МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет «Острозька академія»

Економічний факультет

Кафедра економіко-математичного моделювання та інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня магістра

на тему:

«Розробка моделі управління ризиками в ІТ та АСУ проєктах»

Виконав: студент 2 курсу, групи МУП-21
другого (магістерського) рівня вищої освіти
спеціальності 122 Комп'ютерні науки
освітньо-професійної програми «Управління проєктами»
Швець Михайло Борисович

Керівник: *кандидат економічних наук, доцент*

Новоселецький Олександр Миколайович

Рецензент: *кандидат технічних наук, доцент кафедри прикладної математики та кібербезпеки Донецького національного університету імені Василя Стуса*

Загоруйко Любов Василівна

РОБОТА ДОПУЩЕНА ДО ЗАХИСТУ

Завідувач кафедри економіко-математичного моделювання та інформаційних технологій _____ (проф., д.е.н. Кривицька О.Р.)

Протокол № ____ від « ___ » _____ 2024 р.

Острог, 2024

Міністерство освіти і науки України
Національний університет «Острозька академія»

Факультет: *економічний*
Кафедра: *економіко-математичного моделювання та інформаційних технологій*
Спеціальність: 122 Комп'ютерні науки
Освітньо-професійна програма: Управління проєктами

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Ольга КРИВИЦЬКА
«____» _____20__ р.

ЗАВДАННЯ
на кваліфікаційну роботу студента

Швеця Михайла Борисовича

1. Тема роботи «**Розробка моделі управління ризиками в ІТ та АСУ проєкта**»
керівник роботи кандидат економічних наук, доцент Новоселецький Олександр Миколайович.
Затверджено наказом ректора НаУОА від "_03__" __листопада_ 2023 року №_98__

2. Термін здачі студентом закінченої роботи: 05.12.2024.
3. Вихідні дані до роботи: наукові праці та нормативні документи щодо розробки моделей управління ризиками і ІТ та АСУ проєктах.

4. Перелік завдань, які належить виконати: 1. Теоретичні аспекти управління ризиками в ІТ та АСУ проєктах. 2. Розробка моделі управління ризиками в ІТ та АСУ проєктах. 3. Дослідження ефективності управління ризиками в ІТ та АСУ проєктах.
5. Перелік графічного матеріалу: таблиці, рисунки, діаграми
6. Консультанти розділів роботи:

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Новоселецький О.М., канд. екон. наук, доцент	01.12.23	01.12.23
2	Новоселецький О.М., канд. екон. наук, доцент	01.12.23	01.12.23

3	Новоселецький О.М., канд. екон. наук, доцент	01.12.23	01.12.23

7. Дата видачі завдання: _____01.12.23_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів	Примітка
1	Вибір теми, затвердження її на засіданні кафедри та закріплення наукового керівника.	жовтень 2023	+
2	Вивчення джерел літератури, матеріалів архівів, періодичних видань, збір та узагальнення фактів, даних.	лютий-березень 2024	+
3	Складання плану магістерської роботи та узгодження з науковим керівником.	квітень-травень 2024	+
4	Написання кваліфікаційної роботи в цілому, ознайомлення з її першим варіантом наукового керівника.	червень-жовтень 2024	+
	Розділ 1. Теоретичні аспекти управління ризиками в ІТ та АСУ проєктах.	червень-липень 2024	+
	Розділ 2. Розробка моделі управління ризиками в ІТ та АСУ проєктах.	липень-серпень 2024	+
	Розділ 3. Дослідження ефективності управління ризиками в ІТ та АСУ проєктах	серпень-вересень 2024	+
5	Повне завершення написання кваліфікаційної роботи, оформлення її згідно з вимогами й подання на відгук науковому керівнику.	жовтень 2024	+
6	Підготовка до захисту кваліфікаційної роботи на засіданні кафедри: написання доповіді та виготовлення ілюстративного матеріалу.	листопад 2024	+
7	Публічний захист кваліфікаційної роботи перед екзаменаційною комісією.	грудень 2024	+

Студент: _____ Швець М.Б.

Керівник кваліфікаційної роботи _____ Новоселецький О.М.

АНОТАЦІЯ

кваліфікаційної роботи на здобуття освітнього ступеня магістра за спеціальністю
122 Комп'ютерні науки ОПП «Управління проєктами»
Національний університет «Острозька академія».
Кафедра економіко-математичного моделювання та інформаційних технологій.

Тема: **«Розробка моделі управління ризиками в ІТ та АСУ проєктах»**

Загальний обсяг роботи становить 90 с., зокрема 7 таблиць, 1 рисунок та 45 джерел використаної літератури, три розділи, вступ і висновки.
Автор: ***Швець Михайло Борисович***
Науковий керівник: кандидат економічних наук, доцент
Новоселецький Олександр Миколайович

Захищена «_____» _____2024 року

Короткий зміст кваліфікаційної роботи. Робота присвячена дослідженню теоретичних, методологічних і практичних аспектів управління ризиками в інформаційно-технологічних (ІТ) та автоматизованих системах управління (АСУ).

У вступі висвітлені загальні проблеми управління ризиками в ІТ та АСУ проєктах. Представлено актуальність теми, сформульовано мету, основні завдання, а також об'єкт та предмет дослідження. Обгрунтовано теоретичну базу та методологію дослідження

У першому розділі роботи розглянуто теоретичні аспекти управління ризиками. Виокремлено основні концепції ризик-менеджменту в ІТ та АСУ, проведено аналіз підходів до ідентифікації потенційних ризиків, що виникають на всіх етапах проєкту. Окрему увагу приділено аналізу методів оцінки ймовірності настання ризиків та їх впливу на проєктну діяльність.

Другий розділ присвячений розробці моделі управління ризиками для ІТ та АСУ проєктів. Визначено основні критерії створення інтегрованої системи управління ризиками, запропоновано методику її інтеграції у процеси розробки програмного забезпечення та автоматизованих систем. Проаналізовано впровадження розробленої моделі та обґрунтовано її ефективність.

У третьому розділі представлено результати дослідження ефективності впровадження запропонованої моделі. Здійснено аналіз зниження рівня ризиків, оптимізацію стратегій управління ризиками з урахуванням отриманих даних та запропоновано напрями для підвищення ефективності управління ризиками в ІТ та АСУ проєктах.

Практична значущість роботи полягає у можливості застосування розроблених підходів до управління ризиками в реальних ІТ та АСУ проєктах, що сприяє підвищенню їхньої ефективності та забезпечує досягнення стратегічних цілей компаній. Основні положення та висновки роботи можуть бути використані в проєктному менеджменті, ризик-менеджменті та системному аналізі.

Ключові слова: ризик, управління, управління ризиками, інформаційні технології (ІТ), автоматизовані системи управління (АСУ)

ANNOTATION

qualifying work for obtaining a master's degree in the specialty 122 Computer Science EPP «Project Management»
The National University of Ostroh Academy
Department of Economic and Mathematical Modeling and Information Technology.

Topic: «Development of a Risk Management Model in IT and Automated Control Systems Projects"

The total volume of the work is 90 pages, including 7 tables, 1 figure, and 45 references. The study consists of three chapters, an introduction, and conclusions.
Author: ***Mykhailo Borysovych Shvets***
Academic Supervisor: candidate of economic sciences, associate professor
Oleksandr Mykolayovych Novoseletskyi

Protected «_____», _____, 2024

Brief Summary of the Qualification Work
This study is devoted to the theoretical, methodological, and practical aspects of risk management in information technology (IT) and automated control systems (ACS).
The introduction outlines general issues of risk management in IT and ACS projects. The relevance of the topic is presented, along with the research goal, primary tasks, and the object and subject of the study. The theoretical foundation and research methodology are substantiated.
The first chapter examines the theoretical aspects of risk management. Key concepts of risk management in IT and ACS are highlighted. Approaches to identifying potential risks that arise at all stages of a project are analyzed. Particular attention is paid to assessing the probability of risks and their impact on project activities.
The second chapter is dedicated to developing a risk management model for IT and ACS projects. The main criteria for creating an integrated risk management system are defined, and a methodology for its integration into software development and automated systems processes is proposed. The implementation of the developed model is analyzed, and its effectiveness is substantiated.
The third chapter presents the results of research on the effectiveness of the proposed model. An analysis of risk reduction levels is provided, along with the optimization of risk management strategies based on the obtained data. Directions for improving risk management efficiency in IT and ACS projects are suggested.
The practical significance of this work lies in the applicability of the developed approaches to risk management in real IT and ACS projects, enhancing their efficiency and ensuring the achievement of strategic goals for companies. The key provisions and conclusions of this study can be used in project management, risk management, and systems analysis.
Keywords: risk, management, risk management, information technology (IT), automated control systems (ACS).

ЗМІСТ

ВСТУП

Сучасна економіка вимагає від підприємств постійного адаптування до змін, що забезпечує їхню стабільність і конкурентоспроможність. Одним із ключових чинників успіху є ефективне управління ризиками, особливо в сфері інформаційних технологій (ІТ) та автоматизованих систем управління (АСУ). Ці проєкти характеризуються високим рівнем невизначеності, технологічною складністю та динамічністю середовища. Ефективне управління ризиками у таких проєктах сприяє зниженню негативного впливу ризиків, оптимальному використанню ресурсів та досягненню поставлених цілей.

Сфера ІТ в останні десятиліття стала потужним драйвером світової економіки, спричинивши трансформації у багатьох галузях. В Україні розвиток ІТ-галузі перевищує середньосвітові темпи, демонструючи щорічне зростання кількості компаній і фахівців. Українські ІТ-компанії зарекомендували себе як якісні розробники програмного забезпечення, що створює сприятливе середовище для збільшення кількості проєктів. Проте, зростання темпів і обсягів роботи супроводжується збільшенням ризиків, пов'язаних із недостатньо визначеними вимогами, змінами штатного розкладу та технологій та невідповідною комунікацією між зацікавленими сторонами.

Як свідчить практика, превентивні заходи управління ризиками потребують менших витрат і зусиль, ніж виправлення наслідків. Тому створення інтегрованої системи управління ризиками є нагальною необхідністю для успішної реалізації ІТ- та АСУ-проєктів.

Питанням управління ризиками присвятили свої праці як вітчизняні, так і зарубіжні дослідники. Такі вчені, як Френк Найт та Т. Колеман, заклали фундаментальну теорію ризику, описавши його як невід'ємний елемент

господарської діяльності [6]. Д. Канеман, лауреат Нобелівської премії, дослідив психологічні аспекти ризик-менеджменту, зокрема упередження, що впливають на прийняття рішень.

Серед вітчизняних дослідників особливу увагу слід звернути на роботи В. Вітлінського та Г. Великоіваненка, які дослідили математичні підходи до оцінки ризиків [1]; І. Бланка, який розробив концепцію ризик-менеджменту на рівні підприємства; В. Козика та О. Кузьміна, що зосередили увагу на ризиках у підприємницькій діяльності; І. Федулової та Н. Скопенко, які дослідили особливості управління ризиками у контексті інноваційних проєктів [2].

Зарубіжні автори, такі як Пітер Друкер та Девід Грінберг [3], наголошують на стратегічному значенні управління ризиками у сучасному бізнесі. Джеймс Таттам у своїх працях розробив концепцію "ризик-апетиту", а Бернард Літтерман проаналізував фінансові аспекти ризиків у масштабних проєктах.

Проте, зважаючи на швидкий розвиток ІТ-індустрії, існує необхідність адаптації класичних підходів до сучасних реалій та умов роботи ІТ-компаній

Метою дослідження є розробка ефективної моделі управління ризиками, яка враховує специфіку ІТ- та АСУ-проєктів та сприяє їх успішній реалізації.

Для досягнення мети визначені такі завдання:

1. Вивчити основні концепції управління ризиками у сфері ІТ та АСУ.
2. Провести ідентифікацію основних ризиків, властивих ІТ-проєктам.
3. Проаналізувати сучасні методики оцінки ймовірності та впливу ризиків.
4. Розробити інтегровану систему управління ризиками для ІТ та АСУ.
5. Визначити методики інтеграції ризик-менеджменту у процеси розробки ІТ- та АСУ-проєктів.
6. Провести аналіз результатів впровадження моделі ризик-менеджменту.
7. Розробити рекомендації для оптимізації процесу управління ризиками.

Об'єктом дослідження є ІТ та АСУ проєкт, а **предмет дослідження** – особливості ідентифікації та управління ризиками в ІТ та АСУ проєктах інструментами математичного моделювання.

Дослідження ґрунтується на широкому спектрі наукових джерел та методологічних підходів, які сприяють його обґрунтованості та достовірності.

У дослідженні використані різноманітні методи, включаючи аналітичний, статистичний, порівняльний, узагальнюючий та графічний аналіз. Це допомагає у ретельному обґрунтуванні висновків та розробці стратегій управління ризиками.

