УДК 336.71:330.131.7

В. В. Чаплига

Управління операційним ризиком в забезпеченні ефективності функціонування банку

Розглянуто питання визначення та управління операційним ризиком, його безперервного моніторингу і аудиту. Запропоновано інтегрований підхід до формування системи управління операційним ризиком на основі національних та міжнародних стандартів як важливого чинника забезпечення безперервності та підвищення ефективності діяльності банку.

Ключові слова: операційний ризик, оцінка, моніторинг, система управління ризиком, інтегрований підхід, стандарти, ефективність функціонування, банк.

Постановка проблеми. Глобалізація, нестабільність ринків, безпрецедентний темп змін зовнішнього та внутрішнього середовища банків, який, як очікується, збережеться, призводить до того, що банки постійно піддаються впливу все нових ризиків, помилок, шахрайських схем, проблем із забезпеченням відповідності нормативним вимогам тощо, які в результаті хибних рішень можуть призвести до масштабних матеріальних втрат або навіть до банкрутства як самого банку, так і його клієнтів. Остання фінансова криза показала, що гонитва за прибутком без урахування стратегічних бізнес-ризиків, впливу вжитих заходів на компенсацію ризиків у ринкових умовах може мати катастрофічні наслідки у всіх галузях економіки і банківському секторі зокрема. Враховуючи суспільну значимість, банківської системи можна з упевненістю стверджувати, що ризики банківської діяльності суттєво впливають на економічний розвиток країни.

Загострюється також конкурентна боротьба між банками, яка характеризується розширенням спектра банківських продуктів і послуг на основі впровадження високоавтоматизованих технологій, ускладненням і підвищенням якості банківських операцій, збільшенням їх обсягів, що вимагає від банків серед інших ризиків приділяти особливу увагу управлінню операційним ризиком, який суттєво впливає на забезпечення безперервності та ефективності діяльності банків. Вже зараз у банках зростають втрати від операційних ризиків і, на думку аналітиків, в перспективі саме вони вийдуть на перше місце. Так, останнім часом у банківському секторі відбувся ряд серйозних інцидентів у сфері захисту інформації, які загрожують безперервності та безпеці банківської діяльності. Вразливість банків також може різко підвищуватися з поширенням електронної торгівлі, аутсорсингу, а також у результаті злиття або купівлі банків, коли здійснюється реінжиніринг бізнес-процесів та впроваджуються нові інформаційні системи і технології.

Проблема формування та впровадження надійних і комплексних систем управління операційним ризиком у наш час є надзвичайно актуальною для банків України, що забезпечить зменшення втрат та підвищення ефективності банківської діяльності.

Аналіз останніх досліджень і публікацій. Класифікація банківських ризиків та методичні підходи до їх кількісної оцінки визначені в документах Базельського комітету з банківського нагляду [1] та Націо-

нального банку України [2-4]. Перший з документів є регулятивним, що не містить конкретних методів управління операційними ризиками та практичних рекомендацій і зосереджений головним чином на обчисленні резервів капіталу під можливі втрати від реалізації операційного ризику та правилах переходу на удосконалені методи обчислення.

Проблеми оцінки та управління ризиками банку розглядаються в наукових працях багатьох вітчизняних і зарубіжних економістів: І. В. Волошина, О. А. Кириченка, П. П. Ковальова, Т. Д. Косової, В. І. Міщенка, Л. О. Примостки, П. М. Чуба, Н. Р. Швеця, А. А. Лобанова, К. Крішнана, Г. Марковіца, У. Шарпа, П. Роуза, Х. Грюнінга, С. Брайнович-Братановича, А. В. Чугунова та ін. У роботах згаданих авторів розкривається сутність банківського ризику як економічної категорії, визначаються його складові і класифікаційні ознаки різних видів ризиків, пропонуються методики аналізу та управління ними.

Теоретичним та методологічним аспектам оцінки і управління операційним ризиком банку присвячені роботи таких вітчизняних і зарубіжних вчених і практиків, як: А. М. Бухтін, Н. І. Валенцова, О. С. Дмитров, М. А. Камінський, В. В. Коваленко, О. І. Лаврушин, Д. С. Нехороших, В. С. Романов, Б. В. Сазикін, Н. Катілова, Е. Сорін, А. В. Смирнов, А. А. Сиротін та ін.

