УДК 004.942:004.4-049.87
DOI https://doi.org/10.15589/znp2025.1(499).19

CONCEPTUAL RISK MANAGEMENT MODEL FOR THE DEVELOPMENT OF AN ONLINE PLATFORM FOR HIGH-VALUE GOODS

КОНЦЕПТУАЛЬНА МОДЕЛЬ УПРАВЛІННЯ РИЗИКАМИ В ПРОЄКТІ СТВОРЕННЯ ОНЛАЙН-ПЛАТФОРМИ ВИСОКОВАРТІСНИХ ТОВАРІВ

Vadym I. Ziuziun
vadym.ziuziun@knu.ua
ORCID: 0000-0001-6566-8798
Denys O. Liashenko
liashenkoden@knu.ua
ORCID: 0009-0007-5590-9587

В. І. Зюзюн,
канд. техн. наук, доцент
Д. О. Ляшенко,
магістрант

Taras Shevchenko National University of Kyiv, Kyiv
Київський національний університет імені Тараса Шевченка, м. Київ

Abstract. The objective of this article is to develop an integrated conceptual risk management model for IT projects focused on the creation of online platforms that facilitate high-value transactions, such as the sale of luxury watches, real estate, stocks, or cryptocurrencies. In the modern digital landscape, where operations are accompanied by a high risk of fraud and cyber threats, traditional risk management methodologies – such as ISO 31000, PMBOK, and MSF – do not always align with the specific requirements of digital platforms.
This study examines the limitations of these standards and proposes a novel approach that integrates classical methods with contemporary quantitative analysis techniques, including mathematical modelling using a cross-entropy loss function and optimization algorithms. The research is based on a systematic review of literature, mathematical modelling, and simulation analysis, implemented in Python using the SimPy and PuLP libraries. The developed model enables the forecasting of potential risk events, accurate financial impact assessment, and optimization of security expenditure. Special attention is given to the integration of data from project management systems, such as Jira and Trello, and communication platforms, ensuring real-time risk monitoring and adaptive responses to operational changes.
The scientific novelty of this study lies in the creation of a universal risk management model tailored to the specific characteristics of digital platforms handling high-value transactions, thereby ensuring flexibility and efficiency in managerial decision-making.
The practical significance of this research is its potential application in optimizing security measures in IT projects, contributing to a reduction in financial losses and an enhancement of transaction security.
Key words: risk management; IT project; online platform; mathematical modelling; simulation analysis; security optimization.

Анотація. Метою даної статті є розробка інтегрованої концептуальної моделі управління ризиками для ІТ-проєктів, спрямованих на створення онлайн-платформ, що забезпечують високовартісні транзакції, такі як продаж годинників, нерухомості, акцій або криптовалют тощо. У сучасному цифровому середовищі, де операції супроводжуються високим ризиком шахрайства та кіберзагроз, традиційні методики управління ризиками, такі як ISO 31000, PMBOK і MSF, не завжди відповідають специфіці цифрових платформ.
У статті розглянуто обмеження цих стандартів і запропоновано новий підхід, який інтегрує класичні методи з сучасними кількісними засобами аналізу, зокрема математичним моделюванням за допомогою кросентропійної функції втрат та оптимізаційних алгоритмів. Дослідження базується на системному аналізі літературних джерел, математичному моделюванні та симуляційному аналізі, реалізованому мовою Python з використанням бібліотек SimPy та PuLP. Розроблена модель дозволяє прогнозувати потенційні ризикові події, точно оцінювати їх фінансовий вплив та оптимізувати витрати на заходи безпеки. Особливу увагу приділено інтеграції даних із систем управління проєктами, наприклад Jira та Trello, та комунікаційних платформ, що забезпечує можливість моніторингу ризиків у режимі реального часу та адаптивного реагування на зміни в операціях.
Наукова новизна статті полягає у створенні універсальної моделі управління ризиками, адаптованої до специфіки цифрових платформ з високовартісними транзакціями, що дозволяє забезпечити гнучкість та ефективність управлінських рішень.

Практична значущість дослідження полягає у можливості застосування отриманих результатів для оптимізації заходів безпеки в ІТ-проєктах, що сприяє зниженню фінансових втрат та підвищенню захищеності операцій.
Ключові слова: управління ризиками; ІТ-проєкт; онлайн-платформа; математичне моделювання; симуляційний аналіз; оптимізація заходів безпеки.