Робота складається з трьох розділів, зокрема, в першому розділі «Теоретичні аспекти управління ризиками» визначено ключові поняття ризику та досліджено основні підходи до ідентифікації ризиків у ІТ- та АСУ-проєктах; в другому розділі «Розробка моделі управління ризиками» створено інтегровану систему управління ризиками та запропоновано методику інтеграції ризик-менеджменту у процес розробки; в третьому розділі «Дослідження ефективності впровадження моделі» проведено моніторинг результатів застосування моделі у веб-студії та розроблено рекомендації для оптимізації управління ризиками.

Дослідження спрямоване на розв’язання проблеми ефективного управління ризиками у динамічному середовищі ІТ-індустрії. Внесок вітчизняних і зарубіжних науковців слугував фундаментом для адаптації найкращих практик до умов сучасного бізнесу, а запропонована модель забезпечує підвищення стабільності, ефективності та якості реалізації ІТ та АСУ проєктів.

РОЗДІЛ 1
ТЕОРЕТИЧНІ АСПЕКТИ УПРАВЛІННЯ РИЗИКАМИ В ІТ ТА АСУ ПРОЄКТАХ

1.1. Основні концепції управління ризиками в контексті ІТ та АСУ

Діяльність будь-якого підприємства завжди супроводжується певним рівнем невизначеності у зовнішньому та внутрішньому середовищі. Це створює ризики, які потенційно можуть впливати на досягнення поставлених цілей, ефективність управління ресурсами та стійкість самого підприємства. Своєчасний аналіз і управління ризиками є не лише засобом зниження негативних наслідків, а й важливим індикатором зрілості системи управління організації.

Походить термін «ризик» від грецьких слів «ridsikon» і «ridsa», що означають «стрімчак» або «скеля». Цей термін вперше почав широко використовуватися в контексті мореплавства для позначення небезпек, пов’язаних із навігацією серед скель. З часом його значення розширилося і стало застосовуватися в економічній, соціальній та технічній сферах. Сьогодні ризик трактується як ймовірність виникнення події, яка може мати як негативні, так і позитивні наслідки.

Розвиток наукового підходу до вивчення ризику пов'язаний із становленням теорії ймовірностей. Уже у XVII столітті роботи Блеза Паскаля та П'єра Ферма заклали основи для аналізу випадкових подій, які стали базою для подальшого розвитку ризик-менеджменту.

Термін «ризик» набув особливої популярності в економічній літературі на початку XX століття завдячуючи праці Френка Найта «Ризик, невизначеність та прибуток» [6]. У цій праці Найт зробив важливе розмежування між ризиком і невизначеністю:

- Ризик — це ситуація, в якій ймовірності результатів відомі.

- Невизначеність — це стан, коли ймовірності результатів невідомі або неможливо визначити.

Інший видатний дослідник, Дуглас Хаббард, у своїй книзі «Збій управління ризиками: чому він зламаний і як це виправити» [7], запропонував трактування ризику як стану невизначеності, де деякі можливості включають небажані наслідки, а вимірювання ризику — це аналіз ймовірностей і очікуваних втрат.

З розвитком господарської діяльності та диверсифікацією її форм ризик став важливим елементом управління. У другій половині XX століття значного розвитку набула концепція проєктного менеджменту, спричинена потребами космічної галузі США (проєкти NASA). У 1969 році засновано Інститут управління проєктами (PMI), який вперше стандартизував підходи до управління проєктами та ввів поняття ризику як невизначеної події чи умови, яка може вплинути на цілі проєкту.

Розвиток проєктного підходу у XXI столітті значно розширив поняття ризику. Згідно з ДСТУ ISO 73:2013 «Керування ризиком: словник термінів», ризик визначається як невизначеність, яка впливає на досягнення цілей. У сучасній економіці ризик сприймається не лише як небезпека, але й як можливість отримання вигоди.

Значний внесок у вивчення ризику зробили такі відомі дослідники:

- Френк Найт [6]— обґрунтував фундаментальну відмінність між ризиком і невизначеністю.

- Блез Паскаль і П'єр Ферма [25]— заклали основи теорії ймовірностей, яка є базовою для оцінки ризиків.

- Дуглас Хаббард [7] - досліджував практичні аспекти вимірювання ризику.

- Том ДеМарко і Тімоті Лістер [24]— запропонували нові підходи до управління ризиками в проєктах розробки програмного забезпечення.

Серед українських науковців слід відзначити роботи:

- В. Вітлінського [5], який досліджував математичні моделі оцінки ризиків.

- О. Барановського та Л. Гутко [26, 27], які аналізували ризики у банківській та фінансовій сферах.

- І. Башинської [8], яка зосередила увагу на ризиках у розробці програмного забезпечення.

Зарубіжні дослідники, такі як Є. Верзух, Філліпс Д. та Кліффорд Ф. Грей, активно досліджували ризики в контексті проєктного менеджменту, підкреслюючи важливість їхньої ідентифікації, оцінки та реагування.

У проєктному менеджменті ризик визначається як невизначена подія або умова, яка може мати як негативні, так і позитивні наслідки для проєкту. Наприклад, В. Москаленко [9] акцентує, що ризик проєкту пов'язаний із досягненням поставлених цілей, а О. Гавриш [10] визначає його як сукупність загроз, які впливають на економічну ефективність проєкту.

У своїх роботах українські вчені, такі як І. Грабовський і М. Латків [12, 13], запропонували концепцію системи управління ризиками проєктів (СУРП), яка включає процеси ідентифікації, оцінки та реагування на ризики. Згідно з цими підходами, ризик-менеджмент є невід'ємною складовою управління проєктом, що забезпечує його успішність у складному, динамічному середовищі.

Таким чином, ризик є багатогранним явищем, яке пронизує всі аспекти господарської діяльності. Вивчення його природи, оцінки та управління є необхідною умовою для забезпечення ефективності проєктів, особливо у сфері інформаційних технологій та автоматизованих систем управління. Використання сучасних підходів і методик, таких як стандарти PMBOK і ISO 31000, дозволяє підприємствам знизити негативний вплив ризиків і підвищити успішність реалізації проєктів.

Ризик - це невизначена подія або умова, яка, якщо настане, може мати негативний або позитивний вплив на проєкт.

Основними характеристиками ризику є [4]:

- Імовірність виникнення — наскільки ймовірно, що ризик реалізується.
- Вплив на проєкт — наскільки серйозні наслідки для проєкту або системи можуть виникнути у разі реалізації ризику.
- Тривалість впливу — скільки часу потрібно для відновлення після настання ризику.

У сучасному проєктному менеджменті особливе місце займає концепція "золотого трикутника" — взаємозв’язку між бюджетом, часом та обсягом робіт. У цьому контексті проєктний ризик можна визначити як ймовірність виникнення події, спричиненої певними факторами (джерелами ризику), наслідки якої можуть як негативно, так і позитивно вплинути на реалізацію проєкту в межах запланованих строків, бюджету та затвердженого обсягу, водночас відповідаючи очікуванням зацікавлених сторін.

ІТ-проєкт, у свою чергу, розглядається як комплекс робіт, пов’язаних з інформаційними технологіями, спрямованих на створення, впровадження, розвиток та підтримку інформаційних систем. У межах проєктів розробки програмного забезпечення особливо актуальним є уточнення поняття ризику, який можна визначити як ризикову подію, що може виникнути через технічну складність, перевищення бюджету чи затримки в розробці. Такі ризики можуть бути пов’язані з труднощами інтеграції нових технологій, непередбаченими технічними проблемами або нестабільністю платформ розробки. Їхні наслідки впливають не лише на своєчасну реалізацію проєкту, але й на загальну відповідність інтересам зацікавлених сторін протягом усього життєвого циклу розробки.

Проєктно-орієнтована діяльність завжди реалізується в умовах невизначеності. Це зумовлює необхідність коректної оцінки та управління ризиками, що є критично важливим для успішної реалізації проєктів. Своєчасна ідентифікація, аналіз і превентивні заходи щодо мінімізації ризиків відіграють ключову роль у забезпеченні ефективності проєктного менеджменту.

Концепція ризик-менеджменту передбачає систему управління ризиками, яка спрямована на забезпечення оптимального балансу між досягненням прибутковості та зменшенням наслідків ризикової діяльності. Ця система має бути інтегрована в загальну управлінську політику організації, плани її роботи та операційну діяльність. Лише при виконанні цієї умови ризик-менеджмент стає ефективним. Управління ризиками враховує як негативні, так і позитивні наслідки, визначає потенційні відхилення від запланованих результатів та забезпечує контроль над ними з метою покращення перспектив, зменшення втрат та підвищення обґрунтованості прийнятих рішень.

Ключовою метою ризик-менеджменту є виявлення перспектив удосконалення діяльності, запобігання небажаним подіям або мінімізація їх наслідків. Формування політики та стратегії ризиків вимагає залучення кваліфікованих спеціалістів, для чого створюються спеціалізовані підрозділи. Західні моделі ризик-менеджменту наголошують на чіткому координуванні управлінських процесів на всіх рівнях, при цьому кожен співробітник несе відповідальність за свої ризики, а менеджери забезпечують впровадження культури оцінювання ризиків.

Управління ризиками передбачає низку важливих принципів. Серед них – інтеграція ризик-менеджменту в усі організаційні процеси, його систематичність, використання найкращої доступної інформації, врахування людських і культурних факторів, а також адаптивність до змін. Крім того, ризик-менеджмент забезпечує прозорість, інклюзивність, динамічність та сприяє постійному вдосконаленню.

Перед розробкою концепції ризик-менеджменту слід ретельно проаналізувати зовнішній і внутрішній контекст організації, оскільки ці фактори суттєво впливають на її реалізацію. Політика ризик-менеджменту повинна відображати цілі організації, зобов’язання щодо розподілу відповідальності, вирішення конфліктів інтересів, забезпечення необхідними ресурсами та регулярне вдосконалення. Дотримання цих вимог гарантує ефективність впровадженої системи.

Управління ризиками в ІТ та автоматизованих системах управління (АСУ) є важливим компонентом забезпечення надійності та ефективності їх функціонування. Концепції управління ризиками в АСУ охоплюють широкий спектр підходів, які адаптовані до специфіки цих систем.

Однією з ключових концепцій є *інтегрована концепція управління* ризиками, яка передбачає взаємопов’язану роботу всіх компонентів АСУ для ідентифікації, оцінювання, моніторингу та мінімізації ризиків. Особливістю цього підходу є його націленість на врахування всіх можливих загроз, включаючи технічні збої, кібератаки, людський фактор та зовнішні впливи. Інтеграція процесів управління ризиками у всі етапи життєвого циклу АСУ дозволяє забезпечити їх безперервність та системність.

Ця концепція передбачає комплексний підхід до ідентифікації, оцінювання, моніторингу та мінімізації ризиків, охоплюючи всі рівні функціонування системи. Основним принципом інтегрованої концепції є її спрямованість на включення процесів управління ризиками в усі аспекти діяльності організації, від стратегічного планування до операційного управління. Завдяки цьому створюється цілісна структура, яка забезпечує узгодженість заходів із ризик-менеджменту з основними цілями та завданнями організації.

Особливістю інтегрованого підходу є його універсальність та системність, що дозволяє враховувати як внутрішні, так і зовнішні фактори, які можуть впливати на

функціонування АСУ. Зокрема, концепція орієнтована на управління ризиками, пов'язаними з технічними збоями, інформаційною безпекою, людським фактором і зовнішніми впливами, такими як економічні чи політичні зміни. Інтеграція управління ризиками у всі бізнес-процеси організації сприяє підвищенню адаптивності системи до змін середовища та мінімізації негативних наслідків потенційних загроз.

Важливою складовою інтегрованої концепції є її гнучкість, яка дозволяє адаптувати заходи ризик-менеджменту до особливостей конкретної системи чи організації. Наприклад, для складних систем із великою кількістю підсистем інтегрований підхід забезпечує узгодженість ризик-менеджменту на всіх рівнях. Це досягається завдяки створенню єдиної платформи для аналізу, прогнозування та координації дій, спрямованих на зменшення ймовірності ризиків і посилення ефективності заходів реагування. Таким чином, інтегрована концепція виступає як основа для забезпечення стабільного функціонування АСУ в умовах невизначеності.

Інша концепція – *процесно-орієнтована*, яка базується на принципах управління ризиками в окремих процесах системи. Вона передбачає розробку алгоритмів для кожного етапу роботи АСУ, що дозволяє точно оцінити ймовірність виникнення ризиків на конкретному етапі. Такий підхід має переваги в детальному аналізі загроз, але може бути менш ефективним для комплексного управління ризиками в масштабних системах.

