УДК 336.7

Безштанько Д.В.

ІНФОРМАЦІЙНА БЕЗПЕКА БАНКУ В СИСТЕМІ УПРАВЛІННЯ ОПЕРАЦІЙНИМ РИЗИКОМ

Анотація. В роботі висвітлено основні проблеми безпеки інформаційної системи банку. Досліджено суперечності та виявлено ризики, що заважають ефективній реалізації системи управління операційним ризиком в напрямку інформаційної безпеки. запропоновано заходи по оптимізації рівня інформаційних ризиків, що загрожують, або можуть загрожувати банківській установі.

Ключові слова: операційний ризик банку, інформаційні технології, шахрайство, інформаційна безпека.

Вступ. Входження України до світового співтовариства неможливе без адаптації національного законодавства до світових вимог. Підписання ІІ Базельської домовленості виявило нові закономірності у побудові діяльності фінансових установ. Серед нововведень виділяють необхідність створення резервів під операційні ризики банку.

Впровадження в банківську діяльність системи управління операційним ризиком покликане зменшити втрати банку від недбалості персоналу, нестабільної роботи інформаційної системи та зовнішнього впливу, що сприяє банківській установі досягнути поставленої стратегічної мети з мінімальними фінансовими, ресурсними та інформаційними втратами.

Питання інформаційної безпеки фінансової установи широко представлене в роботах таких вітчизняних та зарубіжних учених-економістів як: А. Володина, А. Козлова, А. Лукацького, А. Мамонтова, Н. Романова, А Румянцева, Б. Сазикина, В. Сердюка, А. Синцова, А. Смирнова. Однак в їхніх роботах не виділяються механізми для вирішення питань інтеграції інформаційних активів до системи контролю операційного ризику, а також особливості, що можуть виникати при спробі такої інтеграції.

Постановка завдання. Метою статті є висвітлення питань інтеграції інформаційної безпеки банку до системи управління операційним ризиком відповідно до вимог ризик-менеджменту. Досягнення даної мети реалізується через аналіз проблем інформаційної системи банку, пошук протиріч в інформаційній системі, і як наслідок – визначення місця інформаційної безпеки в системі управління операційним ризиком банку.

Результати. Більшість банків України на сьогоднішній день не мають комплексної системи накопичення та аналізу даних про втрати від операційних ризиків. Створення такої системи – довгий процес, і якщо не розпочати його формувати в найближчому майбутньому, то банк ще довго не матиме можливості реально оцінювати власні операційні ризики і визначати економічно обґрунтовану необхідність в капіталі для покриття операційних ризиків.

Не можна виділити практично жодної операції в банку, що прямо чи опосередковано не була б пов’язана з інформаційними системами банку. Однак, передумовами концентрації операційних ризиків банку саме в області інформаційних технологій наступні:

1. Витрати на інформаційні технології складають значну долю в структурі сукупних витрат банку, але не на розробку стратегії чи тактичного розвитку. Недоліки

процесу закупівлі обладнання чи проведення тендеру можуть привести до завищення вартості проекту.

2. Суттєві додаткові збитки можуть виникати в результаті неефективного виконання проекту по впровадженню інформаційних систем в процесі взаємодії з розробниками програмного продукту [8, с. 77].

3. Останнім часом спостерігається виникнення залежності банку від внутрішніх спеціалістів по інформаційним технологіям – поява незамінних співробітників.

Система управління інформаційним ризиком банку в структурі операційного ризику повинна містити елементи: Вибір цілі введення системи управління ризиком, ідентифікація основних ризиків, пошук та управління ризиками, вияв суперечностей, що заважають банку в оцінці ризику, мінімізація негативних наслідків, створення механізму подолання ризиків.

Інформаційна система банку – це сукупність носіїв інформації та самої інформації у її русі та взаємодії. Елементами такої системи є зв'язок, програмне забезпечення та обладнання.

Обладнання компанії, на нашу думку, являється тим основним активом, що дає змогу адекватно і в повному обсязі здійснювати операційну діяльність банку, однак, без програмного забезпечення та можливостей зв'язку, банк не матиме можливості здійснити навіть найпростішу операцію. Лише взаємодія цих елементів забезпечує нормальне функціонування банківської інформаційної системи, однак, виникнення та реалізація банківських ризиків, може викликати значні втрати. Для їхньої мінімізації і потрібне створення системи управління операційним ризиком.

Розпочинаючи впровадження системи управління ризиками, банк може ставити перед собою наступні цілі:

1. Відчитатися «бо треба» перед регулятором. Особливістю української банківської системи є те, що НБУ ще не ввів вимоги до формування капіталу на покриття операційного ризику в нормативи достатності капіталу. Однак кілька банків вже самостійно прийняли рішення про формування таких резервів.