ПОСТАНОВКА ПРОБЛЕМИ

У сучасному цифровому середовищі дедалі більше організацій впроваджують онлайн-платформи для торгівлі високовартісними товарами, де безпека транзакцій та управління ризиками набувають критичного значення. Під час розробки онлайн-платформи для годинникових колекціонерів було виявлено, що традиційні методики управління ризиками, зокрема підходи, закладені в стандартах ISO 31000, PMBOK і MSF, не завжди адекватно враховують специфіку проєктів, пов'язаних із високою фінансовою відповідальністю та значними вимогами до захищеності операцій. Такі проєкти характеризуються особливою чутливістю до кіберзагроз і шахрайських схем, що ускладнює процес прийняття оперативних управлінських рішень.

Виникає необхідність створення узагальненої концептуальної моделі управління ризиками, яка поєднуватиме найкращі практики традиційних стандартів із сучасними методами кількісного аналізу та оптимізації. Така модель повинна систематизувати процеси ідентифікації, оцінки та контролю ризиків, одночасно оптимізуючи витрати на впровадження заходів безпеки. Важливо, щоб вона враховувала як зовнішні чинники (ринкові умови, конкурентне середовище), так і внутрішні особливості ІТ-проєкту, зокрема швидкість змін і адаптивність процесів управління.

Таким чином, актуальність дослідження полягає у розробці інтегрованої моделі управління ризиками, здатної забезпечити високий рівень захищеності транзакцій та ефективність управлінських процесів у цифрових платформах, що здійснюють торгівлю високовартісними товарами. Розроблена модель може стати фундаментом для формулювання практичних рекомендацій щодо оптимізації заходів безпеки не лише для онлайн-платформи для годинникових колекціонерів, але й для інших ІТ-проєктів у високоризикових сферах, наприклад онлайн-продажу нерухомості, акцій, криптовалют та інших, де характерні високі обсяги транзакцій і високий рівень ризиків шахрайства.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

У сфері управління ризиками в ІТ-проєктах існує значний обсяг літератури, присвяченої як загальним стандартам, так і спеціалізованим підходам, адаптованим до умов складних проєктів, що функціонують у високо ризикованих умовах. Зокрема, стандарт ISO 31000:2018 встановлює систематизований підхід до управління ризиками, охоплюючи всі етапи – від ідентифікації до моніторингу та корекції [1]. Проте численні дослідники підкреслюють, що універсальний характер цього стандарту вимагає адаптації до специфіки цифрових середовищ, де високий рівень кіберзагроз та стрімкість змін потребують більш гнучких і оперативних методів оцінки ризиків [2].

PMBOK Guide, що широко застосовується у сфері проєктного менеджменту, інтегрує управління ризиками як невід'ємну складову життєвого циклу проєкту та пропонує використання як якісних, так і кількісних методів їх оцінки [3]. Однак традиційні підходи PMBOK можуть бути недостатньо адаптованими для онлайн-платформ, особливо тих, що торгують високовартісними товарами, де безпека транзакцій і фінансові наслідки кіберзагроз набувають особливого значення.

Microsoft Solutions Framework (MSF) орієнтований на ІТ-проєкти і пропонує адаптивний підхід, заснований на безперервному моніторингу ризиків протягом усього життєвого циклу проєкту. Проте можливості MSF щодо кількісного вимірювання фінансових втрат і витрат на заходи безпеки часто виявляються обмеженими, що стимулює пошук додаткових методичних рішень [4].

Сучасні дослідження дедалі частіше звертають увагу на застосування математичних моделей та алгоритмів оптимізації для оцінки ризиків. Наприклад, у роботах Whitman і Mattord було продемонстровано, що використання оптимізаційних моделей дозволяє мінімізувати витрати на заходи безпеки при збереженні заданого рівня захищеності системи [5]. Додатково, алгоритми машинного навчання стають важливим інструментом для своєчасного виявлення кіберзагроз, що сприяє зниженню потенційних фінансових втрат за рахунок швидкого реагування [6].

Важливим напрямком досліджень є також інтеграція даних із різних систем управління проєктами та комунікаційних платформ для побудови комплексної системи моніторингу ризиків. Основні принципи інтеграції даних описані у роботі Doan, Halevy і Ives, що може бути застосовано для покращення процесів управління ризиками в ІТ-проєктах [7].

Питання управління ризиками в ІТ-проєктах та ІТ-компаніях досліджувалися в працях [8–9], а підходи до концептуального графічного та математичного моделювання інформаційних систем з допомогою проєктного підходу розглядалися в дослідженні [10].

