

Колектив авторів

Керівник авторського колективу д.е.н., професор **Л.О. Примостка** (вступ; розділ 1; п.п.2.4; 5.1–5.3; 5.7; п.п. 6.1–6.5 у співавторстві; розділ 7; п.п. 8.3–8.7; п.п. 10.4 – у співавторстві; п.п. 11.1, 11.3; п.п. 12.1, 12.2, 12.4), к.е.н., професор **І.В. Краснова** (розділ 4, п.п. 4.5 – у співавторстві), д.е.н., професор **О.О.Примостка** (п.п. 2.1– 2.2), к.е.н., доцент **В.В. Лавренюк** (п.п. 5.5–5.6; п.п. 10.1–10.3, 10.5), к.е.н., доцент **П.М. Чуб** (розділ 3; п.п. 5.4; п.п. 6.3–6.5 у співавторстві), к.е.н., доцент **А.В. Нікітін** (п.п. 11.4), к.е.н., доцент **В.Г. Шевалдіна** (п.п. 4.5 – у співавторстві), к.е.н., доцент **О.І. Шварц** (розділ 9), к.е.н., доцент **А.М. Суторміна** (п.п. 8.1 у співавторстві), к.е.н., доцент **К.М. Суторміна** (п.п. 10.4 у співавторстві), к.ф.н., доцент **Є.В. Позднишев** (п.п. 11.5), к.е.н. **Н.С Білань** (п.п. 6.1–6.2 у співавторстві, 8.1 у співавторстві; 8.2), к.е.н. **А.О. Примостка** (п.п. 12.3), **М.Я. Білань** (п.п. 2.3), **І.В. Домінова** (п.п.11.2).

Рецензенти

О. І. Береславська, д.е.н., проф.
(Університет державної фіскальної служби України)

О. Д. Вовчак, д.е.н., проф.
(ДВНЗ «Університет банківської справи»)

О. О. Терещенко, д.е.н., проф.
(Київський національний економічний університет ім. Вадима Гетьмана)

Редакційна колегія фінансово-економічного факультету

Голова редакційної колегії: Хлівний В. К., проф., к.е.н.

Відповідальний секретар редакційної колегії: Мурашко О. В., доц., к.е.н.

Члени редакційної колегії: Аржевітін С. М., д.е.н.; Гаманкова О. О., проф., д.е.н.; Гапонюк М. А., проф., к.е.н.; Майорова Т. В., проф., д.е.н.; Опарін В. М., проф., д.е.н.; Примостка Л. О., проф., д.е.н.; Терещенко О. О., проф., д.е.н.; Федосов В. М., проф., д.е.н.

Рекомендовано до друку Вченою радою КНЕУ
Протокол № 9 від 22.06.2017

У 67 Управління банківськими ризиками [Електронний ресурс]: підручник /
Л. О. Примостка, І. В. Краснова, В. В. Лавренюк та ін. — Київ : КНЕУ, 2018.
— 535, [1] с.
ISBN 978-966-926-201-1

Підручник підготовлено відповідно до програми навчальної дисципліни «Управління банківськими ризиками», включеної до навчального плану підготовки магістрів з банківської справи. У підручнику викладено питання економічної сутності та класифікації ризиків у банківській сфері; принципи побудови та складові системи ризик-менеджменту в банку; прийоми ідентифікації та оцінювання банківських ризиків; методи управління ризиками; інструментарій управління ринковими ризиками; механізми хеджування ризиків; особливості оцінювання системного та комплаєнс ризиків; процедури контролю та моніторингу банківських ризиків. Матеріал викладено з урахуванням вимог Національного банку України щодо організації систем ризик-менеджменту у вітчизняних банках та міжнародного досвіду управління банківськими ризиками. Розгляд базових положень супроводжується значною кількістю прикладів.

Підручник дозволить сформулювати системні знання з теорії та практики управління банківськими ризиками, вивчити методи ідентифікації, оцінювання, контролю та моніторингу банківських ризиків, оволодіти навичками раціональної організації систем ризик-менеджменту в банках.

Для студентів вищих навчальних закладів економічних спеціальностей магістерського рівня підготовки, аспірантів, викладачів, спеціалістів банківської системи.

УДК 336.71:005.52:005.334(075.8)