Основою цього підходу є детальний розгляд кожного етапу функціонування системи, що дозволяє виявити специфічні ризики для кожного процесу та розробити індивідуальні методи їх мінімізації. Такий підхід особливо ефективний у системах із чітко визначеною структурою процесів, де кожен елемент має визначені цілі, завдання та критерії оцінювання.

Перевагою процесно-орієнтованої концепції є її здатність забезпечити глибокий аналіз ризиків у межах конкретних операцій чи функцій системи. Це дозволяє точніше визначати причини виникнення ризиків та оцінювати їх вплив на результати діяльності. Завдяки фокусуванню на окремих процесах ця концепція сприяє підвищенню ефективності ресурсного планування та оперативному прийняттю управлінських рішень, що знижує ймовірність системних збоїв. Крім того, процесно-орієнтований підхід сприяє посиленню відповідальності конкретних підрозділів або співробітників за якість виконання своїх завдань.

Втім, одним із недоліків процесно-орієнтованої концепції є ризик втрати загальної картини функціонування системи. Фокус на окремих процесах може призвести до недостатньої координації між ними, що вимагає створення додаткових механізмів для забезпечення цілісності управління ризиками. Зокрема, важливо інтегрувати результати аналізу кожного процесу в загальну стратегію організації. Таким чином, процесно-орієнтована концепція є ефективним інструментом для локального управління ризиками, але її результативність значно підвищується за умови поєднання з іншими підходами, такими як інтегрована концепція чи сценарне моделювання.

Модульна концепція управління ризиками зосереджується на поділі системи на окремі функціональні блоки або модулі. Кожен модуль оцінюється незалежно, що дає можливість виявити ризики на локальному рівні та швидше реагувати на них. Це особливо важливо для складних АСУ, які обслуговують різноманітні процеси. Проте відсутність інтегрованого підходу може створювати прогалини між модулями.

Цей підхід дозволяє виявляти, оцінювати та контролювати ризики на рівні конкретних компонентів системи, що робить його особливо ефективним для великих, багатофункціональних АСУ. Основний принцип модульної концепції

полягає у побудові незалежних, але взаємопов’язаних механізмів управління ризиками, які працюють автономно, але в контексті загальної стратегії організації.

Головною перевагою модульної концепції є її гнучкість та масштабованість. Завдяки розподілу системи на модулі забезпечується локалізація ризиків, що зменшує ймовірність їх поширення на інші частини системи. Такий підхід дозволяє швидко адаптуватися до змін середовища, замінюючи або модернізуючи окремі модулі без необхідності перебудови всієї системи. Крім того, модульна структура сприяє спеціалізації, оскільки кожен модуль можна налаштувати на вирішення специфічних завдань та управління певними типами ризиків, що підвищує ефективність управління.

Водночас модульна концепція вимагає чіткої координації між окремими модулями для забезпечення їхньої сумісності та узгодженості дій. Недостатня взаємодія між модулями може призводити до фрагментації управління ризиками, ускладнюючи побудову єдиної стратегії. Для подолання цього обмеження необхідно впроваджувати механізми інтеграції результатів ризик-менеджменту модулів у загальну систему управління організації. У результаті модульна концепція є ефективним підходом для децентралізованого управління ризиками, який дозволяє підтримувати баланс між автономністю модулів та загальною цілісністю системи.

Концепція управління ризиками на основі *сценарного моделювання* передбачає побудову ймовірнісних сценаріїв розвитку подій у системі. Вона враховує потенційні варіанти порушень у роботі АСУ та їх наслідки. Використання цього підходу дозволяє не лише оцінювати ризики, але й розробляти плани дій для їх мінімізації. Проте сценарне моделювання потребує значних ресурсів для створення точних моделей.

Цей підхід базується на прогнозуванні різних варіантів поведінки системи в умовах невизначеності, враховуючи потенційні ризики та їх наслідки. Основою

концепції є створення моделей сценаріїв, які відображають вплив ключових факторів ризику на систему, що дозволяє заздалегідь розробляти стратегії реагування та адаптації до змін зовнішнього чи внутрішнього середовища.

Сценарне моделювання забезпечує системний підхід до управління ризиками завдяки врахуванню різних аспектів та динаміки розвитку подій. Воно дозволяє ідентифікувати критичні точки системи, на яких можливий найбільший вплив ризиків, і оцінити ймовірність їх реалізації. Це сприяє розробці проактивних заходів, спрямованих на мінімізацію можливих негативних наслідків або використання сприятливих можливостей. Крім того, сценарне моделювання надає змогу враховувати фактори взаємозалежності між ризиками, що є важливим для складних багаторівневих АСУ.

Однією з головних переваг концепції є її адаптивність до змінного середовища, але вона також потребує значних ресурсів для створення й актуалізації сценаріїв. Успішне впровадження сценарного моделювання вимагає наявності високоякісних даних, експертного аналізу та сучасних інструментів для моделювання. Попри це, концепція має значний потенціал для підвищення ефективності управління ризиками, оскільки дозволяє заздалегідь передбачити ризики та забезпечити гнучкість системи в умовах невизначеності. У результаті сценарне моделювання є потужним інструментом стратегічного управління, який допомагає організаціям адаптувати свої АСУ до різноманітних викликів і змін.

Кіберефективна концепція фокусується на ризиках, пов’язаних із загрозами інформаційній безпеці. У сучасних умовах значна частина ризиків в АСУ пов’язана з можливими кібератаками, витоками даних та іншими загрозами в інформаційному просторі. Ця концепція передбачає використання спеціалізованих засобів кіберзахисту, включаючи системи виявлення загроз, управління доступом і моніторинг мережевої активності.

Аналіз зазначених концепцій дозволяє зробити висновок, що кожна з них має як переваги, так і обмеження. Інтегрована концепція забезпечує загальну системність, проте може бути менш детальною для специфічних задач. Процесно-орієнтований та модульний підходи ефективні для аналізу окремих частин системи, але потребують додаткової координації для створення єдиної картини ризиків. Сценарне моделювання є корисним для прогнозування, однак вимагає значних ресурсів. Кіберефективна концепція актуальна для сучасних систем, проте орієнтована лише на інформаційні ризики.

Представимо порівняльний аналіз вищезазначених концепцій.

Таблиця 1.1.

Порівняльний аналіз концепцій управління ризиками в автоматизованих системах управління

Критерій	Інтегрована концепція	Процесно-орієнтована концепція	Модульна концепція	Сценарне моделювання	Кіберефективна концепція
Основна ідея	Включення управління ризиками у всі процеси АСУ на всіх рівнях.	Фокус на аналізі ризиків у кожному процесі системи.	Поділ системи на модулі для окремого оцінювання ризиків у кожному з них.	Розробка сценаріїв імовірних подій і реагування на них.	Спрямована на захист від кіберзагроз, пов’язаних з інформаційною безпекою.
Рівень деталізації	Високий, але охоплює всю систему загалом.	Високий у межах окремих процесів.	Середній, орієнтований на модулі.	Високий у прогнозуванні ризиків та розробці стратегій реагування.	Середній, фокус на інформаційних ризиках.
Масштаб застосування	Для великих та складних систем, які потребують цілісного підходу.	Для систем із чітко структурованими процесами.	Для систем, що мають багато автономних модулів.	Для систем із високою потребою у прогнозуванні подій.	Для систем, які є об’єктами частих кіберзагроз.

Продовження таблиці 1.1.

Гнучкість	Висока, за рахунок інтеграції у всі процеси.	Обмежена через фокусування на окремих процесах.	Висока на рівні окремих модулів, але слабка міжмодульна координація.	Помірна, залежить від точності прогнозування та сценаріїв.	Низька, орієнтована переважно на кіберзагрози.
Переваги	Системність.	Точний аналіз на кожному етапі.	Швидка реакція на ризики на локальному рівні.	Ефективне прогнозування майбутніх подій.	Висока ефективність захисту інформаційних систем.
Можливості	Врахування всіх типів ризиків.	Можливість глибокого опрацювання окремих завдань.	Локалізація ризиків у межах окремих модулів.	Забезпечення стратегій мінімізації наслідків ризиків.	Спрямованість на актуальні загрози.
Недоліки	Вимагає значних ресурсів для впровадження.	Обмежена системним поглядом, ризик втрати загальної картини.	Недостатня координація між модулями.	Висока складність і витратність моделювання.	Фокус лише на інформаційній безпеці, недостатньо охоплює інші ризики.
Сфера найкращого застосування	Великі підприємства з високим рівнем складності управлінських процесів.	Проекти з чітко визначеною структурою процесів.	Системи з децентралізованою архітектурою.	Критично важливі системи, де ризики мають значний вплив на кінцевий результат.	IT-системи, що працюють із конфіденційними даними чи піддаються частим кіберзагрозам.

*Розроблено автором

Для забезпечення надійного управління ризиками в IT та АСУ доцільно поєднувати різні підходи залежно від специфіки системи, її масштабів та функціональних вимог. Інтеграція методів, адаптація концепцій до сучасних викликів та застосування автоматизованих інструментів ризик-менеджменту є запорукою успішного функціонування таких систем.

1.2. Ідентифікація потенційних ризиків у ІТ та АСУ проєктах

Ідентифікація ризиків — це початковий і надзвичайно важливий етап процесу управління ризиками в ІТ та автоматизованих системах управління (АСУ). Основне завдання цього етапу полягає у виявленні та систематизації всіх можливих загроз, які можуть негативно вплинути на проєкт або функціонування системи. Це дозволяє команді передбачити потенційні проблеми та вжити заходів для їх уникнення або мінімізації ще до того, як вони можуть вплинути на результат проєкту.

Проєкти в галузі ІТ та АСУ зазвичай характеризуються високою складністю, динамічністю та певним ступенем невизначеності. Через це виникає потреба ідентифікувати ризики на початкових етапах життєвого циклу проєкту. Навіть незначні ризики можуть призвести до серйозних наслідків, таких як затримки в реалізації, перевищення бюджету, втрати даних, збій у роботі систем або порушення безпеки.

Одним із фундаментальних питань у цьому контексті є правильна ідентифікація ризиків. Основи цього процесу закладені в міжнародному стандарті ISO/IEC 31010:2022 "Risk management – Risk assessment techniques", який пропонує 31 техніку ідентифікації ризиків. Як зазначає І.В. Федулова у своїй статті "Ідентифікація ризиків як складова ризик-менеджменту", серед запропонованих методів найбільш доцільними для проєктної діяльності є 13 основних технік, що охоплюють широкий спектр інструментів аналізу.

Особливість проєктів з розробки програмного забезпечення полягає в їхній залежності від умов невизначеності, зокрема через різноманітність способів реалізації проєкту (вибір мов програмування, інструментів розробки, архітектурних рішень тощо). Для таких проєктів найбільш актуальними методами ідентифікації ризиків є:

1. SWOT-аналіз — оцінка сильних та слабких сторін проєкту, а також зовнішніх можливостей і загроз.

2. Аналіз зацікавлених сторін — виявлення очікувань та вимог клієнтів, інвесторів і користувачів.

3. Аналіз сценаріїв — моделювання можливих сценаріїв розвитку подій, включаючи найгірший і найкращий.

4. Експертні оцінки — залучення досвідчених фахівців для виявлення прихованих загроз.

5. Перевірка чек-листів — використання стандартних переліків ризиків, характерних для подібних проєктів.

Згідно з підходами, закладеними в PMBOK та інших стандартах управління проєктами, ризики повинні бути ідентифіковані на всіх етапах життєвого циклу проєкту. Ідентифікація ризиків включає систематичний аналіз внутрішніх і зовнішніх факторів, які можуть вплинути на реалізацію проєкту. Для IT-проєктів важливим є врахування таких специфічних ризиків:

- Затримки через залежність від сторонніх постачальників або інтеграцію з іншими системами.

- Непередбачені технічні проблеми через недостатню тестову базу.

- Зміни у вимогах замовника на пізніх етапах розробки.

Таким чином, застосування сучасних методик ідентифікації та оцінки ризиків у проєктному менеджменті забезпечує виявлення ключових загроз, їхній аналіз та розробку превентивних заходів, які дозволяють мінімізувати негативний вплив ризикових подій на результати проєкту. У контексті IT та АСУ, ризики можуть бути пов'язані як з технічними аспектами (збої в програмному забезпеченні, апаратурі), так і з організаційними питаннями (порушення термінів, недостатня кваліфікація персоналу).

Ідентифікація ризиків є ключовим етапом управління ризиками, що дозволяє визначити потенційні небезпеки та можливості, які можуть вплинути на реалізацію проєкту. Для цього застосовуються різноманітні методи, що відрізняються за підходами, інструментами і рівнем деталізації. Нижче наведено основні методи ідентифікації ризиків, які використовуються в управлінні проєктами:

Таблиця 1.2.