Таким чином, аналіз останніх досліджень свідчить про те, що існуючі стандарти управління ризиками потребують подальшої адаптації до специфіки цифрових платформ високовартісних товарів. Інтеграція

традиційних підходів з сучасними кількісними методами аналізу дозволить підвищити точність прогнозування ризиків і оптимізувати витрати на заходи безпеки, що є критично важливим для ефективного управління ІТ-проєктами.

ВІДОКРЕМЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ

Попри значний прогрес у розробці стандартних методик управління ризиками, сучасна література вказує на декілька невирішених аспектів, що залишаються актуальними для сервісів, які включають в себе операції з товарами високої вартості. По-перше, традиційні стандарти, такі як ISO 31000 та PMBOK, надають загальні підходи до управління ризиками, але не завжди враховують специфіку швидкоплинного ІТ-середовища. Ці стандарти орієнтовані переважно на якісну оцінку ризиків, що може бути недостатньо для точного визначення фінансового впливу ризикових подій у середовищі, де важлива оперативність і гнучкість.

По-друге, Microsoft Solutions Framework (MSF) забезпечує адаптивність управління ризиками в ІТ-проєктах, проте його можливості щодо кількісного вимірювання фінансових наслідків залишаються обмеженими. Це створює необхідність інтеграції традиційних підходів з сучасними математичними моделями та алгоритмами оптимізації, які дозволяють здійснювати точні розрахунки витрат на заходи безпеки.

Крім того, останні дослідження з використання алгоритмів машинного навчання для прогнозування ризиків демонструють потенціал підвищення точності виявлення загроз. Проте інтеграція цих інноваційних підходів у традиційні методики управління ризиками залишається недостатньою. Деякі автори відзначають, що об'єднання даних із систем управління проєктами та комунікаційних платформ може забезпечити більш комплексну систему моніторингу ризиків, але практичні рішення у цій галузі досі залишаються фрагментарними.

Отже, основна невирішена проблема полягає в тому, що існуючі методики управління ризиками не забезпечують достатньої гнучкості та точності для цифрових платформ, що торгують високовартісними товарами. Ця прогалина створює передумови для подальших досліджень і розробки нових інтегрованих підходів, які дозволять ефективно прогнозувати ризикові події і оптимізувати витрати на заходи безпеки.

МЕТА ДОСЛІДЖЕННЯ

Метою даного дослідження є розробка інтегрованої концептуальної моделі управління ризиками для ІТ-проєктів, подібних до онлайн-платформ у сфері високовартісних товарів. Основне завдання дослідження полягає в адаптації традиційних стандартів управління ризиками до специфіки цифрових середовищ, в яких високий рівень кіберзагроз та швидкість змін вимагають застосування сучасних кількісних методів аналізу.

Дослідження спрямоване на створення моделі, яка дозволить прогнозувати потенційні ризикові події та оптимізувати витрати на заходи безпеки. Застосування методів математичного моделювання, оптимізаційних алгоритмів і аналізу великих даних має забезпечити комплексну оцінку ризиків, що сприятиме ухваленню адаптивних та ефективних управлінських рішень. Важливим аспектом є інтеграція даних з різноманітних джерел, таких як системи управління проєктами, комунікаційні платформи тощо, що дозволить побудувати єдину систему моніторингу ризиків.

Практична значущість дослідження полягає у можливості використання отриманої концептуальної моделі для підвищення ефективності управління ризиками не лише в рамках досліджуваного ІТ-проєкту, але й у більш широкому спектрі цифрових платформ. Результати дослідження дозволять розробити практичні рекомендації щодо оптимізації заходів безпеки, що сприятимуть зниженню фінансових втрат та підвищенню адаптивності управлінських рішень у подібних ІТ-проєктах.

МЕТОДИ, ОБ'ЄКТ ТА ПРЕДМЕТ ДОСЛІДЖЕННЯ

У даному дослідженні використано комплекс методів, що забезпечують як якісний, так і кількісний аналіз процесів управління ризиками в ІТ-проєктах, де передбачається здійснення високовартісних транзакцій. По-перше, застосовано системний аналіз для ідентифікації ключових компонентів процесу управління ризиками, а також встановлення взаємозв'язків між зовнішніми та внутрішніми факторами, що впливають на ефективність прийняття управлінських рішень.

Для аналізу ризикових подій та їхнього потенційного впливу застосовано методи аналізу даних, зокрема статистичний аналіз і класифікаційні алгоритми, що дозволяють оцінити ймовірність виникнення ризиків і розрахувати їх можливий фінансовий вплив [11]. З метою кількісної оцінки невідповідності між фактичним та прогнозованим станом проєкту, використано математичне моделювання із застосуванням крос-ентропійної функції втрат [12]. Цей підхід дозволяє визначити ступінь відхилення від заданого стану та оптимізувати витрати на заходи безпеки шляхом мінімізації цільової функції.

