від загальної кількості клієнтів банку, %	1,25	0,00	0,31	2,44
К20	Кількість рахунків, обслуговування яких здійснюється дистанційно	2,44	0,26	1,28	0,02
К21	Кількість недіючих рахунків клієнтів	0,38	3,13	0,48	0,00
К22	Сума залишку коштів за недіючими рахунками	0,45	0,26	3,28	0,00
	II. Операційний ризик, пов'язаний з власною діяльністю банку				
К23	Кількість випадків недорезервування коштів під час контролю за щоденними залишками	0,00	0,00	4,00	0,00
К24	Кількість порушень, виявлених Національним банком України	0,56	2,13	0,44	0,88
К25	Сплачено банком штрафів за виявлені Національним банком України порушення	0,00	0,39	0,06	3,54
К26	Сума заборгованості за простроченими та сумнівними до отримання нарахованими доходами (за операціями на міжбанківському ринку)	1,01	0,00	2,99	0,00
К27	Сума заборгованості за простроченими та сумнівними до отримання нарахованими доходами (за кредитними операціями з клієнтами)	0,63	0,52	2,85	0,00
К28	Сума заборгованості за простроченими та сумнівними	2,19	0,64	1,17	0,00

	до отримання нарахованими доходами (за операціями з цінними паперами)				
К29	Сума заборгованості за простроченими та сумнівними до отримання нарахованими доходами (за іншими операціями)	0,67	0,77	2,51	0,05
К30	Кількість фінансових операцій, щодо яких надходили файли про відмову від взяття на облік	0,02	0,03	3,95	0,00
К31	Кількість фінансових операцій, які були анульовані після надання інформації до ДКФМУ	0,43	3,57	0,00	0,00

Таблиця А.4 – Зведена таблиця ознак кількісної оцінки операційного ризику комерційного банку А

№	Показник (нормалізоване значення) (результативна ознака)	Інцидент ризику (факторні ознаки)			
		j=1	*j=2*	*j=3*	*j=4*
А	Б	1	2	3	4
І. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів					
К1	1,67	0	1	0	1
К2	1,20	1	1	1	1
К3	0,59	0	0	1	1
К4	0,00	0	0	0	1
К5	3,98	1	1	1	1
К6	0,00	0	0	1	1
К7	0,00	1	0	1	1
К8	0,74	0	1	1	0
К9	0,69	0	1	1	0
К10	1,62	0	1	1	0
К11	1,14	0	1	1	0
К12	0,73	0	1	1	0
К13	0,67	0	1	1	0
К14	3,61	0	1	1	0
К15	3,07	0	1	1	0
К16	2,00	0	1	1	1
К17	2,13	0	1	1	1
К18	2,47	1	0	1	1
К19	1,25	1	0	1	1
К20	2,44	1	0	1	1
К21	0,38	1	0	1	1
К22	0,45	1	0	1	1
ІІ. Операційний ризик, пов'язаний з власною діяльністю банку					
К23	0,00	1	1	1	1
К24	0,56	1	0	1	0
К25	0,00	1	0	1	0
К26	1,01	1	1	1	1
К27	0,63	1	1	1	1
К28	2,19	1	1	1	1
К29	0,67	1	1	1	1
К30	0,02	1	1	0	0
К31	0,43	1	1	0	0

Таблиця А.5 – Зведена таблиця ознак кількісної оцінки операційного ризику комерційного банку Б

№	Показник (нормалізоване значення) (результативна ознака)	Інцидент ризику (факторні ознаки)			
		j=1	*j=2*	*j=3*	*j=4*
А	Б	1	2	3	4

I. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів					
К1	1,40	0	1	0	1
К2	0,43	1	1	1	1
К3	1,66	0	0	1	1
К4	4,00	0	0	0	1
К5	0,02	1	1	1	1
К6	0,00	0	0	1	1
К7	0,00	1	0	1	1
К8	1,47	0	1	1	0
К9	1,91	0	1	1	0
К10	0,57	0	1	1	0
К11	1,52	0	1	1	0
К12	1,50	0	1	1	0
К13	1,92	0	1	1	0
К14	0,02	0	1	1	0
К15	0,65	0	1	1	0
К16	0,00	0	1	1	1
К17	0,00	0	1	1	1
К18	0,26	1	0	1	1
К19	0,00	1	0	1	1
К20	0,26	1	0	1	1
К21	3,13	1	0	1	1
К22	0,26	1	0	1	1
II. Операційний ризик, пов'язаний з власною діяльністю банку					
К23	0,00	1	1	1	1
К24	2,13	1	0	1	0
К25	0,39	1	0	1	0
К26	0,00	1	1	1	1
К27	0,52	1	1	1	1
К28	0,64	1	1	1	1
К29	0,77	1	1	1	1
К30	0,03	1	1	0	0
К31	3,57	1	1	0	0

Таблиця А.6 – Зведена таблиця ознак кількісної оцінки операційного ризику комерційного банку В

№	Показник (нормалізоване значення) (результативна ознака)	Інцидент ризику (факторні ознаки)			
		j=1	*j=2*	*j=3*	*j=4*
А	Б	1	2	3	4
I. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів					
К1	0,93	0	1	0	1
К2	2,37	1	1	1	1
К3	1,75	0	0	1	1
К4	0,00	0	0	0	1
К5	0,00	1	1	1	1
К6	0,00	0	0	1	1
К7	0,00	1	0	1	1
К8	0,60	0	1	1	0
К9	0,00	0	1	1	0
К10	1,81	0	1	1	0
К11	1,34	0	1	1	0
К12	1,18	0	1	1	0
К13	1,40	0	1	1	0
К14	0,37	0	1	1	0
К15	0,28	0	1	1	0

К16	2,00	0	1	1	1
К17	1,87	0	1	1	1
К18	1,24	1	0	1	1
К19	0,31	1	0	1	1
К20	1,28	1	0	1	1
К21	0,48	1	0	1	1
К22	3,28	1	0	1	1
ІІ. Операційний ризик, пов'язаний з власною діяльністю банку					
К23	4,00	1	1	1	1
К24	0,44	1	0	1	0
К25	0,06	1	0	1	0
К26	2,99	1	1	1	1
К27	2,85	1	1	1	1
К28	1,17	1	1	1	1
К29	2,51	1	1	1	1
К30	3,95	1	1	0	0
К31	0,00	1	1	0	0

Таблиця А.7 – Зведена таблиця ознак кількісної оцінки операційного ризику комерційного банку Г

№	Показник (нормалізоване значення) (результативна ознака)	Інцидент ризику (факторні ознаки)			
		j=1	*j=2*	*j=3*	*j=4*
А	Б	1	2	3	4
І. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів					
К1	0,00	0	1	0	1
К2	0,00	1	1	1	1
К3	0,00	0	0	1	1
К4	0,00	0	0	0	1
К5	0,00	1	1	1	1
К6	0,00	0	0	1	1
К7	0,00	1	0	1	1
К8	1,19	0	1	1	0
К9	1,41	0	1	1	0
К10	0,00	0	1	1	0
К11	0,00	0	1	1	0
К12	0,59	0	1	1	0
К13	0,00	0	1	1	0
К14	0,00	0	1	1	0
К15	0,00	0	1	1	0
К16	0,00	0	1	1	1
К17	0,00	0	1	1	1
К18	0,03	1	0	1	1
К19	2,44	1	0	1	1
К20	0,02	1	0	1	1
К21	0,00	1	0	1	1
К22	0,00	1	0	1	1
ІІ. Операційний ризик, пов'язаний з власною діяльністю банку					
К23	0,00	1	1	1	1
К24	0,88	1	0	1	0
К25	3,54	1	0	1	0
К26	0,00	1	1	1	1
К27	0,00	1	1	1	1
К28	0,00	1	1	1	1
К29	0,05	1	1	1	1
К30	0,00	1	1	0	0
К31	0,00	1	1	0	0

Таблиця А.8 – Результати проведення регресійного аналізу встановлення ступеня впливу кожного інциденту на операційний ризик банку Б

Інцидент ризику	Коефіцієнти	Стандартна похибка	t -статистика	Нижні 95%	Верхні 95%
А	1	2	3	4	5
Y-перетин	1,05	0,72	1,47	-0,42	2,52
Ризик, пов'язаний з діями працівників та безпекою робочого місця	0,46	0,42	1,09	-0,40	1,31
Ризик систем і технологій	0,01	0,43	0,02	-0,88	0,89
Ризик помилки у банківських процесах (ризик взаємовідносин)	-0,20	0,58	-0,34	-1,38	0,99
Ризик пов'язаний з зовнішніми чинниками	-0,76	0,43	-1,76	-1,65	0,13

Таблиця А.9 – Результати проведення регресійного аналізу встановлення ступеня впливу кожного інциденту на операційний ризик банку В

