УДК 330.131.7:330.13/.37:0615

БОНДАР О.С., канд. екон. наук

ІНФОРМАЦІЙНІ РИЗИКИ БАНКІВ: АНАЛІЗ І КІЛЬКІСНА ОЦІНКА

Вартість інформаційної безпеки та її взаємозв'язок з ризиком втрати ділової репутації і стратегічним ризиком є дуже важливою для ефективної діяльності банків. Існує ефект масштабу – чим крупніший банк, чим більш розгалужена його територіальна мережа, чим активніше він розвивається, тим більш нелінійно можуть зростати його інформаційні ризики. Управління інформаційними ризиками є складовою частиною операційних ризиків. У статті розглядаються проблеми управління інформаційними ризиками, а також основні етапи управління ІТ-ризиком – від його ідентифікації до розробки планів забезпечення безпечної безперервної банківської діяльності .

Ключові слова: ІТ-ризик, оперативні ризики, інформаційна безпека, ІТ-активи, ймовірність реалізації події.

Постановка проблеми. Конкуренція, яка посилюється в українському банківському секторі, примушує банкірів шукати шляхи зниження ризиків і витрат. Найбільші банки не хочуть "годувати" своїми клієнтськими історіями весь ринок, дрібні банки побоюються втратити і без того нечисленну клієнтуру, а регіональні банкіри бояться, що їх клієнтська інформація потрапить до рук іноземців.

Інформаційні ризики – це ризики втрати, несанкціонованої зміни інформації через перебої у функціонуванні інформаційних систем або за їх виходу з ладу, що призводить до втрати інформації. Найбільш широке визначення включає ризик виникнення збитків внаслідок неправильної організації або навмисного порушення інформаційних потоків у системі організації.

Мета і завдання. У статті розглядаються основні аспекти аналізу, оцінки і зменшення інформаційних ризиків у комерційних банках з погляду ризик-менеджменту, а саме з позицій як очікуваних, так і не очікуваних збитків, які банк повинен буде покривати своїми засобами.

Матеріалами досліджень є наукові праці вітчизняних і зарубіжних вчених стосовно інформаційної безпеки комерційних банків, оцінки вартості ІТ-активів, кількісної оцінки ІТ-ризиків, планування діяльності банків на випадок непередбачених обставин.

У **методиці** дослідження враховано, що кожен фактор формується на засадах наукової абстракції, аналізу, синтезу, аналітичного передбачення процесу в умовах ринкової економіки. Для реалізації поставлених завдань використані: історико-економічний і логічний методи, поєднання кількісного та якісного аналізів, експериментальний і розрахунковий методи.

Для кількісної оцінки ризиків необхідно оцінювати частоту і вартість втрат (розподіл величини втрат), які залежать від вартості активів банку. Але вартість інформаційних активів банку не обмежується вартістю заміни даних, апаратних засобів або програмного забезпечення. Якщо для кредитного ризику величина активів, що знаходяться під ризиком, очевидна, то у випадку операційних ризиків, які включають IT-ризики, величину активів досить складно визначити. Можна навести декілька істотних причин, що ускладнюють оцінку можливих втрат:

- IT-активи мають кілька ціннісних характеристик;
- втрати можуть набувати різного вигляду;
- реалізація одної ризикової події може призвести до втрат багатьох видів;
- між виникненням втрат різних видів існують складні системні взаємозв'язки;
- велика кількість факторів впливає на величину втрат.

Для початкової діагностики можна обмежитися побудовою карти ризиків або скоринговою оцінкою, які будуються на основі експертних шкал.

Класичний кількісний алгоритм для оцінки ризику інформаційних втрат був запропонований ще в 1974 році і використовується й по сьогодні [1]. Відповідно до нього:

$$AssetValue \times ExposureFactor \times AnnualizedRateOfOccurrence = AnnualizedLossExpectancy$$

Якщо банк має на меті послідовне впровадження кількісної оцінки величини операційного ризику на основі сучасних технологій, потрібно

вибирати способи моделювання, які дозволяють враховувати як історичні дані про збитки, так і експертні знання.