Методи ідентифікації ризиків

№	Назва методу	Опис методу
1	Імітаційне моделювання за методом Монте-Карло (Monte Carlo Simulation)	Використовує статистичне моделювання для оцінки впливу варіацій вхідних даних на результати системи.
2	Дерево рішень (Decision Tree)	Дозволяє вибрати оптимальний варіант дій у невизначених умовах через візуалізацію варіантів у формі деревоподібної діаграми.
3	Матриця "наслідок/ймовірність" (Consequence/Probability Matrix)	Інтегрує кількісні та якісні оцінки наслідків і ймовірностей для ранжування ризиків.
4	Аналіз видів і наслідків відмов (FMEA)	Дозволяє виявити потенційні відмови системи та оцінити їх вплив на результати проєкту.
5	Аналіз впливу на діяльність (Business Impact Analysis, BIA)	Визначає критичність бізнес-процесів та оцінює час, необхідний для їх відновлення у разі порушень.
6	Метод Делфі (Delphi method)	Залучає групу експертів для досягнення консенсусу у визначенні ризиків, оцінки їх ймовірності та наслідків.
7	Аналіз сценаріїв (Scenario Analysis)	Передбачає розробку ймовірних сценаріїв розвитку подій, аналізуючи їх вплив на проєкт.
8	Мозковий штурм (Brainstorming)	Креативний метод, який передбачає обговорення з командою проєкту для генерації ідей щодо можливих ризиків.
9	Аналіз першопричин (Root Cause Analysis)	Визначає основні причини проблем для уникнення подібних ситуацій у майбутньому.

Продовження таблиці 2.1.

10	Переліки контрольних запитань (Checklist)	Використовує структуровані списки типових ризиків, що допомагає виявити можливі загрози на основі минулого досвіду.
11	Попередній аналіз небезпечних чинників (PHA)	Орієнтований на визначення потенційно небезпечних чинників, які можуть спричинити негативні події у технічних системах або процесах.
12	Дослідження небезпечних чинників і працездатності (HAZOP)	Аналізує відхилення від нормальної діяльності системи, визначає критичність цих відхилень і пропонує заходи для їх мінімізації.
13	Структурований метод "Що якщо" (SWIFT)	Використовується для стимуляції експертної групи до ідентифікації ризиків, задаючи питання "Що якщо станеться...?".
14	Аналіз небезпечних чинників і критичних точок контролю (HACCP)	Систематичний підхід, який спрямований на моніторинг та забезпечення безпеки шляхом аналізу критичних точок у процесах.
15	Аналіз дерева відмов (Fault Tree Analysis)	Визначає всі можливі причини небажаних подій, починаючи з кінцевої небажаної події.
16	Аналіз причин і наслідків (Cause and Consequence Analysis)	Поєднує дерево відмов і дерево подій для врахування часових затримок.
17	Аналіз причино-наслідкових зв’язків (Cause-and-effect Analysis)	Забезпечує класифікацію чинників ризику за категоріями для детального аналізу.
18	Технічне обслуговування, орієнтоване на забезпечення безвідмовності (RCM)	Ідентифікує політики для управління відмовами, забезпечуючи необхідний рівень надійності.
19	Аналіз витрат і вигід (Cost/Benefit Analysis)	Оцінює співвідношення витрат і вигід для вибору найбільш економічно доцільного рішення.
20	Багатокритеріальний аналіз рішень (MCDA)	Використовує множину критеріїв для оцінки варіантів і обрання найкращого рішення.

Кожен із перелічених методів має свої переваги та обмеження, які визначають доцільність їх застосування залежно від специфіки проєкту. Наприклад, мозковий штурм ефективний на ранніх етапах проєкту; метод Дельфі доцільний для складних технічних проєктів; аналіз дерева відмов підходить для систем з високими вимогами до безпеки.

Застосування відповідних методів дозволяє не лише виявити ризики, але й підготувати ефективні стратегії для їх мінімізації.

Класифікація проєктних ризиків є важливим інструментом для їх систематизації та ефективного управління. Правильна класифікація дозволяє визначити природу ризиків, їх джерела, наслідки та потенційні шляхи мінімізації. Сучасна наукова література пропонує численні підходи до класифікації ризиків залежно від різних критеріїв.

Згідно з дослідженнями Гавриш О.А. та Мельникової В.А. [10], ризики класифікуються за такими критеріями:

- Ймовірність настання — визначає, наскільки часто ризик може виникати.
- Фактори — основні причини, що призводять до ризику.
- Фази реалізації проєкту — поділ на етапи, на яких виникають ризики.
- Розмір можливих наслідків — ступінь впливу ризику на проєкт.
- Ступінь ризику — співвідношення ймовірності та тяжкості впливу ризику.

Петренко О.Н. [15] пропонує більш деталізований підхід до класифікації ризиків, зокрема:

1. За фазами (етапами) проєктної діяльності:
    - Ризики доінвестиційної фази.
    - Ризики інвестиційної фази.
    - Ризики експлуатаційної (виробничої) фази.
2. За можливістю впливу на виникнення ризиків:
    - Внутрішні (ендогенні) — ті, що виникають у межах організації.
    - Зовнішні (екзогенні) — ті, що обумовлені зовнішніми факторами.
3. За можливістю захисту від ризиків:
    - Ризики, які страхуються.
    - Ризики, які не страхуються.
4. За динамікою:
    - Динамічні — змінюються у процесі реалізації проєкту.

- Статичні — залишаються постійними.

5. Специфічні ризики — пов’язані із конкретними особливостями проєкту.

Об’єднання підходів дозволяє сформувати універсальну класифікацію:

1. За ймовірністю виникнення:
   - Часті.
   - Рідкісні.
2. За походженням:
   - Внутрішні (ендогенні).
   - Зовнішні (екзогенні).
3. За етапами реалізації проєкту:
   - Підготовчий етап.
   - Етап розробки.
   - Етап впровадження.
   - Етап експлуатації.
4. За характером наслідків:
   - Негативні (збитки, втрати).
   - Позитивні (додаткові можливості).
5. За можливістю страхування:
   - Страховані.
   - Нестраховані.
6. За тяжкістю наслідків:
   - Мінімальні.
   - Критичні.
   - Катастрофічні.

Класифікація проєктних ризиків є ключовим етапом управління ними, адже дозволяє систематизувати інформацію та визначити підходи до їх мінімізації.

Різноманітність класифікацій свідчить про багатогранність ризиків і потребу в їхньому адаптованому аналізі залежно від специфіки проєкту.

За підходом, запропонованим Бутко М.П. [20] ця класифікація базується на джерелах виникнення ризиків і враховує їхній потенційний вплив на проєкт. Подібний підхід також використовується Інститутом управління проєктами (PMI), який пропонує дворівневу класифікацію ризиків залежно від джерела їх походження.

Основні категорії ризиків за PMI [21]:

1. Технічні ризики:
    - Ризики, пов’язані зі змістом робіт.
    - Ризики визначення вимог до результатів діяльності.
    - Ризики правильної оцінки завдань та суб’єктивних суджень.
    - Ризики технічних процесів.
    - Технологічні ризики.
2. Управлінські ризики:
    - Ризики, пов’язані з управлінням проєктом.
    - Ризики портфоліо або програмного менеджменту.
    - Операційні ризики.
    - Організаційні ризики.
    - Ресурсні ризики та інші.
3. Комерційні ризики:
    - Ризики контрактних умов і термінів.
    - Закупівельні ризики.
    - Ризики, пов’язані зі співпрацею з постачальниками та підрядниками.
    - Ризики, що виникають у процесі взаємодії з клієнтами.
4. Зовнішні ризики:
    - Ризики, пов’язані зі зміною законодавства.

- Валютні (курсові) ризики.

- Погодні ризики та інші.

Обидві класифікації, запропоновані Бутко М.П. та PMI, є релевантними та відображають основні джерела ризиків у проєктній діяльності. Вони охоплюють широкий спектр ризиків і дозволяють систематизувати їх залежно від конкретних об’єктів класифікації. Особливістю класифікації PMI є більш детальний поділ ризиків за типами та рівнями, що дозволяє краще враховувати їх у процесі управління проєктами.

Згідно з останніми дослідженнями, проведеними серед українських IT-компаній, проєкти з розробки програмного забезпечення включають понад 130 окремих ризиків. Така різноманітність вимагає ефективного підходу до їх класифікації, що дозволяє визначити основні джерела ризиків,оцінити їхній потенційний вплив на проєкт та розробити превентивні заходи для мінімізації ризиків.

Таким чином, коректна класифікація ризиків є основою для ефективного управління ризиками та успішної реалізації проєктів.

Аналізуючи праці провідних науковців у сфері управління ризиками, була запропонована класифікація основних ризиків, притаманних IT-проєктам. Цей підхід дозволяє врахувати різноманітні аспекти реалізації проєктів у галузі інформаційних технологій.

1. Технологічні ризики:

- Використання неперевірених технологій.

- Можливі технічні збої.

- Проблеми сумісності.

- Вразливість систем безпеки.

- Простій системи.

- Втрата даних.

2. Ризики недотримання плану-графіку реалізації:

- Розширення охоплення проєкту без відповідних ресурсів (scope creep).
- Нереалістичні терміни виконання.
- Некоректна оцінка завдань.
- Обмеження ресурсів у часі.
- Непередбачені затримки.

3. Фінансові ризики:

- Перевитрати бюджету.
- Неочікувані витрати.
- Неякісне фінансове управління.

4. Комунікаційні ризики

- Низька якість внутрішньої комунікації в команді.
- Недостатня комунікація зі стейкхолдерами.
- Неоднозначність або неповнота у формулюванні вимог.
- Відсутність або низька якість зворотного зв'язку.

5. Ризики якості продукту:

- Отримання результату низької якості.
- Наявність дефектів у програмному забезпеченні.
- Неналежне тестування.

6. Ризики людських ресурсів:

- Недостатня кваліфікація членів команди.
- Висока плинність кадрів.
- Конфлікти всередині команди.
- Вигорання працівників.

7. Кон’юнктурні ризики:

- Економічна криза на глобальному або національному рівні.

- Криза в галузі, до якої належить продукт.

- Фінансові труднощі компанії-замовника.

8. Регуляторні ризики:

- Зміни у законодавстві.

- Посилення регуляторних вимог у галузі.

- Міжнародні регуляторні обмеження.

- Недотримання регуляторних вимог.

- Впровадження нових, непередбачуваних обмежень.

Запропонована класифікація охоплює ключові ризики, з якими може стикатися команда ІТ та АСУ-проєкту, і враховує всі основні аспекти реалізації проєктів:

- Технологічні складнощі, що впливають на функціональність і безпеку системи.

- Управлінські обмеження, які можуть вплинути на терміни, бюджет і якість.

- Комунікаційні проблеми, що виникають через недостатнє узгодження дій між учасниками проєкту.

- Ризики зовнішнього середовища, включаючи економічну та регуляторну нестабільність.

Ця класифікація надає команді ІТ-проєкту інструмент для комплексного аналізу ризиків, дозволяючи виявити слабкі місця на кожному етапі розробки продукту. Вона може стати основою для розробки заходів з мінімізації ризиків та оптимізації управління.

Запропонована структура враховує сучасні виклики галузі та може використовуватися як основа для подальших наукових і практичних досліджень у сфері управління проєктними ризиками.

Розглянемо види ризиків у контексті ІТ та АСУ:

Технічні ризики:

- Збої в програмному забезпеченні: програмні помилки, баги, конфлікти між компонентами системи.
- Апаратні ризики: вихід з ладу серверів, мережевого обладнання, відмови систем охолодження або електроживлення.
- Нестача сумісності: проблеми при інтеграції нових компонентів із існуючими системами.
- Недостатня масштабованість: системи можуть не впоратися зі збільшенням навантаження або обсягу даних.

Кіберризики та інформаційна безпека:

- Кіберзагрози: атаки зловмисників, віруси, шкідливе ПЗ, DDoS-атаки, фішинг.
- Загрози витоку даних: несанкціонований доступ до конфіденційної інформації, що може призвести до витоку персональних даних, фінансових даних або комерційної таємниці.
- Вразливості в системах: використання вразливостей у ПЗ та мережевих протоколах для доступу до системи.

Організаційні ризики:

- Нестача кваліфікованих кадрів: відсутність компетентного персоналу може призвести до низької якості розробки та підтримки IT-рішень.
- Затримки у виконанні проєктів: недостатня оцінка ресурсів і термінів може призвести до перевищення бюджету та затримок у впровадженні систем.
- Проблеми комунікації: погана координація між різними підрозділами може призвести до невиконання проєктних завдань.

Фінансові ризики:

- Перевищення бюджету: недостатня оцінка витрат на проєкт.

- Недофінансування: проєкти можуть бути зупинені через нестачу фінансування або скорочення бюджету.
- Клієнтські (зміни у вимогах клієнтів або їх втрата).