Інцидент ризику	Коефіцієнти	Стандартна похибка	t -статистика	Нижні 95%	Верхні 95%
А	1	2	3	4	5
Y-перетин	-0,37	0,73	-0,50	-1,88	1,14
Ризик, пов'язаний з діями працівників та безпекою робочого місця	0,69	0,43	1,61	-0,19	1,57
Ризик систем і технологій	1,20	0,44	2,71	0,29	2,10
Ризик помилки у банківських процесах (ризик взаємовідносин)	0,11	0,59	0,19	-1,10	1,33
Ризик пов'язаний з зовнішніми чинниками	0,69	0,44	1,56	-0,22	1,61

Таблиця А.10 – Результати проведення регресійного аналізу встановлення ступеня впливу кожного інциденту на операційний ризик банку Г

Інцидент ризику	Коефіцієнти	Стандартна похибка	t -статистика	Нижні 95%	Верхні 95%
А	1	2	3	4	5
Y-перетин	0,96	0,62	1,55	-0,31	2,23
Ризик, пов'язаний з діями працівників та безпекою робочого місця	-0,15	0,36	-0,41	-0,89	0,59
Ризик систем і технологій	-0,66	0,37	-1,78	-1,42	0,10
Ризик помилки у банківських процесах (ризик взаємовідносин)	0,45	0,50	0,91	-0,57	1,47
Ризик пов'язаний з зовнішніми чинниками	-0,78	0,37	-2,08	-1,55	-0,01

Таблиця А.11 – Проміжні розрахунки для визначення структури змін інцидентів операційного ризику банку А

№	Середнє квадратичне відхилення показників	Середнє квадратичне відхилення			
		F_1	F_2	F_3	F_4

А	1	2	3	4	5
І. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів					
К1	0,24	0,30	0,13	0,76	0,15
К2	0,00	0,20	0,13	0,02	0,15
К3	0,34	0,30	0,42	0,02	0,15
К4	1,38	0,30	0,42	0,76	0,15
К5	7,88	0,20	0,13	0,02	0,15
К6	1,38	0,30	0,42	0,02	0,15
К7	1,38	0,20	0,42	0,02	0,15
К8	0,19	0,30	0,13	0,02	0,38
К9	0,24	0,30	0,13	0,02	0,38
К10	0,20	0,30	0,13	0,02	0,38
К11	0,00	0,30	0,13	0,02	0,38
К12	0,19	0,30	0,13	0,02	0,38
К13	0,25	0,30	0,13	0,02	0,38
К14	5,94	0,30	0,13	0,02	0,38
К15	3,59	0,30	0,13	0,02	0,38
К16	0,68	0,30	0,13	0,02	0,15
К17	0,91	0,30	0,13	0,02	0,15
К18	1,69	0,20	0,42	0,02	0,15
К19	0,01	0,20	0,42	0,02	0,15
К20	1,62	0,20	0,42	0,02	0,15
К21	0,63	0,20	0,42	0,02	0,15
К22	0,52	0,20	0,42	0,02	0,15
ІІ. Операційний ризик, пов'язаний з власною діяльністю банку					
К23	1,38	0,20	0,13	0,02	0,15
К24	0,37	0,20	0,42	0,02	0,38
К25	1,37	0,20	0,42	0,02	0,38
К26	0,03	0,20	0,13	0,02	0,15
К27	0,29	0,20	0,13	0,02	0,15
К28	1,04	0,20	0,13	0,02	0,15
К29	0,26	0,20	0,13	0,02	0,15
К30	1,32	0,20	0,13	0,76	0,38
К31	0,55	0,20	0,13	0,76	0,38
Загальний рівень	1,08	0,50	0,48	0,34	0,49

Таблиця А.12 – Проміжні розрахунки для визначення структури змін інцидентів операційного ризику банку Б

№	Середнє квадратичне відхилення показників	Середнє квадратичне відхилення			
		F_1	F_2	F_3	F_4
А	1	2	3	4	5
І. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів					
К1	0,42	0,30	0,13	0,76	0,15
К2	0,00	0,20	0,13	0,02	0,15
К3	0,44	0,30	0,42	0,02	0,15
К4	0,44	0,30	0,42	0,76	0,15
К5	0,17	0,20	0,13	0,02	0,15
К6	0,44	0,30	0,42	0,02	0,15
К7	0,17	0,20	0,42	0,02	0,15
К8	6,09	0,30	0,13	0,02	0,38
К9	0,16	0,30	0,13	0,02	0,38
К10	0,44	0,30	0,13	0,02	0,38
К11	0,44	0,30	0,13	0,02	0,38

К12	2,13	0,30	0,13	0,02	0,38
К13	0,08	0,30	0,13	0,02	0,38
К14	0,44	0,30	0,13	0,02	0,38
К15	0,02	0,30	0,13	0,02	0,38
К16	0,00	0,30	0,13	0,02	0,15
К17	0,01	0,30	0,13	0,02	0,15
К18	0,41	0,20	0,42	0,02	0,15
К19	8,41	0,20	0,42	0,02	0,15
К20	0,44	0,20	0,42	0,02	0,15
К21	0,44	0,20	0,42	0,02	0,15
К22	0,44	0,20	0,42	0,02	0,15
ІІ. Операційний ризик, пов'язаний з власною діяльністю банку					
К23	0,44	0,20	0,13	0,02	0,15
К24	2,13	0,20	0,42	0,02	0,38
К25	0,08	0,20	0,42	0,02	0,38
К26	0,44	0,20	0,13	0,02	0,15
К27	0,02	0,20	0,13	0,02	0,15
К28	0,00	0,20	0,13	0,02	0,15
К29	0,01	0,20	0,13	0,02	0,15
К30	0,41	0,20	0,13	0,76	0,38
К31	8,41	0,20	0,13	0,76	0,38
Загальний рівень	1,05	0,50	0,48	0,34	0,49

Таблиця А.13 – Проміжні розрахунки для визначення структури змін інцидентів операційного ризику банку В

№	Середнє квадратичне відхилення показників	Середнє квадратичне відхилення			
		F_1	F_2	F_3	F_4
А	1	2	3	4	5
І. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів					
К1	0,14	0,30	0,13	0,76	0,15
К2	1,13	0,20	0,13	0,02	0,15
К3	0,19	0,30	0,42	0,02	0,15
К4	1,70	0,30	0,42	0,76	0,15
К5	1,70	0,20	0,13	0,02	0,15
К6	1,70	0,30	0,42	0,02	0,15
К7	1,70	0,20	0,42	0,02	0,15
К8	0,50	0,30	0,13	0,02	0,38
К9	1,70	0,30	0,13	0,02	0,38
К10	0,26	0,30	0,13	0,02	0,38
К11	0,00	0,30	0,13	0,02	0,38
К12	0,02	0,30	0,13	0,02	0,38
К13	0,01	0,30	0,13	0,02	0,38
К14	0,87	0,30	0,13	0,02	0,38
К15	1,06	0,30	0,13	0,02	0,38
К16	0,48	0,30	0,13	0,02	0,15
К17	0,32	0,30	0,13	0,02	0,15
К18	0,00	0,20	0,42	0,02	0,15
К19	0,99	0,20	0,42	0,02	0,15
К20	0,00	0,20	0,42	0,02	0,15
К21	0,68	0,20	0,42	0,02	0,15
К22	3,91	0,20	0,42	0,02	0,15
ІІ. Операційний ризик, пов'язаний з власною діяльністю банку					
К23	7,26	0,20	0,13	0,02	0,15

К24	0,75	0,20	0,42	0,02	0,38
К25	1,54	0,20	0,42	0,02	0,38
К26	2,84	0,20	0,13	0,02	0,15
К27	2,38	0,20	0,13	0,02	0,15
К28	0,02	0,20	0,13	0,02	0,15
К29	1,46	0,20	0,13	0,02	0,15
К30	6,98	0,20	0,13	0,76	0,38
К31	1,70	0,20	0,13	0,76	0,38
Загальний рівень	1,19	0,50	0,48	0,34	0,49

Таблиця А.14 – Проміжні розрахунки для визначення структури змін інцидентів операційного ризику банку Г