Для перевірки ефективності запропонованої моделі ризик-менеджменту проведено симуляційний аналіз із застосуванням програмних засобів, а саме – Python з бібліотеками SimPy [13] та PuLP [14]. Цей етап дозволяє змоделювати реальні умови роботи ІТ-проєкту, протестувати адаптивність моделі до змінних вхідних даних та визначити оптимальні параметри заходів безпеки.

Об'єкт дослідження – процес управління ризиками в ІТ-проєктах, що реалізують цифрові платформи для високовартісних товарів. Цей об'єкт охоплює як технічні аспекти, тобто забезпечення кібербезпеки, інтеграція з системами управління проєктами, так і організаційні фактори, такі як розподіл відповідальності, комунікація, адаптація управлінських процесів, що впливають на ефективність управління ризиками.

Предмет дослідження – методи та підходи до управління ризиками, зокрема адаптація традиційних стандартів управління ризиками до умов цифрових середовищ, а також застосування сучасних математичних і симуляційних методів для оптимізації заходів безпеки. Особлива увага приділяється інтеграції кількісних методів аналізу з традиційними підходами для формування адаптивної системи управління ризиками в ІТ-проєктах.

ОСНОВНА ЧАСТИНА

Сучасна наукова література з управління ризиками демонструє значний інтерес до розробки універсальних стандартів, таких як ISO 31000, PMBOK та Microsoft Solutions Framework (MSF), які формують загальну методологію управління ризиками у різних організаціях. ISO 31000:2018 встановлює систематизований підхід до ідентифікації, оцінки, контролю та моніторингу ризиків, однак його універсальність створює певні труднощі при застосуванні до умов цифрових платформ, де особлива увага приділяється кібербезпеці, швидкості змін та високій вартості транзакцій. PMBOK Guide інтегрує як якісні, так і кількісні методи оцінки ризиків, але традиційні підходи, запропоновані в ньому, іноді не дозволяють врахувати специфіку цифрових операцій з високовартісними товарами. MSF, розроблений для ІТ-проєктів, забезпечує більш адаптивний підхід, однак йому часто бракує точних механізмів кількісної оцінки фінансових наслідків ризиків.

Враховуючи ці обмеження, у нашій роботі пропонується інтегрована концептуальна модель управління ризиками для ІТ-проєктів, а саме – цифрових платформ у сфері високовартісних товарів, яка поєднує традиційні підходи з сучасними методами аналізу даних та оптимізації.

Основна ідея моделі полягає в тому, що ризики у цифрових платформах можна ефективно контролювати за допомогою послідовного циклу, який включає:

– *Ідентифікацію ризиків.* Дані надходять із систем управління проєктами (наприклад, Jira, Trello), комунікаційних платформ та звітів безпеки. Аналіз цих даних дозволяє виявити потенційні загрози та оцінити їх вплив.

– *Оцінку ризиків.* Ризики оцінюються як якісно (на основі експертних оцінок), так і кількісно (за допомогою математичних методів). Такий підхід дозволяє розрахувати потенційні фінансові втрати, що можуть виникнути у разі реалізації ризикових подій.

– *Розробку заходів безпеки.* На основі отриманих оцінок формуються заходи управління ризиками – профілактичні дії, заходи реагування на ранні симптоми ризику та заходи для зменшення наслідків у випадку їх реалізації.

– *Моніторинг та контроль.* Інтеграція моделі з інформаційними системами дозволяє в режимі реального часу відстежувати виконання заходів та оперативно реагувати на зміни в умовах проєкту.

– *Корекцію та оптимізацію.* На основі зворотного зв'язку система постійно оновлюється та оптимізується, що забезпечує її адаптивність до швидких змін у середовищі ІТ-проєкту.

Ця модель дозволяє комплексно аналізувати ризики та адаптувати заходи безпеки, забезпечуючи гнучкість управління у динамічному середовищі цифрових платформ.

Для кількісного аналізу ефективності заходів безпеки було розроблено математичну модель, яка інтегрує дані, отримані з оцінки невідповідності між фактичним та прогнозованим станом проєкту. Оцінка невідповідності проводиться за допомогою кросентропійної функції, яка є стандартним методом для вимірювання різниці між двома розподілами.

