

## ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ РИЗИК-МЕНЕДЖМЕНТУ ВЗАЄМОДІЇ БАНКІВ І СТРАХОВИХ КОМПАНІЙ

*В сучасних умовах взаємодії банків і страхових компаній наявність інформаційного забезпечення належної якості та в належних обсягах є необхідною передумовою комерційної успішності. Отже, будь-які відмови в системі оперативного забезпечення керівної підсистеми будь-якої компанії необхідною інформацією здатні завдати їй істотної шкоди, а отже, можуть бути кваліфіковані як джерело ризику.*

*Ключові слова: ризик-менеджмент, взаємодія, банк, страхова компанія, інформаційне забезпечення, ризику, класифікація.*

N. A. PENKAL  
Khmelnitsky National University

## INFORMATION SUPPORT OF RISK MANAGEMENT OF INTERACTION BETWEEN BANKS AND INSURANCE COMPANIES

*The current stage of development of the financial market is characterized by intense integration processes and strengthening cooperation between the institutions. Integration of financial institutions is a relatively new phenomenon for Ukraine's financial market, but it is not exempt from risks arising activities. Risk management (risk management) plays a major role in the process of preventing and neutralizing the risk of interaction between banks and insurance companies, and ensure the quality of information and appropriate amounts is essential for commercial success. Thus, any failure in the system operational support subsystems leadership of any of the necessary information to cause significant damage to it, and thus can be qualified as a source of risk.*

*Keywords: risk management, interaction, bank, insurance company, information, risk classification.*

**Постановка задачі.** В сучасних умовах взаємодії банків і страхових компаній наявність інформаційного забезпечення належної якості та в належних обсягах є необхідною передумовою комерційної успішності. Отже, будь-які відмови в системі оперативного забезпечення керівної підсистеми будь-якої компанії необхідною інформацією здатні завдати їй істотної шкоди, а отже, можуть бути кваліфіковані як джерело ризику.

**Аналіз досліджень та публікацій.** Дослідженню окремих питань у сфері оцінки ризиків і ризик-менеджменту присвячені численні роботи провідних вітчизняних вчених: К. В. Багмет, В. В. Вуколов, А. І. Грищенко, І. Ю. Івченко, М. С. Клапків, Н. І. Машина, А. О. Старостіна, Ю. В. Тюленєва. Серед відомих західних фахівців ризик-менеджменту банківського та страхових ринків варто відзначити роботи Дж. Бессіса, Х. ван Грюнінга, Т. Райса, Ч. Тапієра, С. Фроста, Р. Чепмена І. Школьніка та багатьох інших.

**Виділення невирішених частин.** Сучасний етап розвитку фінансового ринку характеризується інтенсивними інтеграційними процесами та посиленням співпраці між його інститутами. Налагодження дієвого інформаційно-аналітичного забезпечення взаємодії банків та страхових компаній – одна з передумов ефективної співпраці. Аналітичне забезпечення залежить, в першу чергу, від чітко налагодженої роботи базового програмного комплексу взаємодії банку та страхової компанії.

**Формулювання цілей.** З'ясувати, за якими критеріями класифікують інформаційні ризики взаємодії банків і страхових компаній.

**Виклад основного матеріалу дослідження.** Звітно-статистична інформація відображає результати фактичної діяльності організації і призначена для вищих органів управління, органів державної статистики, податкової інспекції тощо, наприклад, річний бухгалтерський звіт про діяльність фірми. Причинами порушення внутрішніх комунікацій можуть бути: неправильна побудова організаційної структури фірми; виникнення міжособистісних конфліктів між співробітниками організації або конфліктів між її підрозділами.