№	Середнє квадратичне відхилення показників	Середнє квадратичне відхилення			
		F_1	F_2	F_3	F_4
А	1	2	3	4	5
І. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів					
К1	0,14	0,30	0,13	0,76	0,15
К2	0,14	0,20	0,13	0,02	0,15
К3	0,14	0,30	0,42	0,02	0,15
К4	0,14	0,30	0,42	0,76	0,15
К5	0,12	0,20	0,13	0,02	0,15
К6	4,28	0,30	0,42	0,02	0,15
К7	0,12	0,20	0,42	0,02	0,15
К8	0,13	0,30	0,13	0,02	0,38
К9	0,13	0,30	0,13	0,02	0,38
К10	0,14	0,30	0,13	0,02	0,38
К11	0,14	0,30	0,13	0,02	0,38
К12	0,26	0,30	0,13	0,02	0,38
К13	10,07	0,30	0,13	0,02	0,38
К14	0,14	0,30	0,13	0,02	0,38
К15	0,13	0,30	0,13	0,02	0,38
К16	0,14	0,30	0,13	0,02	0,15
К17	0,10	0,30	0,13	0,02	0,15
К18	0,14	0,20	0,42	0,02	0,15
К19	0,14	0,20	0,42	0,02	0,15
К20	0,14	0,20	0,42	0,02	0,15
К21	0,14	0,20	0,42	0,02	0,15
К22	0,14	0,20	0,42	0,02	0,15
ІІ. Операційний ризик, пов'язаний з власною діяльністю банку					
К23	0,14	0,20	0,13	0,02	0,15
К24	0,26	0,20	0,42	0,02	0,38
К25	10,07	0,20	0,42	0,02	0,38
К26	0,14	0,20	0,13	0,02	0,15
К27	0,13	0,20	0,13	0,02	0,15
К28	0,14	0,20	0,13	0,02	0,15
К29	0,10	0,20	0,13	0,02	0,15
К30	0,14	0,20	0,13	0,76	0,38
К31	0,14	0,20	0,13	0,76	0,38
Загальний рівень	0,96	0,50	0,48	0,34	0,49

Таблиця А.15 – Встановлення ступеня впливу кожного інциденту на операційний ризик банку Б (коефіцієнтів стандартизованого рівняння лінійної множинної регресії)

Інцидент операційного ризику	Коефіцієнти стандартизованого рівняння лінійної множинної регресії	Абсолютні коефіцієнти стандартизованого рівняння лінійної множинної регресії (взяті по модулю)	Скореговані коефіцієнти стандартизованого рівняння лінійної множинної регресії
А	1	2	3
F1 ризик, пов'язаний з діями працівників та безпекою робочого місця	0,22	0,22	0,34
F2 ризик систем і технологій	0,00	0,00	0,01
F3 ризик помилки у банківських процесах (ризик взаємовідносин)	-0,06	0,06	0,10
F4 ризик пов'язаний з зовнішніми чинниками	-0,36	0,36	0,56

Таблиця А.16 – Встановлення ступеня впливу кожного інциденту на операційний ризик банку В (коефіцієнтів стандартизованого рівняння лінійної множинної регресії)

Інцидент операційного ризику	Коефіцієнти стандартизованого рівняння лінійної множинної регресії	Абсолютні коефіцієнти стандартизованого рівняння лінійної множинної регресії (взяті по модулю)	Скореговані коефіцієнти стандартизованого рівняння лінійної множинної регресії
А	1	2	3
F1 ризик, пов'язаний з діями працівників та безпекою робочого місця	0,29	0,29	0,27
F2 ризик систем і технологій	0,48	0,48	0,44
F3 ризик помилки у банківських процесах (ризик взаємовідносин)	0,03	0,03	0,03
F4 ризик пов'язаний з зовнішніми чинниками	0,28	0,28	0,26

Таблиця А.17 – Встановлення ступеня впливу кожного інциденту на операційний ризик банку Г (коефіцієнтів стандартизованого рівняння лінійної множинної регресії)

Інцидент операційного ризику	Коефіцієнти стандартизованого рівняння лінійної множинної регресії	Абсолютні коефіцієнти стандартизованого рівняння лінійної множинної регресії (взяті по модулю)	Скореговані коефіцієнти стандартизованого рівняння лінійної множинної регресії
А	1	2	3
F1 ризик, пов'язаний з діями працівників та безпекою робочого місця	-0,08	0,08	0,08

F2 ризик систем і технологій	-0,33	0,33	0,34
F3 ризик помилки у банківських процесах (ризик взаємовідносин)	0,16	0,16	0,16
F4 ризик пов’язаний з зовнішніми чинниками	-0,40	0,40	0,41

Таблиця А.18 – Відображення структури операційного ризику в залежності від формуючих їх інцидентів банку А

№ показника	Значення нормалізованого показника	Інциденти операційного ризику			
		ризик, пов’язаний з діями працівників та безпекою робочого місця $j=1$	ризик систем і технологій $j=2$	ризик помилки у банківських процесах (ризик взаємовідносин) $j=3$	ризик пов’язаний з зовнішніми чинниками $j=4$
		Вагові коефіцієнти інцидентів операційного ризику			
		0,13	0,39	0,28	0,20
А	1	2	3	4	5
І. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів					
К1	1,67	0,21	0,65	0,47	0,33
К2	1,20	0,15	0,47	0,34	0,24
К3	0,59	0,08	0,23	0,17	0,12
К4	0,00	0,00	0,00	0,00	0,00
К5	3,98	0,51	1,56	1,13	0,78
К6	0,00	0,00	0,00	0,00	0,00
К7	0,00	0,00	0,00	0,00	0,00
К8	0,74	0,09	0,29	0,21	0,15
К9	0,69	0,09	0,27	0,19	0,13
К10	1,62	0,21	0,63	0,46	0,32
К11	1,14	0,15	0,45	0,32	0,22
К12	0,73	0,09	0,29	0,21	0,14
К13	0,67	0,09	0,26	0,19	0,13
К14	3,61	0,46	1,42	1,02	0,71
К15	3,07	0,39	1,20	0,87	0,60
К16	2,00	0,26	0,78	0,57	0,39
К17	2,13	0,27	0,83	0,60	0,42
К18	2,47	0,32	0,97	0,70	0,49
К19	1,25	0,16	0,49	0,35	0,25
К20	2,44	0,31	0,96	0,69	0,48
К21	0,38	0,05	0,15	0,11	0,07
К22	0,45	0,06	0,18	0,13	0,09
ІІ. Операційний ризик, пов'язаний з власною діяльністю банку					
К23	0,00	0,00	0,00	0,00	0,00
К24	0,56	0,07	0,22	0,16	0,11
К25	0,00	0,00	0,00	0,00	0,00
К26	1,01	0,13	0,40	0,29	0,20
К27	0,63	0,08	0,25	0,18	0,12
К28	2,19	0,28	0,86	0,62	0,43
К29	0,67	0,09	0,26	0,19	0,13
К30	0,02	0,00	0,01	0,01	0,00
К31	0,43	0,06	0,17	0,12	0,08
Середнє значення	X	0,18	0,09	0,05	0,02

нормалізованих зважених показників на вагові коефіцієнти інцидентів операційного ризику					

Таблиця А.19 – Відображення структури операційного ризику в залежності від формуючих їх інцидентів банку Б

№ показника	Значення нормалізованого показника	Інциденти операційного ризику			
		ризик, пов'язаний з діями працівників та безпекою робочого місця $j=1$	ризик систем і технологій $j=2$	ризик помилки у банківських процесах (ризик взаємовідносин) $j=3$	ризик пов'язаний з зовнішніми чинниками $j=4$
		Вагові коефіцієнти інцидентів операційного ризику			
		0,34	0,01	0,10	0,56
А	1	2	3	4	5
І. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів					
К1	0,02	0,01	0,00	0,00	0,01
К2	0,65	0,22	0,00	0,06	0,36
К3	0,00	0,00	0,00	0,00	0,00
К4	0,00	0,00	0,00	0,00	0,00
К5	0,26	0,09	0,00	0,03	0,14
К6	0,00	0,00	0,00	0,00	0,00
К7	0,26	0,09	0,00	0,03	0,14
К8	3,13	1,06	0,02	0,31	1,74
К9	0,26	0,09	0,00	0,03	0,15
К10	0,00	0,00	0,00	0,00	0,00
К11	0,00	0,00	0,00	0,00	0,00
К12	2,13	0,72	0,01	0,21	1,18
К13	0,39	0,13	0,00	0,04	0,22
К14	0,00	0,00	0,00	0,00	0,00
К15	0,52	0,18	0,00	0,05	0,29
К16	0,64	0,22	0,00	0,06	0,35
К17	0,77	0,26	0,00	0,08	0,43
К18	0,03	0,01	0,00	0,00	0,02
К19	3,57	1,21	0,02	0,35	1,99
К20	0,00	0,00	0,00	0,00	0,00
К21	0,00	0,00	0,00	0,00	0,00
К22	0,00	0,00	0,00	0,00	0,00
ІІ. Операційний ризик, пов'язаний з власною діяльністю банку					
К23	0,00	0,00	0,00	0,00	0,00
К24	2,13	0,72	0,01	0,21	1,18
К25	0,39	0,13	0,00	0,04	0,22
К26	0,00	0,00	0,00	0,00	0,00
К27	0,52	0,18	0,00	0,05	0,29
К28	0,64	0,22	0,00	0,06	0,35
К29	0,77	0,26	0,00	0,08	0,43
К30	0,03	0,01	0,00	0,00	0,02

