УДК 330.131.7:[336.71:368](477)

**Пенкаль Н.А.**
*асистент кафедри фінансів та банківської справи*
*Хмельницького національного університету*

# ПІДХОДИ ДО ПОБУДОВИ ДІЄВОГО УПРАВЛІННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНИМИ РИЗИКАМИ ВЗАЄМОДІЇ БАНКІВ І СТРАХОВИХ КОМПАНІЙ

# APPROACHES TO BUILDING AN EFFECTIVE INFORMATION AND ANALYTICAL RISK MANAGEMENT IN INTERACTION BETWEEN BANKS AND INSURANCE COMPANIES

**АНОТАЦІЯ**

Запропоновано підходи до побудови дієвого управління інформаційно-аналітичними ризиками взаємодії банків і страхових компаній. У сучасних умовах взаємодії банків і страхових компаній наявність інформаційного забезпечення належної якості та в належних обсягах є необхідною передумовою комерційної успішності. Тому будь-які відмови в системі оперативного забезпечення керівної підсистеми будь-якої компанії необхідною інформацією здатні завдати їй істотної шкоди, а отже, можуть бути оцінені як джерело ризику.

**Ключові слова:** взаємодія, ризик, банк, страхова компанія, управління, ризик-менеджмент.

**АННОТАЦИЯ**

Предложены подходы к построению эффективного управления информационно-аналитическими рисками взаимодействия банков и страховых компаний. В современных условиях взаимодействия банков и страховых компаний наличие информационного обеспечения надлежащего качества и в надлежащих объемах является необходимым условием коммерческой успешности. Поэтому любые отказы в системе оперативного обеспечения руководящей подсистемы любой компании необходимой информацией способны нанести ей существенный вред, а следовательно, могут быть квалифицированы как источник риска.

**Ключевые слова:** взаимодействие, риск, банк, страховая компания, управление, риск-менеджмент.

**ANNOTATION**

Approaches to building an effective information and analytical risk management in interaction between banks and insurance companies are suggested. In modern conditions of the interaction of banks and insurance companies, the availability of information of high quality and in appropriate quantity is a prerequisite for business success. Thus, any failure in operational support system of the management subsystem to provide any of the necessary information causes significant damage to it, and therefore can be classified as a source of risk.

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

**Постановка проблеми.** В сучасному світі надзвичайно велику роль в економіці відіграє інформація. Вона є основою при прийнятті рішень для здійснення будь-яких дій. При взаємодії банківського та страхового сегментів економіки, інформація відіграє стратегічну роль, вона дає змогу прогнозувати ситуацію на ринку, попит на нові фінансові продукти та, як результат, прибутковість такої співпраці.

**Аналіз останніх досліджень і публікацій.** Дослідженням окремих питань у сфері оцінки ризиків і ризик-менеджменту присвячено численні роботи таких провідних вітчизняних вчених, як: 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 Грюнинга, Т. Райса, Ч. Тапіера, С. Фроста, Р. Чепмена І. Школьніка та багатьох інших.

**Виділення невирішених раніше частин загальної проблеми.** 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.

**Постановка завдання.** Виокремити, які види економічної інформації впливають на ризики при взаємодії банків та страхових компаній; які причини такого впливу. З'ясувати, за якими критеріями класифікують інформаційні ризики взаємодії банків і страхових компаній. Визначити, за якою схемою діє інформаційно-аналітичне забезпечення взаємодії банків і страхових компаній. Проаналізувати етапи управління інформаційними ризиками.

**Виклад основного матеріалу дослідження.** У ризикології поняття «інформація» розуміють як сукупність відомостей про внутрішній і зовнішній стан керованої системи (об'єкта керування) (рис. 1).

Планова (директивна) інформація містить директивні значення планових і контрольованих показників бізнес-планування на деякий період у майбутньому (рік, квартал, місяць, доба).

Облікова інформація відображає фактичні значення запланованих показників за визначений період. На підставі цієї інформації може бути скореговано планову інформацію, проаналізовано діяльність організації, прийнято рішення щодо ефективнішого управління фірмою. Як облікову інформацію, використовують інформацію натурального (планового) обліку.


