УДК 336.743

Д. В. Безштанько, асп.

ВИКОРИСТАННЯ СТРЕС-ТЕСТУВАННЯ ДЛЯ ПЕРЕВІРКИ ЕФЕКТИВНОСТІ УПРАВЛІННЯ ОПЕРАЦІЙНИМ РИЗИКОМ БАНКУ

Обґрунтовано потребу використання стрес-тестування в системі управління операційним ризиком банку, проаналізовано використання застосування стрес-тесту для оцінювання ефективності управління операційним ризиком. Встановлено, що стрес-тестування дасть змогу в повній мірі оцінити загрози операційного ризику для банку, запропоновано алгоритм і вихідні умови здійснення стрес-тестування.

Вступ

Світова фінансова криза загострила увагу на ефективному управлінні власними активами, особливо для банківських установ. Одним із способів оптимізації є управління ризик-менеджментом, разом з операційним ризиком банку, на який щораз більше акцентують увагу банківські установи України після випадку з Промінвестбанком, коли поширення конфіденційної інформації поставили банк на межу банкрутства. Для використання різних методик управління необхідно розвинути інструментарій контролю ефективності прийнятих рішень, наприклад, стрес-тестування.

Питання стрес-тестування широко досліджено, однак використання цього методу для оцінювання ефективності заходів мінімізації операційного ризику досліджувалися лише у працях M. Jones, G. Majnoni, S. M. Peria та А. В. Летчикова, С. О. Дмитрова.

Метою статті є розроблення підходів до формування механізмів оцінки ефективності контролю операційного ризику банку.

Для досягнення мети слід виконати такі завдання:

— визначення сутності та особливостей операційного ризику банку;

— дослідження стрес-тестування, як одного з методів оцінювання операційного ризику;

— розробка алгоритму оцінювання загроз операційного ризику на прикладі комерційного банку.

Управління операційним ризиком банку

Фінансова криза загострила увагу банків до ризиків, в тому числі і до ризиків операційного характеру. Одним з головних питань аналізу банку було збереження ним економічної стійкості, в тому числі через підвищення ефективності управління ризиками.

Управління ризиками — це частина оперативної чи стратегічної управлінської діяльності банку по організації адекватного масштабу та безперервного бізнес-процесу управління ризиками, [1, с. 136] що проводиться з метою:

— забезпечення безперервності його діяльності;

— підтримки високої ділової репутації;

— забезпечення стратегічної та поточної фінансової стійкості.

Одним із видів ризиків є операційний ризик банку, важливість якого зростає через посилення глобалізації, значне поширення новітніх інформаційних технологій. Відповідно до класичного визначення за Базельською угодою II, операційний ризик — це ризик прямих та побічних збитків у результаті неправильної побудови бізнес-процесів, неефективності процедур внутрішнього контролю, технологічних збоїв, несанкціонованих дій персоналу або зовнішніх впливів [2].

Система управління ризиком, в тому числі операційним, включає такі основні елементи:

— організаційний, що визначає орган, який має здійснювати управління ризиками;

— інформаційно-технологічний, який визначає засоби та технології, що будуть основою для здійснення управління;

— методологічний блок, який відповідає за здійснення управління ризиками, відповідно до чинних правил, методів, можливостей. На думку автора, саме на методологічному блоці слід зосередити особливу увагу, оскільки помилки чи неточності важко визначити, а результати можуть бути негативними, наприклад, біржова криза 1987 року була спричинена падінням Інформаційної системи біржі [3, с. 122].

Базельський комітет виділяє три підходи до оцінки капіталу під операційний ризик.

1. Підхід на базі основного індикатора (The Basic Indicator Approach). Відповідно до цього 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, при цьому для кожного банку сума капіталу під операційний ризик дорівнює показнику α, помноженому на розмір валового доходу банку. Поточне значення α — 15 %. Підхід на базі основного індикатора легкий у застосуванні і його можна використовувати для всіх банків при формуванні резерву під операційний ризик. Для забезпечення стимулу просування до складнішого підходу, можливе встановлення α на більш високому рівні. Однак Базельський комітет очікує, що банки з міжнародними операціями та істотним операційним ризиком будуть використовувати складніші підходи і при поточному значенні α.

2. Стандартизований підхід (The Standardised Approach). Стандартизований підхід являє собою подальшу розробку еволюційного спектра підходів до визначення розміру капіталу під операційний ризик. Цей підхід відрізняється від попереднього тим, що діяльність банку як економічної одиниці розділена на визначену кількість стандартизованих ділових одиниць і ділових ліній. Таким чином, стандартизований підхід більше придатний відобразити чим відрізняються профілі ризику банків, обумовлені їх широким спектром ділової активності.

3. Підхід вдосконаленого вимірювання (Advanced Measurement Approach). Підхід вдосконаленого вимірювання забезпечує свободу вибору банку стосовно 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 і непередбачених збитків, якщо тільки банк не зможе довести, що його внутрішні методи роботи в достатній мірі враховують очікувані збитки. 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 [3, с. 25—28].