Практичні підходи до оцінки та управління ризиками визначені в міжнародних стандартах, зокрема COSO ERM, COBIT, ISO 31000 та ISO 27001, а також галузевих стандартах СОУ Н НБУ 65.1 СУІБ:2010.

Проте на сьогодні відсутнє загальноприйняте визначення операційного ризику, залишаються невирішеними питання системного підходу до управління операційним ризиком, його безперервного моніторингу та аудиту, що створює певні складності у формуванні сучасного ефективного та оперативного механізму управління цим ризиком в банку.

Метою дослідження є розробка інтегрованого підходу до формування системи управління операційним ризиком на основі національних та міжнародних стандартів як важливого чинника забезпечення безперервності та підвищення ефективності діяльності банку.

Виклад основного матеріалу. На підвищений інтерес банків до управління операційним ризиком впливають декілька чинників. По-перше, рекомендації та стандарти Базельського комітету з банківського нагляду (Базель ІІ), впровадження яких відбувається в Україні, вказують на необхідність створення ефективної системи управління операційним ризиком.

При цьому, під операційним ризиком розуміємо ризик збитків, викликаних неадекватними або непрацездатними внутрішніми процесами і системами, їх порушенням персоналом або в результаті впливу зовнішніх факторів. Це визначення включає в себе частину правового ризику (в частині невідповідності внутрішніх нормативних та юридичних документів законодавчій базі, в т. ч. ризик штрафів і стягнень з боку наглядових органів, а також ризики за комерційними договірними відносинами), але виключає стратегічний, репутаційний та фінансовий ризики.

По-друге, в документах Національного банку України операційно-технологічний ризик через специфіку загроз та наслідків займає особливе місце серед банківських ризиків. Так, якщо кредитний ризик, ризик ліквідності, ризик зміни процентної ставки, ринковий ризик, валютний

ризик, ризик репутації, юридичний ризик або стратегічний ризик – «це наявний або потенційний ризик для надходжень та капіталу», то операційно-технологічний ризик визначено як «потенційний ризик для існування банку» [4, с. 8]. Там же наведено визначення операційно-технологічного ризику, «що виникає через недоліки корпоративного управління, системи внутрішнього контролю або неадекватність інформаційних технологій і процесів оброблення інформації з точки зору керованості, універсальності, надійності, контрольованості і безперервності роботи».

По-третє, як показують уроки фінансової кризи, рішення, пов'язані з ризиками, так чи інакше зачіпають усі складові банківського бізнесу, тому для банку важливо мати централізоване управління ризиками з можливістю миттєвого доступу до інформації про потенційні проблеми в режимі реального часу. При цьому, такі міжнародні стандарти, як COBIT, COSO ERM, ISO 31000, ISO 27001, ISO 9000 рекомендують побудову інтегрованої системи управління бізнес-процесами і системами, безпекою та безперервністю бізнесу, його ефективністю. В такій системі вагоме місце займає управління операційним ризиком, який притаманний усім процесам банку, інформаційно-комунікаційним системам, договірним відносинам та інвестиційним проектам.

Згідно з визначенням операційного ризику його чинники можна поділити на внутрішні та зовнішні й віднести до таких груп джерел (суб'єктів): технологічні та управлінські процеси з процедурами прийняття рішень, внутрішнього контролю і аудиту; організаційна структура; органи управління (зовнішні стосовно банку); фізичні особи (персонал, клієнти, інші); юридичні особи (структурні одиниці, клієнти, контрагенти, інші); інформаційно-комунікаційні системи (ІКС внутрішньо-корпоративні, зовнішні); явища природнього, техногенного або іншого характеру.

Для кожного із джерел та видів операційних ризиків необхідно встановити можливі причини їх виникнення, оцінити суттєвість, визначити та запровадити контрзаходи щодо унеможливлення реалізації або мінімізації наслідків ризику, організувати моніторинг та дієвий контроль.

