ISSN 2309-82IX (Print), ISSN 2310-2438 (Online)

Збірник наукових праць Дніпропетровського національного університету
залізничного транспорту імені академіка В. Лазаряна «Проблеми економіки транспорту», 2014, вип. 7.

УДК 336.71:004

В. В. БОБИЛЬ[1*]

[1*]Каф. «Облік, аудит та інтелектуальна власність», Дніпропетровський національний університет залізничного транспорту імені академіка В. Лазаряна, вул. Лазаряна, 2, Дніпропетровськ, Україна, 49010

УПРАВЛІННЯ РИЗИКАМИ «ХМАРНИХ» ТЕХНОЛОГІЙ У СИСТЕМІ РИЗИК-МЕНЕДЖМЕНТУ БАНКУ

Мета. Дослідити ризики застосування «хмарних» технологій в операційній діяльності банку та надати рекомендації щодо зменшення таких ризиків. **Методика.** Методологічний підхід передбачає розгляд управління банківськими ризиками (у тому числі операційними, що виникли через застосування «хмарних» технологій) як з позицій прийняття банком оптимізаційних управлінських рішень, так і з позицій реалізації цих рішень через організаційну структуру. **Результати.** У роботі виокремлено ризики «хмарних» технологій, досліджено заходи зменшення операційного ризику за його складовими, запропоновано рекомендації щодо нейтралізації технологічного ризику, який виникає через застосування «хмарних» обчислень. **Наукова новизна.** Запропоновано науковий підхід щодо управління банківськими ризиками, який, на відміну від існуючого, включає інструменти зменшення негативного впливу застосування «хмарних» технологій в операційній діяльності банку. **Практична значимість**. Використання наданих рекомендацій стосовно управління ризиками «хмарних» технологій підвищує ефективність системи ризик-менеджменту банку.

Ключові слова: «хмарні» технології, операційний ризик, банк, система ризик-менеджменту

Вступ

«Хмарні» обчислення беруть початок з 1950-х років, коли вчений Херб Грош у своєму дослідженні написав, що в майбутньому весь світ працюватиме на терміналах, якими будуть керувати приблизно 15 великих центрів обробки даних [1].

Сьогодні категорія «хмарні» технології» включає багато різних понять: програмне забезпечення, інфраструктуру, інформаційну платформу, дані, робоче місце тощо.

Головним є те, що «хмарні» технології надають можливість підприємствам (у тому числі банкам) відмовитися від необхідності створювати й підтримувати власну обчислювальну інфраструктуру.

Таким чином, «хмара» відкриває новий підхід до обчислень, при якому ані обладнання, ані програмне забезпечення не належать банку. Замість цього провайдер за допомогою Інтернету надає банку-замовнику вже готовий технологічний продукт.

Але впровадження «хмарних» технологій у банки може призвести до збільшення певних ризиків (у першу чергу операційних).

Операційні ризики пов`язані не з бізнес-напрямками банку, а з організацією його фінансово-господарської діяльності.

Основною перешкодою, що ускладнює управління операційними ризиками, є низька ймовірність визначення розміру цих ризиків (крім того, перелік інцидентів реалізації операційних ризиків банку є досить широким).

Аналіз останніх досліджень

Проблеми класифікації та оцінки операційних ризиків досліджують такі вітчизняні та зарубіжні науковці, як О. Богданов [2], Ю. Боруч [3], О. Деревська [4], В. Коваленко [5], О. Ковальчук [6], О. Криклій [7], Б. Сазикін [8], В. Харламов [9], А. Шинкаренко [10].

Віддаючи належне наявним науковим напрацюванням українських та зарубіжних економістів, накопиченому досвіду у сфері оцінювання та управління операційним ризиком банку, варто зазначити, що до кінця не вирішеними залишаються питання впливу сучасних IT-технологій (у тому числі «хмарних») на операційний ризик банку.

Мета

Мета статті – дослідження «хмарних» технологій як потенційного фактора збільшення операційного ризику банку, а також надання

рекомендацій стосовно зменшення розміру цього виду ризику.