Ефективна ідентифікація ризиків є запорукою успішного управління проєктами в ІТ та АСУ. Використання різних методів і підходів дозволяє виявляти загрози на ранніх етапах, що допомагає мінімізувати негативні наслідки та підвищити ймовірність успіху проєкту. Це особливо важливо в умовах динамічного розвитку технологій та збільшення кількості кіберзагроз.

1.3. Аналіз підходів до оцінки ймовірності та впливу ризиків на успішність проєктів

Оцінка ймовірності та впливу ризиків є одним із ключових етапів у процесі управління ризиками для ІТ-проєктів та автоматизованих систем управління (АСУ). Цей етап дозволяє не лише визначити потенційні загрози для проєкту, але й зрозуміти, наскільки ймовірно, що ці ризики реалізуються, а також оцінити можливий вплив на проєкт у разі їх виникнення. Результати цієї оцінки допомагають прийняти обґрунтовані рішення про те, на які ризики варто спрямувати ресурси для їхнього усунення або пом'якшення.

У сучасних умовах проєкти у сфері ІТ та АСУ стикаються з численними ризиками, що можуть вплинути на успішність їх виконання. Це можуть бути як технічні загрози (помилки у програмному забезпеченні, збої обладнання), так і організаційні ризики (порушення термінів, брак фінансування).

Оцінка ймовірності та впливу ризиків дозволяє:

- Визначити пріоритети для управління ризиками, тобто зрозуміти, на які загрози слід звертати першочергову увагу.

- Скласти плани реагування для запобігання або пом'якшення негативних наслідків ризиків.
- Підвищити прогнозованість результатів проєкту, мінімізуючи ймовірність його провалу через неочікувані події.

Існує кілька методів для оцінки ймовірності та впливу ризиків, які можуть бути використані в залежності від складності проєкту, доступних ресурсів та необхідної точності:

1. Якісний аналіз ризиків передбачає суб’єктивну оцінку ризиків за допомогою експертних думок та кваліфікаційних методів. Цей підхід використовується для початкового аналізу, коли необхідно швидко виявити та класифікувати ризики.

- Методологія: ризики оцінюються за шкалою (наприклад, низька, середня, висока ймовірність; незначний, помірний, значний вплив).
- Переваги: швидкий аналіз, який не потребує значних витрат часу і ресурсів.
- Недоліки: оцінки можуть бути суб’єктивними, що призводить до можливих упереджень.
- Приклад застосування: матриця ймовірності та впливу, яка дозволяє визначити, які ризики мають високий пріоритет для подальшого управління.

2. Кількісний аналіз ризиків

Кількісний аналіз ґрунтується на використанні математичних та статистичних методів для отримання числових значень ймовірності та впливу ризиків. Цей підхід дозволяє оцінити ризики точніше і глибше.

- Методи: використання статистичних моделей, таких як метод Монте-Карло, аналіз дерева рішень, розрахунок очікуваної грошової вартості (Expected Monetary Value, EMV).
- Переваги: висока точність, можливість прогнозувати фінансові втрати або затримки.

- Недоліки: потребує значних обчислювальних ресурсів і наявності історичних даних для побудови моделей.
- Приклад застосування: метод Монте-Карло часто використовується для моделювання сценаріїв у великих проєктах, де важливо враховувати різні варіанти розвитку подій та їх ймовірність.

До методів оцінки ймовірності та впливу ризиків належать:

1. Матриця ймовірності та впливу

Це один із найпопулярніших інструментів для оцінки ризиків, який дозволяє візуально представити ризики на основі їх ймовірності та впливу. Матриця має дві осі: вісь ймовірності (від низької до високої) та вісь впливу (від незначного до критичного).

- Процедура: кожен ризик оцінюється за двома критеріями — ймовірністю виникнення та потенційним впливом на проєкт. На основі оцінок ризики розподіляються по квадрантах матриці.
- Переваги: проста у використанні, дозволяє швидко ідентифікувати пріоритети.
- Недоліки: суб'єктивність оцінок може призвести до неточних результатів.

2. Метод Монте-Карло

Метод Монте-Карло використовує статистичне моделювання для оцінки ймовірностей різних сценаріїв. Він базується на багатократних симуляціях випадкових значень, що дозволяє оцінити можливі варіанти розвитку подій.

- Процес: проводиться симуляція великої кількості можливих результатів на основі заданих параметрів і розподілів.
- Результат: отримання ймовірнісного розподілу для ключових показників, таких як час завершення проєкту або загальна вартість.
- Переваги: дозволяє враховувати невизначеність і варіативність даних, що підвищує точність прогнозів.

- Недоліки: потребує значних обчислювальних ресурсів та наявності детальних даних для проведення моделювання.

3. Аналіз дерева рішень

Цей метод дозволяє візуалізувати рішення та їх можливі наслідки у вигляді дерева, де кожна гілка представляє можливий сценарій розвитку подій. Використовується він для аналізу складних рішень і вибору оптимальних стратегій реагування на ризики.

- Процедура: будується дерево можливих рішень, де кожна гілка представляє можливий сценарій розвитку подій. На кожному етапі оцінюється ймовірність та потенційний вплив на проєкт.
- Переваги: дає змогу оцінити ймовірні наслідки різних дій та обрати оптимальний варіант.
- Недоліки: може бути складним для великих проєктів з багатьма варіантами розвитку подій.

У сфері ІТ та АСУ проєктів важливо швидко та точно оцінити потенційні ризики, щоб вчасно вжити заходів для їх запобігання. Використання сучасних програмних інструментів, таких як RiskyProject або Primavera, дозволяє автоматизувати процес аналізу та оптимізувати управління ризиками.

- Програмні рішення надають можливість швидко адаптувати плани проєкту у разі зміни оцінок ризиків.
- Використання автоматизованих систем для моніторингу ризиків дозволяє оперативно реагувати на потенційні загрози.

Отже, оцінка ймовірності та впливу ризиків є критично важливою для успішного управління проєктами у сфері ІТ та АСУ. Поєднання якісних та кількісних методів оцінки, таких як матриця ймовірності та впливу, метод Монте-Карло та аналіз дерева рішень, дозволяє не лише оцінити можливі загрози, але й розробити ефективні

стратегії їх усунення. Це підвищує надійність проєктів, мінімізує ризики зриву та сприяє досягненню поставлених цілей.

РОЗДІЛ 2.
РОЗРОБКА МОДЕЛІ УПРАВЛІННЯ РИЗИКАМИ В ІТ ТА АСУ ПРОЄКТАХ

2.1. Створення інтегрованої системи управління ризиками для ІТ та АСУ проєктів

Розробка інтегрованої системи управління ризиками (ІСУР) для ІТ-проєктів і автоматизованих систем управління (АСУ) є життєво важливою для досягнення успіху в сучасному бізнес-середовищі, де зростають вимоги до безпеки, надійності та ефективності проєктів. Сьогодні проєкти у сфері ІТ та АСУ стикаються з численними ризиками, які можуть суттєво вплинути на їх виконання та кінцеві результати. Інтегрована система дозволяє не тільки виявити потенційні загрози, але й оперативно та ефективно реагувати на них, що значно підвищує шанси на успішне завершення проєкту.

Управління ризиками у сфері ІТ та АСУ включає комплекс заходів, спрямованих на ідентифікацію, аналіз, оцінку та мінімізацію ризиків, які можуть вплинути на проєкт або бізнес-процеси. Традиційні методи управління ризиками часто є недостатньо гнучкими для адаптації до динамічних умов сучасних ІТ-систем. Тому інтеграція ризик-менеджменту в єдину систему дозволяє покращити координацію, підвищити ефективність рішень та забезпечити надійний захист проєктів від несподіваних загроз.

Основними завданнями інтегрованої системи управління ризиками (ІСУР), уніфікованої платформи, яка об'єднує різні процеси та інструменти управління ризиками для оптимізації управління ІТ-проєктами та автоматизованими системами управління, є:

- Систематизація та централізоване управління ризиками на всіх етапах життєвого циклу проєкту.
- Виявлення та швидке реагування на загрози, що дозволяє уникнути непередбачуваних збоїв.
- Зменшення фінансових втрат шляхом оптимізації витрат на управління ризиками.
- Забезпечення відповідності міжнародним стандартам, таким як ISO 31000, PMBOK та COBIT.

Інтегрована система управління ризиками — це комплексний підхід, що дозволяє ефективно об’єднати виявлення, оцінку, моніторинг та реагування на ризики в рамках одного інформаційного середовища. Це особливо важливо для ІТ та АСУ проєктів, де високий ступінь взаємозалежності між компонентами системи створює комплексні ризики, які можуть мати масштабний вплив.

Основні принципи, на яких базується інтегрована система управління ризиками:

1. Системний підхід - об'єднання всіх процесів управління ризиками у межах єдиної платформи для досягнення узгодженості дій.

2. Проактивність - попередження ризиків ще до того, як вони почнуть негативно впливати на проєкт.

3. Прозорість забезпечення доступу до актуальної інформації про стан ризиків у режимі реального часу.

4. Адаптивність можливість швидко реагувати на зміни у зовнішньому та внутрішньому середовищі.

Перший крок у розробці ІСУР полягає у виявленні потенційних ризиків для ІТ та АСУ проєктів. Цей етап включає:

- Технічні ризики: проблеми з програмним забезпеченням, апаратними компонентами, мережами.
- Кіберзагрози: несанкціонований доступ, шкідливе ПЗ, витоки даних.
- Організаційні ризики: затримки через погану комунікацію, недостатня кваліфікація персоналу.
- Регуляторні ризики: дотримання законодавчих вимог щодо захисту даних.

Після ідентифікації ризиків необхідно оцінити ймовірність їх реалізації та можливий вплив на проєкт. Для цього використовуються:

- Якісний аналіз (SWOT, метод Делфі) для початкової оцінки ризиків.
- Кількісний аналіз (Метод Монте-Карло, аналіз дерева рішень) для детального прогнозування.

На основі результатів оцінки розробляються стратегії управління ризиками:

- Ухилення - уникнення ризиків шляхом зміни планів проєкту.
- Зниження - впровадження додаткових заходів для зменшення ймовірності ризику.
- Передача - використання аутсорсингу або страхування для мінімізації впливу.
- Прийняття - визнання ризику та підготовка до можливих наслідків.

ІСУР включає модулі для моніторингу ризиків у реальному часі та аналізу ефективності впроваджених стратегій:

- Системи сповіщень для швидкого реагування на зміни в ризиковому середовищі.
- Аналітика та звіти для оцінки ефективності управління ризиками.

ІСУР може бути посилена штучним інтелектом та машинним навчанням. Це дозволяє виконувити ряд додаткових функцій системі.

Щодо переваг, які отриумуються після впровадження інтегрованої системи управління ризиками у ІТ та АСУ проєктах, то можемо віднести:

- Зменшення затримки та перевищення бюджету за рахунок проактивного управління.
- Підвищення якості виконання проєктів завдяки злагодженій роботі команди.
- Забезпечення відповідність міжнародним стандартам і регуляторним вимогам.

Існує ряд рекомендацій щодо впровадження інтегрованої системи управління ризиками, зокрема:

1. Провести аудит наявних процесів управління ризиками перед впровадженням ІСУР.

2. Використовувати сучасні інструменти аналітики для моніторингу ризиків.

3. Регулярно проводити тренінги для персоналу, щоб підвищити обізнаність у сфері ризик-менеджменту.

4. Забезпечити постійну підтримку та оновлення системи для адаптації до нових загроз.

Створення інтегрованої системи управління ризиками для ІТ та АСУ проєктів є необхідним кроком для підвищення стійкості та ефективності проєктів. Завдяки поєднанню сучасних методів аналізу ризиків, автоматизації процесів та використання аналітики, ІСУР забезпечує комплексний підхід до управління ризиками, що дозволяє знизити вплив негативних факторів на проєкт та досягти поставлених цілей.

Розглянемо алгоритм розробки інтегрованої системи управління ризиками для веб-студії.

Інтегрована система управління ризиками (ІСУР) для веб-студії має базуватися на автоматизації, проактивному моніторингу та адаптивному реагуванні на ризики. Алгоритм системи подано нижче.

Початкова фаза: Ініціалізація

1. Визначення цілей управління ризиками:

- Забезпечення мінімізації негативного впливу ризиків на строки, бюджет та якість проєктів.

- Підвищення передбачуваності результатів проєктів.

2. Формування команди управління ризиками:

- Призначення відповідальних осіб (керівник проєкту, менеджер ризиків, технічний аналітик).

3. Розробка політики управління ризиками:

- Документ, який визначає основні принципи, критерії оцінки ризиків та підходи до їхньої мінімізації.

4. Вибір інструментів:

- Jira для управління завданнями та ризиками.

- RiskyProject для моделювання ризиків.

- Power BI для візуалізації й аналізу даних.