К31	3,57	1,21	0,02	0,35	1,99
Середнє значення нормалізованих зважених показників на вагові коефіцієнти інцидентів операційного ризику	0,08	0,00	0,01	0,21	0,08

Таблиця А.20 – Відображення структури операційного ризику в залежності від формуючих їх інцидентів банку В

№ показника	Значення нормалізованого показника	Інциденти операційного ризику			
		ризик, пов'язаний з діями працівників та безпекою робочого місця $j=1$	ризик систем і технологій $j=2$	ризик помилки у банківських процесах (ризик взаємовідносин) $j=3$	ризик пов'язаний з зовнішніми чинниками $j=4$
		Вагові коефіцієнти інцидентів операційного ризику			
		0,27	0,44	0,03	0,26
А	1	2	3	4	5
I. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів					
К1	0,93	0,25	0,41	0,03	0,24
К2	2,37	0,63	1,05	0,07	0,62
К3	1,75	0,46	0,77	0,05	0,46
К4	0,00	0,00	0,00	0,00	0,00
К5	0,00	0,00	0,00	0,00	0,00
К6	0,00	0,00	0,00	0,00	0,00
К7	0,00	0,00	0,00	0,00	0,00
К8	0,60	0,16	0,27	0,02	0,16
К9	0,00	0,00	0,00	0,00	0,00
К10	1,81	0,48	0,80	0,05	0,47
К11	1,34	0,35	0,59	0,04	0,35
К12	1,18	0,31	0,52	0,03	0,31
К13	1,40	0,37	0,62	0,04	0,37
К14	0,37	0,10	0,17	0,01	0,10
К15	0,28	0,07	0,12	0,01	0,07
К16	2,00	0,53	0,89	0,06	0,52
К17	1,87	0,50	0,83	0,06	0,49
К18	1,24	0,33	0,55	0,04	0,33
К19	0,31	0,08	0,14	0,01	0,08
К20	1,28	0,34	0,57	0,04	0,33
К21	0,48	0,13	0,21	0,01	0,13
К22	3,28	0,87	1,45	0,10	0,86
II. Операційний ризик, пов'язаний з власною діяльністю банку					
К23	4,00	1,06	1,77	0,12	1,05
К24	0,44	0,12	0,19	0,01	0,11
К25	0,06	0,02	0,03	0,00	0,02
К26	2,99	0,79	1,32	0,09	0,78
К27	2,85	0,75	1,26	0,08	0,75
К28	1,17	0,31	0,52	0,03	0,31

К29	2,51	0,67	1,11	0,07	0,66
К30	3,95	1,05	1,75	0,12	1,03
К31	0,00	0,00	0,00	0,00	0,00
Середнє значення нормалізованих зважених показників на вагові коефіцієнти інцидентів операційного ризику	0,09	0,26	0,00	0,09	0,09

Таблиця А.21 – Відображення структури операційного ризику в залежності від формуючих їх інцидентів банку Г

№ показника	Значення нормалізованого показника	Інциденти операційного ризику			
		ризик, пов'язаний з діями працівників та безпекою робочого місця $j=1$	ризик систем і технологій $j=2$	ризик помилки у банківських процесах (ризик взаємовідносин) $j=3$	ризик пов'язаний з зовнішніми чинниками $j=4$
		Вагові коефіцієнти інцидентів операційного ризику			
		0,08	0,34	0,16	0,41
А	1	2	3	4	5
I. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів					
К1	0,00	0,00	0,00	0,00	0,00
К2	0,00	0,00	0,00	0,00	0,00
К3	0,00	0,00	0,00	0,00	0,00
К4	0,00	0,00	0,00	0,00	0,00
К5	0,03	0,00	0,01	0,00	0,01
К6	2,44	0,19	0,84	0,40	1,01
К7	0,02	0,00	0,01	0,00	0,01
К8	0,00	0,00	0,00	0,00	0,00
К9	0,00	0,00	0,00	0,00	0,00
К10	0,00	0,00	0,00	0,00	0,00
К11	0,00	0,00	0,00	0,00	0,00
К12	0,88	0,07	0,30	0,14	0,36
К13	3,54	0,28	1,21	0,58	1,46
К14	0,00	0,00	0,00	0,00	0,00
К15	0,00	0,00	0,00	0,00	0,00
К16	0,00	0,00	0,00	0,00	0,00
К17	0,05	0,00	0,02	0,01	0,02
К18	0,00	0,00	0,00	0,00	0,00
К19	0,00	0,00	0,00	0,00	0,00
К20	0,00	0,00	0,00	0,00	0,00
К21	0,00	0,00	0,00	0,00	0,00
К22	0,00	0,00	0,00	0,00	0,00
II. Операційний ризик, пов'язаний з власною діяльністю банку					
К23	0,00	0,00	0,00	0,00	0,00
К24	0,88	0,07	0,30	0,14	0,36
К25	3,54	0,28	1,21	0,58	1,46
К26	0,00	0,00	0,00	0,00	0,00

К27	0,00	0,00	0,00	0,00	0,00
К28	0,00	0,00	0,00	0,00	0,00
К29	0,05	0,00	0,02	0,01	0,02
К30	0,00	0,00	0,00	0,00	0,00
К31	0,00	0,00	0,00	0,00	0,00
Середнє значення нормалізованих зважених показників на вагові коефіцієнти інцидентів операційного ризику	0,00	0,04	0,01	0,06	0,00

Таблиця А.22 – Бінарні характеристики за показниками кількісної оцінки ступеня операційного ризику банку А

№ показника	Інциденти операційного ризику				Сума бінарних характеристик
	ризик, пов’язаний з діями працівників та безпекою робочого місця $j=1$	ризик, пов’язаний з діями працівників та безпекою робочого місця $j=1$	ризик, пов’язаний з діями працівників та безпекою робочого місця $j=1$	ризик, пов’язаний з діями працівників та безпекою робочого місця $j=1$	
I. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів					
К1	1	1	1	1	4
К2	1	1	1	1	4
К3	1	1	1	1	4
К4	0	0	0	0	0
К5	1	1	1	1	4
К6	0	0	0	0	0
К7	0	0	0	0	0
К8	1	1	1	1	4
К9	1	1	1	1	4
К10	1	1	1	1	4
К11	1	1	1	1	4
К12	1	1	1	1	4
К13	1	1	1	1	4
К14	1	1	1	1	4
К15	1	1	1	1	4
К16	1	1	1	1	4
К17	1	1	1	1	4
К18	1	1	1	1	4
К19	1	1	1	1	4
К20	1	1	1	1	4
К21	1	0	1	1	3
К22	1	0	1	1	3
II. Операційний ризик, пов'язаний з власною діяльністю банку					
К23	0	0	0	0	0
К24	1	1	1	1	4
К25	0	0	0	0	0
К26	1	1	1	1	4
К27	0	0	0	0	0

К28	1	1	1	1	4
К29	1	1	1	1	4
К30	0	0	0	0	0
К31	1	0	1	1	3
Разом	-	-	-	-	97

Таблиця А.23 – Бінарні характеристики за показниками кількісної оцінки ступеня операційного ризику банку Б

№ показника	Інциденти операційного ризику				Сума бінарних характеристик
	ризик, пов'язаний з діями працівників та безпекою робочого місця $j=1$	ризик, пов'язаний з діями працівників та безпекою робочого місця $j=1$	ризик, пов'язаний з діями працівників та безпекою робочого місця $j=1$	ризик, пов'язаний з діями працівників та безпекою робочого місця $j=1$	
I. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів					
К1	0	1	0	0	1
К2	1	1	1	1	4
К3	0	0	0	0	0
К4	0	0	0	0	0
К5	1	1	1	0	3
К6	0	0	0	0	0
К7	1	1	1	0	3
К8	1	1	1	1	4
К9	1	1	1	0	3
К10	0	0	0	0	0
К11	0	0	0	0	0
К12	1	1	1	1	4
К13	1	1	1	1	4
К14	0	0	0	0	0
К15	1	1	1	1	4
К16	1	1	1	1	4
К17	1	1	1	1	4
К18	0	1	0	0	1
К19	1	1	1	1	4
К20	0	0	0	0	0
К21	0	0	0	0	0
К22	0	0	0	0	0
II. Операційний ризик, пов'язаний з власною діяльністю банку					
К23	0	0	0	0	0
К24	1	1	1	1	4
К25	1	1	1	1	4
К26	0	0	0	0	0
К27	1	1	1	1	4
К28	1	1	1	1	4
К29	1	1	1	1	4
К30	0	1	0	0	1
К31	1	1	1	1	4
Разом	-	-	-	-	68