Розповсюджувати та тиражувати
без офіційного дозволу КНЕУ забороняється

ISBN 978-966-926-201-1

© Л. О. Примостка, І. В. Краснова,
В. В. Лавренюк та ін., 2018
© КНЕУ, 2018

Розділ 10. СИСТЕМНИЙ РИЗИК В БАНКІВСЬКІЙ ДІЯЛЬНОСТІ.	405
10.1. Сутність, джерела та прояви системного ризику в банківській діяльності.	405
10.2. Зв'язок системного ризику з іншими банківськими ризиками	418
10.3. Оцінювання системного ризику	421
10.4. Системний ризик та економічний капітал банку.	428
10.5. Регулювання системного ризику на макро- та макrorівнях	436
 Розділ 11. УПРАВЛІННЯ ФУНКЦІОНАЛЬНИМИ РИЗИКАМИ БАНКУ	 447
11.1. Управління операційно-технологічним ризиком банку	447
11.2. Управління ризиками електронного банкінгу.	459
11.3. Управління стратегічним, репутаційним та юридичним ризиками банку	471
11.4. Управління маркетинговими ризиками банку.	479
11.5. Управління інформаційними ризиками банку.	489
 Розділ 12. ОРГАНІЗАЦІЯ СИСТЕМИ РИЗИК-МЕНЕДЖМЕНТУ БАНКУ.	 503
12.1. Загальні вимоги до побудови системи ризик-менеджменту в банках	503
12.2. Організаційна структура та суб'єкти управління ризиками в банку	508
12.3. Інформаційні технології в системі ризик-менеджменту банку	518
12.4. Внутрішньобанківське документування процесу управління ризиками	526

Розділ 11

УПРАВЛІННЯ ФУНКЦІОНАЛЬНИМИ РИЗИКАМИ БАНКУ

Після вивчення цього розділу Ви будете знати:

- ✓ види функціональних ризиків банку;
- ✓ джерела виникнення та види операційно-технологічних ризиків банку;
- ✓ особливості управління операційно-технологічним ризиком банку;
- ✓ сутність та специфіку ризиків електронного банкінгу;
- ✓ класифікацію ризиків електронного банкінгу;
- ✓ основні методи управління ризиками електронного банкінгу;
- ✓ управління стратегічним ризиком банку;
- ✓ особливості управління ризиком втрати репутації банку;
- ✓ зміст юридичного ризику банку;
- ✓ методи управління маркетинговими ризиками банку;
- ✓ особливості управління інформаційними ризиками банку.

11.1. Управління операційно-технологічним ризиком банку

На банківську діяльність, крім фінансових ризиків, значно впливають *функціональні ризики*, що виникають через неможливість своєчасно і в повному обсязі контролювати фінансово-господарську діяльність, збирати та аналізувати відповідну інформацію. Функціональні ризики пов'язані з виконанням адміністративно-господарських операцій, процесами створення і впровадження інноваційних банківських продуктів і послуг, функціонуванням електронного банкінгу, збором, обробкою, аналізом і передаванням інформації, підготовкою кадрового потенціалу. Всі функціональні ризики банку тісно взаємопов'язані. Функціональні ризики банку не менш небезпечні, ніж фінансові ризики, але їх важче ідентифікувати та оцінити кількісно. Реалізація функціональних ризиків призводить до значних фінансових втрат банку.

Основні різновиди функціональних ризиків банку:

- 1) операційно-технологічний ризик;
- 2) ризик втрати репутації;
- 3) юридичний ризик;

- 4) стратегічний ризик;
- 5) ризик інформаційних технологій;
- 6) ризик електронного банкінгу;
- 7) ризик упровадження інноваційних продуктів і послуг;
- 8) маркетинговий ризик;
- 9) ризик трансакції;
- 10) документарний ризик;
- 11) ризик зловживань.

До класифікації, запропонованої НБУ, включено чотири функціональних ризики: операційно-технологічний, який віднесено до групи ризиків, що можуть бути виміряні кількісно; а також юридичний, стратегічний ризики і ризик втрати репутації. Останні три види ризиків віднесено до групи ризиків, які не піддаються кількісній оцінці.

Функціональні ризики банку можуть бути знижені через удосконалення систем контролю і внутрішнього аудиту, схем документообігу, застосування спеціального програмного забезпечення, що виявляє помилки і локалізує збої в комп'ютерних мережах, відпрацювання систем повноважень і посадових інструкцій, удосконалення технічних засобів зв'язку та передання інформації, а також розробляючи внутрішні методики та техніко-економічне забезпечення окремих операцій. Зниженню таких ризиків сприяє й адекватна ресурсна, матеріально-технічна та кадрова політика банку, підвищення кваліфікації персоналу банку.

Операційно-технологічний ризик банку — це потенційний ризик для довгострокового існування банківської установи, який виникає через недоліки корпоративного управління, системи внутрішнього контролю або інформаційних технологій і процесів обробки інформації з погляду керованості, універсальності, надійності, контрольованості і безперервності роботи [1, 2]. Такі недоліки в роботі банку можуть призвести до фінансових збитків через помилки, невчасне виконання робіт або шахрайство.

Реалізація операційно-технологічного ризику може стати причиною того, що інтереси банку постраждають у якийсь інший спосіб, наприклад, якщо дилери, кредитні працівники або інші працівники банку перевищать свої повноваження чи здійснюватимуть операції з порушенням етичних норм або із занадто високим ризиком. Джерелами виникнення операційно-технологічного ризику можуть бути збої у роботі інформаційних технологій і процесів обробки інформації з погляду керованості, універсальності, надійності, контрольованості і безперервності роботи, у тому числі через неадекватність стратегії, політики і використання інформаційних технологій. Серед інших причин зростання операційно-технологічного ризику банків — непередбачувані події в різних сферах життя суспільства, наприклад стихійні лиха, пожежі, військові дії, анексія територій та інші форс-мажорні обставини (рис. 11.1).

