

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. Позднішев (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 макрорівнях	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

нак, маркетингові ризики значно впливають на результати фінансово-господарської діяльності банківської установи, наслідки реалізації цих ризиків складно передбачити, адже вони ще недостатньо вивчені та не мають загально-визнаних методик кількісного оцінювання. Між ризик-менеджментом і маркетингом існує зв'язок, адже в маркетингу управлінські рішення стосуються продуктово-ринкової стратегії банку, а ризик-менеджмент охоплює всі функціональні сфери управління банком, у тому числі й маркетинг.

11.5. Управління інформаційними ризиками банку

Захищеність інформаційних ресурсів банку — одна з важливих складових його успішного розвитку. Результатом ігнорування цього чинника в системі управління інформаційними ризиками може стати недоотримання прибутку або збитки як самого банку, так і третіх осіб, з якими у банку є договірні відносини або фінансові зобов'язання.

Інформаційні ризики — це існуючі або очікувані ризики, котрі загрожують доходам і капіталу банку та виникають через небезпеку витоку, руйнування чи втрату необхідної інформації, використання необ'єктивної інформації, відсутність необхідної для прийняття правильних рішень інформації, а також поширення в інформаційному середовищі невігідної, негативної чи небезпечної для банку інформації, що призводить до збитків, матеріальної або моральної шкоди банку. Реалізація цих ризиків негативно впливає на керованість, цілісність, контрольованість та безперервність банківського процесу.

Ці ризики включаються в групу функціональних банківських ризиків та потребують особливої уваги керівництва банку.

Інформаційна діяльність банку здійснюється під впливом певних загроз і характеризується відповідним ступенем ризику.

В інформаційних взаємовідносинах суб'єктів ринку існують два види загроз:

- 1) загрози, пов'язані з посяганням на їх інформаційні ресурси;
- 2) загрози, що виникають при формуванні інформаційного середовища діяльності таких суб'єктів.

Основними способами реалізації інформаційних загроз є:

- 1) маніпулювання інформацією (дезінформація, викривлення інформації тощо);
- 2) запуск в інформаційне середовище неповної або неправдивої інформації;
- 3) порушення встановленого порядку інформаційного обміну, несанкціонований доступ або необґрунтоване обмеження доступу до інформаційних ресурсів, протиправний збір і використання інформації;
- 4) руйнування і використання чужих інформаційних ресурсів;
- 5) інформаційний тероризм (незаконне використання чи порушення роботи інформаційно-телекомунікаційних систем, нав'язування фальшивої та оприлюднення компрометуючої інформації тощо) [18].

Згідно з чинним законодавством інформація є об'єктом права власності, а також об'єктом володіння, використання та розпорядження. З огляду на це, ризики, які виникають під час інформаційної діяльності (інформаційні ризики)

суб'єктів ринку, виходять за межі загальновідомого технічного поняття і набувають ще і властивостей майнових чи фінансових ризиків.

Інформаційні ризики тісно пов'язані зі створенням, передачею, зберіганням і використанням інформації за допомогою електронних носіїв або інших засобів зв'язку. Інформаційні ризики характеризують можливість виникнення збитків, неотримання прибутку і інших негативних наслідків для банку в результаті застосування інформаційних технологій.

Інформаційні ризики в банку — це:

- 1) втрата або несанкціонований доступ до конфіденційної інформації;
- 2) вихід з ладу банківських інформаційних систем;
- 3) поширення шкідливого програмного коду;
- 4) несанкціоноване використання інформаційних ресурсів банку;
- 5) розкрадання / несанкціоноване розкриття або збиток, нанесений інформації третіх осіб з вини банку.

Реалізація інформаційних ризиків може призвести до порушення конфіденційності, цілісності та доступності банківської інформації або до втрати (часткової або повної) інформаційних активів банку і / або третіх осіб — клієнтів банку [22].

Інформаційні ризики за своїм походженням поділяються на три підгрупи:

- 1) ризики, пов'язані з утратою (витоком, руйнуванням, знищенням) інформації;
- 2) ризики, пов'язані з формуванням інформаційного ресурсу (використання неповної, неправдивої інформації, відсутність необхідної інформації, дезінформація тощо);
- 3) ризики, пов'язані з інформаційним впливом на діяльність банків (поширення неправдивої та негативної для банків інформації, інформаційно-психологічний вплив на працівників, клієнтів та акціонерів банків, інформаційний тероризм тощо) [21].

Для управління інформаційними ризиками потрібно ідентифікувати всі можливі небезпеки, які загрожують інформаційній системі. Для розрахунку цих ризиків використовується формула: [17]

$$AV \times EF \times ARO = ALE, \quad (11.5)$$

де AV (Asset Value) — вартість ресурсу;

EF (Exposure Factor) — міра уразливості ресурсу до загрози;

ARO (Annualized Rate of Occurrence) — оцінка ймовірності реалізації загрози;

ALE (Annualized Loss Expectancy) — підсумкові очікувані втрати від конкретної загрози за певний період часу.