У нашій моделі ми припускаємо, що проєкт можна характеризувати певним «станом», який відображає рівень ризиків, що впливають на його реалізацію. Нехай R_i – фактичний стан проєкту в i-му періоді, який характеризується певним рівнем ризиків, а $\hat{R}_i$ – бажаний або прогнозований стан, до якого ми прагнемо дійти. Тоді цільова функція визначається як сума втрат за всіма періодами:

$$F = \sum i = 1^N L(R_i, \hat{R}_i), \quad (1)$$

де $L(R_i, \hat{R}_i)$ – функція втрат, яка вимірює невідповідність між фактичним і прогнозованим станом. Для оцінки цієї невідповідності ми використовуємо кросентропійну функцію втрат, яка є популярним методом для оцінки відхилень у системах класифікації.

Функція крос-ентропії дозволяє оцінити, наскільки добре модель прогнозує ризиковий стан проєкту. Для кожного i-го періоду функція втрат може бути представлена наступним чином:

$$L(R_i, \hat{R}_i) = -\left[R_i \log \hat{R}_i + (1 - R_i) \log(1 - \hat{R}_i)\right]. \quad (2)$$

Цей вираз дозволяє врахувати як випадки, коли фактичний стан відповідає прогнозованому (низькі втрати), так і коли виникають значні відхилення (високі втрати). Використання крос-ентропійної втрати обґрунтовано її здатністю ефективно відображати якісні розбіжності між прогнозованими і фактичними значеннями у випадках класифікації ризиків

Окрім мінімізації цільової функції, модель повинна задовольняти ряд обмежень, що відображають практичні вимоги ІТ-проєкту.

Обмеження часу реагування, тобто час, витрачений на аналіз і реагування на ризики (T), не повинен перевищувати максимально допустимого часу (T_{max}):

$$T \leq T_{max}. \quad (3)$$

Фінансові обмеження, тобто витрати на заходи безпеки не повинні перевищувати заданий бюджет B. Це можна формалізувати як:

$$\sum_{i=1}^{N} C_i \leq B, \quad (4)$$

де C_i – витрати на заходи безпеки в i-му періоді.

Обмеження на точність прогнозування, тобто для забезпечення ефективності моделі необхідно, щоб точність прогнозування, визначена як відношення фактичних і прогнозованих значень, перевищувала встановлений поріг τ:

$$\frac{1}{N}\sum_{i=1}^{N} \mathbb{1}\{|R_i - \hat{R}_i| \leq \tau\} \geq \alpha, \quad (5)$$

де α – мінімально прийнятний рівень точності, τ – поріг, а $\mathbb{1}$ – індикаторна функція.

Завдання математичної моделі полягає у знаходженні таких параметрів заходів безпеки, які мінімізують цільову функцію F при дотриманні вищезазначених обмежень.

Для валідації математичної моделі та перевірки ефективності заходів безпеки проведено симуляційний аналіз. Реалізація моделі здійснюється мовою Python, що дозволяє перевірити, як зміна параметрів (наприклад, ймовірність ризикової події, час реагування, витрати на заходи) впливає на загальні витрати.

При кожному запуску коду значення сумарних втрат F змінюються через випадкову генерацію даних, що відображає варіабельність реальних умов. Оптимальне значення x визначається шляхом мінімізації загальних витрат, і таким чином, інтегровані дані про втрати безпосередньо впливають на оптимізацію заходів безпеки (рис. 1).

Запущені симуляції показують, що сума варіюється при кожному запуску – це очікувана поведінка, оскільки дані генеруються випадково. Водночас оптимізаційна задача знаходить оптимальне значення x, яке мінімізує загальні витрати згідно з формулою. Наприклад, у першому запуску сума втрат склала 9.94,оптимальне x=0.09тамінімальнівитрати=9.04;удругомузапускусума втрат склала 12.56, x = 0.11 та мінімальні витрати = 11.16. Це демонструє, що наша модель адаптується до змінних вхідних даних та видає оптимальні рішення, що підтверджує її наукову та практичну значущість.

Інтеграція даних, отриманих з оцінки невідповідності між фактичним і прогнозованим станом проєкту, безпосередньо в оптимізаційну задачу дозволяє:

– Отримати кількісну оцінку ефективності заходів безпеки.

– Визначити оптимальний компроміс між витратами на впровадження заходів і зменшенням потенційних втрат.

– Реагувати на зміни в умовах проєкту шляхом постійного аналізу та оптимізації.

Таким чином, запропонована модель не лише об'єднує теоретичні засади та сучасні методи аналізу ризиків, але й демонструє практичну можливість їх інтеграції для прийняття обґрунтованих управлінських рішень у сфері IT-проєктів цифрових платформ високовартісних товарів.