Стрес-тестування для оцінки ефективності системи управління операційним ризиком

Одним із методів методологічного блоку є стрес-тестування — це оцінка потенційного ефекту на фінансовий стан банку при зміні ризиків його діяльності, базуючись на ймовірності потенційних подій та явищ. Цей метод в системі оцінки операційного ризику відносять до найбільш прогресивної, з точки зору повноти та адекватності оцінювання ризику, групи підходів вдосконаленого вимірювання.

Цілями стрес-тестування в системі оцінки операційного ризику банку є:

— оцінка ймовірностей втрат від реалізацій операційного ризику;

— вироблення комплексу заходів щодо мінімізації ризику.

Стрес-тестування, як один з підходів оцінки операційного ризику банку, можна поділити на:

1. Сценарний аналіз, при якому джерело шоку, або стресового явища, чітко визначене, як і параметри фінансових ризиків, на які цей шок впливає.

2. Аналіз чутливості — джерело шоку не задається, а оцінювані параметри ризиків наперед визначені.

Сутність сценарного аналізу стрес-тестування полягає у моделюванні кількох, зазвичай трьох, моделей розвитку ситуації, порівнянні результатів та інтерпретація отриманих результатів, а саме:

— базовий сценарій, що виконується в рамках найімовірніших змін факторів ризику. Допущення коливань заданих параметрів коливається в межах 10 %.

— негативний сценарій, який розраховується в рамках найменш характерних змін у некризових етапах економічного циклу. Допущення коливань заданих параметрів можливе в межах 20 %.

— максимально негативний сценарій, що формується тоді, коли існує значна ймовірність зростання факторів ризику в умовах кризової фази економічного циклу. Допущення коливань заданих параметрів коливається в межах 30 %.

Для того, щоб отримати оптимальний варіант, який би враховував всі сторони можливого ризику, слід зосередити увагу на особливостях методики. Вибір методики, на нашу думку, полягає у акцентуванні уваги на одному з методів (одно-, багатофакторна модель, історичний тип (1998 р., 2004 р. , 2008 р.), гіпотетичний тип тощо) та вибором факторів, що стимулюють зростання ризику (стійкі причинно-наслідкові зв'язки, вимоги до якості інформації, істотність припущень щодо коливань параметрів: ±5 %, ±10 %, ±15 %) [4, с. 17—23].

Стрес-тестування, по суті, включає в себе кількісний та якісний аналіз. Кількісний аналіз спрямований перш за все на визначення масштабу і послідовності виникнення негативних явищ та їх впливу на різноманітні показники банківської діяльності. В той час як якісний — сконцентрований на оцінці можливостей банку щодо мінімізації потенційних втрат і визначенні комплексу можливих заходів, що мають здійснюватися для зниження рівня ризику і збереження необхідного рівня стійкості банківської установи [5, с. 159].

У результаті можна сформувати механізм проведення стрес-тестування:

1. Виявлення найбільш істотних ризиків, що можуть негативно вплинути на банк;

2. Формулювання сценарію (певної послідовності виникнення та сили прояву подій);

3. Визначення методики або алгоритму, які б дозволили спроектувати послідовність реалізації певного фактору ризику на діяльність банку;

4. Здійснення кількісного аналізу — розрахунку наслідків розвитку вибраного сценарію за алгоритмом;

5. Інтерпретацію отриманих результатів.

Під час здійснення стрес-тесту по операційним ризикам слід зосередити увагу на 4 напрямках: персонал, інформаційна система, помилки в методології здійснення операцій та зовнішні фактори.

Якщо зосередити увагу на конкретних варіантах джерел ризику, то прикладами можуть бути такі сценарії:

— тестування навантаження на програмні засоби та обладнання;

— моделювання інформаційних атак;

— навчання по забезпеченню неперервної роботи інформаційної банківської системи;

— моделювання шахрайства з метою оцінки засобів контролю (прикладом реалізації такого ризику може слугувати випадок, коли служба безпеки одного з комерційних банків на прохідній, де вимагалося проведення візуального контролю, користувалася перепусткою з фотографією негуманоїда).

Стрес-тестування операційного ризику банку «Морський»

Наведемо приклад моделювання ситуації для стрес-тестування: відбулася інформаційна атака хакерської групи на сервери головного офісу комерційного банку, оскільки саме такий вид ризику найхарактерніший для банківських IT структур [6].

На першому етапі, на нашу думку, слід визначити основний ризик — ризик вдалої інформаційної атаки хакерської групи на банківський сервер банку «Морський».

На другому етапі, за сценарієм деталізуємо результати атаки:

а) в рамках найвірогідніших змін факторів ризику: відбулася втрата інформації поточної діяльності (базовий сценарій);

б) в рамках негативного сценарію, який відповідає достатньо ймовірним факторам ризику, банком втрачено конфіденційну інформацію про клієнтів (негативний сценарій розвитку);

в) в рамках настання екстремального, але ймовірного випадку: інформаційна система банку вийшла з ладу (максимально-негативний сценарій).

На третьому етапі — визначимо алгоритм для розрахунку наслідків реалізації операційного ризику.