2. Формально підвищити свій рейтинг перед західними партнерами, оголосивши про наявність у банку системи управління операційним ризиком. Іноземні банки і фінансові компанії із країн Базельської домовленості дуже уважно і вимогливо відносяться до оцінки системи операційного ризик-менеджменту своїх партнерів як показника стабільності.

3. Побудувати у банку реальну систему управління операційними ризиками в першу чергу для власних цілей – оцінки адекватності і моніторингу власного операційного середовища для своєчасного виявлення та імунізації джерел операційних ризиків [2, с. 44]. Вирішення останньої цілі автоматично вирішує і дві попередні

Для фінансових компаній інформаційні ризики являються одними з найбільш критичних та явних проявів операційного ризику діяльності банку. В той же час в умовах нестабільності економічного середовища, ці ризики суттєво зростають, так як зростають конкуренція, тиск з боку клієнтів та держави, тощо. Серед усього різноманіття інформаційних ризиків**,** на нашу думку слід виділити такі:

- Ризик втрати чи витоку конфіденційної інформації.
- Ризик використання в діяльності банку необ'єктивної чи сфальсифікованої інформації. Нещодавні (2006 року) дослідження, що були проведені журналом Risk Waters і фірмою SAS, показали, що неточні чи застарілі данні стають причиною втратою фінансовими організаціями значних сум (до 120 млн. дол. США в рік) за рахунок операційних ризиків. В дослідженні брало участь близько 400 ризик менеджерів із 300 фінансових компаній. [5, с. 12]
- Ризик відсутності у керівництва об'єктивної і актуальної інформації.

- Поширення невигідної або ж небезпечної для фінансової установи інформації: ризик втрати банком репутації та юридичні ризики.

- Ризик перевищення лімітів за операціями трейдерів і співробітників кредитних відділів при відсутності контролю за такими операціями.

Для управління (мінімізації, прийняття, нівелювання чи ігнорування) ризиками, необхідно визначити причини їхнього виникнення. Серед основних причин виникнення ризиків в інформаційній сфері можна виділити:

1. Низький рівень підготовки персоналу і відсутність, або ж недостатність заходів по підвищенню інформаційної грамотності працівників банку.

2. Відсутність якісної програми та стратегії управління ризиком через нерозуміння керівництвом необхідності введення системи управління операційним ризиком та важливості існуючих загроз. Внаслідок чого, слабка підтримка та мінімальне фінансування значно підвищують рівень ризиків фінансової установи. При розгляді стратегії, на нашу думку, слід виокремити три елементи: роздрібний бізнес, дистанційне банківське обслуговування та інформаційна безпека.

3. Відсутність плану дій у випадку реалізації ризику – так звана «безперебійна робота» банківської інформаційної системи. Незалежні дослідження, що були проведені на території СНД і країн Балтії, показали, що якщо результатом умисних або випадкових дій системного адміністратора, вірусної атаки чи апаратного збою була знищена база даних інформаційної системи, то:

– лише 15% банків змогли б відновити операційну діяльність день в день;

– 60% банків знадобиться на відновлення від 2-х до 4-х днів;

– 25% банків відновили б свою діяльність 5 і більше робочих днів. [6, с. 12].

4. Неякісні інформаційні системи банку (програмне забезпечення). Прикладом може слугувати ситуація з одним із найбільших українських банків , коли внаслідок проведення агресивної експансії в регіонах, була відкрита значна кількість філій. При цьому, зростання ІТ-інфраструктури не було передбачено, і вона зростала екстенсивно.

Через це, виникли значні труднощі, навіть при проведенні незначних операцій, оскільки програмно-апаратне забезпечення системи не було розраховано на навантаження з боку додаткових відділень. В результаті – незадоволення клієнтів, працівників та керівництва банку. Бюджет для виправлення ситуації значно перевищив той, який би був затрачений на превентивні заходи [8, с. 76].

5. При поглинанні банків існує ряд проблем щодо інтеграції даних в нову інформаційну систему.

6. Направленість інформаційної системи сучасних банків на облікову діяльність, бізнес-планування та бюджетування, що значно ускладнює аналіз можливих ризиків в роботі автоматичної банківської системи.

7. Цільове введення неправдивих даних клієнтами в оперативному режимі:

1) введення скорочень;
2) помилки в даних 3-іх осіб;
3) різні формати при інтеграції даних з різних інформаційних систем.

В ході дослідження сучасної літератури щодо управління інформаційними ризиками фінансової установи, було виявлено ряд суперечностей.

По-перше, необхідно уніфікувати існуючі інформаційні системи для оптимізації інформаційних потоків і вирішення поточних завдань управління (в тому числі фінансовий моніторинг, ризик-менеджмент відповідно до вимог Базеля ІІ) з одного боку. З іншого, ж існують індивідуальні інформаційні системи що розробляються самими банками, або ж на їхні замовлення. Програмне забезпечення має недоліки, які зловмисники можуть активно використовувати.