**Рис. 1. Види економічної інформації та причини її ризиків при взаємодії банків та страхових компаній**

*Джерело: на основі власних досліджень та [1]*

Нормативно-довідкова інформація містить різноманітні довідкові і нормативні дані, пов'язані з процесами і зв'язками. Це найбільший за обсягом і різноплановий вид інформації. Зазначимо, що в загальному обсязі інформації, якою користуються в організації, нормативно-довідкова становить 50–60%.

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.

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 2.

Для мінімізації інформаційних ризиків необхідно дотримуватися певних принципів. При взаємодії банків і страхових компаній пропонуємо враховувати такі 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 забороняти фізичний доступ до особливо вразливих зон особам, діяльність яких не передбачає роботу в них. Третій складник – мінімізація будь-яких засобів, за допомогою яких виконують функціональні обов'язки персоналу і дії клієнтів;

– принцип взаємодії і співробітництва спрямований на створення сприятливої вну-

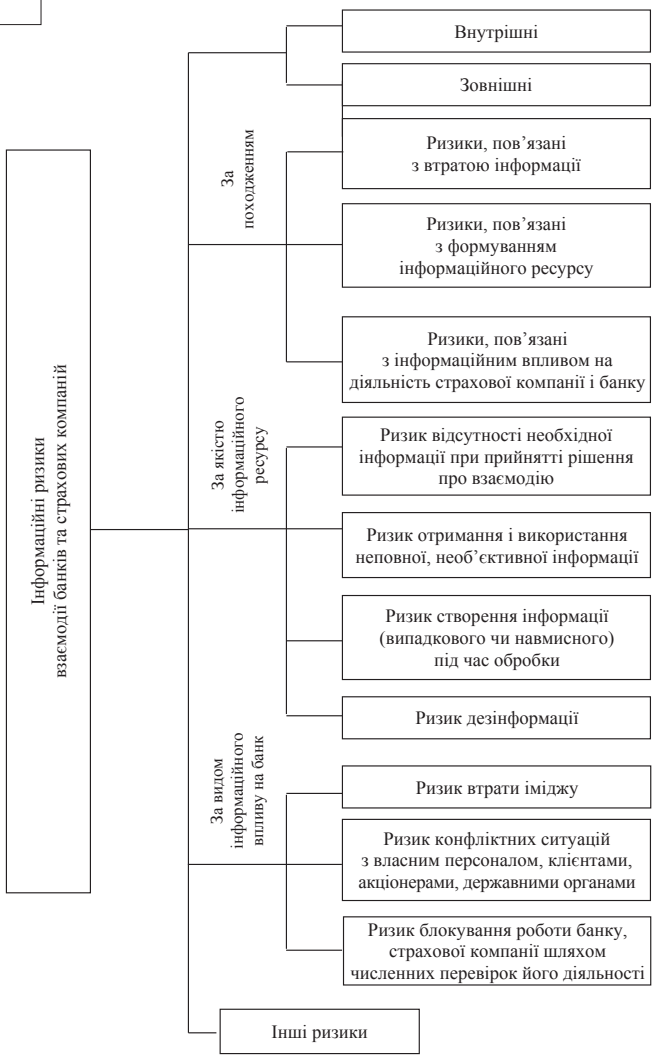


**Рис. 2. Класифікація інформаційних ризиків взаємодії банків і страхових компаній**

*Джерело: розроблено на основі [3; 2; 1] та власних досліджень*

трішньої і зовнішньої атмосфери в організації. Взаємодія досягається довірчими стосунками співробітників, відповідальними за ризикозахищеність організації, і рештою персоналу, а також іншими допоміжними заходами та стимулюванням, зокрема матеріальним.

Налагодження дієвого інформаційно-аналітичного забезпечення взаємодії банків і страхових компаній – одна з передумов ефективної співпраці.

На нашу думку, інформаційно-аналітичне 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. Детальніше розглянемо рисунок 3.

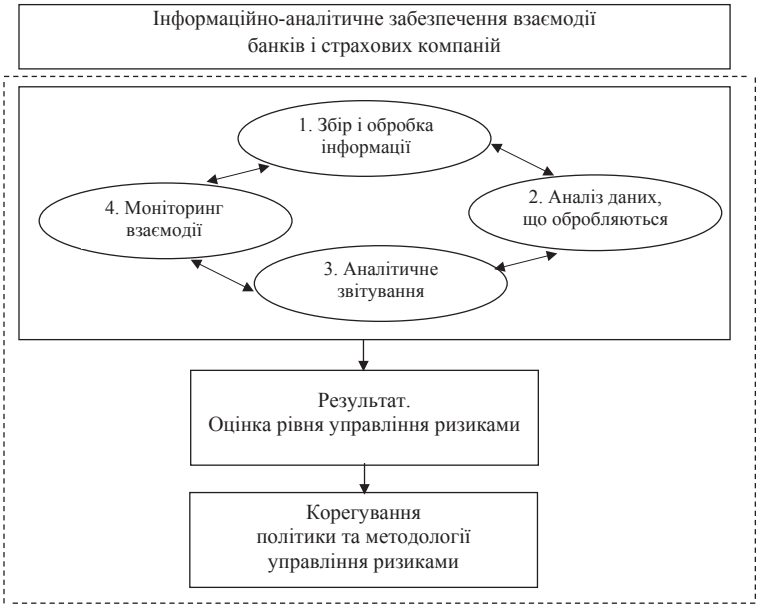


**Рис. 3. Схема інформаційно-аналітичного забезпечення взаємодії банків і страхових компаній**

*Джерело: складено автором*

1. Збір і обробка інформації може здійснюватись за рахунок таких джерел:

– зовнішніх інформаційних ресурсів – це огляди взаємодії банків і страхових компаній у різних країнах світу з метою вивчення досвіду, аналітичні звіти страхового і банківського ринків, загальні відомості про діяльність основних конкурентів, інформація про запровадження нових спільних фінансових продуктів з боку конкуруючих компаній тощо;

– внутрішніх інформаційних ресурсів – це насамперед програмні комплекси у вигляді баз даних страхових компаній і банків.

Ступінь інтегрованості баз даних визначається залежно від виду взаємодії страхових компаній і банків. Можливе запровадження окремого програмного продукту до повної інтеграції інформаційних комплексів.

2. Для проведення аналізу оброблених даних потрібно сформувати сукупність ключових показників оцінювання взаємодії банків і страхових компаній:

– показника оцінки фінансового стану страхової компанії у контексті взаємодії з банком;

– ефективності продажу страхових продуктів через банківські канали дистрибуції або спільні фінансові продукти у разі спільної діяльності чи повної інтеграції організацій;

– виконання плану продажу страхових або спільних фінансових продуктів;

– питомої ваги витрат на провадження банківського страхування або на розробку і реалізацію спільних послуг у загальному обсязі витрат страхової компанії.

3. Результатом проведеного аналізу має бути комплексний аналітичний звіт, який, на наш погляд, має складатися із:

– аналізу конкурентного середовища компанії: відстеження основних тенденцій на страховому і банківському ринках, дослідження діяльності конкурентів, відбір потенційних загроз і можливостей зовнішнього середовища;

– аналізу внутрішнього середовища в контексті інтеграції з банками: результати і висновки стосовно розрахунку наведеної системи показників (показники оцінювання фактичного фінансового стану страхової компанії, ефективності продажу страхових продуктів через банківські канали тощо);

– висновки щодо стану реалізації стратегії інтеграції страхової компанії і банку та внесення необхідних коректівів;

– обов'язковою умовою інформаційно-аналітичного забезпечення є проведення моніторингу взаємодії фінансових установ, що являє собою сукупність заходів, спрямованих на створення системи безперервного аналізу стану взаємовідносин з метою відстеження досягнення цілей або корегування розробленої в цьому напрямі стратегії.

Аналіз найбільш поширених методів, способів і підходів оцінки ризиків інформаційної безпеки свідчить про те, що всі вони базуються на певній методологічній основі, визначеній нормативно-правовими актами країни, політиками і стандартами організації, запозиченими і прийнятими зарубіжними національними або міжнародними стандартами, що визначають вимоги інформаційної безпеки. Згідно з попереднім аналізом найбільш значущими є рекомендації міжнародних і зарубіжних національних організацій стандартизації, таких як ISO, NIST та ін. [3; 2].

Внаслідок того, що нормативно-правова основа процедури оцінки ризиків інформаційної безпеки базується на документах, стандартах, положеннях, офіційно прийнятих на рівні держави, галузі, установи, це додає офіційного статусу як документам, так і результатам самої

процедури. Нормативно-методичною основою процедур оцінки ризиків інформаційної безпеки є документи, які являють собою методичне керівництво, якого необхідно дотримуватись під час оцінки ризиків інформаційної безпеки для інформаційної інфраструктури установи або будь-якої її частини.

Кількісна оцінка інформаційних ризиків ускладнена і часто виявляється неточною та ненадійною з причин, притаманних усім операційним ризикам, а також причин, характерних для окремого типу ризиків.

По-перше, складно розібрати дані, необхідні для кількісної оцінки інформаційних ризиків, оскільки потрібна точність реєстрації, її безперервність і досить тривалий період, щоб дані були придатні для побудови робочої моделі. По-друге, сучасне інформаційне середовище схильне до частих змін через постійне вдосконалення програмного і апаратного забезпечення. Таким чином, необхідно побудувати максимально гнучку модель інформаційного середовища державної установи, яку можна було б оперативно змінювати зі зміною складових цього середовища [1]. І по-третє, витрати часу і людських ресурсів на аналіз уразливості до ризиків досить високі, що не дозволяє проводити його з необхідною періодичністю. Для державних установ процес грамотного систематизованого збору даних, їх відстеження і перевірка, періодичний аналіз і налагодження звітності – поки невирішене завдання. Для того, щоб реалізувати цей процес, необхідно спочатку провести ідентифікацію інформаційних ризиків.

Процес управління ризиками визначає шість логічних кроків [2], за допомогою яких відбувається управління поточними ризиками, розробка та виконання стратегії управління ризиками і робляться висновки з власного досвіду щодо використання на рівні всієї установи (рис. 4).

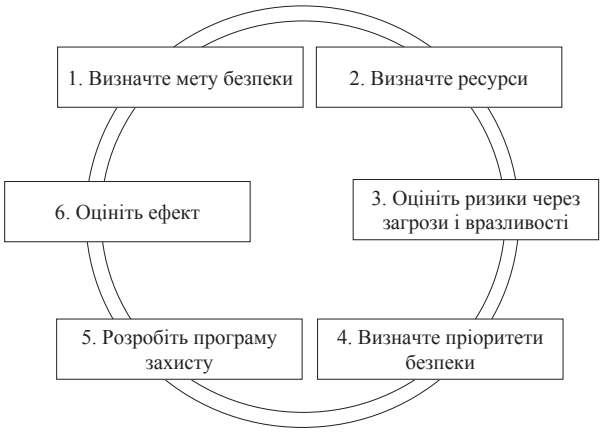


**Рис. 4. Процес управління інформаційними ризиками**

Першим етапом в ідентифікації інформаційних ризиків є вибір аналізованих об'єктів і рівня деталізації, на якому їх аналізуватимуть, при цьому доцільно створити карту інформаційної інфраструктури банку та страхової компанії з тим, щоб бачити, які об'єкти інформаційної інфраструктури вибрано для аналізу ризиків, а які залишилися поза його межами.

Аналіз інформаційної інфраструктури призначений для формування і документування цілісної картини технологічних та інформаційних активів при взаємодії банків і страхових компаній, тобто складу і структури апаратних, програмних засобів, взаємозв'язків між ними, їх фізичного знаходження, включаючи носії інформації, а також потоки даних.

Пропонується виокремити такі рівні інформаційної інфраструктури: фізичні (лінії зв'язку, апаратні засоби тощо); мережеві (мережеві апаратні засоби: маршрутизатори, комутатори, концентратори тощо); мережеві додатки і сервіси; операційні системи; системи управління базами даних; технологічні процеси і додатки. При цьому особливу увагу слід приділити програмним інтерфейсам, тобто додаткам, які забезпечують взаємодію зовнішніх користувачів і персоналу з засобами та системами автоматизації.