Причинами відмови автоматизованих систем можна вважати наступні:

а) помилки персоналу. Їх можна поділити на чотири групи за характером дій персоналу:

- навмисні дії в межах делегованих прав доступу;
- ненавмисні дії персоналу в межах делегованих прав доступу;
- дії персоналу або сторонніх осіб, пов'язані з порушенням прав доступу;
- вірусні атаки, що є наслідком дій персоналу;

б) програмні помилки – це одна з основних, постійно наявних вад використовуваних програм, що зумовлюється явними помилками, які виникають на етапі написання, так і несумісністю окремих програм між собою або з певними апаратними пристроями (складовими модулями комп'ютерів);

в) апаратні збої – це порушення нормального режиму функціонування комп'ютерних комплексів, зумовлені фізичним пошкодженням комунікаційних каналів, відмовами в системах живлення, виходом з

ладу окремих модулів обчислювальних машин;

г) інформаційні помилки. Можна виокремити три типи помилок:

– структурні (викривлення в структурі бази даних) – помилки такого типу зустрічаються найчастіше; вони викликані, як правило, поновленням структури бази даних і виявляються досить швидко, хоча теоретично можливі випадки незначного впливу таких помилок;

– перекручування або втрата інформації (джерело цих помилок, зазвичай, перебуває поза системою.

Вони можуть бути викликані різними причинами, починаючи з вірусної атаки та помилок у комунікаційному устаткуванні і закінчуючи похибками в роботі персоналу; виявити такі помилки дуже складно, наприклад, для їх усунення консультант змушений візуально перевіряти всі щоденні баланси, що надсилаються з філій);

– викривлення інформації при узагальненні.

За чинним законодавством України, інформація є об'єктом права власності, а також об'єктом володіння, використання та розпорядження. Інформаційні ризики слід розглядати і враховувати як економічні (майнові, виробничі, фінансові). Детальну класифікацію інформаційних ризиків взаємодії банків і страхових компаній наведено на рисунку 1.