По-друге, вимоги регулятора – НБУ та функціональні можливості існуючих у

банку інформаційних систем. Суперечність полягає у неможливості деякого інформаційного забезпечення розвиватися, а купівля нового нестиме зростання витрат на впровадження та адаптацію програмного забезпечення. Таким чином, комерційний банк, в умовах розвитку або ж занепаду, встає перед дилемою – використовувати старі АБС і мати претензії від користувачів і штрафи від НБУ, або ж вкладати кошти в нові, можливо «сирі» програмні продукти.

По-третє, з одного боку необхідність формування баз даних по операційним ризикам, так як за вимогами Базеля II репрезентативними є оцінка ризику, агрегована за 3-5 років. З іншого ж боку, відсутність законодавчої необхідності у формуванні системи управління операційного ризику не змушує банки формувати такі бази даних. Одночасно з цим об'єктивна оцінка ризиків в Україні ускладнена через відсутність зовнішньої бази даних по ризикам, так, як лише внутрішні дані, навіть за 5 років не дають переліку та ваги всіх можливих ризиків.

По-четверте, суперечність між вимогами Базельської домовленості та українськими стандартами ведення звітності вимагатимуть від банківської установи значної модифікації звітності. Крім того, деякі положення, які входять до Базелю II в сучасних (1 січня 2012 року) умовах, суперечать існуючим інформаційним системам.

По-п'яте, при формуванні системи оцінювання операційного ризику, банк може її формувати сам по вимогам Базеля, або ж звернутися до консалтингової компанії, яка б допомогла створити індивідуальну систему, під особливості конфігурації банку. В залежності від цілей, банк обере оптимальне рішення за співвідношенням витрати/ефективність.

По-шосте, існує проблематика оцінки ефективності діяльності відділу IT-технологій. Так, як аудит не може описати всі особливості IT-діяльності банку, а зовнішній аудит має певну ціну, виходить, що керівник сам оцінює свою діяльність.

По-сьоме, необхідно здійснити розподіл відповідальності і механізмів управління між відділом IT, службою безпеки, та ризик-менеджментом. Інакше, за порушення цілісності інформаційної безпеки, нести відповідальність буде керівник, або відповідальний IT відділу, навіть у випадку інсайдерської шахрайської діяльності.

Наслідками реалізації ризиків можуть стати:

- Внутрішнє та зовнішнє шахрайство.
- Помилки персоналу.
- Збої АБС та іншого програмного забезпечення.
- Порушення процесів зберігання та обробки даних.
- Недостатня захищеність конфіденційної інформації.

Зосередимо свою увагу на шахрайстві, як найбільш ймовірній та руйнівній проявів інформаційного ризику банку. Слід виокремити тих суб'єктів, які можуть здійснювати шахрайські дії по відношенню до конфіденційної інформації фінансової установи:

- конкуренти;
- працівники банку (інсайдери);
- спецслужби;
- рейдери;
- торгівці конфіденційною інформацією;
- хакери [1, с. 98].

Найбільшою загрозою для банку є втручання до бази даних клієнтів, що може радикально змінити як його положення на ринку, так і фінансовий стан. Розглянемо приклади шахрайства, що найбільш часто трапляються в банківських установах:

1. Крадіжка банківської картки і спроба зняття готівки через банкомат.
2. Доступ до конфіденційної інформації через систему дистанційного банківського

обслуговування («фішинг»).

3. Встановлення злоякісного програмного забезпечення тощо. [3, с.74-77]

Таким чином, можна зробити висновок, що шахрайські дії можуть бути спрямовані як на клієнта, так і на всю інформаційну систему банка, навіть інсайдером.

Основні механізми управління інформаційними ризиками банку полягають у:

І Організаційних заходах:

1. Планування процедур управління операційним ризиком та інформаційних ризиків, як складових операційного. При формуванні таких процедур, слід усвідомлювати, що виділяють дві основні моделі створення підрозділу з питань регулювання операційного ризику:

а) концентраційна модель – всі питання щодо управління ризиком концентруються в руках 1-го структурного підрозділу (до складу такого підрозділу повинні входити економіст, працівник ІТ-сфери, юрист), що дасть можливість оптимально визначати межі відповідальності.

б) розподільна модель - де існує підрозділ моніторингу ризику, що розробляє корпоративну політику, специфічні методи оцінки ризику, а функції по збиранню та управлінню – в відповідні підрозділи (кредитний, служби безпеки, ІТ тощо).