Етап ідентифікації ризиків

1. Збір інформації:

- Методи: SWOT-аналіз, інтерв’ю з командою, аналіз історичних даних.

- Джерела: технічне завдання (ТЗ), проєктна документація, специфікації API.

2. Формування реєстру ризиків:

- Включення кожного ризику до реєстру з наступними параметрами:

  - Опис ризику.

  - Джерело виникнення (технічний, клієнтський, організаційний).

  - Ймовірність реалізації.

  - Потенційний вплив (строки, бюджет, якість).

3. Класифікація ризиків:

- Визначення пріоритетності ризиків за допомогою матриці ймовірності та впливу.

Етап оцінки ризиків

1. Якісна оцінка:

- Оцінка кожного ризику за шкалою (високий, середній, низький).

- Визначення критичних ризиків.

2. Кількісна оцінка:

- Використання методу Монте-Карло для прогнозування впливу ризиків на строки та бюджет.

- Розрахунок очікуваної грошової вартості (EMV) ризиків.

3. Результати оцінки:

- Створення звіту про ризики з графічним представленням (дашборд у Power BI).

Розробка стратегій реагування

1. Розробка заходів для кожного ризику:

- Ухилення ризику: виключення певних дій, що можуть призвести до ризику.

- Зниження ризику: впровадження профілактичних заходів (наприклад, тестування).

- Передача ризику: делегування частини відповідальності через страхування або аутсорсинг.

- Прийняття ризику: погодження з можливими наслідками та підготовка резервів.

2. Інтеграція заходів у план проєкту:

- Включення завдань для мінімізації ризиків у Jira.

- Планування додаткових ресурсів та часу у графіках проєкту.

Моніторинг ризиків

1. Регулярний перегляд реєстру ризиків:

- Щотижневі зустрічі команди для оновлення статусу ризиків.

2. Використання автоматизації:

- Моніторинг завдань, пов’язаних із ризиками, у Jira.

- Генерація інтерактивних звітів про статус ризиків у Power BI.

3. Оновлення стратегій:

- Коригування плану управління ризиками відповідно до змін у проєкті.

Оцінка ефективності

1. Ключові метрики ефективності:

- Відсоток реалізованих ризиків.

- Відхилення від строків (у днях).

- Перевищення бюджету (у %).

- Рівень задоволеності клієнта (за шкалою опитування).

2. Порівняння результатів:

- Аналіз результатів виконання проєкту з використанням моделі управління ризиками.

- Порівняння із попередніми проєктами, де управління ризиками не застосовувалося системно.

Даний алгоритм дозволяє здійснювати управління ситуаціями, які виникають при реалізації проєкту. Подивимося як це працює:

1.Ідентифікація ризику:

- Затримка затвердження дизайну клієнтом.

- Ймовірність: 70%, вплив: високий.

2. Оцінка ризику:

- Потенційна затримка: +7 днів.

- Додаткові витрати: $500.

3. Реагування:

- Запланувати буфер у графіку на 7 днів.

- Включити регулярні зустрічі з клієнтом для прискорення затвердження.

4. Моніторинг:

- Оновлення статусу ризику у Jira.

- Контроль впливу на графік через Power BI.

5. Результат:

- Затримка дизайну склала 3 дні, вплив на строки було мінімізовано.

Реалізація інтегрованої системи надає ряд переваг для успішного впровадження проєкту, зокрема:

- ✔ Прозорість через залучення всіх членів команди та клієнта до процесу управління ризиками.
- ✔ Автоматизацію через використання інструментів, таких як Jira, RiskyProject, Power BI, для підвищення ефективності.
- ✔ Гнучкість як адаптація системи до змін у реальному часі.
- ✔ Економія ресурсів через мінімізація витрат і затримок завдяки проактивному реагуванню.

Ця інтегрована система управління ризиками забезпечує стабільність та передбачуваність реалізації проєктів веб-студії, що дозволяє мінімізувати втрати та підвищити рівень задоволеності клієнтів.

2.2. Методика інтеграції управління ризиками у процес розробки IT та АСУ систем

Розробка IT-систем та автоматизованих систем управління (АСУ) у сучасному світі супроводжується високим рівнем невизначеності та складності. Наявність

технічних, організаційних, фінансових та інших ризиків може негативно вплинути на успішність виконання проєктів. Для забезпечення стабільного розвитку та ефективності таких проєктів необхідно впроваджувати інтегровану систему управління ризиками.

Як стверджував Пітер Друкер, відомий теоретик менеджменту: "Ризик є побічним продуктом кожного рішення. Його необхідно не уникати, а управляти ним".

Цей підхід лежить в основі сучасних методик управління ризиками, що спрямовані на проактивний контроль ризиків і інтеграцію відповідних процесів у всі етапи життєвого циклу проєкту.

Інтеграція управління ризиками у процес розробки дозволяє забезпечити безперервний моніторинг ризиків, своєчасну оцінку їх впливу та оперативне прийняття рішень щодо їх мінімізації. Цей підхід базується на міжнародних стандартах, таких як ISO 31000:2022, PMBOK та інших.

Метою інтеграції є забезпечити ефективне виявлення, аналіз, оцінку та управління ризиками на всіх етапах розробки IT та АСУ систем. Для досягнення мети ставляться наступні завдання:

- Ідентифікувати всі потенційні ризики, які можуть вплинути на реалізацію проєкту.
- Оцінити ймовірність виникнення та потенційний вплив ризиків.
- Розробити стратегії для мінімізації негативного впливу ризиків.
- Забезпечити прозорість управління ризиками для всіх зацікавлених сторін.
- Інтегрувати управління ризиками в загальну систему управління проєктом.

Інтеграція управління ризиками базується на системному підході, де управління ризиками інтегрується у всі аспекти проєкту. Як зазначав Генрі Мінцберг, відомий дослідник у сфері стратегічного менеджменту: "Справжній

менеджмент полягає не лише у плануванні, а й у здатності адаптуватися до змін". Це твердження підкреслює важливість гнучкості в інтегрованій системі управління ризиками, що враховує як внутрішні, так і зовнішні чинники впливу.

До ключових принципів методики можна віднести:

- ✔ Системність: управління ризиками охоплює всі етапи проєкту — від планування до завершення.
- ✔ Проактивність: виявлення потенційних загроз до їх реалізації.
- ✔ Прозорість: доступність інформації для всіх зацікавлених сторін.
- ✔ Гнучкість: адаптація процесів до змін у проєкті.
- ✔ Автоматизація: використання сучасних інструментів моніторингу ризиків.

Процес інтеграції управління ризиками охоплює кілька ключових етапів, кожен із яких спрямований на забезпечення системного та проактивного підходу до мінімізації ризиків.

1. Планування управління ризиками

На етапі планування розробляється стратегія управління ризиками, яка включає:

- Визначення цілей управління ризиками.
- Призначення відповідальних осіб за управління ризиками.
- Вибір методів і інструментів для аналізу ризиків.
- Розробку плану дій у разі виникнення ризиків.

Результатом цього етапу є створення документу "План управління ризиками", який стане базовим керівництвом для всіх учасників проєкту.

2. Ідентифікація ризиків

Ідентифікація ризиків передбачає систематичний процес виявлення потенційних загроз. Використовуються такі методи:

- Мозковий штурм: залучення команди для обговорення можливих ризиків.
- Аналіз історичних даних: використання досвіду попередніх проєктів.
- SWOT-аналіз: виявлення сильних і слабких сторін проєкту, можливостей і загроз.
- Інтерв’ю з експертами: консультації з досвідченими фахівцями галузі.

Результатом такого етапу є створення реєстру ризиків із зазначенням їх характеристик (джерело ризику, тип, ймовірність, наслідки).

3. Оцінка ризиків

На етапі оцінки ризиків проводиться їх класифікація за рівнем впливу та ймовірністю виникнення. Використовуються такі методи:

- Матриця ймовірності та впливу: оцінка ризиків за шкалами від "низького" до "високого".
- Метод Монте-Карло: моделювання сценаріїв для прогнозування ймовірності виникнення ризиків.
- Очікувана грошова вартість (EMV): оцінка фінансового впливу ризиків.

Результатом такого етапу є пріоритетний список ризиків для розробки стратегій реагування.

4. Розробка стратегій управління ризиками

На основі результатів оцінки розробляються стратегії реагування:

- Ухилення ризику: виключення можливості його виникнення.
- Зниження ризику: зменшення ймовірності або впливу ризику.
- Передача ризику: делегування відповідальності через страхування або аутсорсинг.
- Прийняття ризику: погодження на можливі наслідки з підготовкою резервних заходів.

Результатом такого процесу є стратегічний план реагування на ризики.

5. Моніторинг і контроль ризиків

Моніторинг ризиків здійснюється протягом усього життєвого циклу проєкту. Основні заходи:

- Регулярний перегляд реєстру ризиків.
- Відстеження ефективності впроваджених стратегій.
- Використання автоматизованих інструментів для моніторингу ризиків, таких як Jira, RiskyProject.

Результатом такого процесу є актуалізований список ризиків і звіти про їх стан.

Для ефективного впровадження управління ризиками використовуються сучасні програмні рішення:

1. **RiskyProject**: для моделювання ризиків і їхнього впливу на графіки проєкту.

RiskyProject — це спеціалізоване програмне забезпечення для управління ризиками в проєктах, яке дозволяє моделювати ризики, аналізувати їхній вплив на графіки, витрати та кінцевий результат. Програма інтегрується з популярними інструментами управління проєктами, такими як Microsoft Project, Primavera та інші.

Функціонал RiskyProject:

1. Моделювання ризиків:
    - Використовує метод Монте-Карло для симуляції можливих сценаріїв розвитку подій у проєкті.
    - Прогнозує вплив ризиків на графіки та бюджети проєктів.
2. Оцінка ризиків:
    - Автоматично визначає ймовірність виникнення ризиків та їх вплив на проєкт.
    - Підтримує матриці ймовірності та впливу.
3. Розробка стратегій управління ризиками:
    - Дозволяє створювати стратегії для зниження або ухилення від ризиків.

4. Моніторинг і звітність:
    - Генерує докладні звіти про стан ризиків у реальному часі.
    - Підтримує візуалізацію даних у вигляді графіків і діаграм.

Переваги використання:

- Простота інтеграції з іншими інструментами управління проєктами.
- Потужний функціонал для аналізу й оцінки ризиків.
- Підходить для великих і складних проєктів з багатьма залежностями.

Застосування:

RiskyProject найчастіше використовується в інженерних, будівельних, IT-проєктах та розробці складних автоматизованих систем, де критично важливий детальний аналіз ризиків.

2. **Microsoft Project:** для моніторингу завдань і ризиків у проєкті.

Microsoft Project — це широко використовуване програмне забезпечення для управління проєктами, яке забезпечує гнучкість і прозорість у плануванні, моніторингу та оцінці ризиків. Інструмент підходить для комплексного управління проєктами різного масштабу.

Функціонал Microsoft Project для управління ризиками:

1. Планування ризиків:
    - Дозволяє створювати спеціальні завдання або етапи для управління ризиками.
    - Інтеграція з календарями для врахування ризиків у графіку.
2. Моніторинг ризиків:
    - Відстеження змін у планах проєкту, викликаних виникненням ризиків.
    - Функції прогнозування для оцінки впливу ризиків на загальний план.
3. Аналітика ризиків:

- Візуалізація ризиків за допомогою діаграм Ганта, таблиць завдань і графіків.
- Можливість оцінювати ризики у фінансовому контексті.

4. Управління змінами:
    - Легке внесення змін до плану проєкту у відповідь на реалізацію ризиків.

Переваги використання:

- Зручний інтерфейс і легка інтеграція з іншими продуктами Microsoft.
- Сумісність із системами управління ризиками, такими як RiskyProject.
- Широкий функціонал для аналізу впливу ризиків на графіки проєкту.

Застосування:

Microsoft Project активно використовується в IT, інфраструктурних, маркетингових і наукових проєктах, де потрібно одночасно управляти ресурсами, графіками та ризиками.

3. **Power BI:** для створення інтерактивних дашбордів та аналізу даних у реальному часі.

Power BI — це потужний інструмент для аналітики та візуалізації даних, що дозволяє створювати інтерактивні дашборди та звіти, які допомагають відстежувати ризики у реальному часі. Завдяки інтеграції з різними системами управління проєктами Power BI дозволяє об'єднувати дані з різних джерел для глибшого аналізу.

Функціонал Power BI для управління ризиками:

1. Інтерактивні дашборди:
    - Створення візуалізацій, які дозволяють аналізувати стан ризиків у реальному часі.
    - Відображення основних показників ризиків: ймовірності, впливу, стану реагування.
2. Аналіз великих обсягів даних:

- Об'єднання інформації про ризики з різних джерел, включаючи CRM, ERP, системи управління проєктами.
- Виявлення тенденцій і закономірностей у даних.