При цьому управління операційними ризиками та їх моніторинг здійснюються відповідно до вимог, які висуває кожен конкретний банк до своєї системи ризик-менеджменту. Такі вимоги можуть бути різними, однак обов'язковою є необхідність здійснювати збір, систематизацію та аналіз різних кількісних і якісних даних, які забезпечують отримання цілісної, повної і надійної інформації про операційні ризики банку, дозволяють виявляти зони концентрації ризику та недоліки в системі контролю. Збір даних про інциденти операційного ризику також є одним із ключових елементів для переходу на AMA-підхід до оцінки величини операційного ризику відповідно до Базель II.

Слід зазначити, що проблема виявлення, кількісної оцінки, моніторингу, контролю та прогнозування суттєвих операційних ризиків пов'язана з їх особливостями які, зокрема, полягають у наступному:

– типовим є незначна ймовірність подій та їх розрідженість у часі в поєднанні з руйнівним характером фінансових та інших наслідків реалізації подій;
– характерним є не повторення подій, а виникнення і створення нових ризикових ситуацій та факторів ризику;

– часто операційні ризики виникають у зв'язці з іншими ризиками або їх групами;
– частина операційних ризиків має латентний характер, тобто реалізація ризиків виявляється не одразу після настання події, а згодом (або й ніколи), і сума збитків від невиявлення низки таких подій може досягати критичних для бізнесу значень;
– катастрофічні події в основному стають наслідком збігу найменших обставин, окремі з яких можуть перебувати в межах допустимих операційних відхилень, і тому винних за саму подію може й не бути.

Це ставить перед менеджментом банку завдання на основі аналізу й моделювання розробки ефективних механізмів виявлення та недопущення або обмеження можливих нових операційних ризиків.

Однак при моделюванні операційних ризиків банки стикаються з проблемами невеликої кількості історичних даних по втратах, відсутності стандартних методик як оцінки ймовірності ризикових подій і втрат, так і прогнозування складних випадків реалізації операційного ризику, коли одне або кілька випадкових подій операційного ризику є причиною виникнення основної події, що й призвело до втрат. Через нерегулярний та нерегламентований характер операційного ризику статистичні дані по втратах зазвичай нечисленні й розріджені.

Математичною основою вирішення завдання аналізу операційних втрат із використанням наявних статистичних даних може слугувати, як показано, наприклад, у [5], так звана теорія екстремальних значень (extreme value theory – EVT) і засновані на ній методи. До отриманих при цьому оцінок, звичайно, потрібно ставитися з обережністю.

Особливо важливою для аналізу, оцінки та прогнозування є якість даних про події (втрати) операційних ризиків. Одним із способів перевірки якості зібраних даних вважається застосування до масиву операційних втрат універсального закону, що описує розподіл частоти вживання перших значущих цифр у числових рядах (закону Бенфорда). В [6] підтверджено, що відхилення розподілу сум операційних втрат банку від розподілу Бенфорда можна розглядати як попередження про те, що зібрані дані вимагають детальнішої перевірки з метою виявлення у великому масиві операційних втрат тих подій, повторюваність яких потребує пильнішої уваги та вказує на необхідність вдосконалення процесу реєстрації операційних подій.

Слід зауважити [7], що ймовірнісно-статистичні методи застосовуються до операційних ризиків, які мають характер елементів масового обслуговування: технологічних збоїв чи відмов систем, технологічних помилок персоналу при обслуговуванні потоку клієнтів тощо. Крім того, ймовірнісні моделі нерідко є своєрідним виправданням втрат. Якщо втрати вкладаються в рамки очікуваних з точки зору теорії ймовірностей, то це приймається як належне без виявлення реальних причин втрат, що, своєю чергою, сприяє приховуванню можливих помилок, шахрайства тощо. Тому для виявлення зон підвищеного ризику, визначення ступеня відповідності процедур установленим нормам виконання операцій корисно також застосовувати індикаторний і комбінований підходи, експертні якісні оцінки з використанням методів нечіткої логіки.

Зважаючи на те, що операційні ризики суттєво впливають на ефективність, стабільність та безперервність управління банком, важливо враховувати й оцінювати ризики переривання бізнесу, аналізуючи, до яких фінансових втрат призведе той чи інший ризик і у скільки обійдеться підтримка бізнес-процесів на достатньому рівні. Для цього в банку необхідно, зокрема, встановити залежність певних ресурсів банку (персонал, технології, інформаційно-комунікаційні системи тощо) з критично важливими продуктами і послугами, які вони забезпечують, розглянути наслідки можливого руйнування цих ресурсів та розробити стратегічний план забезпечення безперервності діяльності банку, спираючись на міжнародні стандарти, зокрема на стандарт ISO 22301:2012.