Методика

Методологічну основу дослідження становить комплексний підхід до управління операційними ризиками банку. Підхід передбачає розгляд управління операційними ризиками (у тому числі тими, що виникли через застосування «хмарних» технологій) як з позицій прийняття банком оптимізаційних управлінських рішень, так і з позицій реалізації цих рішень через організаційну структуру. З цих особливостей випливає поєднання методу власне економічного аналізу з методами системного аналізу функціонування банків.

Результати

Система ризик-менеджменту банку – це складова його економічної безпеки, завданням якої є ідентифікація, оцінка та управління ризиками, що виникають через здійснення активно-пасивних операцій, недосконалу організацію фінансово-господарської діяльності банку та зміни чинників зовнішнього середовища.

Серед банківських ризиків через складність управління особливе місце займають операційні ризики.

У Базелі ІІ операційний ризик визначається як «ризик виникнення збитків у результаті недоліків та помилок у внутрішніх процесах банку, допущених з боку співробітників через інформаційні системи, а також зовнішніх подій» [11].

При цьому Базельський комітет вказує на особливе місце операційного ризику в системі ризик-менеджменту банку, оскільки в діяльності західних банківських організацій цей ризик за величиною потенційних втрат посідає друге місце, розташовуючись між кредитним (1-ше місце) і ринковим (3-тє місце). Враховуючи це, Базель ІІ обґрунтовано рекомендує розглядати операційний ризик як окрему категорію ризиків, яка повинна підтримуватися певною частиною власного капіталу банку, що має назву «економічний капітал під операційний ризик» [11].

У Базелі ІІ пропонується розглядати такі категорії операційного ризику: ризик персоналу; ризик систем і технологій; ризик бізнес-процесів; ризик зовнішнього середовища функціонування банку.

Низка зарубіжних фінансових інститутів використовує класифікацію операційних ризиків, запропоновану Бенкер Траст (Banker Trust) [12]:

– ризик персоналу – усі ризики, пов'язані зі співробітниками компанії, зокрема їх несанкціонованими діями, недостатньою компетентністю, залежністю від окремих фахівців тощо;

– технологічний ризик – ризик, викликаний збоями і відмовами інформаційних систем, програм або баз даних, систем передачі інформації та іншого устаткування, необхідного для діяльності банку;

– ризик фізичної шкоди – ризик, який настає в результаті природних катастроф та інших факторів, які можуть завдати шкоди основному обладнанню, системам, технологіям і ресурсам банку (такий ризик зазвичай мінімізується шляхом страхування майна);

– ризик взаємин – ризик, який настає в результаті відносин, що виникають в бізнес-процесах, таких як труднощі у взаємодії з клієнтами і недостатність внутрішнього контролю;

– зовнішній ризик – настає в результаті злочинних дій сторонніх організацій, фізичних осіб, а також у результаті змін вимог регуляторних органів.

У методичних рекомендаціях Національного банку України (НБУ) із системи оцінки ризиків вводиться такий термін, як «операційно-технічнологічний ризик». Під цим ризиком спеціалісти НБУ розуміють «потенційний ризик для довгострокового існування банківської установи, що виникає через недоліки корпоративного управління, системи внутрішнього контролю або інформаційних технологій і процесів обробки інформації з точки зору керованості, універсальності, надійності, контрольованості і безперервності роботи» [13].

На наш погляд, сучасний операційний ризик найбільш доцільно поділяти на такі підвиди [14]:

1. Технологічний – ймовірність відхилення від запланованих фінансових показників через неефективність інформаційних технологій та процесів обробки інформації тощо.

2. Ризик виконавця – ймовірність відхилення від запланованих фінансових показників у

результаті ненавмисного порушення чи недбалого виконання професійних обов'язків.

3. Шахрайство – фінансові втрати в результаті обману або незаконного присвоєння коштів, власності тощо.