Операційно-технологічний ризик є комплексним видом ризику, який пронизує всю діяльність банку — від проведення певної операції до функціонування банківської установи як єдиного механізму.

Операційно-технологічний ризик пов'язаний з такими видами ризиків:

- ризик людського фактору (помилки, крадіжки, перевищення службових повноважень та ін.);
- ризик процесів (неадекватність процесів чи контролю);
- ризик технологій (помилки обладнання, його невідповідність, системні збої тощо);
- ризик зовнішніх подій (війни, стихійні лиха і т. п.).

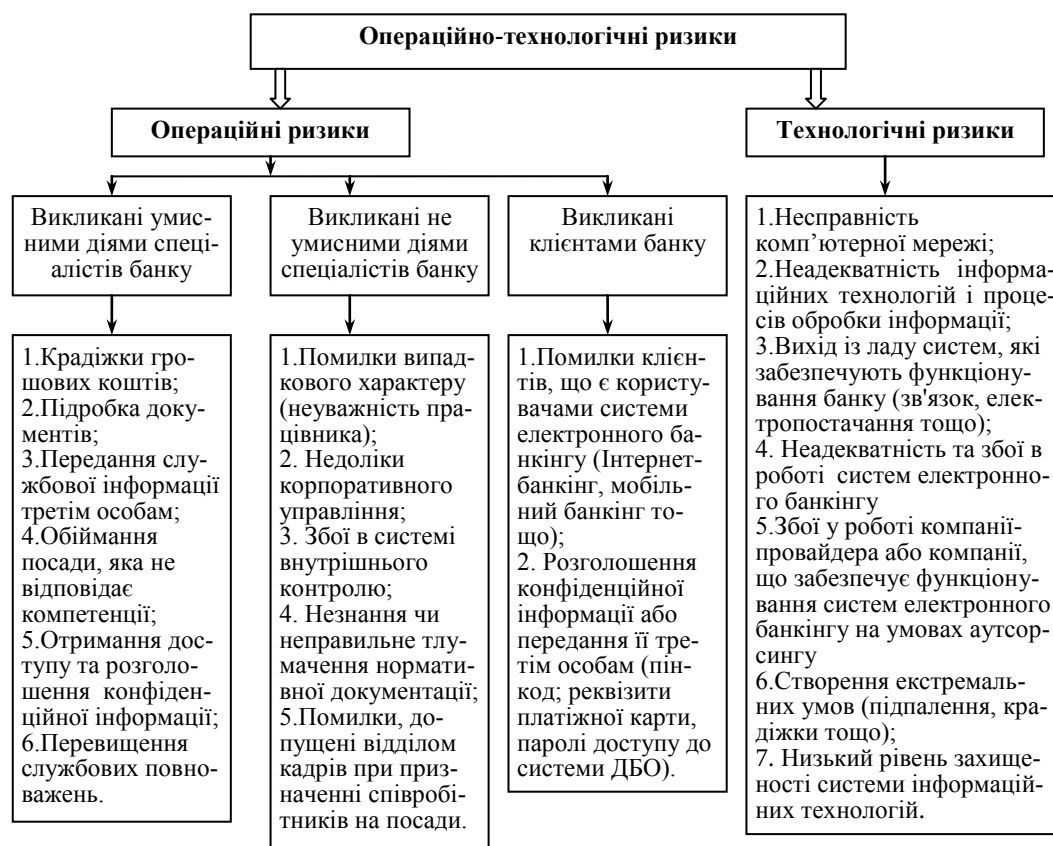


Рис. 11.1. Види операційно-технологічних ризиків банку

За методикою НБУ *для оцінювання величини операційно-технологічного ризику* визначають чотири параметри:

- величина ризику (незначна, помірна, значна);
- якість систем управління ризиком (висока, така, що потребує вдосконалення, низька);
- сукупний ризик (низький, помірний, високий);
- напрям зміни ризику протягом наступного року (такий, що зменшується, стабільний, збільшується).

Параметр сукупний ризик визначається за результатами співставлення перших двох параметрів — величина ризику та сукупний ризик.