Реалізація розробленої моделі управління ризиками передбачає її інтеграцію із сучасними системами управління проєктами, такими як Jira чи Trello, що дозволяє автоматично збирати дані про завдання, комунікації та статуси виконання. Для цього використовуються API відповідних сервісів, які забезпечують оперативний доступ до інформації з різних каналів комунікації та систем моніторингу безпеки.

Основна мета практичної реалізації полягає в тому, щоб побудована математична модель, яка оптимізує витрати на заходи безпеки, отримала своє практичне підтвердження в умовах реального IT-проєкту. У цьому контексті інтеграція моделі полягає у наступному:

1. Збір та обробка даних.

Інформаційна система інтегрується із системами управління проєктами для автоматичного збору даних про виконання завдань, швидкість комунікацій та інші ключові показники. Це дозволяє постійно оновлювати параметри математичної моделі та перераховувати сумарні втрати у реальному часі. Таке рішення значно покращує точність оцінки ризиків.

2. Реалізація оптимізаційної моделі.

Розроблена математична модель, що мінімізує загальні витрати (сумарні втрати за крос-ентропією та витрати на заходи безпеки), інтегрується в систему прийняття рішень. Наприклад, автоматизований модуль, розроблений на Python, може періодично запускати оптимізаційну задачу, оновлювати оптимальне значення заходів безпеки (значення змінної x) та видавати рекомендації керівнику проєкту щодо оптимізації розподілу ресурсів. Цей модуль може бути реалізований як мікросервіс, що взаємодіє з іншими компонентами IT-екосистеми через REST API.

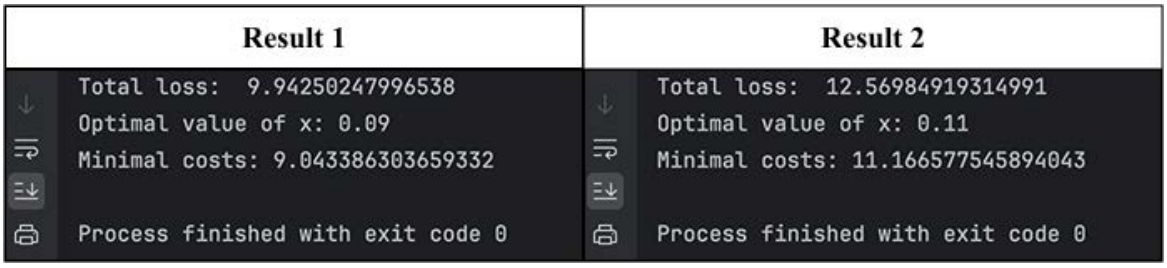

Рис. 1. Результати виконання коду

3. Симуляційний аналіз і валідація.

За допомогою симуляційного аналізу, наприклад, із використанням бібліотеки SimPy, проводиться тестування моделі в умовах змінного навантаження та ризикових подій. Симуляції дозволяють перевірити, як зміна параметрів (ймовірність виникнення ризику, час реагування, фінансові обмеження) впливає на оптимальне значення заходів безпеки. Отримані результати використовуються для калібрування моделі та корекції алгоритмів прогнозування.

4. Взаємодія з користувачем.

Результати аналізу та оптимізації інтегруються в інформаційну панель (dashboard), доступну для керівників проєкту. Це дозволяє оперативно відслідковувати показники ризиків, переглядати прогнозовані втрати та отримувати рекомендації щодо необхідних коригувань. Відображення даних в режимі реального часу сприяє підвищенню якості прийняття рішень та адаптації стратегії управління ризиками.

Таким чином, практична реалізація інтегрованої моделі передбачає не тільки розробку концептуальних та математичних засад, але й їх впровадження в реальну IT-середовище. Це забезпечує адаптивне управління ризиками в цифрових платформах високовартісних товарів, що є критично важливим в умовах сучасного швидкоплинного ринку.

ОБГОВОРЕННЯ ОТРИМАНИХ РЕЗУЛЬТАТІВ

Проведене дослідження включає низку етапів, що починаються з теоретичного аналізу стандартів управління ризиками, продовжуються розробкою інтегрованої концептуальної моделі, математичної моделі та її реалізацією у вигляді програмного коду. Отримані результати демонструють практичну цінність підходу для управління ризиками IT-проєктів цифрових платформ високовартісних товарів.

Перш за все, теоретичний аналіз дозволив окреслити обмеження традиційних стандартів, таких як ISO 31000, PMBOK та MSF, що не завжди враховують специфіку цифрових середовищ. На базі цього аналізу була розроблена концептуальна модель, яка інтегрує методи системного аналізу та сучасні підходи до оцінки ризиків. Модель включає етапи ідентифікації, оцінки, розробки заходів безпеки, моніторингу та оптимізації, що забезпечує гнучкість управління у динамічному середовищі.