4. Корпоративний – ймовірність відхилення від запланованих фінансових показників через помилки в корпоративному управлінні (конфлікт інтересів, помилки у визначенні бізнес-процесів, розподілу функціональних обов`язків тощо).

5. Інноваційний – ймовірність відхилення від запланованих фінансових показників через помилки на стадіях розробки та впровадження нових (удосконалення існуючих) банківських продуктів.

6. Стратегічний – ймовірність відхилення від запланованих фінансових показників через помилки у формуванні цілей та стратегії розвитку банку та неадекватне реагування на зміни в бізнес-середовищі банку.

Заходи зменшення операційного ризику за його складовими вказані в табл. 1.

Таблиця 1

Заходи зменшення операційного ризику за його складовими

Складові операційного ризику	Заходи зменшення ризику	Структури банку, що контролюють складові операційного ризику
1	2	3
Технологічний ризик	Здійснювати моніторинг, оновлення та тестування інформаційних систем, обладнання, каналів зв’язку тощо; формувати плани відновлення ІТ–сервісу; запроваджувати системи архівації та збереження банківських даних; розподіляти функції між відділами, що займаються розробкою програмного забезпечення та обслуговуванням інформаційних систем тощо	Правління банку; Управління (відділ) автоматизації банківських технологій; Виконавчий орган з ризик-менеджменту
Ризик виконавця	Розробляти та впровадити кодекс поведінки банківського працівника; підвищувати стандарти обслуговування і здійснювати регулярний моніторинг якості обслуговування клієнтів; запроваджувати систему мотивації персоналу; здійснювати хронометраж надання банківських послуг; аналізувати показники з управління персоналом (плинність кадрів, кількість навчених співробітників тощо)	Правління банку; Бек-офіси; Виконавчий орган з ризик-менеджменту
Шахрайство	Запроваджувати механізм своєчасного виявлення та припинення можливостей шахрайства через банківські інформаційні системи	Управління (відділ) автоматизації банківських технологій; Бек-офіси
Корпоративний ризик	Забезпечувати однакове ставлення до акціонерів, незалежно від кількості належних їм акцій; впроваджувати принципи незалежного внутрішнього контролю; впроваджувати процедури визначення пов’язаних осіб банку, а також контролю і нагляду за операціями з пов’язаними особами; розробляти та впроваджувати систему оцінки впливу управлінських рішень на фінансовий результат банку; здійснювати чіткий розподіл функціональних обов`язків підрозділів банку; визначати та описувати бізнес-процеси фінансової установи;	Спостережна рада; Правління банку; Виконавчий орган з ризик-менеджменту

Продовження таблиці 1

1	2	3
	забезпечувати надання своєчасної та повної фінансової інформації	
Інноваційний ризик	Впроваджувати систему визначення пріоритетності розробки нових банківських продуктів (з урахуванням ризиків); встановлювати стандарти якості нового або удосконаленого банківського продукту (технологічна карта); забезпечувати всі установи банку необхідною нормативною документацією, технічним і програмним забезпеченням, рекламними матеріалами; проводити навчання персоналу; здійснювати пробний продаж нового продукту лояльним клієнтам; розробляти ефективну рекламну кампанії з метою стимулювання збуту	Спостережна рада; Правління банку; Виконавчий орган з ризик-менеджменту
Стратегічний ризик	Розробляти план щодо структурної реорганізації банку (наприклад, злиття або приєднання); здійснювати моніторинг банків-конкурентів; впроваджувати систему контролю за якістю реалізації цілей банку (виконанням стратегічних планів та бюджетів); розробляти план щодо збільшення ринкової позиції банку (диверсифікація продуктів, географії та клієнтури); здійснювати маркетингові дослідження ринку	Спостережна рада; Правління банку; Виконавчий орган з ризик-менеджменту

«Хмарні» технології збільшують розмір технологічного ризику.

Перед тим як розглянути інструменти зменшення негативного впливу застосування «хмарного» обчислення в операційній діяльності банку, необхідно визначити основні переваги «хмарних» технологій, а саме:

1. Економічність. «Хмарні» технології дозволяють істотно знизити капітальні витрати банку на побудову центрів обробки даних, закупівлю серверного обладнання, апаратних і програмних рішень тощо (значна частка таких видатків поглинається провайдером «хмарних» послуг). Додатково банк економить на утриманні ІТ-персоналу, адмініструванні тощо.

2. Еластичність. «Хмарні» технології забезпечують можливість оперативно змінювати конфігурацію корпоративної ІТ-інфраструктури залежно від поточних потреб банку (фінансова установа купує стільки ресурсів, скільки потрібно на даний момент). Ресурсів «хмари» цілком вистачає для замовлення віртуального «суперкомп'ютера» або інфраструктури для банку, і при цьому не виникає проблем з оновленням програмного забезпечення (завжди доступні його останні версії), сумісністю різних операційних систем тощо. У періоди пікових навантажень (наприклад, під час складання річної фінансової звітності) не потрібно планувати введення додаткових інформаційних потужностей, оскільки «хмарні» сервіси можуть масштабуватися автоматично і практично необмежено. Послуги можуть бути надані, розширені, звужені в будь-який момент часу, без додаткових витрат на взаємодію з провайдером, як правило, у автоматичному режимі.

3. Мобільність. «Хмарні» технології надають можливість в буквальному сенсі носити своє робоче місце з собою – за наявності мобільного термінального пристрою і доступу до Інтернету працівник банку, незалежно від свого місцезнаходження, завжди має доступ до власного віртуального комп'ютера, корпоративних мереж, баз даних тощо.

4. *Самообслуговування на вимогу*. Банк самостійно визначає і змінює обчислювальні потреби (серверний час, швидкість доступу та обробки даних, обсяг збережених даних) без взаємодії з представником постачальника послуг.

5. *Висока доступність*. «Хмарні» сервіси доступні протягом 99,5 відсотків часу, а деякі провайдери гарантують доступність на рівні 99,9 відсотків.

6. Збереження даних. Працівникам банку не потрібно піклуватися щодо резервування інформації, дані безпечно зберігаються в «хмарі» («хмарна» інфраструктура гарантує збереження даних).

Незважаючи на вищевказані переваги, «хмарний» ринок України, на відміну від ринків США чи ЄС, нині є у процесі акумулювання первинного досвіду споживання «хмарних» рішень. Але за експертними прогнозами, вже з 2015 року він демонструватиме експоненціальне зростання, характерне для «хмарних» ринків розвинених країн. Багаторазове збільшення ринку найближчими роками приведе до виникнення нового специфічного і значущого сектору української економіки та інфраструктури [15].

Пропонуємо розглянути основні ризики «хмарних» технологій:

1. Атаки на гіпервізор. Гіпервізор є одним з ключових елементів «хмарних» технологій. Основною його функцією є розподіл ресурсів між віртуальними машинами. Атака на гіпервізор може призвести до того, що одна віртуальна машина зможе отримати доступ до пам'яті і ресурсів іншої. Також вона зможе перехоплювати мережевий трафік, відбирати фізичні ресурси і навіть витісняти віртуальну машину з сервера.

2. Атаки на системи управління. Велика кількість віртуальних машин, які використовуються в «хмарних» технологіях, потребує наявності певної системи управління, що здатна ефективно контролювати створення, перенесення та утилізацію віртуальних машин. Втручання в систему управління може призвести до появи віртуальних машин - невидимок, які здатні блокувати роботу інших віртуальних машин.

3. *Стабільність з'єднання.* Сама суть «хмарних» технологій потребує постійного перебування онлайн (підключення до Інтернету). З'єднання через мережу Інтернету має бути стабільним і, бажано, широкосмуговим. Частково ризик відсутності з'єднання може бути зменшено шляхом кешування даних або розробкою алгоритму переходу в режим повільного зв'язку задля обміну тільки критично важливими даними.