Оцінювання якості систем управління операційно-технологічним ризиком банку базується на аналізі таких факторів:

1) існування адекватної, ефективної, доведеної до виконавців 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 та складність обробки операцій порівняно з рівнем розвитку і потужністю операційних і контрольних систем;

3) імовірність технологічних та операційних збоїв, перевищення повноважень персоналом, недоліки в попередньому аналізі операцій під час прийняття рішень, а також відсутність (у тому числі тимчасова) моніторингу чи реєстрації операцій з клієнтами або контрагентами;

4) наявність та дотримання банком технологічних карт проведення банківських операцій;

5) наявність, кількість, причини та характер порушень процедур адміністративного і облікового контролю;

6) потенційна можливість фінансових збитків унаслідок:

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

7) історія та характер скарг і звернень клієнтів до банку, пов'язаних з недоліками роботи операційних систем та реакція на них банку;

8) обсяги та адекватність засобів контролю за банківським програмним забезпеченням та його супроводженням, а також іншими послугами, які здійснюються із залученням третіх осіб (аутсорсингу);

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 в банку методик та технологій для:

- визначення інформаційних потреб для ефективного управління банком;
- визначення архітектури інформаційно-аналітичних систем банку;
- забезпечення достовірності та збереження інформації (наприклад, створення, опрацювання, зберігання та надання даних);
- планування заходів для забезпечення безперервної діяльності;
- забезпечення своєчасної підготовки і використання управлінської інформації;

11) рівень кваліфікації та навичок менеджерів і працівників банку;

12) існування механізмів контролю точності інформації, належних облікових підходів і дотримання нормативних положень та законів.

Врахування цих факторів оцінювання операційно-технологічного ризику дозволяє визначити, в якій сфері діяльності банку існують проблеми або де вони можуть з'явитися в майбутньому. Отримана інформація є основою для визначення профілю операційно-технологічного ризику банку з метою зосередження зусиль на найризикованіших напрямках його діяльності.

Базельським комітетом з банківського нагляду виділено три основні **методи оцінювання операційно-технологічного ризику банку**:

- 1) метод ключового індикатора;
- 2) стандартизований метод;
- 3) метод поглиблених вимірів.

Ці методи оцінки використовуються для розрахунку можливих збитків банку від операційно-технологічного ризику з метою формування відповідних резервів та визначення величини капіталу банку, необхідної для покриття збитків у разі реалізації ризику.

1. **Метод ключового індикатора** ґрунтується на розподілі коефіцієнта операційного ризику при використанні єдиного індикатора як орієнтовного показника для всієї «сфери дії» операційного ризику (діяльності банку взагалі). За індикатор пропонується взяти показник валового прибутку банку. Кожен банк створює резерв на покриття збитків від операційного ризику, який обчислюється як добуток фіксованого коефіцієнта операційного ризику банку (α), який визначається за історичними даними, та прибутку банку [24].

Цей метод оцінювання операційно-технологічного ризику досить простий та універсальний, однак він може використовуватись у невеликих банках з обмеженим і доволі простим асортиментом послуг. Банки ж, які працюють на міжнародних ринках, мають застосовувати більш точні методи оцінки величини операційного ризику з урахуванням усього спектра банківських продуктів та послуг. Відповідно до рекомендацій Базельського комітету коефіцієнт α дорівнює 15%.

2. **Стандартизований метод** вважається більш досконалим підходом до оцінювання величини операційного ризику. Стандартизований метод відрізняється від методу ключового індикатора тим, що в ньому враховується спеціалізація стандартизованих підрозділів і бізнес-напрямів діяльності банку. Для кожного бізнес-напрямку визначається індикатор, який відображає обсяг та інтенсивність цього виду діяльності банку. Такий індикатор є приблизною оцінкою суми збитків від операційного ризику в межах кожного бізнес-напрямку банку. Для кожного підрозділу та бізнес-напрямку визначаються відповідні індикатори, які використовуються при визначенні операційного ризику банку (табл. 11.1). За кожним напрямом діяльності банку розраховують добуток від множення фінансового індикатора на коефіцієнт F , який відображає залежність показника обсягу збитків, завданих банку в разі реалізації операційного ризику у цьому секторі за минулий період, від фінансового індикатора (характеризує даний банк у конкретному виді діяльності), скоригованого на стандартний показник, встановлений органами банківського нагляду. Отримана сума є тим об-

сягом капіталу, яку банку необхідно зарезервувати для покриття збитків в разі реалізації операційного ризику.

Таблиця 11.1

**ІНДИКАТОРИ ДЛЯ РОЗРАХУНКУ РЕЗЕРВНОГО КАПІТАЛУ
НА ПОКРИТТЯ ЗБИТКІВ ВІД ОПЕРАЦІЙНОЇ ДІЯЛЬНОСТІ БАНКУ**

Підрозділ	Напрямок діяльності	Індикатор
Інвестиційна діяльність банку	Корпоративні фінанси Торговельна діяльність	Валовий прибуток Валовий прибуток
Банківська діяльність	Роздрібна діяльність Комерційна діяльність Платежі та розрахунки	Щорічні середні активи Щорічні середні активи Щорічний обсяг розрахунків
Інше	Роздрібна брокерська діяльність Управління активами	Валовий прибуток Сукупний обсяг активів в управлінні

Наприклад, величина капіталу, необхідного для покриття операційного ризику у сфері роздрібно-брокерської діяльності банку, розраховується так:

$$Kr = Fr \cdot Вп, \quad (11.1)$$

де Fr — коефіцієнт, який застосовується до даного виду діяльності (задається регулятивним органом); $Вп$ — індикатор для даного напрямку діяльності (для роздрібного бізнесу — це валовий прибуток).