Таблиця А.24 – Бінарні характеристики за показниками кількісної оцінки ступеня операційного ризику банку В

№ показника	Інциденти операційного ризику				Сума бінарних характеристик
	ризик, пов’язаний з діями працівників та безпекою робочого місця $j=1$	ризик, пов’язаний з діями працівників та безпекою робочого місця $j=1$	ризик, пов’язаний з діями працівників та безпекою робочого місця $j=1$	ризик, пов’язаний з діями працівників та безпекою робочого місця $j=1$	
I. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів					
К1	1	1	1	1	4
К2	1	1	1	1	4
К3	1	1	1	1	4
К4	0	0	0	0	0
К5	0	0	0	0	0
К6	0	0	0	0	0
К7	0	0	0	0	0
К8	1	1	1	1	4
К9	0	0	0	0	0
К10	1	1	1	1	4
К11	1	1	1	1	4
К12	1	1	1	1	4
К13	1	1	1	1	4
К14	1	0	1	1	3
К15	0	0	1	0	1
К16	1	1	1	1	4
К17	1	1	1	1	4
К18	1	1	1	1	4
К19	0	0	1	0	1
К20	1	1	1	1	4
К21	1	0	1	1	3
К22	1	1	1	1	4
II. Операційний ризик, пов'язаний з власною діяльністю банку					
К23	1	1	1	1	4
К24	1	0	1	1	3
К25	0	0	1	0	1
К26	1	1	1	1	4
К27	1	1	1	1	4
К28	1	1	1	1	4
К29	1	1	1	1	4
К30	1	1	1	1	4
К31	0	0	0	0	0
Разом	-	-	-	-	88

Таблиця А.25 – Бінарні характеристики за показниками кількісної оцінки ступеня операційного ризику банку Г

№ показника	Інциденти операційного ризику				Сума бінарних характеристик
	ризик, пов’язаний з діями працівників та безпекою робочого місця $j=1$	ризик, пов’язаний з діями працівників та безпекою робочого місця $j=1$	ризик, пов’язаний з діями працівників та безпекою робочого місця $j=1$	ризик, пов’язаний з діями працівників та безпекою робочого місця $j=1$	
I. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів					

К1	0	0	0	0	0
К2	0	0	0	0	0
К3	0	0	0	0	0
К4	0	0	0	0	0
К5	0	0	0	0	0
К6	1	1	1	1	4
К7	0	0	0	0	0
К8	0	0	0	0	0
К9	0	0	0	0	0
К10	0	0	0	0	0
К11	0	0	0	0	0
К12	1	1	1	1	4
К13	1	1	1	1	4
К14	0	0	0	0	0
К15	0	0	0	0	0
К16	0	0	0	0	0
К17	1	0	0	0	1
К18	0	0	0	0	0
К19	0	0	0	0	0
К20	0	0	0	0	0
К21	0	0	0	0	0
К22	0	0	0	0	0
ІІ. Операційний ризик, пов'язаний з власною діяльністю банку					
К23	0	0	0	0	0
К24	1	1	1	1	4
К25	1	1	1	1	4
К26	0	0	0	0	0
К27	0	0	0	0	0
К28	0	0	0	0	0
К29	1	0	0	0	1
К30	0	0	0	0	0
К31	0	0	0	0	0
Разом	-	-	-	-	22

Таблиця А.26 – Бінарні характеристики показників кількісної оцінки ступеня операційного ризику банку А

Інцидент ризику	I. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів																					
	К1	*К2*	*К3*	*К4*	*К5*	*К6*	*К7*	*К8*	*К9*	*К10*	*К11*	*К12*	*К13*	*К14*	*К15*	*К16*	*К17*	*К18*	*К19*	*К20*	*К21*	*К22*
F1	1	1	1	0	1	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
F2	1	1	1	0	1	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0
F3	1	1	1	0	1	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
F4	1	1	1	0	1	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

II. Операційний ризик, пов'язаний з власною діяльністю банку								
К23	*К24*	*К25*	*К26*	*К27*	*К28*	*К29*	*К30*	*К31*
0	1	0	1	1	1	1	0	1
0	1	0	1	1	1	1	0	0
0	1	0	1	1	1	1	0	1
0	1	0	1	1	1	1	0	1

Таблиця А.27 – Бінарні характеристики показників кількісної оцінки ступеня операційного ризику банку Б

Інцидент ризику	I. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів																					
	К1	*К2*	*К3*	*К4*	*К5*	*К6*	*К7*	*К8*	*К9*	*К10*	*К11*	*К12*	*К13*	*К14*	*К15*	*К16*	*К17*	*К18*	*К19*	*К20*	*К21*	*К22*
F1	0	1	0	0	1	0	1	1	1	0	0	1	1	0	1	1	1	0	1	0	0	0
F2	1	1	0	0	1	0	1	1	1	0	0	1	1	0	1	1	1	1	1	0	0	0
F3	0	1	0	0	1	0	1	1	1	0	0	1	1	0	1	1	1	0	1	0	0	0
F4	0	1	0	0	0	0	0	1	0	0	0	1	1	0	1	1	1	0	1	0	0	0

II. Операційний ризик, пов'язаний з власною діяльністю банку								
К23	*К24*	*К25*	*К26*	*К27*	*К28*	*К29*	*К30*	*К31*
0	1	1	0	1	1	1	0	1
0	1	1	0	1	1	1	1	1
0	1	1	0	1	1	1	0	1
0	1	1	0	1	1	1	0	1

Таблиця А.28 – Бінарні характеристики показників кількісної оцінки ступеня операційного ризику банку В

Інцидент ризику	I. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів																					
	К1	*К2*	*К3*	*К4*	*К5*	*К6*	*К7*	*К8*	*К9*	*К10*	*К11*	*К12*	*К13*	*К14*	*К15*	*К16*	*К17*	*К18*	*К19*	*К20*	*К21*	*К22*
F1	1	1	1	0	0	0	0	1	0	1	1	1	1	1	0	1	1	1	0	1	1	1
F2	1	1	1	0	0	0	0	1	0	1	1	1	1	0	0	1	1	1	0	1	0	1
F3	1	1	1	0	0	0	0	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1
F4	1	1	1	0	0	0	0	1	0	1	1	1	1	1	0	1	1	1	0	1	1	1

II. Операційний ризик, пов'язаний з власною діяльністю банку								
К23	*К24*	*К25*	*К26*	*К27*	*К28*	*К29*	*К30*	*К31*
1	1	0	1	1	1	1	1	0
1	0	0	1	1	1	1	1	0
1	1	1	1	1	1	1	1	0
1	1	0	1	1	1	1	1	0

Таблиця А.29 – Бінарні характеристики показників кількісної оцінки ступеня операційного ризику банку Г

Інцидент ризику	I. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів																					
	К1	*К2*	*К3*	*К4*	*К5*	*К6*	*К7*	*К8*	*К9*	*К10*	*К11*	*К12*	*К13*	*К14*	*К15*	*К16*	*К17*	*К18*	*К19*	*К20*	*К21*	*К22*
F1	0	0	0	0	0	1	0	0	0	0	0	1	1	0	0	0	1	0	0	0	0	0
F2	0	0	0	0	0	1	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0
F3	0	0	0	0	0	1	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0
F4	0	0	0	0	0	1	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0

II. Операційний ризик, пов'язаний з власною діяльністю банку								
К23	*К24*	*К25*	*К26*	*К27*	*К28*	*К29*	*К30*	*К31*
0	1	1	0	0	0	1	0	0
0	1	1	0	0	0	0	0	0
0	1	1	0	0	0	0	0	0
0	1	1	0	0	0	0	0	0

Таблиця А.30 – Імовірності прийняття бінарними характеристиками значень «0» або «1» в розрізі від j-го (j=1÷4) інциденту для банку Б

Інцидент ризику	b (імовірність прийняття бінарними характеристиками значення «0»)	g (імовірність прийняття бінарними характеристиками значення «1»)
1	0,45	0,55
2	0,35	0,65
3	0,45	0,55
4	0,55	0,45

Таблиця А.31 – Імовірності прийняття бінарними характеристиками значень «0» або «1» в розрізі від j-го (j=1÷4) інциденту для банку В

Інцидент ризику	b (імовірність прийняття бінарними характеристиками значення «0»)	g (імовірність прийняття бінарними характеристиками значення «1»)
1	0,29	0,71
2	0,39	0,61
3	0,19	0,81
4	0,29	0,71

Таблиця А.32 – Імовірності прийняття бінарними характеристиками значень «0» або «1» в розрізі від j-го (j=1÷4) інциденту для банку Г