При розробці такого плану особливу увагу необхідно приділити забезпеченню гарантоздатності (надійності, відмовостійкості, інформаційній безпеці) та інформаційної живучості (здатності підтримувати доступність, цілісність та конфіденційність інформації на рівні, який дозволяє виконувати з заданою якістю цілі функціонування системи, незалежно від зовнішніх і внутрішніх несприятливих впливів або порушень [8]) розподілених ІКС і комплексів, інтегрованих у критичні банківські технології та інфраструктури. Вирішення цієї проблеми ускладнюється тим, що в процесі експлуатації можуть істотно змінюватися не тільки умови зовнішнього середовища, але також і вимоги до характеристик системи, що зумовлює перманентні модернізації протягом життєвого циклу з метою підтримки на належному рівні показників якості її функціонування. Тому потрібно використовувати ризик-орієнтовану методологію проектування та експлуатації ІКС згідно міжнародних, національних і галузевих стандартів, нормативних документів Національного банку України щодо надійності, живучості та інформаційної безпеки [9–10].

Стратегічний план також дозволить визначити, яким чином буде відновлюватися кожен критичний ресурс, методи реагування та відновлення, засоби, технології і відповідальний персонал, необхідні для відновлення, та структуру управління процесами в рамках реалізації принципів безперервності бізнесу. План забезпечення безперервності діяльності повинен бути доведений як до керівництва банку, так і до керівників підрозділів, що задіяні у виконанні заходів згідно зі Стратегічним планом. Тестування плану забезпечення безперервності діяльності банку необхідно здійснювати не рідше 1 разу в рік.

Для підвищення ефективності та забезпечення безперервності бізнесу важливим є інтегрування процедур управління операційними ризиками в управлінські та технологічні процеси банку, яке може передбачати такі етапи з управління ризиками: ідентифікація та оцінка операційних ризиків як поточних так і тих, що розвиваються, їх співставлення з процесами; визначення процесів, ризики яких є найістотнішими; визначення ступеня зрілості процесів (за стандартами, наприклад, CMMI або CobIT) та адекватності управління ризиками; постановка та виконання завдань з реінжинірингу процесів і системи управління ризиками; моніторинг рівня операційного ризику і подій, виявлення відхилень у ключових процедурах контролю (контролях) ризику та звітність.

При цьому виявлення і оцінку ризиків, моніторинг ключових контролів та їх тестування здійснює бізнес або функціональний підрозділ. Підрозділ внутрішнього контролю та ризик-менеджменту здійснює моніторинг

бізнес-підрозділів, здійснює періодичні перевірки адекватності управління моніторингом контролів. Служба внутрішнього аудиту на основі ризик-орієнтованого підходу здійснює тематичні та комплексні перевірки.

Підвищенню ефективності управління операційним ризиком у банку сприяє використання спеціалізованих інформаційних систем автоматизації управління операційним ризиком (SAS OpRisk Management, Centerprise Services OpRiskCenter, IIG ULTOR, RCS OpRisk Suite тощо) та комплексних GRC (корпоративне управління, ризик-менеджмент, відповідність) рішень, зокрема Enterprise GRC Manager, Fusion GRC Intelligence (Oracle), SAP GRC (SAP), Enterprise GRC (SAS), OpenPages GRC Platform (IBM), які забезпечують у реальному часі можливість моніторингу та аудиту GRC процесів в умовах функціонування в банку корпоративних інформаційних систем типу ERP, АБС тощо.

Висновки. Сучасні тенденції в економіці України вимагають від банків приділяти особливу увагу управлінню операційним ризиком, який суттєво впливає на забезпечення ефективності та безперервності їх діяльності.

Особливо важливою для аналізу, оцінки та прогнозування операційних ризиків є якість даних про події (втрати) їх реалізації. Зважаючи на відсутність достатніх історичних даних доцільно, на наш погляд, поряд із ймовірнісно-статистичними методами застосовувати індикаторний і комбінований підходи, експертні якісні оцінки з використанням методів нечіткої логіки.