Загальний показник суми необхідного капіталу для покриття операційного ризику банку за даним методом — це сума капіталу, яку необхідно резервувати за кожним окремим напрямом діяльності банку.

Стандартизований метод доцільно використовувати в тому випадку, коли за браком внутрішньої системи збору даних про ризики й збитки банку, до яких ці ризики призвели, банк не може застосувати більш досконалі методи оцінювання операційного ризику. Оскільки у вітчизняних банках ще не достатньо розвинені внутрішні бази даних та методи зіставлення показників ризикованості й збитків, то перевага надається саме стандартизованому методу. Використання стандартизованого методу оцінювання операційного ризику поступово формує базу даних банку для подальшого розвитку досконаліших методів оцінювання операційного ризику [24].

3. Метод поглиблених вимірів операційного ризику банку реалізується в кількох етапів:

- діяльність банку розглядається як певна сукупність напрямів, за кожним з яких розраховується спектр (набір можливих видів) операційних збитків;
- у межах кожної комбінації «напрямок діяльності/тип можливих втрат (збитків)» регулюючим органом визначається індикатор схильності до ризику (EI), який відображає ступінь схильності до ризику того чи іншого напрямку діяльності банку;

• окрім індикатора схильності до ризику, для кожної комбінації «напряму діяльності/тип можливих втрат» банки розраховують, ґрунтуючись на власній внутрішній інформації про збитки, параметр, який відображає імовірність збиткової події (PE), а також розмір збитку у разі настання вказаної події (LGE). Результат використовується для розрахунку очікуваного збитку (EL) за кожною комбінацією «напряму діяльності/тип можливих втрат»;

• регулюючий орган додає коефіцієнт γ для кожної комбінації «напряму діяльності/тип можливих втрат», який переводить отриманий показник очікуваного збитку (EL) у показник суми капіталу, необхідного для його покриття. Сукупний обсяг необхідного резервного капіталу для конкретного банку визначається за допомогою простої суми всіх результатів за кожним із виокремлених напрямів діяльності банку. Величина резервного капіталу, необхідного для покриття можливих збитків від операційного ризику (KR), розраховується за формулою:

$$KR = \sum_{i=1}^n i \sum_{j=1}^m j [\gamma(i, j) \cdot EI(i, j) \cdot PE(i, j) \cdot LGE(i, j)], \quad (11.2)$$

де i — напряму діяльності ($i = 1, n$);

j — тип ризику ($j = 1, m$);

$EI(i, j)$ — приблизний розмір схильності до операційного ризику конкретного напрямку діяльності;

$PE(i, j)$ — імовірність збиткової події, тобто можливість настання певної події, яка може призвести до збитків (LGE);

$LGE(i, j)$ — величина збитків при настанні певної події.

Показник PE виражається як у відносному вимірі, так і у вартісному, урахувавши те, що визначення показників EI , PE та LGE взаємопов'язані. Наприклад, PE може бути виражений як відношення «кількість збиткових подій / кількість операцій», тоді значення LGE , у свою чергу, дорівнюватиме відношенню «середня сума збитку / сума операції». Кожен банк має використовувати власні історичні дані про збитки і схильність до ризику, комбінуючи їх з відповідними відібраними даними щодо галузі та з інформацією із зовнішніх відкритих джерел так, щоб PE та LGE відображали профіль ризику кожного конкретного банку.

Результат перемноження показників EI , PE , LGE надає інформацію про загальну величину очікуваного збитку (EL) для кожного «напряму діяльності/типу ризику». Водночас, γ є постійним коефіцієнтом, який використовується для трансформації очікуваних збитків у показник ризику або резервний капітал. Він визначається на рівні максимальної суми можливого збитку протягом певного «надійного» часового періоду. Масштаб коефіцієнта γ визначається та має бути зафіксований регулюючим органом для кожного напрямку банківської діяльності окремо [5, с. 82–85].

Для **управління операційно-технологічним ризиком** банк повинен розробити та запровадити адекватну систему управління з чітким розподілом функцій та повноважень (рис. 11.2).