Математична модель, побудована на основі кросентропійної функції втрат, дозволяє кількісно оцінити невідповідність між фактичним і прогнозованим станом проєкту. Вона інтегрує витрати на впровадження заходів безпеки та залишкові втрати, що дозволяє оптимізувати розподіл ресурсів для мінімізації загальних витрат. Реалізація цієї моделі через Python з використанням оптимізаційних бібліотек (PuLP) демонструє, як дані про ризикові події безпосередньо впливають на прийняття управлінських рішень.

Практична реалізація моделі відбувається через розробку програмного коду, який поєднує симуляційний аналіз із оптимізаційною задачею. Запуск коду демонструє змінність сумарних втрат (через випадкову генерацію даних) та визначення оптимального значення змінної x, що символізує міру заходів безпеки. Отримані результати підтверджують адаптивність моделі до варіацій вхідних даних, що свідчить про її практичну застосовність.

Значущість цього підходу полягає в інтеграції теоретичного аналізу, концептуальної моделі, математичної оптимізації та симуляційного аналізу. Такий комплексний підхід дозволяє не лише визначити потенційні ризики, але й розробити обґрунтовану стратегію мінімізації втрат у реальному часі. Результати симуляцій показують, що наша модель здатна адаптуватися до змінних умов і оптимізувати заходи безпеки, що є критично важливим для ефективного управління ризиками в подібних IT-проєктах.

Таким чином, запропонована інтегрована система управління ризиками демонструє високу потенційну ефективність та може стати основою для подальшого впровадження в практичне управління IT-проєктами. Подальші дослідження можуть зосередитися на розширенні функціоналу моделі, інтеграції додаткових джерел даних і удосконаленні алгоритмів оптимізації.

ВИСНОВКИ

У даному дослідженні було розроблено інтегровану концептуальну модель управління ризиками в проєкті створення онлайн-платформи високовартісних товарів, яка поєднує традиційні стандарти управління ризиками, таких як ISO 31000, PMBOK, MSF, із сучасними кількісними методами аналізу. Теоретичний аналіз літературних джерел показав, що універсальні стандарти не завжди адекватно враховують специфіку цифрових середовищ, де високий рівень кіберзагроз і стрімкість змін вимагають більш адаптивних і гнучких рішень.

Розроблена концептуальна модель охоплює всі ключові етапи управління ризиками: від ідентифікації та оцінки ризиків до розробки заходів безпеки, моніторингу та оптимізації. Застосування математичної моделі, побудованої на основі крос-ентропійної функції втрат, дозволило кількісно оцінити невідповідність між фактичним і прогнозованим станом проєкту, інтегрувати ці дані з витратами на заходи безпеки та сформувати оптимізаційну задачу для мінімізації загальних витрат. Симуляційний аналіз, реалізований із застосуванням Python, підтвердив адаптивність моделі до змінних умов та її здатність видавати обґрунтовані управлінські рішення.

Практична значущість розробленої моделі полягає у можливості її інтеграції з існуючими системами управління проєктами, що забезпечує моніторинг ризиків у режимі реального часу та своєчасну реакцію на зміну умов проєкту. Це сприяє оптимізації

розподілу ресурсів і зниженню фінансових втрат, пов'язаних із невдалими транзакціями на цифрових платформах високовартісних товарів.

Отже, запропонована інтегрована система управління ризиками має значний потенціал для впровадження як ефективний інструмент підвищення безпеки та оптимізації операцій у IT-проєктах. Подальші дослідження можуть зосередитися на розширенні функціоналу моделі, інтеграції додаткових джерел даних і вдосконаленні алгоритмів оптимізації з метою підвищення точності прогнозування ризиків у динамічних цифрових середовищах.

REFERENCES

[1] ISO. (2018). ISO 31000:2018 – Risk management – Guidelines. Retrieved from: https://www.iso.org/standard/65694.html

[2] Aven, T. (2014). Risk, Surprises and Black Swans: Fundamental Ideas and Concepts in Risk Assessment and Risk Management. Routledge.

[3] Project Management Institute. (2017). A Guide to the Project Management Body of Knowledge (PMBOK® Guide) – Sixth Edition. Retrieved from https://www.pmi.org/pmbok-guide-standards/foundational/pmbok

[4] Microsoft. (2007). Microsoft Solutions Framework. Retrieved from https://learn.microsoft.com/en-us/previous-versions/tn-archive/bb497060(v=technet.10)?redirectedfrom=MSDN

[5] Whitman, M. E., & Mattord, H. J. (2021). Principles of Information Security. Cengage Learning.

[6] SilvioAndrae.(2025).CyberRiskAssessmentUsingMachineLearningAlgorithms.Retrievedfrom:https://www.igi-global.com/chapter/cyber-risk-assessment-using-machine-learning-algorithms/363129

[7] Doan, A., Halevy, A., & Ives, B. (2012). Principles of Data Integration. Morgan Kaufmann. Retrieved from: https://doi.org/10.1016/C2011-0-06130-6.

[8] Ziuziun, V. (2023). Importance of personnel selection in personnel management of an IT organization. 2nd International Scientific and Practical Internet Conference «Global Society in Formation of New Security System and World Order», 41–42. Retrieved from: http://www.wayscience.com/konferentsiya-2-27-28-lipnya-2023/

[9] Korytnyi, O., & Ziuziun, V. (2024). Justification of the need to create an information system for risk management of IT projects. Information Technology and Implementation (Satellite): Conference Proceedings, 236–237.

[10] Ziuziun, V., Kulkovets, V., & Parasiuk, L. (2024). Development of a Decision Support Information System for Managing Large Agile Teams in IT Projects. Collection of Scientific Papers of Admiral Makarov National University of Shipbuilding, 4(497), pp. 166–172, https://doi.org/10.15589/znp2024.4(497).23

[11] Bishop, C. M. (2006). Pattern Recognition and Machine Learning. Springer. Retrieved from: https://www.springer.com/gp/book/9780387310732

[12] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press. Retrieved from: http://www.deeplearningbook.org

[13] The SimPy Project. (2023). SimPy Documentation. Retrieved from: https://simpy.readthedocs.io/en/latest/

[14] PuLP: A Python Library for Linear Programming. (2023). PuLP Documentation. Retrieved from: https://coin-or.github.io/pulp

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] ISO. (2018). ISO 31000:2018 – Risk management – Guidelines. URL: https://www.iso.org/standard/65694.html

[2] Aven, T. (2014). Risk, Surprises and Black Swans: Fundamental Ideas and Concepts in Risk Assessment and Risk Management. Routledge.

[3] Project Management Institute. (2017). A Guide to the Project Management Body of Knowledge (PMBOK® Guide) – Sixth Edition. URL: https://www.pmi.org/pmbok-guide-standards/foundational/pmbok

[4] Microsoft. (2007). Microsoft Solutions Framework. URL: https://learn.microsoft.com/en-us/previous-versions/tn-archive/bb497060(v=technet.10)?redirectedfrom=MSDN

[5] Whitman, M. E., & Mattord, H. J. (2021). Principles of Information Security. Cengage Learning.

[6] Silvio Andrae. (2025). Cyber Risk Assessment Using Machine Learning Algorithms. URL: https://www.igi-global.com/chapter/cyber-risk-assessment-using-machine-learning-algorithms/363129

[7] Doan, A., Halevy, A., & Ives, B. (2012). Principles of Data Integration. Morgan Kaufmann. URL: https://doi.org/10.1016/C2011-0-06130-6.

[8] Ziuziun, V. (2023). Importance of personnel selection in personnel management of an IT organization. 2nd International Scientific and Practical Internet Conference «Global Society in Formation of New Security System and World Order», 41–42. URL: http://www.wayscience.com/konferentsiya-2-27-28-lipnya-2023/

[9] Korytnyi, O., & Ziuziun, V. (2024). Justification of the need to create an information system for risk management of IT projects. Information Technology and Implementation (Satellite): Conference Proceedings, 236–237.

[10] Ziuziun, V., Kulkovets, V., & Parasiuk, L. (2024). Development of a Decision Support Information System for Managing Large Agile Teams in IT Projects. Collection of Scientific Papers of Admiral Makarov National University of Shipbuilding, 4(497), pp. 166–172, https://doi.org/10.15589/znp2024.4(497).23

[11] Bishop, C. M. (2006). Pattern Recognition and Machine Learning. Springer. URL: https://www.springer.com/gp/book/9780387310732

[12] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press. URL: http://www.deeplearningbook.org

[13] The SimPy Project. (2023). SimPy Documentation. URL: https://simpy.readthedocs.io/en/latest/

[14] PuLP: A Python Library for Linear Programming. (2023). PuLP Documentation. URL: https://coin-or.github.io/pulp

Дата надходження статті до редакції: 20.02.2025
Дата затвердження статті до друку: 03.03.2025