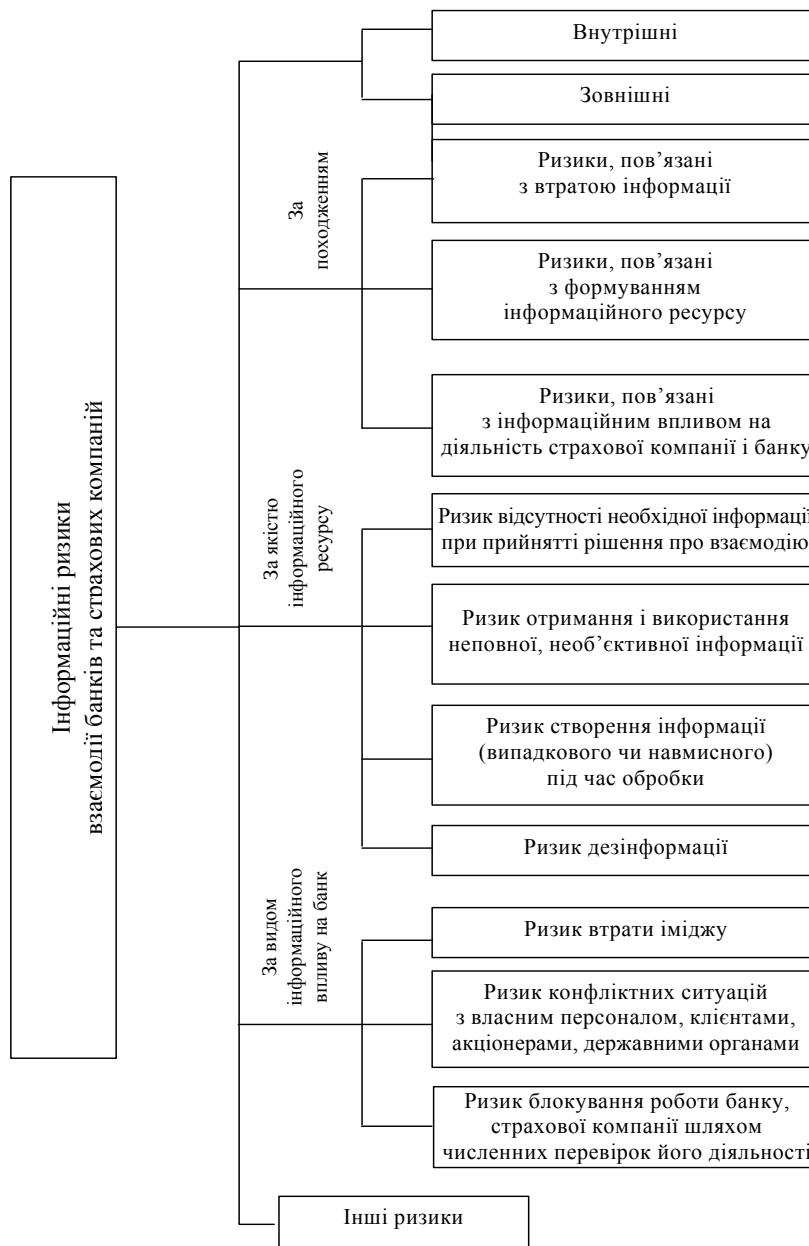


Рис. 1. Класифікація інформаційних ризиків взаємодії банків і страхових компаній (джерело: розроблено на основі [3; 2; 1] та власних досліджень)

Для мінімізації інформаційних ризиків необхідно дотримуватися певних принципів. При взаємодії банків і страхових компаній пропонуємо враховувати наступні принципи:

– Принцип персональної відповідальності, відповідно до якого кожний співробітник або клієнт несе персональну відповідальність за збереження встановлених режимів діяльності в межах своїх повноважень або відповідних інструкцій. Відповідальність за порушення режимів діяльності повинна бути заздалегідь конкретизована і персоніфікована.

– Принцип обмеження повноважень. Стосується персоналу і засобів захисту та обробки інформації. Він охоплює проблему доступу, коли можливість порушення комерційної таємниці або нормального функціонування підприємства, пропорційна кількості поінформованих осіб. Другий складник цього принципу – необхідність заборони фізичного доступу до особливо вразливих зон особам, діяльність яких не передбачає роботу в них. Третій складник – мінімізація будь-яких засобів, за допомогою яких виконуються функціональні обов'язки персоналу і дії клієнтів.

– Принцип взаємодії і співробітництва – спрямований на створення сприятливої внутрішньої і зовнішньої атмосфери в організації. Взаємодія досягається довірчими стосунками співробітників, відповідальними за ризикозахищеність організації, і рештою персоналу, а також іншими допоміжними заходами та стимулюванням, у тому числі матеріальним.

**Висновки.** Однією з умов ефективної співпраці є налагодження дієвого інформаційного забезпечення взаємодії банків та страхових компаній. Налагодження дієвого інформаційного забезпечення взаємодії банків і страхових компаній – одна з передумов ефективної співпраці. Інформаційне забезпечення взаємодії банків і страхових компаній представляє собою систему збору, обробки, аналізу інформації, а також відповідних процедур моніторингу з метою відстеження реалізації цілей коригування стратегії взаємодії.

### Література

1. Вуколов В.В. Інформаційні ризики в державному управлінні [Електронний ресурс] / Вуколов В.В. – Режим доступу : <http://www.dbuara.dp.ua/zbirnik/2010-02/10vvvrdu.pdf> – (Дата звернення 29.01.2015)
2. Модель процессов MSF. Белая книга [Електронний ресурс]. – Режим доступу : [cs.karelia.ru/~kulakov/.../MSF\\_process\\_model\\_rus.doc](http://cs.karelia.ru/~kulakov/.../MSF_process_model_rus.doc) – (Дата звернення 29.01.2015)
3. Парадигма информационных рисков [Електронний ресурс]. – Режим доступу : [http://fa-kit.ru/main\\_dsp.php?top\\_id=591](http://fa-kit.ru/main_dsp.php?top_id=591) – (Дата звернення 15.01.2015)
4. Артищук І. В. Управління ризикозахищеністю підприємства / І. В. Артищук // Науковий вісник НЛТУ України. – 2011. – № 21.5. – С. 153–159.
5. Багмет К. В. Дослідження передумов банківсько-страхової інтеграції / К. В. Багмет // Вісник Української академії банківської справи. – 2010. – № 2. – С. 123–129.
6. Івченко І. Ю. Моделювання економічних ризиків і ризикових ситуацій / І. Ю. Івченко. – К. : ЦУЛ, 2007. – 344 с.
7. Старостіна А. О. Ризик-менеджмент: теорія та практика / А. О. Старостіна, В. А. Кравченко, О. Ю. Пригара // Маркетинг в Україні. – 2007. – № 2. – С. 40–44.

Надійшла 10.09.2015; рецензент: к. е. н. Михайловська І. М.