Вартість ресурсів складається з вартості апаратного забезпечення, програмного забезпечення та інформації. Міра уразливості ресурсу до загрози показує, наскільки той або інший ресурс уразливий стосовно цієї загрози. Для якісної оцінки ризиків ця величина ранжується в діапазоні від 1 до 3, де:

- 1 — мінімальна міра уразливості (слабка дія),
- 2 — середня (ресурс підлягає відновленню),
- 3 — максимальна (ресурс вимагає повної заміни після реалізації загрози).

Оцінка ймовірності реалізації загрози показує, наскільки ймовірна реалізація певної загрози за певний період часу (як правило, протягом року) і також

ранжується за шкалою від 1 до 3 (низька, середня, висока). Управління ризиками зводиться до зниження величин високих і середніх ризиків до значень низьких ризиків, коли стає можливим їх прийняття. Зниження величини ризику досягається за рахунок зменшення складових (AV, EF) шляхом вжиття певних заходів [19].

Оскільки в інформаційній економіці, яка сформувалася в сучасних умовах, виключити ризик з інформаційних взаємовідносин банків неможливо, то для попередження шкоди, заподіяної від реалізації інформаційних загроз, слід створити систему управління інформаційними ризиками. Процес управління інформаційними ризиками передбачає проведення процедур аналізу, контролю і мінімізації ризиків.

Аналіз ризиків передбачає їх визначення та оцінювання. При визначенні ризиків установлюється, які саме інформаційні ризики можуть існувати або існують у діяльності банку або при проведенні ним конкретної банківської операції, як вони можуть вплинути на діяльність чи операцію і яка існує імовірність настання негативної ситуації від дії ризику. Оцінювання інформаційного ризику включає оцінку обсягу збитків, яких може зазнати банк у результаті прояву зазначеного ризику. Контроль інформаційних ризиків передбачає проведення заходів щодо виявлення умов, за яких такі ризики можуть бути мінімальними, істотними або значними. Мінімізація інформаційних ризиків передбачає вжиття заходів, спрямованих на зниження імовірності негативного впливу ризиків, їх уникнення або зменшення величини ризиків.

З огляду на значну роль інформації в діяльності банків **система управління інформаційними ризиками** має включати підсистеми:

- 1) захисту інформації;
- 2) збору інформації та інформаційних досліджень;
- 3) протидії інформаційному впливу;
- 4) управлінську підсистему.

Основними завданнями підсистеми захисту інформації банку є: виявлення інформації, що підлягає захисту, визначення місць зосередження та носіїв інформації, яка підлягає захисту, визначення можливих способів несанкціонованого доступу до такої інформації, розроблення і впровадження організаційних, правових, технічних, програмних, криптографічних та апаратних заходів захисту інформації.

Оцінювання ризиків втрати інформації в банку передбачає оцінювання вартості інформаційних ресурсів, щодо яких існує ризик втрати, та оцінювання, власне, самого ризику як імовірності реалізації певної загрози, у даному разі пов'язаної з втратою інформації.

Вартість інформації оцінюється через її комерційну цінність, яка, у свою чергу, визначається:

- а) величиною збитків, які можуть настати у зв'язку з її втратою;
- б) обсягом (перспективами) вигоди, яку може отримати банк, використовуючи наявну в нього інформацію;
- в) витратами, пов'язаними з виробленням, отриманням та захистом такої інформації.

Наприклад, цінність банківської таємниці може бути визначена через обсяги залучених коштів від клієнтів банку, інформацію про комерційну та фінансову діяльність яких зберігає банк.

На величину інформаційного ризику як імовірності реалізації певної загрози щодо відповідної інформації банку впливає кілька чинників. Головними серед них є привабливість інформації для суб'єктів загроз, її цінність, актуальність, доступність та рівень захисту. Через ці чинники визначається рівень критичності інформації. Виходячи з цього імовірність реалізації загроз (як, власне, ризик втрати інформації) може бути високою (коли всі показники набувають суттєвої актуальності), середньою (за умов високої актуальності хоча б одного показника) і звичайною (для клієнтів банку, які не відрізняються високою активністю на ринку).

Контроль ризиків втрати інформації в банку забезпечується проведенням періодичних перевірок та аналізом стійкості його інформаційної системи до внутрішніх і зовнішніх загроз, своєчасного виявлення уразливих місць в її захисті. Крім того, на основі постійного моніторингу інформаційного середовища діяльності банку виявляються ознаки небезпек та загроз банківській інформації. Особлива увага приділяється виявленню партнерів, взаємовідносини банку з якими можуть створювати для нього певні ризики втрати інформації, а також суб'єктів, діяльність яких може бути спрямована на несанкціоноване оволодіння банківською інформацією.