Основні прийоми і моделі для оцінки IT-ризиків повинні враховувати властивості сфери IT. По-перше, це висока динамічність. Технології постійно оновлюються і стають все більш складними, автоматизуються бізнес-процеси і окремі їх ділянки, змінюються потоки даних, впроваджуються і оновлюються інформаційні системи, модернізується обладнання. Нові інформаційні технології несуть новий ризик. По-друге, це високий комплексний взаємозв'язок в IT-середовищі. Більшість технологічних компонентів банку пов'язані між собою комп'ютерними мережами, бізнес-процеси використовують як ресурси. IT-активи, потоки даних різних систем і різних бізнес-процесів інтегруються в аналітичних та звітних модулях. Для оцінки IT-ризиків на перший план виходять методи й моделі, які дозволяють відобразити причинно-наслідкові зв'язки, оскільки у повністю автоматизованому середовищі реалізація одного фактора може привести до «ефекту доміно».

Враховуючи ці особливості для оцінки IT-ризиків, ідеальним був би метод, який дозволяє використовувати різні за своєю природою дані (експертні оцінки і кількісну інформацію про збитки банків), а також моделювати причинно-наслідкові зв'язки. Такий метод існує – це побудова казуальних моделей оцінки операційних ризиків, зокрема, байєсовські мережі. Додатковою мотивацією щодо застосування цього методу для оцінки ОР в IT-сфері є те, що він органічно дозволяє вбудувати у загальну модель IT-ризику моделі порушників, а також проводити їх своєчасну модифікацію. На підставі даних звіту з ідентифікації IT-ризиків будується «скелет» мережі, невеликий фрагмент якого у спрощеному вигляді наведено на рис.1.