Інцидент ризику	b (імовірність прийняття бінарними характеристиками значення «0»)	g (імовірність прийняття бінарними характеристиками значення «1»)
1	0,77	0,23
2	0,84	0,16
3	0,84	0,16
4	0,84	0,16

Таблиця А.33 – Проміжні розрахунки для визначення імовірності виникнення інциденту операційного ризику банку А

Інцидент ризику	ln(1-b)/(1-g)	λi	I. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів																					
			L1	L2	L3	L4	L5	L6	L7	L8	L9	L10	L11	L12	L13	L14	L15	L16	L17	L18	L19	L20	L21	L22
F1	1,43	-2,85	-2,85	-2,85	-2,85	0,00	-2,85	0,00	0,00	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85
F2	0,89	-1,79	-1,79	-1,79	-1,79	0,00	-1,79	0,00	0,00	-1,79	-1,79	-1,79	-1,79	-1,79	-1,79	-1,79	-1,79	-1,79	-1,79	-1,79	-1,79	-1,79	0,00	0,00
F3	1,43	-2,85	-2,85	-2,85	-2,85	0,00	-2,85	0,00	0,00	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85
F4	1,43	-2,85	-2,85	-2,85	-2,85	0,00	-2,85	0,00	0,00	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85

Продовження таблиці А.33

Інцидент ризику	II. Операційний ризик, пов'язаний з власною діяльністю банку									L (середнє значення масиву L1-L31)	p(s) імовірність виникнення інциденту операційного ризику
	L23	L24	L25	L26	L27	L28	L29	L30	L31		
F1	0,00	-2,85	0,00	-2,85	-2,85	-2,85	-2,85	0,00	-2,85	-2,30	0,71
F2	0,00	-1,79	0,00	-1,79	-1,79	-1,79	-1,79	0,00	0,00	-1,27	0,59
F3	0,00	-2,85	0,00	-2,85	-2,85	-2,85	-2,85	0,00	-2,85	-2,30	0,71
F4	0,00	-2,85	0,00	-2,85	-2,85	-2,85	-2,85	0,00	-2,85	-2,30	0,71

Таблиця А.34 – Проміжні розрахунки для визначення імовірності виникнення інциденту операційного ризику банку Б

Інцидент ризику	ln(1-b)/(1-g)	λi	I. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів																					
			L1	L2	L3	L4	L5	L6	L7	L8	L9	L10	L11	L12	L13	L14	L15	L16	L17	L18	L19	L20	L21	L22
F1	0,19	-0,39	0,00	-0,39	0,00	0,00	-0,39	0,00	-0,39	-0,39	-0,39	0,00	0,00	-0,39	-0,39	0,00	-0,39	-0,39	-0,39	0,00	-0,39	0,00	0,00	0,00
F2	0,60	-1,20	-1,20	-1,20	0,00	0,00	-1,20	0,00	-1,20	-1,20	-1,20	0,00	0,00	-1,20	-1,20	0,00	-1,20	-1,20	-1,20	-1,20	-1,20	0,00	0,00	0,00
F3	0,19	-0,39	0,00	-0,39	0,00	0,00	-0,39	0,00	-0,39	-0,39	-0,39	0,00	0,00	-0,39	-0,39	0,00	-0,39	-0,39	-0,39	0,00	-0,39	0,00	0,00	0,00
F4	-0,19	0,39	0,00	0,39	0,00	0,00	0,00	0,00	0,00	0,39	0,00	0,00	0,00	0,39	0,39	0,00	0,39	0,39	0,39	0,00	0,39	0,00	0,00	0,00

Продовження таблиці А.34

Інцидент ризику	II. Операційний ризик, пов'язаний з власною діяльністю банку									L (середнє значення масиву L1-L31)	p(s) імовірність виникнення інциденту операційного ризику
	L23	L24	L25	L26	L27	L28	L29	L30	L31		
F1	0,00	-0,39	-0,39	0,00	-0,39	-0,39	-0,39	0,00	-0,39	-0,21	0,50
F2	0,00	-1,20	-1,20	0,00	-1,20	-1,20	-1,20	-1,20	-1,20	-0,77	0,54
F3	0,00	-0,39	-0,39	0,00	-0,39	-0,39	-0,39	0,00	-0,39	-0,21	0,50
F4	0,00	0,39	0,39	0,00	0,39	0,39	0,39	0,00	0,39	0,18	0,41

Таблиця А.35 – Проміжні розрахунки для визначення імовірності виникнення інциденту операційного ризику банку В

Інцидент ризику	ln(1-b)/(1-g)	λi	I. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів																					
			L1	L2	L3	L4	L5	L6	L7	L8	L9	L10	L11	L12	L13	L14	L15	L16	L17	L18	L19	L20	L21	L22
F1	0,89	-1,79	-1,79	-1,79	-1,79	0,00	0,00	0,00	0,00	-1,79	0,00	-1,79	-1,79	-1,79	-1,79	-1,79	0,00	-1,79	-1,79	-1,79	0,00	-1,79	-1,79	-1,79
F2	0,46	-0,92	-0,92	-0,92	-0,92	0,00	0,00	0,00	0,00	-0,92	0,00	-0,92	-0,92	-0,92	-0,92	0,00	0,00	-0,92	-0,92	-0,92	0,00	-0,92	0,00	-0,92
F3	1,43	-2,85	-2,85	-2,85	-2,85	0,00	0,00	0,00	0,00	-2,85	0,00	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85
F4	0,89	-1,79	-1,79	-1,79	-1,79	0,00	0,00	0,00	0,00	-1,79	0,00	-1,79	-1,79	-1,79	-1,79	-1,79	0,00	-1,79	-1,79	-1,79	0,00	-1,79	-1,79	-1,79

Продовження таблиці А.35

Інцидент ризику	II. Операційний ризик, пов'язаний з власною діяльністю банку									L (середнє значення масиву L1-L31)	p(s) імовірність виникнення інциденту операційного ризику
	L23	L24	L25	L26	L27	L28	L29	L30	L31		
F1	-1,79	-1,79	0,00	-1,79	-1,79	-1,79	-1,79	-1,79	0,00	-1,27	0,59
F2	-0,92	0,00	0,00	-0,92	-0,92	-0,92	-0,92	-0,92	0,00	-0,56	0,53
F3	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	-2,85	0,00	-2,30	0,71
F4	-1,79	-1,79	0,00	-1,79	-1,79	-1,79	-1,79	-1,79	0,00	-1,27	0,59

Таблиця А.36 – Проміжні розрахунки для визначення імовірності виникнення інциденту операційного ризику банку Г

Інцидент ризику	ln(1-b)/(1-g)	λi	I. Операційний ризик, пов'язаний з банківським обслуговуванням клієнтів																					
			L1	L2	L3	L4	L5	L6	L7	L8	L9	L10	L11	L12	L13	L14	L15	L16	L17	L18	L19	L20	L21	L22
F1	-1,23	2,46	0,00	0,00	0,00	0,00	0,00	2,46	0,00	0,00	0,00	0,00	0,00	2,46	2,46	0,00	0,00	0,00	2,46	0,00	0,00	0,00	0,00	0,00
F2	-1,65	3,30	0,00	0,00	0,00	0,00	0,00	3,30	0,00	0,00	0,00	0,00	0,00	3,30	3,30	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
F3	-1,65	3,30	0,00	0,00	0,00	0,00	0,00	3,30	0,00	0,00	0,00	0,00	0,00	3,30	3,30	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
F4	-1,65	3,30	0,00	0,00	0,00	0,00	0,00	3,30	0,00	0,00	0,00	0,00	0,00	3,30	3,30	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00

Продовження таблиці А.36

Інцидент ризику	II. Операційний ризик, пов'язаний з власною діяльністю банку									L (середнє значення масиву L1-L31)	p(s) імовірність виникнення інциденту операційного ризику
	L23	L24	L25	L26	L27	L28	L29	L30	L31		
F1	0,00	2,46	2,46	0,00	0,00	0,00	2,46	0,00	0,00	0,56	**0,14**
F2	0,00	3,30	3,30	0,00	0,00	0,00	0,00	0,00	0,00	0,53	**0,10**
F3	0,00	3,30	3,30	0,00	0,00	0,00	0,00	0,00	0,00	0,53	**0,10**
F4	0,00	3,30	3,30	0,00	0,00	0,00	0,00	0,00	0,00	0,53	**0,10**

Таблиця А.37 – Вхідна інформація для визначення імовірності виникнення операційного ризику та проведення його структурного аналізу банку Б

Інцидент ризику	p(s) імовірність виникнення інциденту операційного ризику	Група ризику	Бінарні показники	Структура операційного ризику за інцидентами	Зважена структура операційного ризику за інцидентами
A	1	2	3	4	5
F1	0,50	3	1	25,73	37,95
F2	0,54	4	1	27,70	0,61
F3	0,50	3	1	25,73	11,05
F4	0,41	2	0	20,84	50,38

Таблиця А.38 – Вхідна інформація для визначення імовірності виникнення операційного ризику та проведення його структурного аналізу банку В

Інцидент ризику	p(s) імовірність виникнення інциденту операційного ризику	Група ризику	Бінарні показники	Структура операційного ризику за інцидентами	Зважена структура операційного ризику за інцидентами
A	1	2	3	4	5
F1	0,59	2	0	24,52	27,74
F2	0,53	1	0	21,76	41,16
F3	0,71	4	1	29,20	3,70
F4	0,59	2	0	24,52	27,40

Таблиця А.39 – Вхідна інформація для визначення імовірності виникнення операційного ризику та проведення його структурного аналізу банку Г

Інцидент ризику	p(s) імовірність виникнення інциденту операційного ризику	Група ризику	Бінарні показники	Структура операційного ризику за інцидентами	Зважена структура операційного ризику за інцидентами
A	1	2	3	4	5
F1	0,14	4	1	31,99	10,82
F2	0,10	2	0	22,67	33,22
F3	0,10	2	0	22,67	15,98
F4	0,10	2	0	22,67	39,99

Таблиця А.40 – Показники алгоритму визначення кількісної оцінки ступеня операційного ризику банку Б

№	Показники	Інциденти операційного ризику			
		ризик, пов'язаний з діями працівників та безпекою робочого місця $j=1$	ризик систем і технологій $j=2$	ризик помилки у банківських процесах (ризик взаємовідносин) $j=3$	ризик пов'язаний з зовнішніми чинниками $j=4$
А	В	1	2	3	4
1	Імовірність виникнення j-го інциденту операційного ризику	0,50	0,54	0,50	0,41
2	Гранично допустимий коридор імовірнісної (кількісної) оцінки операційного ризику за кожним j-м інцидентом (за сукупністю s банків)	$0{,}00 \le p_K(H1j) < 0{,}49$			
3	Бінарні показники за j інцидентами операційного ризику	1	1	1	0
4	Імовірність виникнення операційного ризику (кількісна оцінку ступеня операційного ризику)	0,63			

Таблиця А.41 – Показники алгоритму визначення кількісної оцінки ступеня операційного ризику банку В

№	Показники	Інциденти операційного ризику			
		ризик, пов'язаний з діями працівників та безпекою робочого місця $j=1$	ризик систем і технологій $j=2$	ризик помилки у банківських процесах (ризик взаємовідносин) $j=3$	ризик пов'язаний з зовнішніми чинниками $j=4$
А	В	1	2	3	4
1	Імовірність виникнення j-го інциденту операційного ризику	0,59	0,53	0,71	0,59
2	Гранично допустимий коридор імовірнісної (кількісної) оцінки операційного ризику за кожним j-м інцидентом (за сукупністю s банків)	$0{,}00 \le p_K(H1j) < 0{,}60$			
3	Бінарні показники за j інцидентами операційного ризику	0	0	1	0
4	Імовірність виникнення операційного ризику (кількісна оцінку ступеня операційного ризику)	0,16			

Таблиця А.42 – Показники алгоритму визначення кількісної оцінки ступеня операційного ризику банку Г

№	Показники	Інциденти операційного ризику			
		ризик, пов'язаний з діями працівників та безпекою робочого місця $j=1$	ризик систем і технологій $j=2$	ризик помилки у банківських процесах (ризик взаємовідносин) $j=3$	ризик пов'язаний з зовнішніми чинниками $j=4$
А	В	1	2	3	4
1	Імовірність виникнення j-го інциденту операційного ризику	0,14	0,10	0,10	0,10
2	Гранично допустимий коридор імовірнісної (кількісної) оцінки операційного ризику за кожним j-м інцидентом (за сукупністю s банків)	$0{,}00 \le p_K(H1j) < 0{,}11$			
3	Бінарні показники за j інцидентами операційного ризику	1	0	0	0
4	Імовірність виникнення операційного ризику (кількісна оцінку ступеня операційного ризику)	0,16			

Таблиця А.43 – Факторний аналіз структури операційного ризик банку Б

№	Показник	Фактори операційного ризику	
		1 група	2 група
	А	1	2
1	Сума бінарних характеристик відповідності показників інцидентам операційного ризику, од.	43	25
2	Частка кожної групи факторів операційного ризику (в розрізі бінарних характеристик, які приймають значення «1»), част. од.	0,63	0,37
3	Вагові коефіцієнти груп факторів, част. од.	0,71	0,29
4	Зважена частка на вагові коефіцієнти кожної групи факторів операційного ризику, част. од.	0,45	0,11
5	Питома вага впливу груп факторів на рівень операційного ризику, %	80,79	19,21

Таблиця А.44 – Факторний аналіз структури операційного ризик банку В

№	Показник	Фактори операційного ризику	
		1 група	2 група
	А	1	2
1	Сума бінарних характеристик відповідності показників інцидентам операційного ризику, од.	60	28
2	Частка кожної групи факторів операційного ризику (в розрізі бінарних характеристик, які приймають значення «1»), част. од.	0,68	0,32
3	Вагові коефіцієнти груп факторів, част. од.	0,71	0,29
4	Зважена частка на вагові коефіцієнти кожної групи факторів операційного ризику, част. од.	0,48	0,09
5	Питома вага впливу груп факторів на рівень операційного ризику, %	83,97	16,03

Таблиця А.45 – Факторний аналіз структури операційного ризик банку Г

№	Показник	Фактори операційного ризику	
		1 група	2 група
	А	1	2
1	Сума бінарних характеристик відповідності показників інцидентам операційного ризику, од.	0,59	0,41
2	Частка кожної групи факторів операційного ризику (в розрізі бінарних характеристик, які приймають значення «1»), част. од.	0,71	0,29
3	Вагові коефіцієнти груп факторів, част. од.	0,42	0,12
4	Зважена частка на вагові коефіцієнти кожної групи факторів операційного ризику, част. од.	77,93	22,07
5	Питома вага впливу груп факторів на рівень операційного ризику, %	0,59	0,41

The ORX Global Operational Risk Database is the world's largest operational risk loss data resource. At 30 June 2010 the Database contained 177,960 loss events to a total value of €62,000,000,000. The data that ORX collects is confidential. In general therefore ORX only makes data available to member institutions who contribute to the database.

ORX does make however publish a high-level data abstract - the ORX Operational Risk Report. The Report is based on high-level ORX data and offers information on trends in loss data and the changes in the industry operational risk loss profile.

Click here to receive a copy of the ORX June 2010 Operational Risk Report.

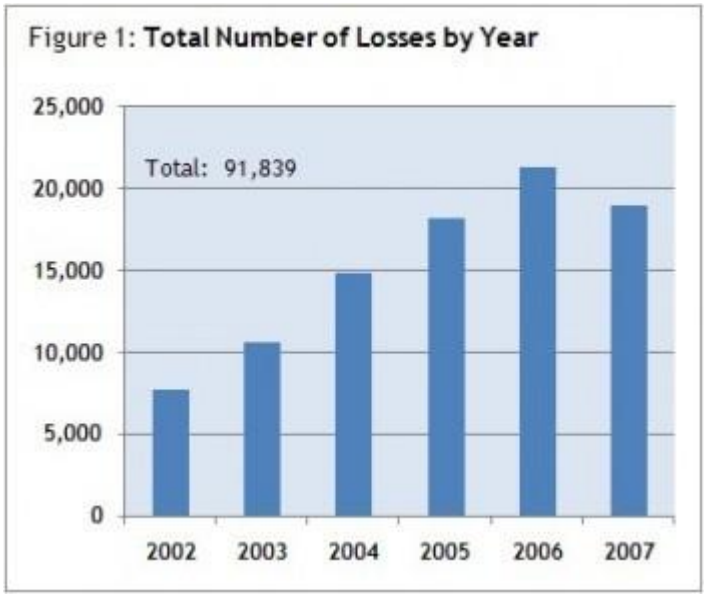
The remainder of this section offers a snapshot of the report content based on data up to 31 December 2007.

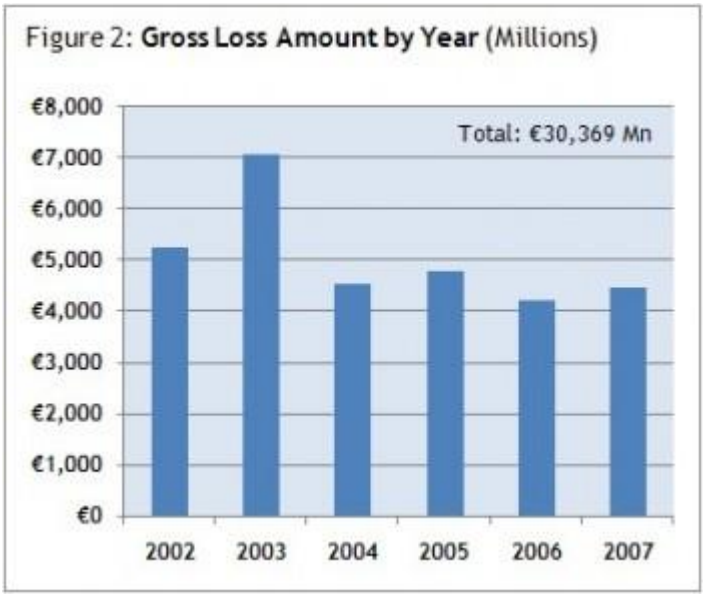
Table 1 below offers a snapshot of how the ORX Global Operational Risk Database has grown since inception. Growth in the database has tracked growth in membership. New member are however only requested to submit historical data which meets current ORX reporting standards. At 31 December 2007 the database contained 91,839 losses to a value of approximately €30,000,000,000.

Table 1: Overall Summary of ORX Data

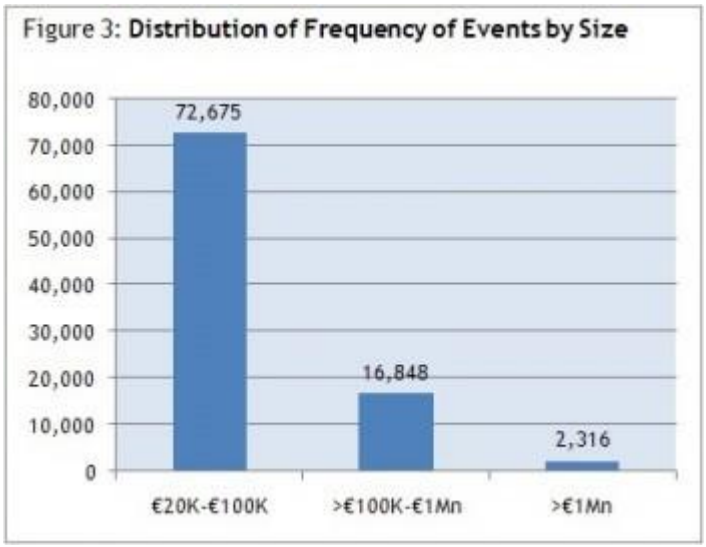
	Total	**2002**	**2003**	**2004**	**2005**	**2006**	**2007**
Total Number of Loss Events	91,839	7,812	10,704	14,892	18,194	21,280	18,957
Total Gross Loss (€ Mn)	30,369	5,263	7,088	4,541	4,790	4,218	4,470
Total Gross Income (€ Mn)	1,839,319	179,707	214,473	302,864	354,461	374,195	413,619

Figures 1 and 2 set out graphically the growth in ORX data by number of events (Figure 1) and by value (Figure 2). It is noticeable that whilst the number of events has steadily grown over the period the value has declined from a peak in 2003.





Figures 3 and 4 present the distribution of events by size. Figure 3 groups losses by size into three buckets and Figure 4, using identically bounded buckets, presents the value of losses in each bucket.



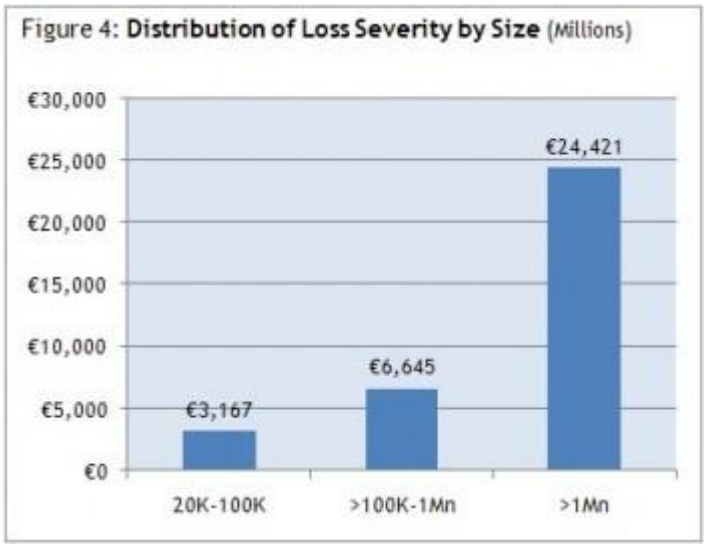


Table 2 offers a different perspective, presenting the frequency of events in the ORX database over a standard Business Line / Event Type matrix. For example approximately 64% (65,000 actual) of ORX losses are Retail Banking, approximately 10% (10,000 actual) are Trading and Sales

Table 2: Relative Number of Losses by Event Type by Business Line

	Internal Fraud	External Fraud	Empolyment Practices	Clients, Products & Business Practices	Disasters & Public Safety	Technology & Infrastructure	Execution, Delivery & Process Management	Malicious Damage	**Total % by Business Line**
Corporate Finance	0.02%	0.09%	0.11%	0.24%	0.00%	0.00%	0.23%	0.00%	0.70%
Trading & Sales	0.08%	0.05%	0.32%	0.59%	0.02%	0.51%	8.26%	0.00%	9.84%
Retail Banking	3.66%	**32.39%**	7.53%	5.60%	0.67%	1.01%	**13.25%**	0.10%	**64.21%**
Commercial Banking	0.15%	3.07%	0.34%	1.21%	0.03%	0.20%	3.73%	0.00%	8.74%
Clearing	0.05%	0.48%	0.12%	0.12%	0.00%	0.13%	1.56%	0.00%	2.45%
Agency Services	0.01%	0.02%	0.07%	0.14%	0.00%	0.04%	1.41%	0.00%	1.70%
Asset Management	0.05%	0.11%	0.14%	0.51%	0.01%	0.07%	1.79%	0.00%	2.67%
Retail Brokerage	0.09%	0.12%	0.48%	1.72%	0.01%	0.04%	0.97%	0.00%	3.43%
Private Banking	0.21%	0.34%	0.14%	1.36%	0.02%	0.04%	2.01%	0.00%	4.12%
Corporate Items	0.04%	0.16%	0.58%	0.30%	0.20%	0.05%	0.80%	0.01%	2.14%
Total % by Event Type	4.36%	**36.84%**	9.83%	**11.77%**	0.97%	2.09%	**34.02%**	0.12%	**100.00%**

Key> 1% - 5% 5% - 10% **>10%**

Table 4 utilizes the same matrix but maps losses by value. For example approximately 28% (€8.4 billion actual) of ORX losses are Retail Banking, approximately 14% (€4.2 billion actual) are Trading and Sales. The contrast, in the instance of some cells, between the frequency of events and severity, is striking.

Table 4: Total Gross Loss by Event Type by Business Line

	Internal Fraud	External Fraud	Empolyment Practices	Clients, Products & Business Practices	Disasters & Public Safety	Technology & Infrastructure	Execution, Delivery & Process Management	Malicious Damage	**Total % by Business Line**
Corporate Finance	0.08%	0.42%	0.18%	**24.79%**	0.00%	0.00%	1.24%	0.00%	**26.71%**
Trading & Sales	1.34%	0.69%	0.30%	4.74%	0.00%	0.28%	7.00%	0.00%	**14.35%**
Retail Banking	1.97%	7.13%	2.12%	8.51%	0.33%	0.61%	7.46%	0.02%	**28.17%**
Commercial Banking	1.04%	2.10%	0.28%	3.35%	0.01%	0.09%	5.08%	0.00%	**11.97%**
Clearing	0.11%	0.26%	0.03%	0.31%	0.00%	0.08%	0.63%	0.00%	1.42%
Agency Services	0.02%	0.03%	0.04%	2.03%	0.00%	0.02%	0.69%	0.00%	2.84%
Asset Management	0.06%	0.05%	0.17%	3.11%	0.00%	0.02%	0.89%	0.00%	4.30%
Retail Brokerage	0.14%	0.09%	0.26%	1.57%	0.01%	0.01%	0.30%	0.00%	2.38%
Private Banking	0.55%	0.20%	0.11%	2.44%	0.00%	0.01%	0.65%	0.00%	3.96%
Corporate Items	0.10%	0.07%	0.33%	1.28%	1.12%	0.03%	0.97%	0.01%	3.90%
Total % by Event Type	5.42%	**11.04%**	3.84%	**52.14%**	1.48%	1.15%	**24.90%**	0.03%	**100.00%**

Key> 1% - 5% 5% - 10% **>10%**

The above offers the highest level overview of the data available in the ORX Global Database. More detail is available in the ORX Operational Risk Report (see above). Beyond this ORX does not make data available to non-members.

http://www.orx.org/orx-data