Для мінімізації ризику втрати інформації банки мають вживати відповідних заходів, диференціюючи їх залежно від характеру загроз [21]. До таких заходів належать:

- 1) формування правових умов захисту інформації безпосередньо у банку;
- 2) створення системи захисту інформації банківської інформаційної мережі (організаційні, технічні, апаратні, криптографічні заходи тощо);
- 3) контроль за носіями інформації;
- 4) запровадження надійної системи документообігу в банку;
- 5) забезпечення надійної охорони банку.

Базовою є підсистема збору інформації та інформаційних досліджень. Процес управління ризиками, які виникають у процесі формування банками інформаційного ресурсу, має особливий характер. Тут існує певна проблема, пов'язана з необхідністю інформаційного забезпечення діяльності банків і відсутністю для цього відповідного правового регулювання. На цей час в Україні немає законодавства, яке б регулювало права, умови та порядок доступу банків до джерел інформації (наприклад, державних баз даних), необхідної їм для забезпечення банківської діяльності. Відсутність такого законодавства спричиняє багато ризиків, які виникають у процесі інформаційного забезпечення банківських операцій.

Аналіз ризиків, що можуть виникати при формуванні інформаційного ресурсу банку за умови відсутності необхідного правового регулювання, показує, що найпоширенішими є:

- 1) ризик відсутності необхідної банку інформації,
- 2) ризик отримання та використання неповної, необ'єктивної чи недостовірної інформації,

3) ризик дезінформації.

Ризик відсутності інформації виникає, коли банку в короткі терміни потрібна буде конкретна інформація, або коли об'єкти і джерела певної інформації невідомі. Особливо такі ризики характерні для кредитної діяльності банків, при проведенні операцій з пластиковими платіжними засобами, а також при прийнятті управлінських рішень у процесі фінансового моніторингу сумнівних операцій та ідентифікації осіб, щодо яких є підозра в легалізації (відмиванні) коштів, отриманих незаконним шляхом. Брак необхідної банку інформації призводить до прийняття неправильних рішень і, як наслідок, неефективних дій банку на ринку банківських послуг.

Ризик отримання та використання неповної та необ'єктивної інформації в банківській діяльності існує завжди. Невизначеність при прийнятті рішень є характерною для бізнес-діяльності. Тобто якщо ризик відсутності інформації менш імовірний для банків, то ризик отримання та використання неповної чи необ'єктивної інформації практично завжди існуватиме в діяльності банків. Разом з тим і перший, і другий ризики мають бути враховані при здійсненні конкретних дій чи проведенні банком конкретної операції.

Ризик дезінформації може виникати в банку через загострені взаємовідносини з конкурентами чи недобросовісну поведінку клієнтів в стосуватися умов, суб'єктів, мети взаємовідносин з банком. У перших двох випадках ризики (ризик відсутності інформації та ризик використання неповної чи необ'єктивної інформації) мають об'єктивний характер, оскільки певні суб'єкти прагнуть захистити свою інформацію, а банк, навпаки, — її отримати. Водночас ризик дезінформації банку створюється певними суб'єктами штучно, з метою ввести банк в оману. За таких умов ризик дезінформації, як правило, завжди має значні негативні наслідки для банку.

Оцінка ризиків, пов'язаних з формуванням інформаційного ресурсу, може визначатись ціною (вартістю) певної банківської операції, щодо якої здійснюється інформаційне забезпечення, або обсягом прибутку, який може отримати банк, приймаючи рішення на основі об'єктивної інформації. Проте обсяги операцій чи прибутків не можуть дати повну уяву (оцінку) ризикам, пов'язаним із формуванням інформаційного ресурсу. Такими показниками може вимірюватися лише ризик відсутності інформації, тоді як на оцінку інших ризиків істотно впливатиме якість інформації, якою забезпечується певна операція чи рішення.

Показниками якості інформації є її *достовірність, повнота та актуальність*.

Достовірною вважається інформація, отримана з трьох і більше незалежних джерел або з одного надійного джерела, а також інформація, об'єктивність якої підтверджена додатковою перевіркою.

Повною вважатиметься інформація, з якої можна скласти характеристику об'єкта, достатню для формування об'єктивного уявлення про нього.

Актуальною є інформація, в якій на даний час має потребу банк. Усі інші характеристики якості інформації, які перебувають у межах від неякісної до якісної, вважаються такими, що формують певний ризик використання інформації.

У практичній діяльності банки за величину ризику при використанні якісної інформації беруть коефіцієнт від 0,8 до 1,0, за наявності неякісної інформації — від 0 до 0,5. Усі інші коефіцієнти беруться для інформації, якість якої вища від такої, що може вважатись неякісною. За таких умов оцінка ризику формування інформаційного ресурсу для інформаційного забезпечення певної банківської операції чи рішення буде визначатись як добуток від обсягу операції (угоди, рішення) та відповідного коефіцієнта якості інформації.