2. Проведення регулярних аудитів фінансової компанії, аудит служби безпеки органом, що незалежний від інших структурних підрозділів, задля усунення конфлікту інтересів. Фактично, аудит – це перевірка правильності виконання стратегічних та тактичних планів компанії, а відсутність таких планів у відділі інформаційних технологій негативно впливає як на оцінку, так і на саму роботу відділу.

3. Як альтернатива власних розробок, банк має змогу передати в аутсорсинг управління ІТ-активами консалтинговій компанії. В даному випадку операційний ризик міняється з ризику діяльності інформаційних систем на зовнішній ризик; позитивними сторонами можна виділити: високу кваліфікацію працівників консалтингової компанії, та можливість через судові установи відшкодувати завдані збитки. Негативним виділимо те, що в випадку реалізації ризику, відшкодування може вимагати значний проміжок часу, а наслідки від поширення інформації про проблеми банку будуть значними відразу.

4. Створення методологічних та технологічних програм по забезпеченню безперебійної діяльності інформаційної системи банку. На випадок втрат баз даних, падіння інформаційних систем, пошкодження інформації тощо.

5. Методологічне закріплення певних функціональних обов’язків за кожним з працівників фінансової установи, в тому числі обов’язок реєструвати всі операційні ризики, що виникають [4, с. 96-97].

6. Посилення мотивації співробітників у напрямку підвищення комп’ютерної грамотності, що дасть змогу уникати більшості типових помилок працівниками.

ІІ Технологічних заходах:

1. Накопичення інформації про ризики, їхня оцінка та аналіз, ранжування та інформування керівництва про реалізацію ризиків та ймовірність їхнього настання.

2. Встановлення для всіх працівників програми, яка б реєструвала всі дії, що виконувалися б на вибраному АРМ. Такий захід дасть змогу виявити інсайдера, а також у випадку постійного моніторингу обмежувати діяльність АРМ, якщо здійснювана операція підвищує ризик банку.

3. Створення внутрішніх банківських вимог до програмного забезпечення, що на нашу думку, повинно:

- Дозволяти вирішити задачу інформаційної підтримки процесу управління операційним ризиком та вписуватися в ІТ-інфраструктуру банку.
- Створювати перспективи для подальшого вирішення інших задач по управлінню

бізнесом.

- Бути оптимальним за співвідношенням затрати/ефективність, інакше кажучи, банк повинен мати змогу розраховувати коефіцієнт ROI програмного продукту.

4. Використання сучасних систем шифрування даних, що направлені на унеможливлення несанкціонованого доступу зсередини банку (до віртуальних образів, на яких можуть зберігатися дані клієнтів).

Отже, на нашу думку існують ряд механізмів як організаційного, так і технологічного спрямування, що дозволить банкові управляти операційними ризиками в напрямку інформаційних активів.

Висновки. Сучасні світові тенденції вимагають від банків бути готовими до зустрічі з ризиками інформаційної системи. Реалізація таких ризиків завдасть значних збитків банкові, так як практично вся діяльність банківської установи залежить від інформаційних систем.

Існує ряд перешкод технологічного, методологічного та організаційного характеру, подолання яких дозволить значно зменшити інформаційні ризики банку та інтегрувати даний вид ризику до системи управління операційним ризиком відповідно до вимог ІІ Базельської домовленості.

Література

1. Володин А. Как бороться с киберпреступниками / А. Володин // Аналитический банковский журнал. – 2010. - № 5 (179).

2. Лукацький А. Операционные риски и угрозы системам финансовых структур /А. Лукацкий // Расчеты и операционная работа в коммерческом банке. – 2005. – № 10.

3. Мамонтов А. Хакеры начинают и… выигрывают? / А. Мамонтов // Банковская практика. – 2010. – №1.

4. Романов Н. Средства защиты от атак кибер-преступников по каналам ДБО / Н. Романов // Аналитический банковский журнал. – 2010. - № 5 (179).

5. Румянцев А. Операционный риск-менеджмент в банках / А. Румянцев // Финансовый директор. – 2006. - №2.

6. Сердюк В. Как защититься от банковского фрода / В. Сердюк // Аналитический банковский журнал. – 2010. - № 5 (179).

7. Синцов А. Банк-клиент против хакеров: чья возьмет? / А. Синцов // Аналитический банковский журнал. – 2010. - № 5 (179).

8. Смирнов А. Операционные риски и ИТ-инфраструктура банка / А. Смирнов // Корпоративные системы. – 2008. - №1

Summary. This article deals with the basic problems of information security in a bank. It was investigated challenges and moreover it was developed and distinguished risks which oppose the effective implementation of risk management operations in the line of information security. It was set forward measures to improve a level of information risks which threaten or can threaten a banking establishment.

Keywords: operational risk of the bank, information technology, fraud, information security.

Стаття надійшла до редакції 29.02.2012