Розрахуємо прогнозований рівень під операційний ризик банку за методикою базового індикатора (усереднені показники операційного доходу за три попередні роки) [7, 8, 9].

Рівень збитків визначається як сума прямих та непрямих втрат від простою інформаційної системи банку, витрати на відновлення інформації, відшкодування моральних та матеріальних втрат клієнтів, та втрат операційного прибутку в залежності від сценарію за 1, 3 та 5 днів.

Крім того, репутаційний ризик теж зросте, буде паралізована діяльність мережі філій, так як інформаційний обмін з головним відділенням буде порушено.

Для четвертого етапу розрахуємо за алгоритмом ефективність формування резервів під операційний ризик за методом базового індикатора.

Розрахунок ефективності заходів щодо мінімізації операційного ризику, тис. грн

Фактори впливу		Базовий сценарій	Негативний сценарій	Максимально негативний сценарій
Формування резервів	Операційний прибуток:	17482		
	за 2008	17349		
	за 2009	20619		
	за 2010	14477		
	Резерви під операційний прибуток	2622		
Рівень збитків	Прямі втрати на відновлення інформації	3	6	9
	Штрафи, пені, судові витрати	10	20	30
	Втрати клієнтів	56	167	278
	Рівень покриття	3 %	7 %	12 %

Отже, за даними таблиці, можна зробити висновок, що навіть за найнесприятливішого сценарію реалізації операційного ризику — інформаційної атаки, банк зможе погасити втрати протягом короткого проміжку часу, оскільки рівень покриття (відношення витрат до резервів) становить 12 %.

На п'ятому етапі наведемо дані опитування східноєвропейських банків, за яким лише 35 % респондентів змогли б відновити інформацію в межах 1—2 днів, 45 % — в межах 5 днів. [11, с. 97—103]

На думку автора, слід зосередити увагу на ідентифікації можливих джерел проникнення зловмисників до банківської мережі, вдосконалення системи резервування даних тощо.

Висновок

У системі управління банківськими ризиками стрес-тестування може займати одне з основних місць, однак система стрес-тестів для операційного ризику, в українських реаліях, тільки починає розвиватися. Особливість методу стрес-тестування полягає в тому, що на відміну від інших методів, які оцінюють так звані «прогнозні/очікувані» втрати, поява яких пов'язана з реалізацією раніше ідентифікованих ризиків (мають значну ймовірність виникнення, мають підтверджену статистичну інформацію, кількісну оцінку), стрес-тестування проводить перспективну оцінку так званих «непрогнозованих/неочікуваних» втрат (наприклад, падіння інформаційної системи через атаку закурів), які зумовлені реалізацією малоймовірних ризиків або реалізацією раніше неідентифікованих ризиків.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Система банківського менеджменту : навч. посіб. / за ред. О. С. Любуня та В. І. Грушко. — К. : Фірма «ІНКОС», 2004. — 480 с.

2. Должны ли предприятия опасаться Базель-2? [Електронний ресурс] — Режим доступу : http://www.finance-dms.com/basel2.html.

3. Моделювання оцінки операційного ризику комерційного банку : моног. / [О. С. Дмитрова, К. Г. Гончарова, О. В. Меренкова та ін.] ; за заг. ред. С. О. Дмитрова. — Суми : ДВНЗ «УАБС НБУ», 2010. — 264 с.

4. Дубков С. Стресс-тестирование – инструмент оценки банковских рисков / С. Дубков // Банкўскі весник. — 2008. — № 4. — С. 17—23.

5. Даньків В. Й. Теоретичні основи управління операційними ризиками / В. Й. Даньків // Науковий вісник Ужгородського університету. — (Серія «Економіка»). — 2009. — Вип. 27. — С. 158—162.

6. Глобальные исследования утечек конфиденциальной информации 2010 [Электронный ресурс] — Режим доступа : http://www.infowatch.ru/ sites/default/files/report/infowatch_global_data_leakage_report_2010_russian.pdf.

7. Годовой отчёт ОАО Банк «Морской» за 2008 год [Електронний ресурс] — Режим доступа : http://www.morskoybank.com/files/Bank_Morskoy JSC_2008.pdf.

8. Годовой отчёт ОАО Банк «Морской» за 2008 год [Електронний ресурс] — Режим доступа : http://www.morskoybank.com/files/Bank_Morskoy JSC_2009.pdf.

9. Годовой отчёт ОАО Банк «Морской» за 2008 год [Електронний ресурс] — Режим доступа : http://www.morskoybank.com/files/Bank_Morskoy JSC_2010.pdf.

10. Послуги відновлення інформації [Електронний ресурс] — Режим доступу : http://www.hddhelp.com.ua/service-ukr.htm

11. Швець Н. Р. Ризики банківських установ: проблеми, визначення та управління / Н. Р. Швець // Регіональна економіка. — 2008. — № 4. — С. 97—103.

Рекомендована кафедрою фінансів та кредиту

Стаття надійшла до редакції 20.03.12
Рекомендована до друку 14.06.12

Безштанько Дмитро Васильович — аспірант.
Університет банківської справи Національного банку України, Київ