Таким чином, сучасний стан економіки (більшість підприємств знаходиться у кризі) вимагає створення загального алгоритму прогнозування банкрутства підприємства з урахуванням методик як вітчизняного, так і закордонного досвіду. Дана модель дасть змогу підприємствам вчасно виявити негативні кризові явища та застосувати заходи антикризової політики управління щодо недопущення чи подолання фінансової кризи на підприємстві. Концепція антикризового управління є переважною в системі антикризового регулювання, оскільки вимагає оперативного втручання в кризову ситуацію, та за допомогою активних антикризових дій запобігти банкрутству підприємств. В цьому контексті поняття банкрутства сприймається не тільки як неспроможність боржника відновити свою платоспроможність, але і як основний критерій до впровадження антикризових заходів. Розгляд форм банкрутства, що існують на сьогоднішній момент, ускладнює процес антикризового управління, оскільки до економічних чинників його виникнення додаються чинники навмисної поведінки певних осіб з метою отримання відповідних вигод, що в свою чергу призводить до спотворення фактичних даних про реальний стан підприємств. Дослідження функцій антикризового управління обумовлює системне бачення напрямів та етапів роботи, які повинні бути проведені для досягнення мети антикризового управління у всіх галузях економіки, взаємозв'язків, що існують між ними, і мають бути враховані під час розроблення плану заходів для забезпечення нормальної роботи підприємства.

Література

1. Антикризисный менеджмент / А.Г. Грязнова и др.; под ред. А.Г. Грязновой. – М.: Экмос, 1999. – 368 с.
2. Никитина Н. Антикризисное финансовое управление предприятием: исследование факторов внутренней и внешней среды // Проблемы теории и практики управления. – 2007. – № 7. – С. 91–101.
3. Бланк І.А. Основи фінансового менеджменту. Т. 2. – К.: Ніка-Центр, 1999. – 512 с.
4. Лігоненко Л.О. Антикризове управління підприємством: теоретико-методологічні засади та практичний інструментарій. – К.: КНЕУ, 2001.
5. Антикризисное управление. Учебник / Под ред. Э.М. Короткова. – М.: Инфра-М, 2000. – 432 с.
6. Фомин Я.А. Диагностика кризисного состояния предприятия. – М.: Юнити-Дана, 2003. – 349 с.
7. Примаченко А. Судьи меньше попадали бы в затруднительное положение // Зеркало недели. – 1999. – № 22.

УДК 338

М. І. ТКАЧЕНКО
Вінницький фінансово-економічний університет

ВИЗНАЧЕННЯ ГРУПИ РИЗИКІВ, ЯКІ ВИНИКАЮТЬ ПРИ ВИКОРИСТАННІ ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ СИСТЕМ У ФІНАНСОВО-КРЕДИТНИХ УСТАНОВАХ

У статті визначається група специфічних ризиків, які можуть виникати при використанні електронних інформаційних систем у діяльності банків та інших фінансово-кредитних установ. Даються рекомендації щодо зменшення впливу цих ризиків.

The group of specific risks that may arise when using electronic information systems of banks and other financial institutions is defined in the article. The recommendations on reducing the impact of these risks are suggested.

Вступ. Ризик постійно супроводжує діяльність різноманітних фінансово-кредитних установ. Особливо це спостерігається при виконанні різних банківських операцій, коли виникає ризик неповернення кредиту та (або) проценту за користування ним, ризик несвоєчасного виконання зобов'язань позичальником, ризик недоотримання прибутку, ризик ліквідності тощо. Актуальним постає питання у спроможності та можливості керувати ризиком, оскільки уникнути його неможливо: ризик є невід'ємною складовою підприємництва. Тому головними завданнями, які повинні вирішуватись при управлінні ризиком є: розпізнавання можливих ситуацій виникнення ризиків; оцінка масштабів передбачуваних збитків, що може підсилюватись при функціонуванні електронних інформаційних систем; пошук способів запобігання або відшкодування ризику.

Тому для управління ризиками повинна бути побудована система обліку і вивчення усіх випадків виникнення збитків, визначення ймовірностей їх виникнення, спосіб упередження або відшкодування збитків.

Основний розділ. Фінансові ризики є групою економічних ризиків, які виникають не тільки при здійсненні операцій фінансово-кредитною установою, але й визначається можливістю збитків у її клієнтів, що також негативного впливає на економічний стан такої установи.