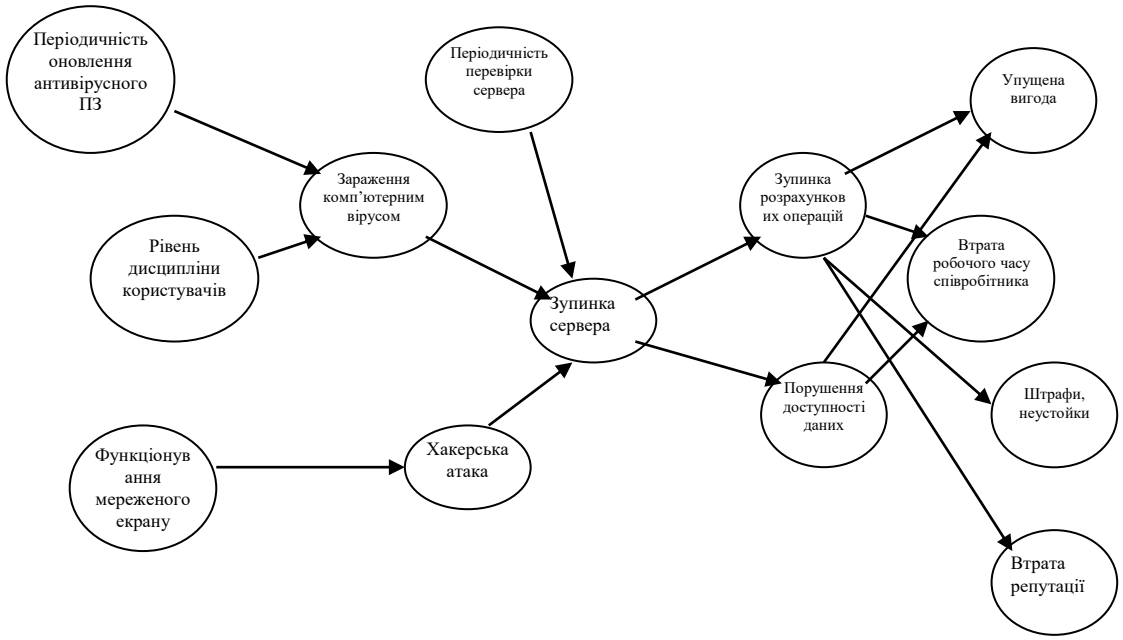

Рис. 1 Структура мережі ІТ-ризиків

Після того, як «скелет» мережі (направлений граф) створено, проводиться оцінка характеристик концептів, які в неї включено. Для рівня контролю (приклад – періодичність оновлення антивірусного ПЗ), який відображає уразливість, допустимою є бальна оцінка. Для ризикових подій (приклад – хакерська атака) проводиться оцінка ймовірності їх реалізації і за ланцюгом пов'язаних з цією подією операційних втрат. Для оцінки ймовірності реалізації подій або станів факторів ризику можна ґрунтуватися на реальних статистичних даних для деяких типів подій, на повністю експертних оцінках для інших і на змішаних оцінках для третіх, наприклад, з метою обліку поправок на майбутні тенденції. Ймовірність реалізації подій може бути вказана в байєсовській мережі у вигляді неперервної функції розподілу або таблиці ймовірностей, тобто у вигляді дискретних ймовірностей. Оскільки неперервні функції розподілу можна отримати тільки в окремих випадках через неточність статистики, далі будемо розглядати дискретні розподіли.

Для концептів, які на графі не мають стрілок, що в них входять, наприклад, подія, яка є драйвером (фактором) ризику, повинна бути вказана абсолютна ймовірність кожного з можливих наслідків події. Для концептів, на які впливають інші концепти, вказується умовна ймовірність для кожної

комбінації пов’язаних концептів. Приклад експертної таблиці умовних ймовірностей наведено в табл. 1.

Таблиця 1

	Результати – умови			
Хакерська атака	Так		Ні	
Зараження вірусом	Так	Ні	Так	Ні
Ймовірність результату події «Зупинка серверу» для різних умов				
Відбудеться	0,3	0,15	0,10	0,02
Не відбудеться	0,7	0,85	0,9	0,98

Потім за допомогою теореми Байєса складається композиція вказаного експертами розподілу з розподілами, побудованими на основі фактичних даних. Отриманий розподіл-композиція приймається для подальших розрахунків в мережі як найбільш точний опис поведінки концепту.

Для проведення кількісної оцінки необхідно обчислити абсолютні ймовірності реалізації події. Для цього застосовується формула умовної ймовірності, яка дозволяє провести розрахунок на основі заданих умовних ймовірностей і відомих ймовірностей реалізації подій, які виникають в об’єкті. Таким чином, послідовно просуваючись мережею і застосовуючи теорему Байєса поряд з формулою умовної ймовірності, можна обчислити ймовірність кожного результату для кожної ризикової події.

Залишилося визначити для кожної події ще одну характеристику – величину можливих збитків від її реалізації, яка визначається на основі статистики, експертно, за даними інших організацій з урахуванням ефекту масштабу. Під час оцінки цих параметрів завдання суттєво спрощується, якщо концепти визначені вірно, тобто присутні всі необхідні типи втрат і немає зайвих. Класифікація типів наслідків може складатися з різних точок зору. При побудові графа корисно розглядати два взаємопов’язаних рівні класифікації. Так, на першому рівні можна розділити наслідки з точки зору змін у технологічних та інформаційних активах. Для інформаційних активів традиційно прийняти три категорії наслідків – порушення цілісності,

доступності, конфіденційності, а для матеріальних активів збитки визначаються за шкалою – від повної втрати активу до збою (зупинки, неполадки) на неістотний проміжок часу. Можлива бальна оцінка. Як другий рівень класифікації можливих збитків можуть розглядатися: упущена вигода, штрафи, пені, неустойки, втрата робочого часу співробітників, зниження продуктивності праці, втрата репутації та ін.