Контроль ризиків, пов'язаних із формуванням інформаційного ресурсу, передбачає проведення аналітичної роботи з усіма видами інформації, яка поступає у банк і планується до використання для забезпечення його діяльності. У процесі аналітичної роботи інформація узагальнюється, порівнюється та перевіряється. Відомості, щодо яких є сумнів у їх достовірності, вилучаються з інформаційного ресурсу. Уся інформація підлягає обробці, у результаті чого отримуються інформаційні дані, використання яких несе в собі мінімальний ризик для банку.

Мінімізація ризиків, що виникають при формуванні інформаційного ресурсу банку та інформаційному забезпеченні його операцій і управлінських рішень, здійснюється шляхом проведення відповідних заходів, передусім створення та виконання інформаційного плану. Насамперед звертається увага на організацію інформаційно-аналітичної роботи в банку, яка є одним із необхідних видів забезпечення банківської діяльності. Така робота передбачає періодичне проведення в підрозділах банку інформаційного аудиту, в процесі якого виявляється необхідна для забезпечення конкретної діяльності банку та його операцій юридична, комерційна, фінансова, технологічна та інша інформація. Уся інформація, отримана від маркетингової діяльності, інформаційного моніторингу та аудиту, а також комерційної розвідки, узагальнюється, аналізується, за необхідності перевіряється і формується у відповідні бази даних.

Основними способами мінімізації ризиків при формуванні інформаційних ресурсів банку є створення *власних інформаційних баз даних* (наприклад, BL — база даних недобросовісних позичальників банку), які мають стати головним джерелом інформації для інформаційного забезпечення банківських операцій та управлінських рішень. Така база повинна постійно оновлюватись та доповнюватись.

Показники якості інформації, якою оперує банк, особливо важливі в процесі здійснення банком кредитної діяльності, оскільки це прямо впливає на рівень кредитного ризику, який є найсуттєвішим в банківській діяльності.

Дуже низький ризик визначається за умови, коли наявність інформації про позичальника становить не менше 90 % від необхідної банку. До позичальників з низьким ризиком відносять тих суб'єктів, щодо яких отримана інформація дає змогу зробити висновки про відсутність у їхній діяльності кримінальних зв'язків, стабільну комерційну діяльність, позитивну кредитну історію, багатопрофільну діяльність, наявність філій, задовільний фінансовий стан.

Низький ризик визначається, якщо банк отримав не менше, ніж 80 % необхідної йому інформації про позичальника і якщо така інформація дає змогу характеризувати позичальника як суб'єкта, у діяльності якого немає кримінальних зв'язків, підтримується стабільна комерційна діяльність на основі

перспективного бізнесу, який здійснюється за участі багатьох партнерів. Крім того, отримана інформація дає змогу зробити висновок про задовільний фінансовий стан та позитивну кредитну історію позичальника.

Середній ризик визнається для позичальників, щодо яких банк отримав не менше як 70 % необхідної йому інформації. У такому разі інформаційні характеристики можуть вказувати на діяльність позичальника в ризиковій сфері бізнесу, на факти несвоєчасного повернення кредитів та сплати податків або відсутність досвіду роботи з кредитними коштами, велику кількість рахунків у різних банках, частина з яких (рахунків) є непрацюючими.

Високий ризик визнається для позичальників, щодо яких банк отримав не менше 60 % необхідної йому інформації, з якої можна зробити висновок про факти неповернення кредитів у діяльності позичальника, судові розгляди справ за позовами до позичальника, наявність кредиторських боргів, часту реорганізацію структури позичальника, велику плінність кадрів, нестійкий фінансовий стан, факти недобросовісної конкуренції, до яких вдається позичальник.

Дуже високий ризик виникає за умови, коли банк отримує менше 60 % необхідної йому інформації про позичальника. До того ж отримана інформація характеризує останнього як такого, у якого немає ознак реальної господарської діяльності, є непорозуміння з правоохоронними органами та факти недбалого ставлення до виконання своїх зобов'язань. З отриманої інформації неможливо скласти об'єктивного висновку про фінансовий стан позичальника та можливості і перспективи його підприємницької діяльності.

За такого підходу у сукупності з аналізом інших видів ризику кредитний менеджер отримує об'єктивний висновок щодо надійності позичальника у його взаємовідносинах з банком.

Важливою складовою ризик-менеджменту банку є підсистема протидії інформаційному впливу.

Інформаційний вплив — це використання спеціальних інформаційних технологій з метою формування або зміни поведінки окремих осіб чи груп осіб стосовно певних подій, об'єктів, діяльності. Формування або зміна поведінки залежно від того, на кого спрямована дія інформаційних технологій, може здійснюватися через застосування технологій маніпулювання свідомістю. Технології маніпулювання свідомістю здатні викликати у людей певне ставлення до суб'єкта чи організації (недовіру, розчарування, огиду тощо), а також формувати певну поведінку (страйки, демонстрації, саботаж, акти масової непокорі, безладдя).