3. Моніторинг у реальному часі:
   - Автоматичне оновлення даних із підключених систем.
   - Можливість встановлення тригерів для сповіщення про критичні ризики.
4. Звіти та прогнози:
   - Генерація автоматичних звітів для керівників проєктів і зацікавлених сторін.
   - Моделювання сценаріїв для оцінки можливого впливу ризиків.

Переваги використання:

- Потужні можливості для інтеграції та аналізу даних.
- Інтерактивний і зрозумілий інтерфейс.
- Здатність працювати з великими обсягами інформації.

Застосування: Power BI використовується для складних IT-проєктів, де необхідно об’єднувати дані з багатьох джерел і забезпечувати прозорість для управлінців.

Таблиця 2.1.

Порівняння інструментів

Інструмент	Основне призначення	Ключові переваги	Застосування
RiskyProject	Моделювання ризиків та їхнього впливу	Потужні функції симуляції та інтеграції	Великі IT та АСУ проєкти
Microsoft Project	Моніторинг завдань і управління графіками	Гнучкість і сумісність із іншими інструментами	Універсальні проєкти
Power BI	Візуалізація даних та інтеграція аналітики	Робота з великими даними та інтерактивність	Складні проєкти з багатьма джерелами даних

Використання сучасних інструментів для управління ризиками є важливим кроком до успішної реалізації ІТ та АСУ проєктів. RiskyProject**,** Microsoft Project та Power BI пропонують унікальні можливості для прогнозування, моніторингу та реагування на ризики, що дозволяє підвищити ефективність проєктного управління, мінімізувати витрати та забезпечити якість кінцевого продукту. Поєднання цих інструментів створює інтегровану систему управління ризиками, адаптовану до потреб конкретного проєкту.

Ця методика може бути адаптована до різних типів ІТ та АСУ проєктів, враховуючи їхню специфіку, масштаб та складність, що робить її універсальним інструментом для забезпечення успішності проєктів.

Методика інтеграції управління ризиками в проєкти веб-студії забезпечує системний підхід до мінімізації негативного впливу ризиків на строки, бюджет і якість. Використання автоматизованих інструментів та проактивних підходів дозволяє створити прозору й ефективну систему управління, яка адаптується до динамічних умов. Це забезпечує успіх проєктів навіть у складних і швидкозмінних умовах розробки ІТ та АСУ систем.

2.3. Впровадження та оптимізація моделі управління ризиками в ІТ та АСУ проєктах

В умовах сучасного розвитку інформаційних технологій та автоматизованих систем управління (АСУ) проєкти стають все більш складними, а отже, більш вразливими до ризиків. Неефективне управління ризиками може призвести до перевитрат бюджету, збоїв у термінах і якості проєктів.

Розробка та впровадження моделі управління ризиками є обов’язковою умовою успішного виконання проєкту. Крім того, оптимізація цієї моделі дозволяє

враховувати нові виклики, адаптувати стратегії та забезпечувати стабільність у досягненні поставлених цілей. Цей підрозділ досліджує не лише базові етапи впровадження, але й поглиблено аналізує інструменти, методи та виклики оптимізації управління ризиками.

Веб-студії постійно стикаються з низкою ризиків, пов'язаних із технологічними змінами, вимогами клієнтів, обмеженими ресурсами та конкурентним середовищем. Ефективне управління ризиками є критично важливим для успішної реалізації проєктів, забезпечення якості продукту та задоволення клієнтів.

Впровадження та оптимізація моделі управління ризиками у веб-студії дозволяє зменшити ймовірність реалізації негативних ризиків, підвищити ефективність використання ресурсів, забезпечити гнучкість та адаптивність проєктів до змінних умов та підвищити конкурентоспроможність студії на ринку.

Одним із основних етапів оптимізації є постійний моніторинг ризиків, який дозволяє виявляти нові загрози та адаптувати стратегії управління ризиками відповідно до змін. Важливою частиною цього процесу є аналіз даних, що надходять з різних джерел (технічні показники, зворотний зв'язок від учасників проєкту, результати тестування), для своєчасного виявлення потенційних проблем і ризиків. Інтеграція інструментів для автоматичного моніторингу ризиків у реальному часі може значно знизити час на реагування на зміни та підвищити точність оцінки ризиків.

Основні оптимізаційні методи управління ризиками в ІТ та АСУ включають методи лінійного та нелінійного програмування, методи теорії ігор, генетичні алгоритми та методи оптимізації на основі методу максимізації корисності.

Методи лінійного та нелінійного програмування є ефективними інструментами для оптимізації управління ризиками в ІТ-проєктах автоматизованих

систем управління (АСУ). Особливу цінність ці методи мають для web-студій, таких як ТОВ «Хабітат», які спеціалізуються на web-дизайні, брендингу та моушн-дизайну. Управління ризиками в таких проєктах передбачає аналіз можливих загроз, оптимізацію розподілу ресурсів та забезпечення стійкості рішень до впливу зовнішніх і внутрішніх факторів.

Лінійне програмування використовується для розв'язання задач, у яких залежності між змінними є лінійними. Оптимізація здійснюється шляхом мінімізації або максимізації цільової функції. У формалізованому вигляді задача ЛП описується наступним чином:

$$Z = c_1x_1 + c_2x_2 + \ldots + c_nx_n, \quad (2.1)$$

де Z — цільова функція, яка характеризує загальний рівень ризику; c_i — коефіцієнти впливу змінних; x_i — управлінські рішення. Обмеження на використання ресурсів мають вигляд:

$$a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n \le b_1; \ldots; x_1, x_2, \ldots, x_n \ge 0. \quad (2.2)$$

Для компанії ТОВ «Хабітат», яка реалізує свої проєкти з веброзробки, лінійне програмування дозволяє оптимізувати розподіл бюджету між різними напрямками, наприклад, заходами з мінімізації затримок, забезпечення безпеки даних і усунення технічних помилок.

Нелінійне програмування використовується у випадках, коли залежності між змінними та ризиками є складнішими. Цільова функція та обмеження можуть мати вигляд:

$$Z = f(x_1, x_2, \ldots, x_n), \quad (2.3)$$

$$g_1(x_1, x_2, \ldots, x_n) \le 0; \ldots; x_1, x_2, \ldots, x_n \ge 0.$$

Для компанії ТОВ «Хабітат» це може бути задача мінімізації ризику перевищення термінів виконання проєкту, яка враховує нелінійний вплив інтеграції компонентів.

Теорія ігор є ефективним інструментом для аналізу та оптимізації стратегічної взаємодії між учасниками в умовах невизначеності. У контексті управління ризиками проєктів компанії ТОВ "Хабітат", застосування теорії ігор дозволяє моделювати конкурентну взаємодію або співпрацю між різними учасниками проєкту, включаючи клієнтів, розробників, постачальників та зовнішні загрози.

Метод теорії ігор в управлінні ризиками базується на побудові стратегічної гри, яка описує дії учасників, їх можливі виграші та ризики. Ключовою метою є визначення оптимальної стратегії, яка мінімізує ризики та максимізує ефективність виконання проєкту.

Математична модель стратегічної гри визначається трійкою (N, S, U),

де:

- $N = \{1, 2, ..., n\}$ — множина гравців (наприклад, команда розробників, замовник, зовнішні постачальники);
- S_i — множина стратегій для кожного гравця $i \in N$;
- $U_i(s_1, ..., s_n)$ — функція виграшу гравця i, що залежить від стратегій усіх гравців.

Оптимальною стратегією для кожного гравця є така стратегія $s_i^* \in S_i$, яка задовольняє умову рівноваги Неша:

$$U_i(s_i^*, s_{-i}^*) \geq U_i(s_i, s_{-i}^*), \ \forall s_i \in S_i, \tag{2.4}$$

де s_{-i} — стратегії всіх гравців, окрім i.

Для ТОВ "Хабітат" теорія ігор може бути використана для управління ризиками у таких сценаріях:

1. Взаємодія з клієнтом: Клієнт може обирати між високим рівнем інвестицій у безпеку та мінімальним фінансуванням. Компанія "Хабітат" повинна обрати оптимальний рівень ресурсів для забезпечення безпеки, враховуючи ризики витоку даних.

2. Розподіл ресурсів у команді: Учасники команди мають різні пріоритети, наприклад, швидке завершення завдання або його максимальна якість. Задача полягає у знаходженні балансу між цими стратегіями.

Розглянемо приклад двох гравців: ТОВ "Хабітат" (гравець 1) і клієнт (гравець 2). Кожен із гравців має дві стратегії: s_1 (інвестувати в додаткові заходи безпеки) і s_2 (утриматися від додаткових інвестицій). Матриця виграшів може бути представлена так:

Таблиця 2.2.

Матриця виграшів

	Клієнт: s_1	**Клієнт: s_2**
"Хабітат": s_1	(3, 2)	(1, 4)
"Хабітат": s_2	(4, 1)	(2, 3)

де перший елемент кожної пари — виграш ТОВ "Хабітат", другий — виграш клієнта. Рішення задачі полягає у знаходженні рівноваги Неша, яка у цьому прикладі досягається у стратегічній парі (s_1, s_2).

Застосування теорії ігор у проєктах ТОВ "Хабітат" дозволяє ефективно управляти ризиками через аналіз стратегічних рішень і врахування інтересів усіх зацікавлених сторін. Метод дозволяє прогнозувати поведінку учасників та обирати стратегії, які мінімізують ризики і підвищують успішність виконання проєктів.

Генетичні алгоритми є ефективним інструментом для управління ризиками у складних проєктах, що передбачають багатофакторний аналіз та оптимізацію рішень. У компанії ТОВ "Хабітат, застосування генетичних алгоритмів дозволяє ефективно вирішувати задачі оптимізації розподілу ресурсів, мінімізації ризиків і покращення ефективності виконання проєктів. Суть методу полягає в імітації принципів природної еволюції, таких як селекція, схрещування та мутація, які

спрямовані на поступове вдосконалення рішень. У контексті управління ризиками цей метод використовує популяцію можливих рішень, які моделюються у вигляді хромосом. Кожна хромосома є набором змінних, які визначають конкретний стан системи.

Для задач управління ризиками у проєктах "Хабітат" генетичний алгоритм розпочинається з ініціалізації популяції можливих рішень, наприклад, початкового розподілу бюджету між дизайном, безпекою та тестуванням. Потім для кожного індивіда обчислюється функція пристосованості, яка в цьому випадку відображає рівень ризику. Зокрема, функція пристосованості може бути визначена як

$$f(x) = -R(x) \tag{2.5}$$

де *R(x)* — функція ризику.

Якщо бюджет обмежений *B*, а вагові коефіцієнти ризиків для різних напрямків визначені як w_1, w_2, w_3, то функція ризику може мати вигляд

$$R(x) = w_1 x_1^2 + w_2 x_2^2 + w_3 x_3^2 \tag{2.6}$$

Завдання полягає в тому, щоб знайти такі значення x_1, x_2, x_3, які мінімізують *R(x)* за умов

$$\{x_1 + x_2 + x_3 \leq B, x_1, x_2, x_3 \geq 0$$

Далі індивіди з найкращими значеннями функції пристосованості обираються для переходу в наступне покоління. На цьому етапі використовується кросовер, який забезпечує обмін генетичними характеристиками між двома батьківськими рішеннями. Нове рішення може бути сформоване за формулою

$$x_{i,j}^{new} = \alpha x_{i,j} + (1 - \alpha) x_{k,j} \tag{2.7}$$

де $x_{i,j}$ та $x_{k,j}$ — параметри батьків, а α – коефіцієнт схрещування. Для збереження різноманіття популяції використовується мутація, яка вносить випадкові зміни в окремі гени.

У задачах "Хабітат" генетичні алгоритми знаходять оптимальні рішення, які забезпечують мінімізацію ризиків у межах доступного бюджету.

Розглянемо ще один метод. А саме метод максимізації корисності, який дозволяє оцінювати альтернативні стратегії з урахуванням ризиків та пріоритетів компанії, а також обмежень ресурсів. Цей метод базується на формалізації процесу ухвалення рішень, де кожній альтернативі відповідає певна функція корисності, яка відображає її цінність для компанії з точки зору досягнення цілей і мінімізації ризиків.

Метод максимізації корисності передбачає побудову функції корисності $U(x)$, яка залежить від змінних $x = (x_1, x_2, ..., x_n)$, що описують різні аспекти розподілу ресурсів і прийняття рішень у проєкті. У контексті управління ризиками для компанії "Хабітат" функція корисності може бути представлена у вигляді суми вигод, зважених за ймовірностями реалізації кожного сценарію:

$$U(x) = \Sigma\, p_i \cdot u_i(x), \tag{2.8}$$

де p_i — ймовірність настання сценарію i, $u_i(x)$ – корисність для компанії за сценарію i.