Фінансові ризики досить активно розглядаються в сучасній економічній літературі [1–3], їх вивченню присвячена значна кількість публікацій, тому не вважаємо за доцільне розглядати їх в цій статті більш детально. Будемо вважати їх традиційними, тобто такими, які мають місце в процесі діяльності фінансово-кредитної установи та виникають лише внаслідок здійснення фінансових операцій. Але, з огляду на інтенсивний розвиток та впровадження інформаційних технологій у галузі надання фінансових послуг, зокрема послуг, які

надаються комерційними банками, зосередимо нашу увагу на визначенні групи специфічних ризиків, які можуть виникнути внаслідок використання електронних засобів обробки та пересилання інформації.

У широкому розумінні, ризики завжди присутні при будь-якому використанні можливостей електронних засобів. Лише інформаційний веб-сайт, який використовується для рекламних цілей, може бути пошкодженим від неавторизованого доступу третіх осіб з метою викривлення інформації, яка надається банком або іншою фінансово-кредитною установою. Або ж електронна пошта, у якій міститься конфіденційна або приватна інформація, також може бути пошкоджена. Мережеві системи, які так чи інакше обмінюються інформацією з головною базою даних рахунків та транзакцій, можуть бути досяжними для неавторизованих осіб, які зможуть отримати доступ до чутливих даних чи програмних засобів. Також мають місце системні збої. Вони можуть вплинути на цілісність чутливої інформації внаслідок відключення електроенергії і системних дефектів.

Електронні платіжні системи і системи пересилки фінансової інформації спричиняють виникнення деяких окремих ризиків. Використання електронних каналів для надання фінансових послуг є причиною виникнення унікальних ризиків під впливом таких факторів: підвищеної швидкості роботи електронних інформаційних систем; доступу до чутливих фінансових даних, банківських рахунків; розширеної географії діяльності установи; груп користувачів інформаційної системи; інтегрованих конфіденційних баз даних і віддалених периферійних систем. На додаток до унікальних ризиків, традиційні ризики, пов'язані з фінансовою діяльністю, також будуть присутні. Наприклад, якщо банк надає позику, або залучає депозит з використанням електронного каналу, кредитний і ліквідний ризики повинні враховуватись в контексті високошвидкісного електронного середовища. Отже, розглянемо більш детально групу специфічних ризиків, які виникають внаслідок використання сучасних електронних інформаційних систем. Ці ризики виникають в наступних аспектах впровадження і використання електронних інформаційних систем у фінансово-кредитних установах:

Планування і впровадження інформаційної системи:

– прийняття невірних рішень у розрахунках, при плануванні і впровадженні електронних технологій;

– вплив ціни технології на фінансовий стан установи;

– доцільність використання обраної технології в контексті стратегічної глобальної діяльності установи;

– дизайн, структура системи може не відповідати вимогам клієнтів;

– зростаюча конкуренція;

– невизначеність застосування електронних боргових зобов'язань, віртуальних платіжних знаків тощо.

Операційний порядок процедур:

– некомпетентність керівництва, недосконаліть технологій здійснення електронної фінансової діяльності, зокрема, електронного банківського обслуговування;

– існуюча організація діяльності недостатньо захищає конфіденційну електронну фінансову інформацію;

– існуючі порядки і процедури можуть не враховувати швидкість транзакцій і розширену географію досяжності електронних каналів, які використовуються.

Внутрішні спостереження: результати внутрішнього моніторингу фінансової установи, звітність, інформація про фінансовий стан та інша чутлива внутрішня інформація можуть бути доступними в електронних інформаційних системах.

Правові питання:

– невизначеність застосування електронних контрактів, угод, підписів;

– питання захисту приватної інформації клієнтів;

– невизначеність правових заходів за податковим, кримінальним і цивільним законодавством;

– внаслідок ведення міжрегіональної і міжнародної банківської діяльності можуть виникати різноманітні правові колізії;

– невизначене середовище юридичного впливу на використання чутливої фінансової інформації у електронних інформаційних системах і мережах (локальне, національне і міжнародне);

– невизначеність поняття електронних грошей і застосування їх банками та користувачами;

– невизначена юридична сила електронних банківських документів.

Адміністрування і системне управління:

– збої обладнання та у програмному забезпеченні;

– вплив зовнішніх ризиків на банківські електронні системи і бази даних;

– недостатня потужність банківської комп'ютерної автоматизованої системи;

– моральний знос системи;

– адміністрування різних технічних стандартів та протоколів даних, їх недостатня сумісність між собою;

– недостатній захист електронних комунікацій;

– недостатня системна безпека і її контрольованість.

Сторонні розробники (треті особи):

– вплив рівня компетенції стороннього розробника;

– внутрішні правила контролю можуть не розповсюджуватись на третіх осіб;

– слаба технічна підтримка з боку сторонніх розробників електронних банківських систем;

– підтримка і адміністрування взаємодіючих систем;

– помилки при нагляді за відносинами між декількома банками-учасниками спільних платіжних систем.

Специфічні ризики пов'язані з високою швидкістю обміну інформацією і широким доступом до окремих банківських систем, що притаманно електронним каналам передачі даних. Надія на третіх осіб-розробників банківських електронних технологій і юридична невизначеність також є причиною унікальних ризиків в електронних інформаційних системах та платіжних системах.

З наведеного переліку зрозуміло визначення численних ризиків; однак, так чи інакше, ризик збою або пошкодження в будь-якій системі більше спричиняється в середовищі з'єднаних комп'ютерних систем – ***мережевому середовищі***. Потенційні випадки порушень у системі, збої в учасників системи або спроби несанкціонованого доступу до системи можна визначити таким чином:

– ***стихійні лиха***. Ризики, спричинені стихійними лихами, ростуть з географічним розмахом мережі. Наприклад, серверне обладнання для окремої банківської електронної системи може бути віддаленим та вимагати доступу через публічні телекомунікаційні мережі. Ушкодження у будь-якій точці з'єднання може відбитися на виконанні певної операції чи при наданні послуги;

– ***спроби несанкціонованого доступу до системи***. Слід передбачати, що під час роботи електронних інформаційних систем можуть здійснюватись внутрішні або зовнішні спроби доступу з метою пошкодження цілісності системи, надання певної несанкціонованої фінансової послуги, доступу до внутрішньобанківських баз даних, маніпулювання банківськими програмними засобами або фінансовими потоками. Окрім фінансових інтересів, мотиви можуть поширюватись також на бажання обійти захист системи для комерційного шпіонажу. Багато зловмисників можуть приховати атакуючі дії, ускладнюючи визначення методів їх здійснення;

– ***збої в роботі систем учасників***. Наприклад, збої в роботі систем одного або більше учасників платіжної, або іншої інтегрованої фінансової інформаційної системи, можуть завдати відчутного фінансового удару по інших учасниках. Контракти на участь у системі можуть вимагати від всіх учасників погашення фінансових витрат при збої у одного учасника. В найгіршому випадку, сильний окремий збій може відбитися на інших учасниках і системі в цілому та призвести навіть до її відключення. Довіра і конфіденційність у відносинах між банками-учасниками платіжної системи також важливі, оскільки реакція клієнтів банків на мінімальні збої може спричинити небезпеку всій системі.

Ефекти збоїв у системі можуть швидко розповсюдитись за межі кола зацікавлених осіб. Як наслідок, може бути заподіяна шкода репутації установи, а також втрата забезпечення конфіденційності фінансової інформації. Тому програми управління ризиками, які враховують ці специфічні ризики, критично важливі при їх визначенні і потребують відповідної реакції на будь-які інциденти, що можуть виникнути. Одночасне врахування усіх факторів підвищує ступінь захисту від ризику, але також є причиною більших сумарних витрат кошів та інтелектуальних зусиль.

Управління ризиками є постійний процес визначення, виміру, нагляду і усунення потенційних наслідків ризикових ситуацій. З огляду на електронні системи доставки та платіжні системи, цей процес повинен включати всі важливі операційні, правові і репутаційні області впливу ризиків. В залежності від рівня активності, увага може бути приділена:

– загальному спостереженню, що включає: планування і аналіз, порядки і процедури, відповідальності і посади, регуляційна узгодженість і легальні границі, людські ресурси, аудит;

– обробці транзакцій, яка включатиме в себе: визначення користувача, інтеграція інформації, безвідмовність транзакції, забезпечення конфіденційності даних;

– системній адміністрації, до якої повинні входити: оцінка вимог до ресурсів, системна безпека, системна надійність і визначення передбачуваності, системна ємність, порядки зміни кодів, контроль за оновленням системи.

Результати процесу управління ризиками в загальному повинні інтегруватись в стратегічне планування і аналіз придатності; управлінський нагляд і внутрішній контроль; операційні порядки і процедури; системне адміністрування, аудит і тестування; фізичну, транзакційну і системну безпеку; роботи розробника, внутрішня команда підтримки, або команда розробника; реакція на випадкові події, плани готовності; відновлення після стихійних лих, відновлення ведення діяльності і плани на непередбачувані випадки; постійний перегляд технологічних розробок і удосконалень можливостей.

Зазначений перелік в загальному включає у себе традиційні технології управління ризиками, які можуть бути застосовані до електронних систем доставки і платіжних систем. Так чи інакше, технології управління ризиками, що мають конкретну значимість для електронної банківської діяльності підлягають подальшому розгляду. Це – стратегічне планування і аналіз придатності, реакція на непередбачувані випадки і готовність до них, внутрішні регулятори. Багато інституцій користуються електронними системами доставки та платіжними системами частково або повністю розробленими третіми особами. Але керівництво банку несе значну відповідальність за стан банківської комп'ютерної автоматизованої системи, управління сторонніми розробниками, нагляд за електронною поштою і іншими засобами запобігання витоку інформації.

Після впровадження, кожна фінансова інформаційна система повинна підлягати постійному спостереженню, щоб оцінити швидкодію та пристосованість поточним планам і цілям, операційним вимогам і технологічним розробкам. Будь-які збої повинні бути зареєстровані для подальшого більш ефективного вико ристання системи. Компоненти комп'ютерної мережевої системи можуть бути ушкоджені певною кількістю природних чи інших факторів. Ймовірність цього зростає із збільшенням мережі інформаційної системи, вона стає більш вразливою. Так чи інакше, можливість ушкодження може зменшитись з впровадженням певних важелів, які у своїй комбінації захищають фінансову електронну інформаційну систему і дані, що в ній зберігаються.

Ефективна програма захисту не залежить від одного вдалого рішення, а від сукупності рішень, які разом сприяють визначенню, спостереженню, управлінню і запобіганню потенційно можливих ризиків. Найбільш ефективні програми управління ризиками спрямовані на відповідне налаштування апаратної та програмної частин фінансової електронної інформаційної системи під час її розробки. Тому системне управління є невід'ємною частиною будь-якої програми управління ризиками. Міра впливу такої програми повинна бути співрозмірна рівню і складності діяльності фінансово-кредитної установи. Через всеохоплюючі огляди і тести системи, повинні бути розроблені засоби адміністрування для захисту апаратної і програмної частини, даних і систем електронної передачі даних. Для забезпечення максимальної ефективності управління також визначається важливість професійної підготовки та освіченості користувачів і адміністраторів відповідно до стандартів системи.

Висновки. Визначивши потенційні ризики, що виникають внаслідок використання фінансових інформаційних систем, запропонуємо заходи їх запобігання або зменшення їх впливу, які доцільно враховувати при побудові програми управління ризиками фінансово-кредитної установи (табл. 1). Також в програмі управління ризиками повинна бути передбачена сукупність внутрішніх стандартів на кожному етапі впровадження і функціонування будь-якої фінансової електронної інформаційної системи, що забезпечує надання фінансових послуг.

Таблиця 1

Потенційні ризики та засоби їх зменшення

Потенційний ризик	Засоби зменшення ризику
Неавторизований доступ до інформації Системна безпека ушкоджена в результаті доступу до системи зловмисника, при перехваті даних в момент їх передачі або при підключенні до кабелю напряму	Контроль доступу Запровадження фізичного та системного контролю доступу, що включає захист на сайті, системні паролі, файерволи, кодування і механізми визначення зловмисника
Втрата цілісності системи Точність і достовірність даних, пошкоджених в результаті підробки неавторизованою особою, невірні дані внутрішніх спостережень, відсутні електронні підписи клієнтів, помилки системи, викривлення даних	Ідентифікація Використання ідентифікаційного контролю для запобігання цілісності даних. Він включає підтвердження про отримання даних, комп'ютерні автоматичні реєстраційні дані, цифрові підписи, контрольне редагування, розподіл обов'язків
Неповна завершеність транзакції і неможливість відправки транзакції Втрата транзакції під час передачі, дублювання транзакцій через повторне проведення або неможливість проведення транзакції	Підтвердження транзакції Вимагає контролю підтвердження (сумування, послідовне нумерування, перевірка "один до одного" з контрольним файлом), відповідність протоколам, антивірусне програмне забезпечення, резервування даних, планування ситуацій

Література

1. Лук'янова В.В., Головач Т.В. Економічний ризик. Навч. посібник. – К.: Академвидав, 2007. – 464 с.

2. Ткаченко М.І. Система електронних послуг комерційного банку. Монографія. – Тернопіль: Бліц-принтер, 2003. – 135 с.

3. Галіцин В.К. Моделі і методи оцінки інвестиційних проектів. Монографія / О.П. Суслов, Ю.О. Кубрушко. – К.: КНЕУ, 2005. – 168 с.

Підп. до друку 20.08.2010. Ум. друк. арк. 25,90. Обл.-вид. арк. 25,16
Формат 30×42/4, папір офсетний. Друк різографією
Наклад 100, зам. № 222/10

Тиражування здійснено з оригінал-макету, виготовленого
редакцією журналу "Вісник Хмельницького національного університету"
редакційно-видавничим центром Хмельницького національного університету
29016, м. Хмельницький, вул. Інститутська, 7/1, тел. (8-0382) 72-83-63