За таких обставин *основними видами ризику інформаційного впливу* для банку є:

- 1) ризик втрати позитивного іміджу банку на ринку банківських послуг;
- 2) ризик потрапити у конфліктні ситуації з власним персоналом, клієнтами, акціонерами, державними органами;
- 3) ризик блокування роботи банку через численні перевірки його діяльності.

Ризики інформаційного впливу можуть мати постійний характер, як результат певних відносин банків з різними суб'єктами, або формуватись ситуативно як результат цілеспрямованої дії певних суб'єктів. В останньому випадку найбільш

характерним є так звані інформаційні атаки, коли з різних джерел одночасно або в невеликий проміжок часу в інформаційне середовище банку подається негативна для нього інформація. Найбільш імовірно, що інформаційні атаки можуть здійснюватись за умов, коли банк перебуває у стані конфронтації, конкурентного суперництва чи протиборства з певними суб'єктами ринку або іншими особами. За таких обставин ризик потрапляння банку в ситуацію активного нагнітання навколо нього негативної інформації буде істотним. У цьому разі, як наслідок, виникають інші види ризиків різного характеру — ризик втрати репутації, ризик погіршення або втрати іміджу, ризик втрати клієнтів, зменшення обсягів операцій, отримання збитків.

Основними формами інформаційних атак, унаслідок яких може виникати ризик погіршення іміджу банку, є: поширення чуток про недоліки в діяльності банку, порушення його ліквідності та платоспроможності, безпідставне акцентування уваги у масових виданнях та виступах на окремих негативних випадках та подіях, що відбулися в банку, особливо пов'язаних з втратою ним коштів, поширення недостовірної та компрометуючої інформації стосовно окремих посадових осіб банку, тенденційне висвітлення окремих фактів з діяльності банку у засобах масової інформації, модифікація виступів, публікацій, викладених посадовими особами банку, проведення інформаційних заходів, у яких банк та його діяльність перебуває в центрі уваги.

Так само може поширюватись інформація, що створює ризик потрапляння банку у різного роду конфліктні ситуації. Ризик блокування роботи банку через численні перевірки його діяльності виникає внаслідок поширення в інформаційному середовищі та безпосередньо доведення до органів контролю і банківського нагляду негативної інформації про діяльність банку.

Отже, ризики інформаційного впливу виникають через поширення в інформаційному середовищі банку відповідним чином спрямованої інформації. Оцінка ризиків впливу спрямовується на визначення сфери діяльності та взаємовідносин банку, щодо яких може поширюватись негативна для банку інформація в той чи інший період його діяльності і таким чином виникати певний ризик.

Управлінська підсистема пов'язана з організацією менеджменту банківської діяльності. У процесі контролю ризиків здійснюється моніторинг інформаційного середовища банку з погляду виявлення ознак, які можуть вказувати на передумови появи або безпосередню появу ризиків інформаційного впливу.

Для мінімізації інформаційних ризиків впливу банкам слід вживати такі заходи:

- 1) періодичне поширення через різні інформаційні канали позитивної інформації про банк;
- 2) періодичне поширення в інформаційному середовищі банку інформації про результати його роботи;
- 3) формування банківського патріотизму, пропаганда позитивного іміджу банку на ринку;
- 4) проведення спеціальних інформаційних операцій стосовно зміни об'єктів інформаційного впливу, дезорієнтації суб'єктів, що застосовують заходи впливу, контрпропаганди та антикомпрометації.

Особливу небезпеку в сучасних умовах становить для банку **ризик інформаційного тероризму**, під яким розуміють використання різноманітних інформаційних технологій та продуктів для ураження інформаційних об'єктів (комп'ютерних мереж та систем, засобів комунікації, електронних засобів масової інформації), інформаційно-психологічного пригнічення свідомості людей, соціальних груп на основі формування страху, високого емоційного напруження в їх поведінці. Інформаційний тероризм реалізується через розповсюдження комп'ютерних «вірусів», установлення програмних і апаратних закладних пристроїв, упровадження радіоелектронних приладів перехоплення інформації, незаконне використання чи порушення роботи інформаційних і телекомунікаційних систем, нав'язування фальшивої інформації, оприлюднення компроментуючої інформації і т. п.

Особлива небезпека інформаційного тероризму полягає у тому, що він має глобальний характер через глобалізацію високих технологій інформаційного обміну, а тому може зумовлювати системні кризи не тільки окремих об'єктів, а й у цілих галузях, сферах діяльності чи навіть у країнах. Прикладом ризику інформаційного тероризму є атака на інформаційні системи банків, державних установ та великих фірм («вірус Петя»), яка була здійснена влітку 2017 року одночасно в кількох країнах світу.

Основними засобами інформаційного тероризму в атаках на мережі і системи комунікації є засоби електронної розвідки та радіоелектронної боротьби, за допомогою яких може вилучатись мовна чи електронна інформація, що циркулює по радіоканалах та технічних каналах зв'язку. У процесі оцінювання ризиків інформаційного тероризму слід визначити, які наслідки можуть настати для банку через інформаційні атаки терористів як з погляду фінансів, так і з погляду погіршення іміджу банку. Мінімізація ризиків інформаційного тероризму здійснюється проведенням заходів захисту технічного, програмного, криптографічного, апаратного, адміністративного, правового характеру власних інформаційних мереж та систем, а також заходів формування стійкого позитивного іміджу банку на ринку банківських послуг, пропаганди його послуг та реклами банківських продуктів.

Таким чином, інформаційні ризики, які виникають в діяльності банків, слід розглядати та аналізувати не як окремо взяті, а системно, із врахуванням взаємовпливу на інші ризики банківської діяльності.

ОСНОВНІ ПОНЯТТЯ ТА ПІДСУМКИ

Функціональні ризики пов'язані з процесами створення і впровадження нових банківських продуктів і послуг, збору, обробки, аналізу і передавання інформації, підготовкою кадрового потенціалу і виконанням інших адміністративно-господарських операцій.

Функціональні ризики банку не менш небезпечні, ніж фінансові ризики, але їх важче ідентифікувати та визначати кількісно.

Операційно-технологічний ризик банку — потенційний ризик для довгострокового існування банківської установи, що виникає через недоліки корпоративного управління, системи внутрішнього контролю або інформаційних технологій і процесів обробки інформації з погляду керованості, універсальності, надійності, контролюваності і безперервності роботи.

Три основні методи оцінювання операційного ризику:

- 4) метод ключового індикатора;
- 5) стандартизований метод;
- 6) метод поглиблених вимірів.

Ризики електронного банкінгу — це сукупність ризиків, що властиві процесу електронного банківського обслуговування клієнтів, які характеризуються ймовірністю виникнення певних подій чи збоїв в програмному забезпеченні, що ускладнюють чи унеможливають здійснення банківських операцій чи послуг клієнтами у дистанційному режимі обслуговування.

Операційний ризик у контексті функціонування електронного банкінгу — це ймовірні поточні або перспективні фінансові втрати, що зумовлені помилками при виконанні банківських операцій у результаті шахрайських дій по відношенню до кредитної організації, а також порушення безперервності дії її автоматизованих систем, за допомогою яких здійснюється електронне банківське обслуговування.

Ризик ліквідності в контексті функціонування електронного банкінгу — це ймовірні у перспективі фінансові втрати, що зумовлені нездатністю кредитної організації своєчасно та в повному обсязі виконати свої фінансові зобов'язання перед клієнтами за рахунок змін характеру управління ліквідністю в умовах відкритої мережевої взаємодії.

Ризик втрати репутації — наявний або потенційний ризик для надходжень та капіталу, який виникає через несприятливе сприйняття іміджу фінансової установи клієнтами, контрагентами, акціонерами (учасниками) або органами нагляду.

Юридичний ризик — наявний або потенційний ризик для надходжень та капіталу, який виникає через порушення або недотримання банком вимог законів, нормативно-правових актів, угод, заведеної практики або етичних норм, а також через можливість двозначного тлумачення законів або правил.

Стратегічний ризик — наявний або потенційний ризик для надходжень та капіталу, який виникає через неправильні управлінські рішення, неналежну реалізацію рішень і неадекватне реагування на зміни в бізнес-середовищі. Цей ризик виникає внаслідок несумісності

Ризик інформаційних технологій — це існуючий або очікуваний ризик, котрий загрожує доходам і капіталу та виникає через неадекватність інформаційних технологій та обробки інформаційних потоків.

Ризик упровадження інноваційних продуктів і послуг — це ймовірність не досягти запланованого рівня окупності нових банківських продуктів, послуг, операцій чи технологій.

Маркетингові ризики — сукупність ризиків, які супроводжують маркетингову діяльність банку та характеризуються ймовірністю виникнення певних подій та їх наслідками, що ускладнюють чи унеможливають досяг-

нення цілей на окремих етапах маркетингової діяльності чи цілком у сфері маркетингу.

Макросередовище банківського маркетингу — це комплекс факторів, які чинять безпосередній вплив на будь-якого учасника банківського ринку ззовні. До них відносять демографічні, економічні, природно-географічні, науково-технічні, культурні та правові.

Мікросередовище банківського маркетингу складає група ринкових факторів, на які банківська установа може безпосередньо вплинути.

Внутрішні маркетингові ризики банку — група маркетингових ризиків, що визначається характеристикою внутрішнього середовища маркетингу банку

Внутрішні комунікації (внутрішній PR) у банку — система комунікаційних взаємин всередині банку, між керівництвом та співробітниками, співробітників між собою.

Життєвий цикл банківського продукту — період функціонування банківського продукту — від ідеї до припинення „виробництва”; включає фази розробки продукту, впровадження на ринку, зростання продаж, зрілості, насичення та занепаду (зняття з пропозиції); на практиці продукт не знімається назавжди, а модифікується.

Зовнішній PR у банку — пропаганда, направлена на формування благозичливого відношення до зовнішніх, відносно банку, суспільних груп (клієнти, потенційні клієнти, громадські та благодійні організації, особи, які проживають на компактній території тощо)

Маркетинговий план банку — це головний інструмент ухвалення маркетингових управлінських рішень вищим керівництвом банку, інструмент підтримки діяльності бізнес-підрозділів і філіалів. Він об'єднує стратегічні, маркетингові і фінансові цілі продажів банківських продуктів, координує основні маркетингові види діяльності.

Інструментальні маркетингові ризики у банку — ймовірність неефективного використання інструментів маркетингу у банку.

Ризики клієнтів банку — ризики зміни обсягів та структури клієнтської бази на основі зміни потреб, поведінки, лояльності та інших характеристик клієнтів.

Ризики комунікацій у банку — ймовірність помилок у комунікаційній політиці банку. Мають наслідком недостатнє інформування клієнтів про існуючі й нові продукти і послуги або банк у цілому, зниження або втрату лояльності клієнтів до банку, створення несприятливого для банку політичного, морального та іншого середовища, що кінець кінцем призведе до падіння попиту на банківські продукти (окремі або банку в цілому).

Ризики конкурентів банку — ризик зміни конкурентної позиції старих конкурентів банку, ризик появи нових конкурентів банку.

Ризики контактних аудиторій банку — ризики банку, що пов'язані із вірогідністю втрати впливу на контактні аудиторії або втрати відповідного відношення контактних аудиторій до банку або із появою нових контактних аудиторій, або із втратою важливості певної контактної аудиторії, на контакт із якою банк продовжує витрачати кошти. Вимірюється ймовірністю додаткових витрат банку на комунікації із контактними аудиторіями як результат настання несприятливих подій.

Ризики інструментів продукту банку — можливі втрати внаслідок невідповідності стратегії банку сформованому продуктовому ряду банку.

Ризики маркетингових інструментів ціни у банку — ймовірність негативних наслідків політики ціноутворення на банківські продукти та послуги.

Ризики маркетингового планування (стратегічні, тактичні та оперативні маркетингові ризики) у банку — ризики невідповідності маркетингових планів очікуваним результатам, або ризики невідповідності результатів, які плануються, тим результатам, що реально міг досягти банк завдяки маркетинговому плануванню.

Ризики розподілу — ймовірність невідповідності каналів та інструментів доставки банківських продуктів потребам існуючих та перспективних клієнтів.

Інформаційні ризики — це існуючі або очікувані ризики, котрі загрожують доходам і капіталу банку та виникають через небезпеку витоку, руйнування чи втрату необхідної інформації, використання необ'єктивної інформації, відсутність необхідної для прийняття правильних рішень інформації, а також поширення в інформаційному середовищі невігідної, негативної чи небезпечної для банку інформації, що призводить до збитків, матеріальної або моральної шкоди банку.

Ризик інформаційного впливу — це ризик використання спеціальних інформаційних технологій з метою формування або зміни поведінки окремих осіб чи груп осіб стосовно певних подій, об'єктів, діяльності.

Ризик інформаційного тероризму — це використання різноманітних інформаційних технологій та продуктів для ураження інформаційних об'єктів (комп'ютерних мереж та систем, засобів комунікації, електронних засобів масової інформації), інформаційно-психологічного пригнічення свідомості людей, соціальних груп на основі формування страху, високого емоційного напруження в їх поведінці.

Система управління інформаційними ризиками включає підсистеми: 1) захисту інформації; 2) збору інформації та інформаційних досліджень; 3) протидії інформаційному впливу; 4) управлінську підсистему.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Які види банківських ризиків належать до функціональних?
2. Які з функціональних банківських ризиків можна оцінити кількісно, а які ні?
3. Назвіть види операційно-технологічних ризиків.
4. Які основні критерії використовують для оцінювання якості управління операційно-технологічним ризиком?
5. Які існують три основні методи оцінювання операційного ризику та в чому полягає їх відмінність?
6. Назвіть основні ризики електронного банкінгу та поясніть їх специфіку?
7. Який міжнародний нормативний акт контролює процес управління ризиками електронного банкінгу?

8. Назвіть основні принципи управління ризиками електронного банкінгу відповідно до вимог Базельського комітету з питань банківського нагляду?
9. В чому полягає відмінність між групами принципів А. Нагляд з позиції вищого керівництва банку та В. Управління безпекою?
10. Як пов'язаний ризик втрати репутації з іншими видами банківських ризиків?
11. Які основні критерії використовують для оцінювання рівня управління ризиком репутації?
12. З чим пов'язане виникнення юридичного ризику для банку?
13. Які основні критерії оцінювання рівня управління юридичним ризиком?
14. Які основні критерії оцінювання рівня управління стратегічним ризиком?
15. Назвіть джерела виникнення інформаційних ризиків в банку.
16. Які заходи має вживати банк для зниження ризику втрати інформації?
17. В чому полягає ризик інформаційного тероризму в банківській діяльності?

ЛІТЕРАТУРА

1. Методичні вказівки з інспектування банків «Система оцінки ризиків»: Постанова Правління НБУ від 15.03.2004 р. № 104.
2. Про методичні рекомендації щодо організації та функціонування систем ризик-менеджменту в банках України: Постанова Правління Національного банку України від 02.08.2004 р.
3. Губенко С. М. Операційний ризик // Український інвестиційний журнал WELCOME. — 2001. — № 7—8. — С. 56—58.
4. Богданов А. Операционный риск и его влияние на устойчивую работу финансовой организации // Банковские технологии. — 2003. — № 7. — С. 80—88.
5. Коноваленко Н. Методология определения операционного риска // Банковская практика за рубежом. — 2003. — № 7. — С. 80—88.
6. Недилько А. Автоматизация управления рисками // Банковская практика за рубежом. — 2003. — № 9. — С. 81—85.
7. Запорожець З. Управління банківськими ризиками в контексті інформаційних технологій // Вісник НБУ. — 2004. — № 10. — С. 54—59.
8. Старостіна А. О., Кравченко В. А. Ризик-менеджмент: теорія та практика: Навч. посіб. — К.: ІВЦ «Вид-во “Політехніка”», 2004. — 200 с.
9. Лямин Л. Применение технологий электронного банкинга. Риск-ориентированный подход [Текст] / Л. Лямин. — М.: КНОРУС; ЦИПСИР, 2011. — 336 с.
10. Ревенков, П. В. Актуальные направления регулирования электронного банкинга / П. В. Ревенков, А. Л. Поспелов // Финансы и кредит. — 2015. — № 24(648). — С. 2—13.
11. Risk Management Principles for Electronic Banking. — Basle: Basle Committee on Banking Supervision, July 2003. — 35 с.
12. Нікітін А.В., Бортніков Г.П., Федорченко А.В. Маркетинг у банку: Навч. посіб. / за ред. А.В. Нікітіна — К.: КНЕУ, 2006 — 432 с.
13. Маркетинг у банку. Навчально-методичний посібник для самостійного вивчення дисципліни. // А.В. Нікітін (керівник авт. колективу), Іванова Т.Г., Брітченко І.Г., Момот О.М. — К.: КНЕУ, 2010. — 475 с.
14. Старостіна А.А., Кравченко В.В. Ризик-менеджмент у маркетингу. // «Стратегія економічного розвитку України», 2002 — с. 10-16
15. Кузнецова Л.В., Завадська Д.В. Жердецька Л.В. Маркетинг у банку: теорія та методологія: Монографія. — Одеса, Видавництво «Атлант», 2010 — 717 с.

16. *Александров А.* Private banking в Украине. Опыт становления: Научное изд. // Киев: Изд-во «Кисс», 2011 — 303 с.
17. *Вуколов В.В.* Інформаційні ризики в державному управлінні [Електронний ресурс]. — Режим доступу: http://archive.nbuv.gov.ua/e-journals/Patp/2010_2/10vvvrdu.pdf.
18. *Зинкевич В., Штатов Д.* Информационные риски: анализ и количественная оценка // Бухгалтерия и банки. — 2007. — № 1.
19. *Кузнецова Н.В.* Деякі аспекти мінімізації інформаційних ризиків у банківській діяльності // Системні дослідження та інформаційні технології. — 2014. — № 1.
20. *Петренко С.А., Симонов С.В.* Методики и технологии управления информационными рисками [Электронный ресурс]. — Режим доступу: <http://citforum.ru/security/articles/risk/>.
21. *Романенко Л.Ф.* Ризики у банківській діяльності / Л.Ф. Романенко, А.В. Коротеєва // Фінанси України.-2003.- №5.
22. *Спильниченко В.К.* Информационные риски в банкинге [Электронный ресурс]. — Режим доступу: <https://cyberleninka.ru/article/n/informatsionnye-riski-v-bankinge>
23. *Яременко С.М.* Інформаційні ризики в банківській діяльності / С.М. Яременко, М.І. Диба, М.І. Зубок // Вісник Національного банку України. — 2007. — № 9. — С. 28–35.
24. *Управління банківськими ризиками: Навчальний посібник / За ред. Л. О. Примостки.* К.: КНЕУ, 2007. — 600 с.