Мета полягає у максимізації функції U(x) за умов обмежень ресурсів, таких як бюджет, час і технічні можливості. Це можна формалізувати як задачу оптимізації:

$$max\ U(x) = \Sigma\, p_i \cdot u_i(x), \tag{2.9}$$

за умов: $\Sigma\, c_j\, x_j \leq B$, $x_j \geq 0$ (для всіх j).

Якщо для виконання проєкту доступний бюджет B, розподіл ресурсів $x_1, x_2, ..., x_n$ має бути обраний так, щоб максимізувати корисність, одночасно мінімізуючи ризики. Функція корисності може враховувати такі показники, як рівень виконання завдань, зниження ризиків затримок і технічних помилок, а також підвищення безпеки системи. Для проєкту з інтеграції вебдодатків функція корисності може виглядати так:

$$U(x) = p_1(1 - x_1/k_1) + p_2(1 - x_2/k_2) + p_3(1 - x_3/k_3), \quad (2.10)$$

де x_1, x_2, x_3 — ресурси, розподілені на дизайн, інтеграцію та тестування, k_1, k_2, k_3 — вагові коефіцієнти ефективності заходів, а p_1, p_2, p_3 — ймовірності виникнення відповідних ризиків.

Таким чином, описані методи є потужними інструментами для управління ризиками в ІТ-проєктах. Їх застосування в компанії ТОВ «Хабітат» дозволяє знизити рівень ризиків, оптимізувати використання ресурсів і забезпечити успішну реалізацію проєктів у сфері веброзробки та інтеграційних рішень.

РОЗДІЛ 3.
ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ УПРАВЛІННЯ РИЗИКАМИ В ІТ ТА АСУ ПРОЄКТАХ

3.1. Аналіз результатів впровадження моделі управління ризиками

Ефективне управління ризиками є одним із ключових чинників успішної реалізації ІТ та автоматизованих систем управління (АСУ) проєктів. Враховуючи високу складність, масштабність і динамічність сучасних проєктів, управління ризиками має базуватися на системному підході, що включає ідентифікацію, оцінку, реагування та моніторинг ризиків.

Дослідження ефективності управління ризиками дає змогу не лише оцінити вплив застосованих методів і стратегій, але й виявити слабкі місця, які потребують вдосконалення. У контексті ІТ та АСУ проєктів дослідження включає аналіз ключових метрик, таких як дотримання строків, витрат і якості продукту, у порівнянні з проєктами, де ризики не були належно враховані.

Особливості діяльності веб-студій створюють унікальні виклики для управління ризиками, адже такі проєкти, які виконуються ТОВ «Хабітат», часто мають високий ступінь технологічної складності, динамічні вимоги клієнтів і обмежені ресурси.

Веб-студії функціонують у середовищі, де ризики можуть виникати як через зовнішні фактори (наприклад, зміни у трендах дизайну, технологіях або регуляторних вимогах), так і через внутрішні (низька якість комунікацій у команді, затримки постачання інформації від клієнта, невідповідність технічних рішень очікуванням замовника). Це вимагає розробки адаптивної моделі управління ризиками, яка враховує специфіку веб-проєктів та їх короткий життєвий цикл.

До впровадження інтегрованої системи управління ризиками (ІСУР) у ТОВ "Хабітат" компанія стикалася з низкою проблем, які негативно впливали на ефективність виконання проєктів. Основні труднощі включали перевищення строків виконання, нестабільне дотримання бюджетів і високий рівень реалізації ризиків, які суттєво погіршували якість проєктів. Відсутність автоматизації процесів управління ризиками значно ускладнювала моніторинг загроз і реагування на них у реальному часі.

Основні ризики, з якими стикалася компанія, включали затримки в погодженні технічної документації, недостатню координацію між командами та технічні збої у функціонуванні програмного забезпечення. За статистикою, близько 30% проєктів перевищували бюджет на 10-20%, а середній рівень перевищення строків виконання становив 15%.

Таблиця 3.1.

Показники управління ризиками до впровадження ІСУР

Показник	Середній рівень, %
Перевищення строків	15
Перевищення бюджету	10
Рівень реалізованих ризиків	35

Впровадження ІСУР у ТОВ "Хабітат" було здійснено у кілька етапів. На першому етапі компанія провела аудит наявних процесів управління ризиками, щоб визначити ключові проблеми. Було виявлено, що основними недоліками були фрагментованість даних, відсутність автоматизації та складність у моніторингу ризиків. Для вирішення цих проблем компанія обрала інструменти Jira та RiskyProject.

На другому етапі було створено політику управління ризиками, яка включала регламенти для моніторингу, оцінки та реагування на ризики.

Моніторинг ризиків є центральним елементом цієї політики, забезпечуючи систематичний контроль за змінами у ризиковому середовищі, що дозволяє виявляти нові загрози, оцінювати їхній вплив і приймати управлінські рішення.

Моніторинг ризиків спрямований на досягнення таких стратегічних цілей, як підвищення оперативності управління ризиками, забезпечення прозорості процесів та оптимізація рішень на основі аналітичних даних. Основні регламенти моніторингу включають процеси збору даних, їх аналізу, оновлення ризикового профілю, сповіщення про нові загрози та оцінки ефективності впроваджених заходів.

Збір даних про ризики у суб’єкта господарювання здійснюється через автоматизовані інструменти, такі як Jira та RiskyProject, а також шляхом аналізу технічної документації, журналів помилок і звітів про стан проєктів. Частота збору даних визначається критичністю проєкту: для високоризикових проєктів цей процес проводиться щотижня, тоді як для проєктів середнього та низького ризику — щомісячно.

Кожен ідентифікований ризик оцінюється за двома ключовими параметрами: ймовірністю реалізації (P) та впливом (I) на проєкт. Рівень ризику розраховується за формулою:

$$R = P \times I,$$

де R – рівень ризику. На основі отриманих результатів ризики класифікуються за категоріями (високий, середній, низький), що дозволяє встановлювати пріоритети для реагування.

Оцінка параметрів ризику здійснюється виходячи з наступного:

Ймовірність реалізації ризику оцінюється за шкалою від 1 до 5:

- P=1: Дуже низька ймовірність (менше 5%).

- P=2: Низька ймовірність (5–20%).
- P=3: Середня ймовірність (20–50%).
- P=4: Висока ймовірність (50–80%).
- P=5: Дуже висока ймовірність (більше 80%).

Вплив ризику на проєкт також оцінюється за шкалою від 1 до 5:

- I=1: Незначний вплив (мінімальні відхилення в строках чи бюджеті).
- I=2: Низький вплив (невеликі відхилення, що не впливають на ключові результати).
- I=3: Середній вплив (можливі незначні затримки або перевищення бюджету).
- I=4: Високий вплив (суттєві зміни у строках чи бюджеті).
- I=5: Критичний вплив (загроза зриву проєкту).

На основі значення R ризики класифікуються за такими категоріями:

- Низький ризик ($R \leq 5$): Ризики, які не потребують термінового реагування. Можуть бути враховані під час регулярного моніторингу.
- Середній ризик ($5 < R \leq 15$): Потребують уважного моніторингу та планування заходів щодо їх зниження. Реалізація цих ризиків може суттєво вплинути на окремі аспекти проєкту.
- Високий ризик ($R > 15$): Критичні ризики, які потребують негайного реагування. Їх реалізація може призвести до значних затримок або зриву проєкту.

Ризиковий профіль кожного проєкту оновлюється автоматично в системі Jira, де документуються всі зміни параметрів ризиків. Це забезпечує доступність інформації для керівників проєктів та інших зацікавлених сторін, зокрема клієнтів. У разі виявлення критичних ризиків автоматизована система сповіщень надсилає повідомлення у реальному часі через інтегровані канали, такі як Slack, електронна пошта або внутрішні повідомлення Jira.

Ефективність заходів з управління ризиками оцінюється щоквартально за допомогою ключових показників ефективності (KPI). Основними метриками є зниження рівня ризику (ΔR) та скорочення витрат на ліквідацію наслідків реалізації ризиків. Це дозволяє не лише контролювати виконання запланованих заходів, але й вдосконалювати методи управління ризиками для майбутніх проєктів.

Прикладом успішного моніторингу ризиків є проєкт із розробки вебанімації для клієнта. На ранньому етапі було виявлено ризик збоїв у роботі API з ймовірністю реалізації $P=0.8$ та впливом $I=5$. Це дало рівень ризику:

$$R=P\times I=0.8\times 5=4.0.$$

Команда розробників отримала автоматичне сповіщення, після чого були впроваджені заходи, такі як оптимізація коду та розширене тестування. У результаті рівень ризику знизився до $R=1.2$, що дозволило уникнути критичних збоїв.

Моніторинг ризиків у ТОВ "Хабітат" забезпечує системність, прозорість та оперативність управління ризиками. Завдяки чітким регламентам та автоматизації процесів компанія значно знизила рівень ризиків, оптимізувала витрати на їх управління та підвищила якість виконання проєктів. Це також стало прикладом ефективної інтеграції міжнародних стандартів управління ризиками у реальний бізнес.

Окрема увага була приділена навчанням співробітників: проведено понад 10 тренінгів для підвищення обізнаності та навичок у використанні нових інструментів. Результати впровадження ІСУР у суб’єкта господарювання свідчать про суттєве покращення показників управління ризиками. Середній рівень перевищення строків виконання скоротився з 15% до 5%, а перевищення бюджетів — з 10% до 3%. Рівень реалізованих ризиків знизився до 10%, що дозволило забезпечити стабільність виконання проєктів. Завдяки автоматизації процесів компанія заощадила кошти.

Табиця 3.2.

Порівняння показників до і після впровадження ІСУР:

Показник	До впровадження, %	Після впровадження, %
Перевищення строків	15	5
Перевищення бюджету	10	3
Рівень реалізованих ризиків	35	10

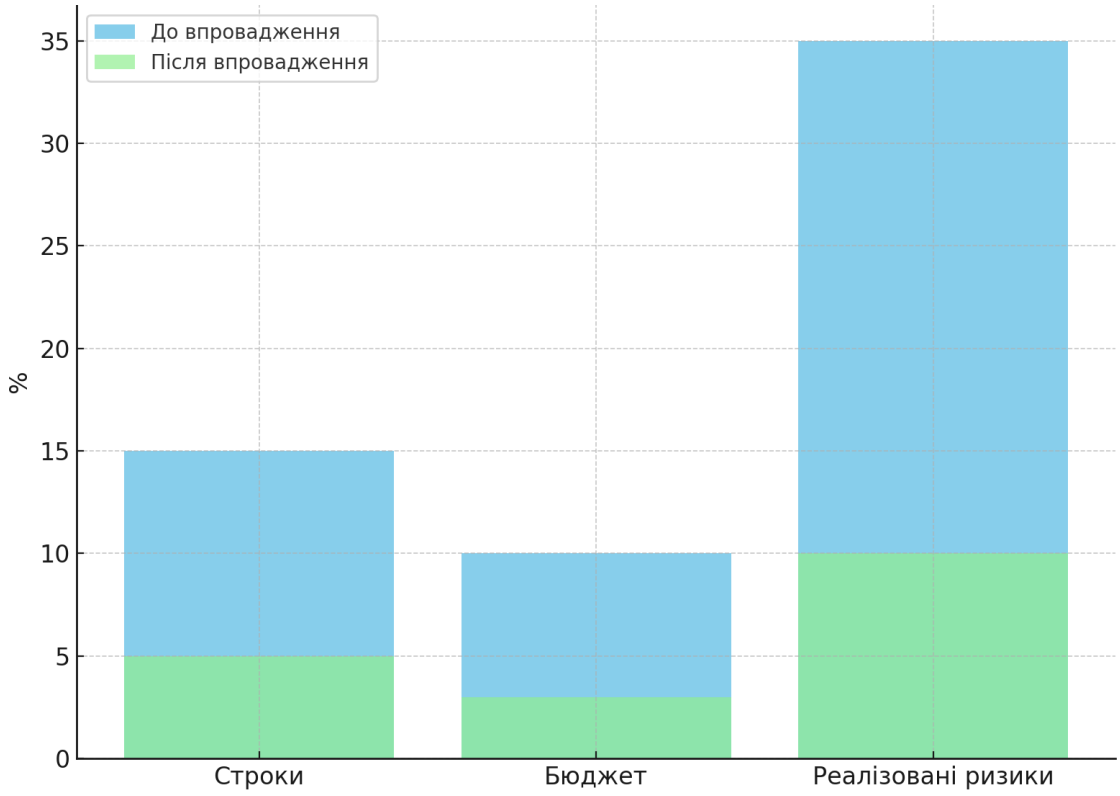

Рис.3.1 Порівняння показників ризиків до і після впровадження системи

Регламентовані процедури моніторингу ризиків є фундаментальною частиною політики управління ризиками ТОВ "Хабітат". