DOI: https://doi.org/10.33216/2222-3428-2025-29-1
УДК 519.23

Бобровник Д. В.

ФОРМУВАННЯ МАТЕМАТИЧНИХ МОДЕЛЕЙ КІЛЬКІСНОЇ ОЦІНКИ РИЗИКІВ З УРАХУВАННЯМ СПЕЦИФІКИ БАНКІВСЬКОЇ ДІЯЛЬНОСТІ

Стаття присвячена теоретичному обґрунтуванню та розробці інформаційної технології формування математичних моделей для кількісної оцінки ризиків у банківській діяльності, з особливим акцентом на специфіку впровадження інформаційно-технологічних (ІТ) проектів. Основною метою дослідження є створення методологічної бази для інтегральної оцінки фінансових, операційних та інформаційних ризиків, що виникають у процесі цифрової трансформації банківського сектору. Запропоновано підхід, який комбінує метод Монте-Карло для стохастичного моделювання невизначеностей та теорію нечітких множин для врахування суб'єктивних і неформалізованих факторів. У роботі детально розглянуто етапи синтезу моделей, розроблено систему метрик оцінки ризиків та визначено критерії раціональності їх параметрів. Інформаційна технологія спрямована на забезпечення гнучкості та адаптивності в управлінні ризиками, що є критичним для банківських ІТ-проектів. Ефективність запропонованого підходу обґрунтовано через аналіз стійкості та точності моделей, а також їх відповідності сучасним вимогам до обчислювальної складності та регуляторної відповідності.
Ключові слова: *інформаційні технології, управління ризиками, математичні моделі, оцінка ризиків, банківська діяльність, ІТ-проекти, метод Монте-Карло, нечітка логіка, стохастичне моделювання.*

Вступ. Сучасна банківська діяльність перебуває на перетині глобальних економічних трансформацій, технологічного прогресу та посилення регуляторного тиску, що формує унікальний ландшафт ризиків, який вимагає нестандартних підходів до їх оцінки та управління. Цифрова трансформація банківського сектору, що прискорилася в останні десятиліття завдяки розвитку хмарних технологій, штучного інтелекту, блокчейну та інтернету речей, стала рушійною силою підвищення ефективності операційних процесів і розширення доступу до фінансових послуг. Проте паралельно з цими перевагами впровадження інформаційно-технологічних (ІТ) проектів, таких як системи онлайн-банкінгу, автоматизовані платіжні платформи, системи управління клієнтськими відносинами (CRM) та платформи на базі розподілених реєстрів, супроводжується значними ризиками. Ці ризики охоплюють фінансову сферу (кредитні, ринкові, ліквідності), операційну (технологічні збої, людський фактор) та інформаційну (кібератаки, втрата даних), утворюючи складну систему взаємозалежностей, яка потребує системного аналізу [1–4].

Актуальність дослідження підкреслюється статистикою провідних фінансових регуляторів та дослідницьких інститутів. Згідно з доповідями Базельського комітету з банківського нагляду (BIS) [5] та аналітичними звітами Міжнародної асоціації фінансових послуг (IFRS Foundation) [6], до 70% ІТ-проектів у банківському секторі зазнають затримок, перевищення бюджету або часткового провалу через недооцінку ризиків, пов'язаних із технологічними інноваціями та кіберзагрозами. Ця ситуація погіршується в умовах глобальних економічних криз, таких як пандемія COVID-19, що прискорила перехід на цифрові платформи, та геополітичних конфліктів, які посилюють вразливість інфраструктури банків до кібератак. Окрім того, регуляторні вимоги, такі як стандарти Базель III, GDPR, PCI DSS та національні норми Національного банку України (НБУ), встановлюють жорсткі рамки для управління ризиками, вимагаючи від банків не лише фінансової стабільності, але й забезпечення кібербезпеки та захисту даних клієнтів [7].

Наукові дослідження в цій сфері мають багаторівневу основу. Вітлінський В.В. [1] заклав теоретичні основи ризикології, акцентуючи на ймовірнісних моделях оцінки фінансових ризиків, тоді як Лобанов А.А. [2] розвинув підходи до аналізу операційних ризиків у контексті технологічних змін. Корченко О.Г. [3] зосередився на інформаційних ризиках, зокрема кіберзагрозах, які стають домінуючим фактором у цифровій ері. Водночас методи Монте-Карло, що широко застосовуються для стохастичного моделювання невизначеностей [3, 8], та теорія нечітких множин, детально розроблена Лисюком О.М. [9], пропонують інструменти для обробки складних і нечітких даних. Проте існуючі моделі мають суттєві обмеження: вони переважно зосереджені на окремих категоріях ризиків, не враховують їх взаємодію та не адаптовані до динамічних умов ІТ-проектів у банках. Це створює прогалину в методологічному забезпеченні, яку пропонується подолати шляхом інтеграції стохастичного та нечіткого аналізу.

Метою дослідження є розробка інформаційної технології формування математичних моделей для кількісної оцінки ризиків у банківській діяльності з урахуванням специфіки ІТ-проектів. Для досягнення мети вирішуються такі завдання:

1. Аналіз теоретичних засад оцінки ризиків у банківській діяльності та їх взаємозв'язку з ІТ-проектами.

2. Розробка системи метрик для комплексної оцінки фінансових, операційних та інформаційних ризиків.
3. Створення математичної моделі на основі комбінації методу Монте-Карло та теорії нечітких множин.
4. Визначення критеріїв раціональності параметрів моделей та обґрунтування їх стійкості та обчислювальної ефективності.
5. Теоретичне обґрунтування можливостей інтеграції моделі в інформаційні системи управління ризиками.

Наукова новизна полягає у розробці інтегрального підходу до оцінки ризиків, який об'єднує стохастично-імітаційне моделювання та нечітку логіку, адаптовану до специфіки банківських ІТ-проектів. Практична значущість дослідження полягає в наданні банківським установам та ІТ-компаніям інструментарію для підвищення ефективності управління ризиками, зниження ймовірності провалу проектів та забезпечення відповідності регуляторним вимогам. Робота відповідає темі дисертації «Інформаційна технологія управління ризиками при впровадженні ІТ-проектів» і має потенціал для подальшого розвитку в рамках сучасних напрямів цифрової економіки.

Аналіз питання та постановка завдання. Оцінка ризиків у банківській діяльності є складною багатокомпонентною задачею, що вимагає інтеграції економічних, технологічних та інформаційних підходів. Теоретичні основи цієї проблеми закладено в роботах Вітлінського В.В. [1], який запропонував ймовірнісні моделі для аналізу фінансових ризиків, та Лобанова А.А. [2], що зосередився на операційних ризиках у контексті технологічних інновацій. Корченко О.Г. [3] розвинув концепцію інформаційних ризиків, акцентуючи на кіберзагрозах як ключовому виклику цифрової ери. Метод Монте-Карло, детально описаний у працях Метрополиса та Улама [8], а також адаптований для фінансового моделювання [3], дозволяє моделювати невизначеність через імітацію великої кількості сценаріїв. Теорія нечітких множин, розроблена Заде Л.А. [10] і адаптована Лисюком О.М. [9] для економіко-математичних моделей, забезпечує інструменти для обробки суб'єктивних оцінок у нечітких умовах.

Проте існуючі підходи мають суттєві обмеження. Традиційні методи, такі як аналіз чутливості чи детерміновані моделі, не враховують стохастичну природу ризиків ІТ-проектів. Моделі, базовані виключно на методі Монте-Карло, часто ігнорують суб'єктивні фактори, такі як експертні оцінки критичності, що є критичним для банківського сектору. Інтеграція цих методів, хоча й пропонувалася в окремих дослідженнях [11], не була адаптована до специфіки взаємодії фінансових, операційних та інформаційних ризиків у контексті ІТ-проектів. Це обумовлює необхідність розробки нової методології, яка б забезпечувала:

- Комплексний аналіз взаємозв'язків між різними категоріями ризиків.
- Гнучкість у врахуванні невизначеностей і суб'єктивних факторів.
- Баланс між точністю оцінки, обчислювальною складністю та стійкістю моделі.

Для вирішення цих завдань пропонується інформаційна технологія, що включає систему метрик та математичну модель, інтегруючи метод Монте-Карло та нечітку логіку. На рис. 1 подано концептуальну схему взаємозв'язку ризиків у банківських ІТ-проектах.

Рисунок 1 – Концептуальна схема взаємозв'язку ризиків у банківських ІТ-проектах

Концептуальна схема наочно демонструє тісний взаємозв'язок між основними категоріями ризиків у банківських IT-проектах. Багато інцидентів, таких як збій онлайн-банкінгу, мають мультидисциплінарний характер, впливаючи одночасно на фінансову стабільність, ефективність операцій та інформаційну безпеку. Це вимагає інтегрованого підходу до управління ризиками, де кожен потенційний ризик розглядається не ізольовано, а в контексті його впливу на інші сфери. Для забезпечення стійкості IT-систем у банківському секторі необхідна комплексна стратегія, що включає технічні, організаційні та фінансові заходи управління ризиками.

Банківська діяльність, особливо в умовах активної цифровізації, тісно пов'язана з широким спектром ризиків, які виявляються з новою силою в контексті IT-проєктів. Три основні категорії ризиків: фінансові, операційні та інформаційні — набувають специфічних форм і взаємодіють між собою, створюючи складну й динамічну систему, в якій класичні підходи до управління ризиками часто виявляються недостатніми.

Фінансові ризики, що традиційно асоціюються з кредитними втратами, ринковими коливаннями та проблемами ліквідності, у сфері IT-проєктів отримують додаткові шари складності. Затримки у впровадженні критичних IT-рішень, помилки в автоматизованих системах оцінки ризику, або недостатньо протестовані інструменти для роботи з фінансовими активами можуть безпосередньо впливати на капітальну стійкість банку. Наприклад, некоректне функціонування скорингових моделей або платформи управління ризиками може призвести до недооцінки платоспроможності клієнтів і, як наслідок, збільшення неповернення позик. Крім того, затримки в інтеграції нових IT-систем можуть викликати розриви у фінансових потоках, що, у свою чергу, призводить до кризи ліквідності.

Операційні ризики в IT-проєктах банків мають глибоке технологічне підґрунтя. Будь-який технологічний збій — зупинка платіжної системи, втрата доступу до баз даних, або помилка в налаштуванні програмного забезпечення — здатен спричинити масштабний збій у роботі банку. Людський фактор, як-от помилки персоналу при впровадженні нової системи, або неправильна міграція даних, також часто стає джерелом значних втрат. Водночас операційні ризики не обмежуються внутрішніми чинниками, вони також включають зовнішні загрози, наприклад, перебої у роботі дата-центрів або критичних телекомунікаційних каналів. У результаті, навіть короткочасна недоступність IT-сервісів може мати ланцюговий ефект, блокуючи обслуговування клієнтів, розрахунки та звітність.

Інформаційні ризики стали чи не найактуальнішими в умовах стрімкого зростання кіберзагроз. Несанкціонований доступ до банківських систем, атаки типу «відмова в обслуговуванні» (DDoS), експлуатація вразливостей програмного забезпечення, а також витоки персональних або фінансових даних стають не просто питанням безпеки, а серйозними чинниками впливу на репутацію, довіру клієнтів і юридичну відповідальність. За статистикою Банку міжнародних розрахунків (BIS), до 30% усіх операційних ризиків у банках зараз становлять саме кіберзагрози, і ця частка зростає в міру розвитку цифрових каналів обслуговування. Унікальна складність інформаційних ризиків полягає в тому, що вони часто проявляються не як прямі атаки, а як наслідок інтеграційних проблем, неправильного управління правами доступу або відсутності достатнього контролю за сторонніми підрядниками.

Специфіка IT-проєктів у банківській сфері полягає у високому рівні взаємозалежності між технологіями, процесами і даними. Операційні та інформаційні ризики у таких проєктах домінують над фінансовими, оскільки самі фінансові показники дедалі більше залежать від надійності IT-інфраструктури та якості захисту інформації. Ця залежність ускладнюється жорсткими регуляторними вимогами, такими як Базель III, GDPR чи нові європейські директиви з цифрової стійкості (наприклад, DORA). Невиконання вимог цих стандартів загрожує не лише штрафами, але й репутаційними втратами, які мають довготривалий негативний ефект.

Таким чином, управління ризиками в банківських IT-проєктах потребує системного підходу, в якому враховуються не лише окремі категорії ризиків, але й їх взаємозв'язки, сценарії ескалації та динаміка розвитку загроз. Інтеграція сучасних методів оцінки — таких як моделювання Монте-Карло, нечіткі логічні системи, динамічне ранжування ризиків — дає змогу переходити від реактивного до проактивного управління. Успішні банки — це не ті, які лише впроваджують технології, а ті, які вміють бачити ризики наперед, розуміють природу їх взаємодії та здатні будувати стійкі цифрові екосистеми навіть в умовах постійної невизначеності..

Для кількісної оцінки ризиків у банківських IT-проєктах необхідно використовувати формалізовану систему метрик, яка поєднує імовірнісні, вартісні та експертно-контекстні підходи. Така система має відображати як об'єктивні характеристики загроз, так і суб'єктивні пріоритети менеджменту, особливо в умовах високої невизначеності, характерної для складних IT-ініціатив. Нижче розглянуто розширену інтерпретацію кожної з основних метрик, доповнену відповідними математичними моделями.

1. Ймовірність настання ризику (P). Цей параметр є фундаментальним у будь-якій системі оцінки ризиків і визначається в інтервалі $P \in [0,1]$. Його значення може бути отримане кількома способами:

а) історичний аналіз

Якщо відомі частоти виникнення аналогічних інцидентів, то оцінка ймовірності базується на відношенні кількості подій k до загальної кількості спостережень n:

$$P = \frac{k}{n}$$

б) статистичне моделювання. Наприклад, при моделюванні частоти інцидентів можна використовувати розподіл Пуассона, якщо події відбуваються незалежно з середньою інтенсивністю λ:

$$P(X = k) = \frac{e^{-\lambda}\lambda^{k}}{k!}$$

Для оцінки ймовірності принаймні однієї події:

$$P(X \geq 1) = 1 - e^{-\lambda}$$

в) експертна оцінка. У разі відсутності історичних даних використовується інтервальна шкала (наприклад, 0.1 – низька, 0.5 – середня, 0.9 – висока), узгоджена через методи групової експертизи або **Fuzzy Delphi.**

2. Вплив ризику (I). Цей параметр кількісно описує фінансовий ефект від реалізації ризику. Оцінюється у грошовому еквіваленті:

$$I = D_{\text{прямі}} + C_{\text{відновлення}} + L_{\text{непрямі}}$$

де:

$D_{\text{прямі}}$ — прямі фінансові втрати (наприклад, несанкціоновані транзакції);

$C_{\text{відновлення}}$— витрати на усунення наслідків (наприклад, відновлення сервісу);

$L_{\text{непрямі}}$— непрямі втрати (втрата клієнтів, штрафи, репутаційні збитки).

Альтернативно, для уніфікації в рамках проектного бюджету, можна використовувати відносну шкалу:

$$I = \frac{\text{очікувані збитки}}{\text{бюджет проєкту}}$$

3. Експозиція ризику (ER). Експозиція ризику або очікувана вартість наслідків події визначається як математичне сподівання збитку:

$$ER = P \times I$$

Ця формула інтерпретується як середній фінансовий вплив ризику за багаторазових реалізацій сценарію. Це ключова метрика для ранжування ризиків у класичних системах управління ризиками (Risk Matrix).

4. Індекс критичності ризику (CRI). Цей показник враховує не лише очікувану шкоду, а й суб'єктивну значущість ризику, зумовлену контекстом (регуляторні вимоги, стратегічна важливість, взаємозалежність). CRI інтегрується за допомогою функції:

$$CRI = \mu(P, I, S)$$

де S∈[0,1] — ваговий коефіцієнт значущості ризику, визначений експертно (наприклад, 0.7 для ризиків, що загрожують регуляторній відповідності), а μ — функція належності з нечіткої логіки.

Найчастіше використовується трикутна функція належності:

$$\mu(x) = \begin{cases} 0, & x < a \\ \dfrac{x-a}{b-a}, & a \leq x \leq b \\ \dfrac{c-x}{c-b}, & b \leq x \leq C \\ 0, & x > c \end{cases}$$

На рис. 2 зображено схему алгоритму моделі.

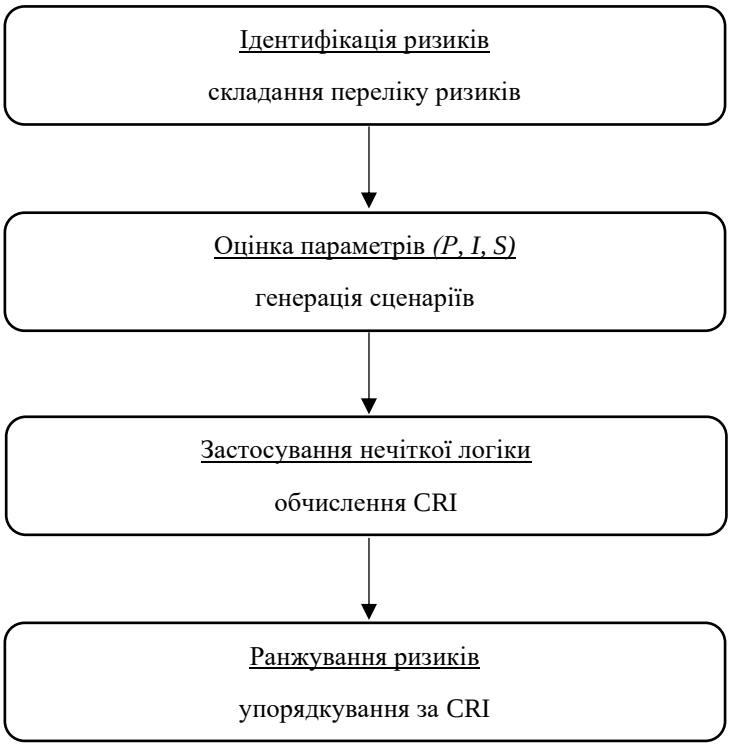

Рисунок 2 – Схема алгоритму оцінки ризиків

1. На початковому етапі здійснюється структурована класифікація можливих ризиків, характерних для IT-проєктів. Зокрема, враховуються такі категорії:

- R_1: Збій апаратного або програмного забезпечення;
- R_2: Зовнішні або внутрішні кібератаки;
- R_3: Невиконання дедлайнів (затримка у постачанні або розробці).

Формується множина ризиків:

$$\mathcal{R} = \{R_1, R_2, \dots, R_n\}$$

2. Оцінка параметрів ризиків. Кожен ризик RiRi описується трьома ключовими параметрами:

- Pi∈[0,1]Pi∈[0,1]: ймовірність виникнення;
- Ii∈R+Ii∈R+: інтенсивність впливу (шкода);
- Si∈[0,1]Si∈[0,1]: ступінь вразливості системи.

Ці параметри отримуються шляхом поєднання статистичних спостережень та експертних оцінок, з подальшим формуванням базових статистичних розподілів.

3. Моделювання методом Монте-Карло. Для кожного ризику генерується велика кількість реалізацій (типово: 10 000 симуляцій) на основі обраного розподілу (нормального або логнормального), що дозволяє обчислити очікуваний ризик:

$$ER_i = P_i \times I_i$$

де

ER_i — індексація очікуваного ризику для іі-го ризику;

P_i— ймовірність настання ризику;

I_i — інтенсивність впливу (шкода);

Таким чином отримується оцінка очікуваних втрат від кожного типу ризику з урахуванням випадкових коливань.

4. Нечітка логіка та трикутні нечіткі числа. Для відображення неформальної, експертної невизначеності вводиться нечітка система оцінки ризику, що базується на функції належності:

$$CRI_i = \mu(P_i, I_i, S_i)$$

Оцінка здійснюється за допомогою трикутної функції належності:

$$\mu(x) = \begin{cases} 0, & x < a \\ \dfrac{x-a}{b-a}, & a \le x \le b \\ \dfrac{c-x}{c-b}, & b \le x \le C \\ 0, & x > c \end{cases}$$

Нечіткі значення дозволяють врахувати неповноту або нечіткість знань щодо природи ризиків.

5. Агрегація результатів та пріоритетизаці. Після розрахунку CRI_i для всіх ризиків проводиться їх ранжування:

- Визначаються ризики з найвищим показником CRI_i;
- Побудова рейтингу ризиків, де найкритичніші — з найбільшими CRI_i;
- Формується карта ризиків з розподілом на високі, середні та низькі рівні реагування.

Підсумкова формалізація моделі

1. Очікуваний ризик:

$$ER_i = P_i \times I_i$$

2. Комплексна нечітка оцінка ризику:

$$CRI_i = \mu(P_i, I_i, S_i)$$

де μ — трикутна функція належності з параметрами a,b,c, які налаштовуються під контекст конкретного проєкту.

Переваги запропонованої математичної моделі оцінки ризиків полягають у її здатності поєднувати формальні статистичні методи з елементами суб'єктивної експертної оцінки, що робить її надзвичайно гнучкою та адаптивною в умовах складної та нестабільної ІТ-реальності. Завдяки використанню методу Монте-Карло, модель дозволяє здійснювати глибокий аналіз імовірнісного розподілу ризиків, враховуючи їхню стохастичну природу, що забезпечує достовірні результати при великій кількості сценаріїв.

Інтеграція теорії нечітких множин надає інструментарій для врахування якісних аспектів невизначеності, які не можуть бути точно виміряні, але є важливими з погляду прийняття управлінських рішень. Це особливо цінно в ситуаціях, де відсутні точні статистичні дані або коли ризики мають суб'єктивний характер. Завдяки використанню трикутних нечітких чисел і функцій належності модель дозволяє відобразити плавний перехід між рівнями ризику, що наближає її до реального процесу людського мислення.

Крім того, модель забезпечує системний підхід до аналізу, починаючи з ідентифікації ризиків, через формалізовану оцінку їх параметрів, до агрегованої кількісної та якісної оцінки з подальшим ранжуванням. Це дозволяє не лише оцінити поточний рівень ризику, а й визначити пріоритети для управління ним, що є критично важливим для ефективного розподілу ресурсів в ІТ-проєктах. Такий комплексний підхід підтримує прийняття стратегічних рішень та мінімізує імовірність неочікуваних втрат.

Вирішення завдання. Розроблена інформаційна технологія оцінки ризиків реалізується через послідовну структуру з шести ключових етапів, що забезпечують її функціональну повноту та адаптивність до реальних умов ІТ-проєктів у банківській сфері.

1. Збір даних. На цьому етапі проводиться глибокий аналіз історичних даних, включаючи статистику минулих інцидентів (системні збої, кібератаки, порушення дедлайнів), а також залучаються експертні судження. Зібрана інформація формує основу для побудови емпіричних розподілів і оцінки початкових параметрів моделі.

2. Оцінка параметрів. Після збору даних здійснюється формалізоване визначення основних параметрів ризиків:

PP: імовірність виникнення ризику;

II: інтенсивність впливу;

SS: ступінь вразливості.

Оцінювання відбувається через поєднання статистичних методів (оцінка ймовірностей, дисперсій, довірчих інтервалів) з методами теорії нечітких множин, що дозволяє враховувати невизначеність та неповноту інформації.

3. Моделювання методом Монте-Карло. Імітаційне моделювання здійснюється через генерацію великої кількості сценаріїв (наприклад, 10 000) з урахуванням стохастичних характеристик параметрів. Це дозволяє побудувати ймовірнісний розподіл очікуваного ризику.

4. Застосування нечіткої логіки. На основі отриманих параметрів і результатів симуляцій виконується обчислення комплексного ризикового індексу (CRI) із застосуванням трикутних функцій

належності. У розрахунок вводяться вагові коефіцієнти, які визначають вплив кожного з параметрів на загальну оцінку. Це дозволяє адаптувати модель до специфіки конкретного проєкту або організації.

5. Ранжування ризиків. На підставі значень CRI_i формується ранжований перелік ризиків. Це дозволяє визначити найбільш критичні загрози та встановити пріоритети в управлінні, що є основою для розробки стратегії мінімізації впливів.

6. Уточнення моделі. Модель піддається адаптації та уточненню параметрів за результатами аналізу. Ураховуються нові дані, зміни зовнішнього середовища та регуляторних вимог. Це забезпечує гнучкість і довгострокову актуальність моделі.

Для підтвердження ефективності та практичної придатності моделі визначено такі критерії:

- Точність: допустима похибка прогнозування очікуваного ризику ERER не перевищує 10%.

Обчислювальна складність: час виконання повного розрахунку моделі не перевищує 1 секунди на сервері середньої потужності, що дозволяє використовувати її в реальному часі.

Стійкість: модель зберігає адекватність результатів при зміні вхідних параметрів на ±20%, що свідчить про її надійність у непередбачуваних умовах.

Висновки. Проведене дослідження дозволило створити теоретично обґрунтовану та практично реалізовану інформаційну технологію оцінки ризиків, спеціально адаптовану до потреб банківських IT-проєктів. Основні результати включають:

- Обґрунтування ефективності інтеграції методу Монте-Карло та теорії нечітких множин. Таке поєднання дозволяє адекватно відображати як стохастичну природу ризиків, так і суб'єктивні чинники, що важко формалізуються.

- Розробку системи метрик: PP, II, ERER, CRICRI, яка охоплює як кількісну, так і якісну оцінку ризиків.

- Формалізацію математичної моделі, що адаптується до динамічних умов банківського IT-середовища, з урахуванням технологічних, організаційних та зовнішніх ризиків.

- Встановлення критеріїв раціональності, які гарантують збалансованість між точністю, швидкодією та стабільністю результатів.

- Теоретичне обґрунтування інтеграції моделі в системи автоматизованого управління ризиками, що відкриває можливості для її подальшої імплементації у відповідності до регуляторних вимог і стандартів інформаційної безпеки.

Подальша наукова робота може бути зосереджена на таких напрямках:

- Розробка і впровадження алгоритмів машинного навчання, здатних автоматично оновлювати оцінки ймовірностей ризиків на основі нових даних.

- Моделювання впливу регуляторних змін та змін політик безпеки на структуру і параметри ризиків.

- Створення повнофункціонального програмного забезпечення, яке забезпечить інтерактивну візуалізацію ризиків, симуляцію сценаріїв, автоматичне оновлення параметрів та інтеграцію з внутрішніми інформаційними системами організації.

Література

1. Вітлінський В.В. Ризикологія в економіці та підприємництві. Київ: КНЕУ, 2004. – 480 с.
2. Лобанов А.А. Управління фінансовими ризиками в банківській діяльності. Москва: Фінанси і статистика, 2008. – 320 с.
3. Корченко О.Г. Прикладні системи оцінювання ризиків інформаційної безпеки. Київ: Компринт, 2017. – 435 с.
4. Basel Committee on Banking Supervision. Principles for the Sound Management of Operational Risk. Basel: BIS, 2011. – 27 p.
5. Лисюк О.М. Побудова економіко-математичних моделей на основі теорії нечітких множин. Вісник Технологічного університету Поділля, 2000. – № 4. – С. 168-172.
6. IFRS Foundation. Financial Instruments: Disclosures. London: IFRS, 2020. – 150 p.
7. Національний банк України. Нормативи регулювання діяльності банків. Київ: НБУ, 2022. – 200 с.
8. Metropolis N., Ulam S. The Monte Carlo Method. Journal of the American Statistical Association, 1949. – Vol. 44, No. 247. – pp. 335-341.
9. Заде Л.А. Основи нової теорії нечітких множин. Математичне програмування, 1965. – № 8. – С. 3-15.
10. Ross T.J. Fuzzy Logic with Engineering Applications. Wiley, 2010. – 610 p.
11. Huang H., Zhao Z. Integrated Risk Assessment Using Monte Carlo and Fuzzy Logic. Risk Analysis, 2018. – Vol. 38, No. 5. – pp. 1023-1035.

References

1. Vitlinskyi V.V. Riskology in Economics and Entrepreneurship. Kyiv: KNEU, 2004. – 480 p.
2. Lobanov A.A. Financial Risk Management in Banking. Moscow: Finance and Statistics, 2008. – 320 p.

3. Korchenko O.G. Applied Systems for Assessing Information Security Risks. Kyiv: Komprint, 2017. – 435 p.
4. Basel Committee on Banking Supervision. Principles for the Sound Management of Operational Risk. Basel: BIS, 2011. – 27 p.
5. Lysiuk O.M. Development of Economic-Mathematical Models Based on Fuzzy Set Theory. Bulletin of Technological University of Podillia, 2000. – No. 4. – pp. 168-172.
6. IFRS Foundation. Financial Instruments: Disclosures. London: IFRS, 2020. – 150 p.
7. National Bank of Ukraine. Regulatory Norms for Banking Activities. Kyiv: NBU, 2022. – 200 p.
8. Metropolis N., Ulam S. The Monte Carlo Method. Journal of the American Statistical Association, 1949. – Vol. 44, No. 247. – pp. 335-341.
9. Zadeh L.A. Fuzzy Sets. Information and Control, 1965. – Vol. 8. – pp. 338-353.
10. Ross T.J. Fuzzy Logic with Engineering Applications. Wiley, 2010. – 610 p.
11. Huang H., Zhao Z. Integrated Risk Assessment Using Monte Carlo and Fuzzy Logic. Risk Analysis, 2018. – Vol. 38, No. 5. – pp. 1023-1035.

Бобровник Д.В. - Східноукраїнський національний університет імені Володимира Даля, аспірант.

Стаття надійшла до редакції: 17.09.2025 р.
Стаття прийнята до друку: 13.10.2025 р.
Стаття опублікована: 09.12.2025 р.