4. Залежність від постачальника (провайдера) «хмарних» технологій або його банкрутство. Оскільки витрати банку з міграції з локального середовища в «хмару» досить значні, то в разі, якщо постачальник «хмарних» рішень перестане задовольняти потреби банку за якими-небудь критеріями (збільшення плати за використання, виникнення проблем на маршрутах обміну даними), то змінити його буде досить проблематично. По-перше, на ринку ІТ-технологій може бути відсутній провайдер, який зможе запропонувати відповідний рівень «хмарних» рішень, по-друге, грошові та часові витрати можуть бути занадто великими.

5. DDOS-атаки. Це напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними для користувачів. Одним із найпоширеніших методів нападу є насичення атакованого комп'ютера або мережевого устаткування великою кількістю зовнішніх запитів (таким чином атаковане устаткування не може відповісти користувачам або відповідає настільки повільно, що стає фактично недоступним).

6. Безпека даних. Більшість банків побоюються перехоплення інформації під час передання даних, втрати контролю над даними та неможливості знищення інформації в мережі Інтернету.

Основні ризики «хмарних» технологій та інструмени їх зменшення вказані в табл. 2.

Висновки

«Хмарні» технології в найближчому майбутньому виведуть операційну діяльність банків на якісно новий рівень. Ця ІТ-технологія може стати значним фактором покращення конкурентоспроможності сучасних фінансових установ.

Але використання «хмарних» рішень пов'язане з певними операційними ризиками, насамперед технологічним.

На рівні банку (мікрорівень) зменшити розмір ризиків, що виникають у процесі застосування «хмарних» технологій, можливо за допомогою таких управлінських рішень: ретельний підхід до вибору провайдера (постачальника) «хмари»; розробка плану дій із зміни провайдера; впровадження двофакторної аутентифікації, шифрування та маскування даних; навчання працівників банку правилам інформаційної безпеки; проведення консультацій з регулятором та зовнішніми аудиторами щодо ризиків впровадження «хмарних» технологій.

Таблиця 2

Управління основними ризиками «хмарних» технологій

Ризик	Характеристика	Управління
1	2	3
Атаки на гіпервізор	Ризик розподілу ресусів, який може призвести до того, що одна віртуальна машина отримує несанкціонований доступ до пам'яті і ресурсів іншої віртуальної машини	Стандартизація процедур доступу до керуючих засобів хост-сервера; застосовування вбудованого брандмауера (програма, що здійснює захист комп'ютерних мереж) хоста віртуалізації
Атаки на системи управління	Ризик появи віртуальних машин-невидимок, які здатні блокувати роботу інших віртуальних машин	Застосування паролей, сертифікатів та кодів
Стабільність з'єднання	Ризик погіршення (або відсутність) підключення до Інтернету	Кешування даних; розробка алгоритму переходу в режим повільного зв'язку
Залежність від постачальника (провайдера) «хмарних» технологій	Ризик відсутності можливості змінити постачальника «хмарних» технологій через відсутність на ринку інших провайдерів, коштів або часу	Ретельний підхід до вибору провайдера; робота з провайдером, який використовує відкриті стандарти
Банкрутство провайдера	Ризик зупинки надання «хмарних» рішень через банкрутство провайдера	Ретельний підхід до вибору провайдера; робота з декількома провайдерами; наявність плану дій із зміни провайдера
Втрата зв'язку з провайдером	Ризик зупинки бізнес-процесів через відсутність доступу до сервісів провайдера	Вибір провайдера, що має датацентри в декількох країнах; застосування супутникового інтернет-зв'язку; наявність резервної копії критичних систем у приватній «хмарі»
Перехоплення інформації при передачі	Ризик несанкціонованого доступу до інформації у процесі передачі даних	Використання криптографії при передачі інформації; навчання користувачів правилам інформаційної безпеки
Юридичний ризик	Ризик отримання штрафів та інших санкції з боку регулятора через порушення вимог чинного законодавства	Консультація з регулятором та зовнішніми аудиторами
Втрата контролю над даними або інфраструктурою	Ризик відсутності можливості забезпечення належного рівня безпеки через втрату контроля над даними або інфраструктурою	Проведення аудиту безпеки провайдера; укладення угоди з провайдером щодо нерозголошення конфіденційних даних; моніторинг рівня сервісу та інцидентів порушення інформаційної безпеки
Неможливість знищення інформації	Ризик витоку інформації через неможливість знищення даних у «хмарних» технологіях	Шифрування даних в «хмарі»; маскування інформації; включення вимог з процедури знищення інформації в SLA (договір про рівень надання послуг)
Взлом інтерфейсів управління	Ризик шахрайства через взлом інтерфейсу управління «хмарними» технологіями	Двофакторна аутентифікація; шифрування переданих даних
DDOS-атаки	Ризик нападу на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними для користувачів	Вибір ddos-стійкого провайдера; робота з декількома провайдерами

Продовження таблиці 2

1	2	3
Діяльність інших користувачів «хмари»	Ризик несанкціонованого доступу до інформації та зупинка бізнес-процесів через діяльність інших користувачів «хмарних» технологій	Ретельний підхід до вибору провайдера; робота з декількома провайдерами

З позиції Національного банку України (регулятора) доцільним є проведення комплексного аналізу та оцінки стану, тенденцій та перспектив розвитку впровадження «хмарних» технологій у банки, а також розробка національних стандартів, які встановлювали б належні вимоги до якості та надійності «хмарних» технологій і послуг на фінансовому ринку України.

БІБЛІОГРАФІЧНИЙ СПИСОК

1. Grosch H.R.J. Bibliography on Chebyshev Polynomials and Their Use as Optimum Approximation Functions / H.R.J. Grosch // Proeceedings of the 1949 Scientific Computation Seminar, IBM (1951).
2. Богданов А. Операционный риск и его влияние на устойчивую работу финансовой организации / А. Богданов // Банковские технологии. – 2008. – №7. – С. 80–88.
3. Боруч Ю. Консорциум для сбора данных по операционным рискам как инструмент оценки и снижения риска / Ю. Боруч // Банковское дело. – 2009. – № 10. – С. 40.
4. Деревська О. Операційний ризик: категорії управління / О. Деревська // Вісн. УБС НБУ. – 2010. – № 3. – С. 136-140.
5. Коваленко В. Управління операційними ризиками в банківській системі / В. Коваленко // Актуальні проблеми економіки. – 2010. – № 5 (107). – С. 189-197.
6. Ковальчук О. Основні підходи до класифікації видів операційного ризику в банку / О. Ковальчук // Проблеми і перспективи розвитку банківської системи України : зб. наук. праць / Державний вищий навчальний заклад «Українська академія банківської справи Національного банку України». – Суми, 2010. – Т. 30. – С. 142-151.
7. Криклій О. Інструментарій оцінки операційного ризику банку / О. Криклій, О. Крухмаль // Вісн. УАБС. – 2010. – № 4. – С. 45-48.
8. Сазыкин Б. Управление операционным риском в коммерческом банке / Б. Сазыкин. – М.-СПб. : Вершина, 2008. – 291 с.
9. Харламов В. Операционные риски и риски информационной безопасности / В. Харламов // Банковское дело. – 2009. – № 7. – С. 41 – 42.
10. Шинкаренко А. Оцінка операційного ризику інвестиційних операцій банку та формування резерву як метод його мінімізації / А. Шинкаренко // Фінансов-кредитна система. – 2011. – № 3. – С. 309-313.
11. International Convergence of Capital Measuremeht and Capital Standards. – Basel. – November 2005. Access:– http: www. bis.org. – Title from the screen.
12. Моделювання оцінки операційного ризику комерційного банку: монографія / О. С. Дмитрова, К. Г. Гончарова, О. В. Меренкова та ін. – Суми: ДВНЗ «УАБС НБУ», 2010. – 264 с.
13. Методичні вказівки з інспектування банків «Система оцінки ризиків»затверджено Постановою Правління НБУ від 15.03.2004 р. № 104. – Режим доступу: http: // liga.com.ua. – Назва з екрану.
14. Бобиль В. В. Особливості операційного ризику: класифікація, кількісна оцінка, управління / В. В. Бобыль // Банківська справа. – 2012. – № 1 (98). – С. 36 – 50.
15. Аналітична записка Національного інституту стратегічних досліджень при Президентові України «Перспективи розвитку ринку хмарних обчислень в Україні: переваги та ризики». – Режим доступу: http://www.niss.gov.ua/articles/1191/.
16. Бобиль В. В. Антикризове управління банківськими ризиками : монографія / В. В. Бобиль. – Дніпропетровськ : Вид-во «Свідлер А.Л.», 2012. – 270 с.