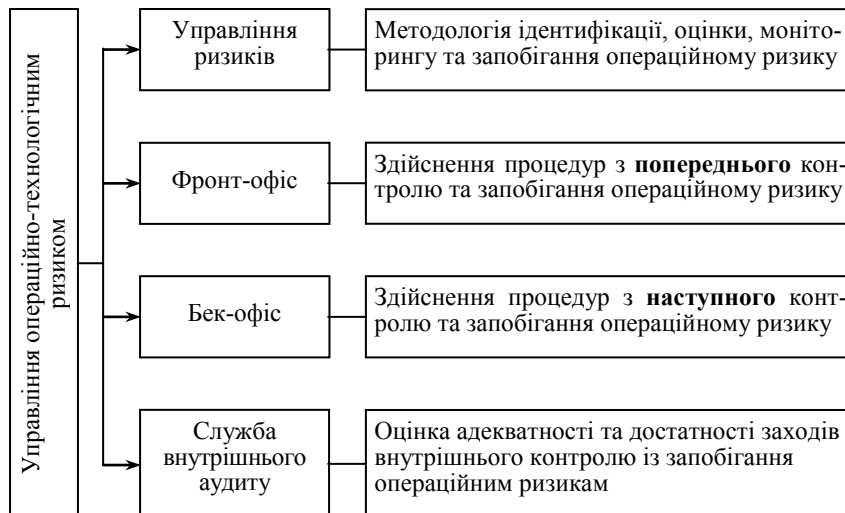


Рис. 11.2. Організаційна структура управління операційно-технологічним ризиком банку [24]

Важливою складовою ефективного управління операційно-технологічним ризиком є сприятливе внутрішнє середовище банку. Базельський комітет виділяє кілька принципів його формування.

Організаційні принципи формування сприятливого внутрішнього середовища банку.

1) Рада банку має бути обізнана з основними джерелами виникнення операційно-технологічного ризику як окремого виду ризику. Рада має ухвалювати та періодично переглядати порядок управління операційними ризиками. Цей порядок має містити визначення операційного ризику та принципи його ідентифікації, оцінювання і контролю.

Отже, банку необхідно описати операційно-технологічний ризик та його склад, визначити політику управління операційним ризиком, адекватну організаційній структурі банку. Обов'язковим є створення незалежного внутрішнього контролю та визначення ключових процесів для моніторингу.

2) Рада забезпечує складові системи ризик-менеджменту — внутрішній аудит та підсистему управління операційно-технологічним ризиком — незалежним, освіченим та компетентним штатом. Проте внутрішній аудит не повинен нести прямої відповідальності за управління операційним ризиком.

3) Правління банку відповідає за впровадження підсистеми управління операційно-технологічним ризиком, яку схвалила рада. Ця підсистема поетапно впроваджується в оргструктурі банку, і персонал на всіх рівнях повинен розуміти всю відповідальність щодо управління операційним ризиком. Правління також відповідає за розроблення та впровадження політики, процедур, процесів управління операційним ризиком у всіх підрозділах, напрямках діяльності, процесах і системах банку.

Реалізація цього принципу можлива за умови наявності кваліфікованого персоналу, взаємодії штату працівників, який відповідає за управління операційним ризиком, із штатом, який відповідає за управління кредитним, ринковим та іншими ризиками. Особливу увагу слід приділяти контролю за якістю документів і практиці обробки трансакцій.

4) Банки повинні ідентифікувати та оцінювати операційно-технологічний ризик у всіх підрозділах, напрямках діяльності, процесах і системах, а також забезпечувати виконання процедури оцінювання операційно-технологічних ризиків перед упровадженням нового продукту, напряму діяльності, процесу чи системи.

Втілення цього принципу передбачає аналіз чинників, які негативно впливають на досягнення цілей банку (недосконала організаційна структура банку, особливості діяльності, низька якість та плинність кадрів, зміни у банківському секторі та технологіях). Інструментами такого аналізу є:

- оцінювання сильних і слабких сторін управління операційним ризиком банку,
- карта ризику — співвідношення різних підрозділів і процесів з різними компонентами ризику для виявлення слабких місць та організації превентивних дій,
- розроблення сукупності індикаторів операційно-технологічного ризику (база даних про втрати, показник плинності кадрів, використання зовнішньої статистики тощо).

5) Банки повинні запровадити регулярний моніторинг позицій за операційно-технологічним ризиком, регулярної звітності перед правлінням і спостережною радою банку. Індикаторами раннього попередження для відображення потенційних джерел операційного ризику можуть бути: швидкий розвиток банку, впровадження нових продуктів, частота і тривалість системних збоїв та ін. Моніторинг повинен відображати величину ризику і частоту змін в операційному середовищі.

6) Банки мають розробити ефективну політику, процеси і процедури для контролю чи зниження операційно-технологічного ризику. Банки мають періодично переглядати свої обмеження щодо ризику і стратегії управління ним згідно з власним загальним рівнем прийнятного ризику.

На практиці для всіх видів операційно-технологічного ризику банк вирішує: знижувати ризик чи приймати його на себе. Для ризиків, які не піддаються мінімізації, банк повинен вирішити питання щодо обмеження обсягів діяльності у відповідному напрямі, або призупинення цієї діяльності.

7) Банки повинні мати план заходів у випадку непередбачуваних ситуацій для забезпечення власної діяльності на безперервній основі та для обмеження втрат у разі істотних відхилень у бізнесі. Реалізація цього принципу передбачає розгляд різних сценаріїв можливої перерви в діяльності банку, визначення критичних процесів, вирішення проблеми перенесення і збереження фізичних та електронних даних, необхідних для продовження банківського бізнесу [3; 4].

