

Отже, криза, викликана коронавірусом, змусила людей задуматись про стан свого здоров'я, що підвищило попит на послуги у секторі особистого страхування. Це в свою чергу стимулювало та прискорило впровадження інноваційних технологій в діяльність страхових компаній. Вітчизняні страховики посилили діджиталізацію своїх послуг, зокрема взаємодію з клієнтами: створили онлайн-сервіси для керування договором та відстеження інформації по ньому. Зарубіжні ж компанії пішли далі і вже почали застосовувати пристрої телематики та телемедицини.

Інноваційні технології значно спрощують співпрацю клієнта та страхової компанії, знижують витрати страховика та полегшують отримання послуг для страхувальника. Тому для підвищення рівня сервісу, конкурентоспроможності та оптимізації своєї роботи страховим компаніям України варто розвивати свою інноваційну діяльність, базуючись на зарубіжному досвіді та потребах національного споживача.

Список використаних джерел

1. Комарова К.О., Рубцова Н.М., Рубцова Н.Н. Перспективи розвитку страхового ринку України в умовах діджиталізації. *Фінансове забезпечення інноваційного розвитку бізнес-середовища в світоінтеграційному просторі: збірник матеріалів Міжнародної науково-практичної конференції у Мелітополі 22-23 квітня 2021 р.* С. 136-143.
2. Офіційний сайт страхової компанії «John Hancock Insurance». URL: <https://www.johnhancock.com/life-insurance/vitality.html>. (Дата звернення: 20.10.21).
3. Жилякова О.В., Жилякова Г.С. Інноваційні технології у страхуванні життя. *Modern Economics*. 2020. № 22 (2020). С. 13-17.

УДК 336.71

Н.С. Соколовська,
аспірантка кафедри банківської справи та страхування,
ДВНЗ «КНЕУ імені Вадима Гетьмана»
ndovhopola@gmail.com

СТРАХУВАННЯ ОПЕРАЦІЙНОГО РИЗИКУ БАНКУ

Банківська діяльність здійснюється в рамках процесів фінансової глобалізації та руху капіталів на міжнародному рівні, концентрації банками

значних обсягів активів та зобов'язань, цифрової трансформації суспільства та економіки України, пов'язаною з цим діджиталізацією банківського бізнесу та посиленням ролі продажу банківських продуктів та послуг через дистанційні канали, а також необхідністю забезпечувати та підтримувати банками на належному рівні капітал з урахуванням норм національного та міжнародного законодавства. В умовах такого функціонування діяльність банків пронизана операційним ризиком, якому особливо притаманні непередбачуваність і руйнівний характер впливу. Операційний ризик супроводжує банк протягом усієї діяльності, притаманний будь-якому етапу життєвого циклу, кожної миті несе загрозу для діяльності банку та може принести банку значущі втрати (збитки).

Банківські бізнес можливості втрачаються під час збоїв інформаційних систем, якщо за спрацювання людського фактору мільйони або тисячі коштів перераховані на інший (неправильний) рахунок. Втрачаються у випадку недосконалості внутрішніх процедур, слабого контролю проведення операцій, що приводить до шахрайських дій. Працівники можуть виводити кошти з банку із застосуванням шахрайських схем, розголошувати дані клієнтів банку іншим конкурентним установам, тим самим приносити банку втрати і підривати його репутацію [1; 2]. Бізнес можливості банку втрачаються у той час, коли зусилля банківської установи спрямовані на врегулювання позову щодо припинення трудових відносин або на вирішення питання щодо застосування штрафних санкцій за несвоєчасне подання документів тощо. Це окремо наведені приклади проявів реалізації операційного ризику в банківській діяльності.

Надзвичайна ситуація природного та техногенного походження, що завдає шкоди банку, також буде подією операційного ризику. Останні десятиліття підтверджують динаміку значного зростання кількості надзвичайних ситуацій в світі, що зумовлено технічним прогресом. Обсяги матеріальних збитків від них постійно зростають. Для прикладу, в Україні збитки від стихійних лих в середньому становлять близько 580 млн грн на рік.

Мінімальна сума збитків - 102,75 млн грн у 2011 році, максимальна - 1625,8 млн грн у 2019 році [2]. Щорічні людські втрати складають 2,5 – 3 млн осіб [3].

Операційний ризик може прийматися банком у повному обсязі. Прийняття ризику - це “утримання ризиків на рівні, що перебуває в межах визначеної банком схильності до ризиків (ризик-апетиту) та не створює загрози для інтересів вкладників, інших кредиторів, власників банку та фінансової стійкості банку” [4, підпункт 29 пункту 3 глави 1 розділу I]. Однак прийняття ризику може негативно позначитись на фінансових результатах та капіталі банку в цілому.