Важливо також враховувати і оцінювати ризики переривання бізнесу та розробити стратегічний план забезпечення безперервності діяльності банку, приділивши значну увагу забезпеченню гарантоздатності та інформаційної живучості систем, інтегрованих у критичні банківські технології та інфраструктури.

При побудові системи управління операційним ризиком необхідно забезпечити відповідність міжнародним та національним стандартам з урахуванням особливостей бізнес-процесів банку, а ефективність управління операційним ризиком необхідно оцінювати разом із консолідованою оцінкою ризиків банку, враховуючи також зв'язок корпоративного управління й управління операційним ризиком.

Для підвищення ефективності та забезпечення безперервності діяльності банку важливим є інтегрування процедур управління операційними ризиками в управлінські та технологічні процеси з використанням спеціалізованих або комплексних (GRC) інформаційних систем автоматизації управління операційним ризиком.

Список використаних джерел

1. Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework. – Basel: BIS. – June 2004. – Режим доступу : http://www.bis.org/publ/bcbs107.htm.
2. Проект Постанови Правління Національного банку України «Про підходи до впровадження Базеля II». – Режим доступу : http://www.aub.com.ua/ua/regulation/?_m=publications&_t=rec&id=8320.
3. Методичні рекомендації щодо організації та функціонування систем ризик-менеджменту в банках України, затверджені постановою Правління Національного банку України 02.08.2004 р. № 361. – Режим доступу : http://www.bank.gov.ua/Bank_supervision/Risks/361.pdf

4. Методичні вказівки з інспектування банків «Система оцінки ризиків», затверджені постановою Правління Національного банку України від 15.03.2004 р. № 104. – Режим доступу : http://www.bank.gov.ua/Bank_supervision/Risks/104.pdf.
5. Журавлев И. Б. Байесовский анализ операционных потерь с выбором порогового значения для оценки капитала под операционным риском. Опыт применения для Российского банка / И. Б. Журавлев // Управление финансовыми рисками. – 2008. – № 03(15). – С. 216–225.
6. Журавлев И. Б. Об одном способе проверки качества собираемых данных по операционным потерям / И. Б. Журавлев // Управление финансовыми рисками. – 2009. –№ 03(19). – 2009. – С. 244-250.
7. Моделювання оцінки операційного ризику комерційного банку : монографія / [О. С. Дмитрова, К. Г. Гончарова, О. В. Меренкова та ін.] ; за заг. ред. С. О. Дмитрова. – Суми : ДВНЗ «УАБС НБУ», 2010. – 264 с.
8. Сербін В. Г. Деякі аспекти живучості складних гарантоздатних комп'ютерних систем критичних умов застосування / В. Г. Сербін, А. І. Сухомлин // Математичні машини і системи. – 2011. – № 4. – С. 189–192.
9. Інформаційні технології. Методи захисту. Зведення правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD): ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. – К. : НБУ, 2010. – 163 с. – Код УКНД 35.040.
10. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України: Лист департаменту інформатизації Національного банку України банкам України від 03 березня 2011 р. № 24-112/365. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/v0365500-11.

Чаплыга В. В. Управление операционным риском в обеспечении эффективности функционирования банка.

Рассмотрены вопросы определения и управления операционным риском, его непрерывного мониторинга и аудита. Предложен интегрированный подход к формированию системы управления операционным риском на основе национальных и международных стандартов как важного фактора обеспечения непрерывности и повышения эффективности деятельности банка.

Ключевые слова: операционный риск, оценка, мониторинг, система управления риском, интегрированный подход, стандарты, эффективность функционирования, банк.

Chaplyha V. V. **Operational Risk Management in Ensuring the Effective Functioning of the Bank.**

The issues of definition and management of operational risk, its continuous monitoring and auditing are considered. An integrated approach to the formation of operational risk management system based on national and international standards as an important factor in ensuring the continuity and effectiveness of the bank activity is proposed.

Key words: operational risk, assessment, monitoring, risk management system, integrated approach, standards, effectiveness of functioning, bank.

Надійшло 13.11.2013 р.