Для *мінімізації операційно-технологічних ризиків* банки використовують різноманітні заходи.

I. *Основні заходи щодо мінімізації операційно-технологічних ризиків з погляду технологічних процедур:*

- упровадження систем ідентифікації та авторизованого доступу до серверів, баз даних, програм, засобів зв'язку та передавання інформації, платіжних систем;
- створення системи резервування та дублювання основних та локальних баз даних, прикладних програм;
- упровадження систем захисту від комп'ютерних вірусів;
- створення мобілізаційного технологічного резерву на випадок виникнення нештатних (аварійних) ситуацій.

II. *Основні заходи щодо мінімізації операційно-технологічних ризиків з погляду облікових процедур:*

- жорстке дотримання стандартів обліку за всіма операціями відповідно до встановлених Національним банком України вимог;
- жорстке дотримання внутрішньобанківських процедур та стандартів управлінського обліку, їх постійна актуалізація;
- дані обліку активів і пасивів банку повинні належним чином підтверджуватися як з позиції повноти їх охоплення, так і з позиції їх відповідності; за наявності відхилень здійснюються відповідні процедури, спрямовані на ліквідацію розбіжностей.

III. *Основні заходи щодо мінімізації операційно-технологічних ризиків з погляду управлінських процедур:*

- упровадження системи повноважень та системи авторизованого доступу співробітників банку до майна і систем життєзабезпечення банку, до отримання інформації щодо операцій за рахунками клієнтів і рахунками банку в суворій відповідності з належно засвідченими повноваженнями співробітників;
- визначення міри відповідальності за порушення чинних внутрішніх правил, норм, стандартів та положень.

В зарубіжній практиці для зниження цього виду банківських ризиків використовуються методи *страхування операційних ризиків*, які дозволяють перекласти ризик на інших учасників ринку. Цей метод реалізується за допомогою страхового полісу BBB (Bankers Blanket Bond) — комплексну програму страхування від злочинів та професійної відповідальності фінансових інститутів. Така програма може включати *три види страхування*, які дозволяють знизити операційні ризики банку [6, с. 82–85]:

- саме страхування BBB;
- страхування від електронних та комп'ютерних злочинів;
- страхування професійної відповідальності фінансового інституту.

Це загальноприйняті у світовій практиці поліси страхування. Наявність таких полісів для зарубіжних фінансових інститутів — справа престижу, а в ряді випадків і обов'язкова вимога. Часто зарубіжний фінансовий інститут купує не один із зазначених видів страхування, а два чи навіть усі три у складі одного комплексного полісу. Перевага комплексності полягає, звичайно, у

знижені вартості. Крім того, перевага єдиного комплексного полісу базується ще й на тому, що ці види страхування є взаємодоповнюючими: ризики, які покриваються за одним видом страхування, виключаються за іншим. А оскільки економічні злочини часто мають дуже складний характер, то не завжди просто визначити, що стало причиною збитку банківської установи — якась злочинна дія чи помилка співробітника. Маючи комплексний страховий поліс, банк може бути впевнений, що всі його збитки будуть відшкодовані.

Головною статтею BVB є страхування від збитків у результаті шахрайства персоналу. Поліс BVB також надає страховий захист від збитків у результаті операцій, здійснюваних банком на основі підроблених письмових документів та інструкцій. Відшкодуванню підлягає і збиток від операцій з підробленими цінними паперами та фальшивою валютою. Покриття охоплює і «класичні» злочини — такі, як пограбування банку (також і в процесі інкасації), крадіжка цінного майна з його приміщення та й взагалі пошкодження і загибель цінного майна з будь-якої причини.

Поліс страхування від електронних та комп'ютерних злочинів, який придбавають як доповнення до стандартного полісу BVB, забезпечує захист від збитків унаслідок:

- несанкціонованого проникнення в електронні та комп'ютерні системи банку і зміни даних, які в них перебувають;
- дії комп'ютерного вірусу;
- здійснення операцій за шахрайськими інструкціями, отриманими електронними каналами зв'язку (наприклад, SWIFT);
- операцій з бездокументарними цінними паперами;
- злом комп'ютерних систем клієнта, здійснюваного з комп'ютерів банку (наприклад, самими ж працівниками банку);
- загибелі і пошкодження електронних даних та їх носіїв.

Третім елементом у системі комплексного страхування банківських ризиків, хоча і не пов'язаним безпосередньо з криміналом, є *поліс страхування професійної відповідальності* (Professional Indemnity Policy) співробітників банку за недбалість та ненавмисні помилки, допущені у процесі виконання ними своїх професійних обов'язків.

Таким чином, комплекс страхових продуктів створює повний захист операційної діяльності банку. Комплексність цієї програми полягає ще й у тому, що за взаємною угодою під покриття потрапляє не тільки головний офіс, а й уся система філій банку, причому нові підрозділи автоматично включаються в застраховану систему з наступною доплатою премії страховій компанії.

Отже, комплексний поліс BVB є важливим інструментом зниження операційного ризику, але вартість його досить висока. Величина страхової премії залежить від багатьох чинників, у тому числі й від суми обраного ліміту відповідальності, та може варіюватися від кількох десятків тисяч доларів до кількох сотень тисяч доларів залежно від обсягу страхового покриття.

Наступним етапом процесу управління є **внутрішній контроль за операційно-технологічним ризиком**, який має бути відповідно організований (рис. 11.3).

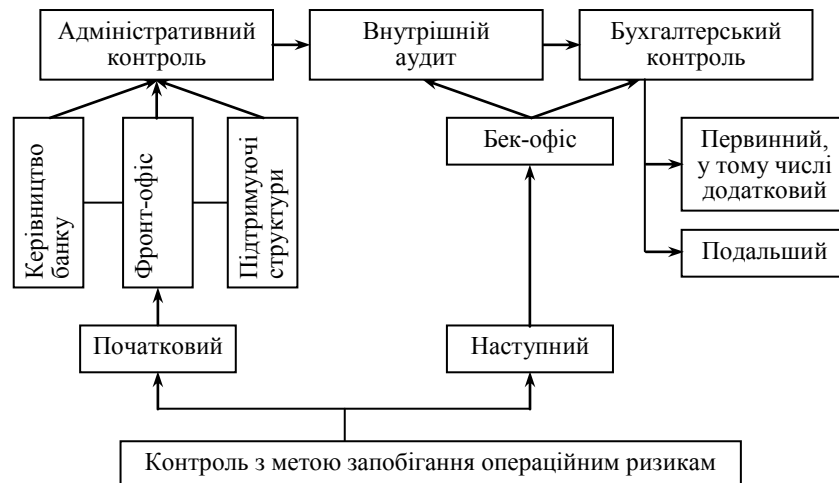


Рис. 11.3. Організація контролю за операційно-технологічним ризиком банку [24]

Внутрішній контроль за операційно-технологічним ризиком реалізується за допомогою таких елементів та процедур:

1) політика і положення щодо контролю за операційно-технологічним ризиком з метою його мінімізації, які мають бути розглянуті й затверджені відповідно до обраної банком форми корпоративного управління, а також періодично переглядатися;

2) процедури і засоби контролю за операційно-технологічним ризиком, що притаманні операціям банку, у тому числі:

— процедури та засоби контролю за дотриманням облікової політики банку та вимог нормативно-правових актів Національного банку щодо методів оцінювання 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 у разі втрати доступу або знищення важливої інформації або технологій;

— інформаційна система управління (форми звітності, схема документообороту тощо) для спостережної ради, правління або профільних колегіальних органів банку щодо моніторингу уразливості всіх видів діяльності банку до операційно-технологічного ризику;

3) програма управління персоналом, яка охоплює:

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

— обґрунтовані і визначені рівні повноважень з прийняття будь-яких рішень;

— доведення до персоналу його обов'язків;

— контроль за діяльністю персоналу;

— розроблення і впровадження процесу навчання з метою підвищення кваліфікації працівників;

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

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

6) процес періодичного тестування встановлених процедур та технологій здійснення операцій, у 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.

Для належного контролю за операційно-технологічним ризиком *банк повинен*:

1) забезпечити надійне позаофісне зберігання всіх важливих резервних документів і файлів банку;

2) у разі використання банком послуг аутсорсингу забезпечити чітку регламентацію таких питань:

— обставин, за яких можуть використовуватися послуги аутсорсингу та переліку операцій, до яких можуть бути залучені сторонні особи;

— процедур та критеріїв вибору постачальників послуг;

— моніторингу якості роботи і ризиків, пов'язаних із використанням сторонніх послуг [2, розд. IV, гл. 12].

Отже, сучасні тенденції в управлінні операційно-технологічним ризиком свідчать про дедалі зростаючу увагу до нього з боку Базельського комітету, НБУ та банків України. В умовах постійно зростаючих обсягів надання дистанційних банківських послуг значна частина причин виникнення операційно-технологічних ризиків пов'язана з функціонуванням електронного банкінгу.

11.2. Управління ризиками електронного банкінгу

Ризики електронного банкінгу — це сукупність ризиків, які супроводжують процес електронного банківського обслуговування клієнтів. Ця група ризиків характеризується ймовірністю виникнення збоїв у програмному забезпеченні чи певних подій, які ускладнюють або унеможливають здійснення банківських операцій чи послуг клієнтами у дистанційному режимі обслуговування.

Електронне банківське обслуговування здійснюється за допомогою різних форм електронного банкінгу. На цей час функціонує близько десяти форм електронного банкінгу. У процесі поетапного розвитку його форми видозмінювались залежно від еволюції програмного інструментарію та технічних засобів, що забезпечують здійснення банківських операцій у дистанційній формі (табл. 11.2).