Рівень прийнятності ризику для кожного банку індивідуальний. На нього впливає розмір банку, складність, обсяги, види, характер здійснюваних банком операцій, організаційна структура, профіль ризику, особливості діяльності банку [5]. Слід врахувати можливості банку та не перейти максимальну межу ризику (risk capacity), яку банк в змозі прийняти з огляду на рівень капіталу, регуляторні обмеження, адекватність та ефективність системи ризик-менеджменту.

Національний банк України передбачив право банків використовувати методи управління операційним ризиком залежно від категорії операційного ризику, зокрема:

“1) прийняття ризику, що передбачає продовження діяльності без змін у разі можливості понесення незначних втрат з низькою ймовірністю настання;

2) передавання ризику, що передбачає страхування, переважно, ризиків з потенційно значними втратами з низькою ймовірністю настання або ризиків, які перебувають під обмеженим контролем банку;” [4, пункт 296 глави 46 розділу VI].

Від банків також вимагається визначення політики страхування в рамках політики управління операційним ризиком, якщо стратегія з управління ризиками передбачає такий підхід щодо передавання ризику [4, підпункт 5 пункту 279 глави 45 розділу VI]. Функції з формування пропозицій щодо політики страхування та контроль за виконанням заходів з передавання

операційного ризику покладається на другу лінію захисту (підрозділ з управління ризиками банку) [4, пункт 281 глави 45 розділу VI].

Передавання ризику передбачає “передавання банком своєї відповідальності за ризик іншим особам за винагороду зі збереженням наявного рівня ризику” [4, підпункт 24 пункту 3 глави 1 розділу I]. Іншими особами є страхові компанії (страховики), які за винагороду (страхову премію) беруть на себе передбачену страховим договором відповідальність захистити банк від страхового випадку (події операційного ризику).

Увага громадськості привертається до операційного ризику, коли виникають нечасті, але високо наслідкові події. Такі події є водночас підтвердженням важливості передавання (страхування) операційних ризиків. База даних OpVar Fitch нараховує майже 500 події в США між 1978 і 2005, де збитки перевищили 10 мільйонів доларів [1; 3]. Банк Норзен Рок у 2006 році перейшов до кредитування іпотек в надлишку 100% оцінок майна. Кредити часто видавалися з урахуванням доходів домогосподарств, що звітували самотійно та не перевірялися. Коли проявилася іпотечна криза у США на 8 трильйонів доларів, бізнес-модель Норзен Року проявила всю недосконалість. Кредитна криза в серпні 2007 року спричинила швидке падіння курсу акцій банку. Брати Леман взяли на себе відповідальність за 100 мільярдів фунтів стерлінгів боргу Норзен Рок [1, с. 4].

Протягом останнього десятиріччя сталися такі значні події операційного ризику:

1. Відмивання грошей. Грудень 2012 рік. HSBS зазнав 1,92 млрд доларів збитків внаслідок не виявлення явища відмивання коштів.
2. Шахрайство. 2012 рік. Махінації LIBOR. Більше 9 млрд доларів збитків.
3. “Fat fingers” операції. 2015 рік. Deutsche Bank відшкодував клієнтам 6 млрд доларів за помилки при проведенні операцій.

4. Неналежне здійснення операцій. 2016 рік. До Goldman Sachs застосовано 5,6 млрд доларів санкцій за операції з іпотечними цінними паперами у 2005 - 2007 роках.

5. Кібератака. 2016 рік. Викрадено 81 млн доларів у Bangladesh Bank та 10 млн доларів в українському банку [6].

6. Вірусна атака вірусом Petya. 2017 рік. За кілька днів вірус, що непомітно вражав популярну програму бухгалтерського забезпечення М.Е.Дос. [7], отримував доступ до адміністративних прав керування комп'ютерною системою та поширював власні копії завдав мільйонних збитків українському бізнесу та державним установам.

2017 р. показав фактичну неготовність українських банків захисти себе від подібних втручань у роботу їхніх інформаційних систем. Від кібератак вірусу Petya постраждали 70 % українських банків: зупинилася роботи терміналів, платіжних систем, відділень банків, а також був обмежений доступ до інтернет-банкінгу та міжнародних переказів [7].

Договір страхування для банку - це захист від значних витрат (збитків) в результаті настання події операційного ризику. Недооцінка потенційних загроз операційного ризику, відсутність належного програмного забезпечення та нехтування бюджетуванням щодо захисту від операційних ризиків є лише свідченням недостатності системного підходу в управлінні операційним ризиком.