Кожен з елементів інформаційної інфраструктури потрібно описувати групою параметрів, з яких можна виділити загальні для всіх описуваних елементів і специфічні. До загальних параметрів належать основне призначення елементу (комп'ютера, програми тощо); склад осіб, що підтримують його функціонування; склад осіб, що використовують цей елемент; рівень значущості елементу для технології обробки інформації; чутливість елементу, під якою розуміється необхідний рівень захисту.

До специфічних параметрів належить:

1) інформація в управління версіями та оновленнями програмного забезпечення (ПЗ);

2) вбудовані у ПЗ засоби гарантування інформаційної безпеки (засоби, шифрування, паролі, засоби мережевого захисту);

3) інвентаризація локальної мережі:

– побудова топології мережі з вказівкою зовнішніх каналів зв'язку (наприклад, інтернет);

– апаратні компоненти мережевої інфраструктури;

– рівень захищеності окремих зовнішніх і внутрішніх каналів;

– засоби контролю мережевої безпеки (мережеві екрани, системи виявлення проникнення і т. ін.);

4) опис інформації та її носіїв.

Для аналізу елементів інформаційної інфраструктури можуть бути використані такі інструменти: спеціально сконструйовані для кожного підрозділу опитувальні листи; спеціально підготовлені для кожного підрозділу інтерв'ю; аналіз документації.

Аналіз уразливості інформаційної інфраструктури необхідно проводити регулярно, але не рідше одного разу на рік. Ця процедура здійснюється в рамках самооцінки середовища контролю ризиків державної установи. При

складанні опитувальних листів для самооцінки можна керуватися положеннями стандарту CobIT, що визначає модель зрілості процесів інформаційної безпеки. Щоб процедури самооцінки були ефективнішими, рекомендується виділити не менше ніж три області аналізу: менеджмент, операційне середовище і технології безпеки.

Менеджмент інформаційної безпеки стосується таких питань управління, як: обов'язки і розмежування прав, розділення повноважень і ролей, забезпечення безперервності підтримки, наявність процедур вимірювання ризиків і незалежного контролю системи менеджменту ризиків, забезпечення безперервності діяльності, регулярне навчання персоналу і т. ін.

**Висновки та перспективи подальшого розвитку.** Однією з умов ефективної співпраці є налагодження дієвого інформаційно-аналітичного забезпечення взаємодії банків та страхових компаній. За результатами проведених досліджень, до завдань побудови дієвого управління інформаційно-аналітичними ризиками взаємодії банків і страхових компаній слід зарахувати:

– комплексну інформаційно-аналітичну підтримку портфеля продуктів банківського страхування, а саме: автоматичне формування резерву незароблених премій і резервів збитків (для ризикових продуктів), математичних резервів (для продуктів страхування життя); друк бланків полісів і договорів; автоматичну пролонгацію договорів (за наявності такої опції); автоматичний розрахунок корегуючих коефіцієнтів для продуктів ризикового страхування; налаштування декількох тарифних планів у межах одного фінансового продукту тощо;

– отримання необхідної інформаційно-аналітичної інформації щодо портфеля продуктів банківського страхування; зниження кількості помилок фінансових посередників завдяки стандартизації параметрів набору тексту і чисел; виключення багаторазового введення однієї і тієї ж інформації до бази даних.

**БІБЛІОГРАФІЧНИЙ СПИСОК:**


1. Вуколов В.В. Інформаційні ризики в державному управлінні [Електронний ресурс] / В.В. Вуколов. – Режим доступу : http://www.dbuapa.dp.ua/zbirnik/2010-02/10vvvrdu.
2. Модель процессов MSF. Белая книга [Электронный ресурс]. – Режим доступа : cs.karelia.ru/~kulakov/.../MSF_process_model_rus.doc.
3. Парадигма информационных рисков [Электронный ресурс]. – Режим доступа : http://fa-kit.ru/main_dsp.php?top_id=591.
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.