ISSN 2309-82IX (Print), ISSN 2310-2438 (Online)

Збірник наукових праць Дніпропетровського національного університету
залізничного транспорту імені академіка В. Лазаряна «Проблеми економіки транспорту», 2014, вип. 7.

В. В. БОБЫЛЬ[1*]

[1*]Каф. «Учет, аудит и интеллектуальная собственность», Днепропетровский национальный университет железнодорожного транспорта имени академика В. Лазаряна, ул. Лазаряна, 2, Днепропетровск, Украина, 49010

УПРАВЛЕНИЕ РИСКАМИ «ОБЛАЧНЫХ» ТЕХНОЛОГИЙ В СИСТЕМЕ РИСК-МЕНЕДЖМЕНТА БАНКА

Цель. Исследовать риски применения «облачных» технологий в операционной деятельности банка и предоставить рекомендации по уменьшению этих рисков. **Методика**. Методологический подход предполагает рассмотрение управления банковскими рисками (в том числе операционными, которые возникли из-за использования «облачных» технологий) как с позиций принятия банком оптимизационных управленческих решений, так и с позиций реализации этих решений через организационную структуру. **Результаты**. В работе выделены риски «облачных» технологий, исследованы меры для уменьшения операционного риска по его составляющими, предложены рекомендации относительно нейтрализации технологического риска, возникающего из-за применения «облачных» вычислений. **Научная новизна.** Предложен научный подход к управлению банковскими рисками, который, в отличие от существующего, включает инструменты уменьшения негативного влияния применения «облачных» технологий в операционной деятельности банка. **Практическая значимость**. Использование предоставленных рекомендаций по управлению рисками «облачных» технологий повышает эффективность системы риск-менеджмента банка.

Ключевые слова: «облачные» технологии, операционный риск, банк, система риск-менеджмента

V. V. BOBYL[1*]

[1*]Department «Accounting, Auditing and Intellectual Property», Dnipropetrovsk National University of Railway Transport named after AcademicianV. Lazaryan, Lazaryan St., 2, Dnipropetrovsk, Ukraine, 49010

RISK MANAGEMENT «CLOUD» TECHNOLOGIES IN BANKS' RISK MANAGEMENT

Purpose. Investigate the risks of using the «cloud» technologies in operating activities and provide recommendations to mitigate those risks. **Methodology** The methodological approach involves consideration of bank risk management (including operational, which arose from the use of «cloud» technologies) as from the standpoint of making the bank optimization of administrative decisions, and from the standpoint of implementation of these solutions through the organizational structure. **Results.** The article highlighted the risks of «cloud» technologies are investigated measures to reduce the operational risk to his constituents, the recommendations regarding the neutralization process risk arising from the use of «cloud» computing. **Findings**. We propose a scientific approach to the management of banking risks, which, in contrast to the existing one, includes tools to reduce the negative impact of the use of «cloud» technologies in the operations of the bank. **The practical significance.** Using the provided recommendations on risk management «cloud» technology improves the efficiency of the risk management system of the bank.

Keywords: «cloud» technology, operational risk, a bank, risk management

Надійшла до редколегії 17.05.2014.
Рекомендована до друку д.е.н. О. М. Гненним, к.е.н. П. Й. Атамасом.