Конкурентоспроможність страхових продуктів та послуг залежить від рівня інноваційного розвитку страхового ринку в Україні, від трансформаційної адаптації до викликів сьогодення та міжнародних стандартів страхової діяльності. Вагомим для інноваційного страхового продукту щодо захисту банків від операційного ризику є адекватне вимірювання операційного ризику банку, його можливого впливу, узгодження розміру дисконтів відносно страхового відшкодування при настанні страхового випадку. Для цього необхідний аналіз сценаріїв на даних банку щодо подій операційного ризику в поєднанні з даними, отриманими із зовнішніх джерел. В інноваційному

страховому продукті має враховуватися оцінка потенційної величини збитків банку при одночасному виникненні кількох подій операційного ризику.

Крім того, інноваційний продукт страхування банку від операційного ризику повинен ґрунтуватися на оцінці всього ланцюга можливого впливу події операційного ризику. Наприклад, якщо сталося стихійне лихо та пошкоджено філію, яка генерувала найбільший дохід по мережі банку, проте на час усунення наслідків стихійного лиха та повернення роботи у штатний режим філія не може обслуговувати клієнтів і приносити дохід банку. На перший погляд, таке малоймовірно, але це небезпека ведення банківської діяльності, яка за реалізації операційного ризику може значно постраждати або й навіть може бути цілком втрачена без можливості відновлення.

Зростає затребуваність не лише інноваційності досконалого страхового продукту, а й передового каналу придбання і системи обслуговування за таким продуктом, у т.ч. дистанційне врегулювання страхової події. У страхуванні операційних ризиків з потенційно значними втратами з низькою імовірністю настання існує висока небезпека того, що страхова компанія не зможе виконати зобов'язання у повному обсязі відповідно до умов укладеного з банком договору страхування. Актуальними є також безперервний страховий захист банку з урахуванням поточного рівня операційного ризику (періодичне продовження дії страхового договору із можливістю перегляду страхової суми відповідно до рівня ризику), ймовірність анулювання договору, нечіткість умов визначення розміру страхового платежу/ суми страхової виплати та ін.

Операційний ризик не можна повністю уникнути та звести до нуля, але негативний вплив такого ризику на банк можна мінімізувати завдяки використанню ефективних заходів управління, включаючи передавання ризику – страхування.

Список використаних джерел

1. Ронді Коулман. Операційний ризик. Лондон. 2011. 25 с. URL: <https://www.researchgate.net/publication/227576075>.
2. Інформація Мінфіну про фінансові ризики та їх вплив на показники державного бюджету в 2021 році. URL: <https://mof.gov.ua/uk/zvity>.

3. Ризик-орієнтований підхід як нова парадигма системи управління техногенно-екологічною безпекою. Матеріали НАН України. 2015. URL: www.nas.gov.ua/text/pdfNews/Hrechaninov_radiointerview_HolosKyieva.pdf.

4. Положення про організацію системи управління ризиками в банках України та банківських групах: Постанова Правління НБУ від 11.06.2018 № 64. URL: <https://zakon.rada.gov.ua/laws/show/v0064500-18#Text>.

5. Закон про банки та банківську діяльність. URL: <https://zakon.rada.gov.ua/laws/show/2121-14/>.

6. Національний банк України. Мінімальні вимоги до капіталу під операційний ризик. 17.10.2019. 17с. URL: https://bank.gov.ua/admin_uploads/article/Operational_risk_2019-10_pr.pdf?v=4.

7. Павловська А., Халімон З. Кібербезпека у банківському секторі: чи допоможе IT-outsourcing? *Юридична Газета*. 06 березня 2018 р., №10 (612). URL: https://www.sk.ua/sites/default/files/kiberbezpeka_u_bankivskomu_sektori.pdf.

8. Юдіна С.В., Нагорнюк Г.О. Проблеми визначення та управління операційними ризиками комерційних банків. *Науковий вісник Ужгородського нац. університету*. 2019. № 26. С. 125 - 130.

УДК 368.02

Т.В. Татаріна,

к.е.н., доц., доцент кафедри банківської справи та страхування,
ДВНЗ «КНЕУ імені Вадима Гетьмана»,
t.v.tatarina@ukr.net

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ ПРОДАЖУ ПОСЛУГ В СТРАХУВАННІ ЖИТТЯ

Сучасні тенденції розвитку міжнародного страхового ринку свідчать про широке використання за кордоном новітніх інструментів та технологій продажу страхових продуктів. Такі інновації є затребуваними і на ринку страхування життя, адже вони сприяють поширенню послуг та заохочують потенційних клієнтів купувати страхові поліси. Особливо актуальним це стало в період пандемії, коли виникла необхідність зменшувати фізичні контакти між людьми і в той же час забезпечувати якісний захист страхувальників.

Зарубіжні страхові компанії активно застосовують цифрові портали, які пропонують прозорі та якісні страхові продукти в сегменті страхування життя, а також надають можливість клієнтам брати участь в розробці нових продуктових пропозицій. Так, німецький портал «Community Life» функціонує