Використання такої дворівневої класифікації дозволяє зіставити збитки у розумінні технічних спеціалістів із вартісною оцінкою, яка необхідна для управління ризиками. Величина прямих фінансових збитків може бути оцінена на основі професійного досвіду експертів або даних бази операційних збитків, причому збитки також можуть бути оцінені у термінах теорії ймовірностей, тобто на основі довірчих інтервалів або розподілу. Вартість нематеріальних збитків, таких як втрата репутації, оцінити складніше. На Заході вони оцінюються за змінами в ринковій вартості компанії, але в Україні такий підхід практично не можна застосувати, оскільки більшість банків не мають акцій, які вільно обертаються на ринку цінних паперів. Тому доцільно було б застосовувати експертний метод, який заснований на кількісних характеристиках, таких як відтік клієнтів, зниження темпів відкриття нових рахунків, депозитів та ін. Інструментом для таких оцінок може виступати модифікований метод Делфі, що дозволяє виробляти обґрунтовані і погоджені оцінки для групи експертів.

Якщо потрібно оцінити сукупний ризик деякого IT-активу, наприклад інформаційної системи, то можна знайти суму розподілу втрат за деякими ризикованими подіями, які потенційно можуть бути реалізовані в цій системі. Сума розподілу втрат за окремими ризикованими подіями, крім того, необхідна для визначення очікуваних і неочікуваних втрат, які отримуються на основі розрахунку математичного сподівання і VaR – агрегованого розподілу IT-ризику банку. Таке підсумовування по байєсовській мережі проводиться, як правило, за допомогою методу Монте-Карло-симуляції, суть

якої є імітація випадкового виникнення різних результатів подій-драйверів, які потрапляють на вхід мережі.

Висновок. Головною проблемою розробки методів оцінки IT-ризиків банку є визначення найкращого за часом, витратами і продуктивністю поєднання об'єктивних (формалізованих, математичних) і суб'єктивних (побудованих за експертними оцінками) методів в одному алгоритмі.

Література

1. Банки и банковские операции/Под ред. проф. Е.Ф. Жукова. - М.: Банки и биржи, ЮНИТИ, 1997.
2. Крамер Харальд. Полвека с теорией вероятностей: наброски воспоминаний. - М.: Знание, 1979.
3. Ларичев О.И. Объективные модели и субъективные решения. - М.: Наука, 1987.
4. Норткотт Дерил. Принятие инвестиционных решений. - М.: Банки и биржи, ЮНИТИ, 1997.
5. Банк по международным расчетам (материалы Basel 2) (www.bis.org)
6. Федеральное агентство по чрезвычайным ситуациям (США): (www.fema.gov/)
7. RiskCenter: в основном – финансовые риски (www.riskcenter.com)
8. RiskInfo: широкий спектр вопросов по управлению рисками (www.riskinfo.com)

Информационные риски банков: анализ и количественная оценка

О.С. Бондарь

Обеспечение информационной безопасности – тема, далеко не новая для украинских банков. Наши банкиры прекрасно понимают стоимость информационной безопасности и ее взаимосвязь с риском потери деловой репутации и стратегическим риском, а также эффект масштаба – чем более крупный банк, чем более разветвлена его территориальная сеть, чем активнее он развивается, тем более нелинейно могут увеличиваться его информационные риски. Однако понятие обеспечения информационной безопасности не совсем совпадает с управлением информационными рисками как частью операционных рисков, а включается в него. Эти и другие трудности управления информационными рисками, а также основные этапы управления ИТ-риском – от его идентификации к разработке планов обеспечения непрерывности деятельности – рассматриваются в статье.

Ключевые слова: ИТ-риск, оперативные риски, информационная безопасность, ИТ-активы, вероятность реализации события.

Information risks of banks: analysis and quantitative estimation

O. Bondar

Providing of information safety is not a new problem for the Ukrainian banks. Our bankers perfectly understand the value of information safety and its interdependance with the risk of business reputation loss and strategic risk, and also effect of scale – the larger bank, the more ramified its territorial network is, the more active its developing is, the more nonlinear its information risks increase. However the concept informative safety providing does not quite coincides with informative risk management by, as the part of operationa risks, but includes it. These and other difficulties of information risk management , and also basic stages of IT- risk management - from its identification to development of plans of activity continuity providing – are examined in the article.

Key words: IT- risk , operative risks, informative safety, IT- assets, probability of realization of event.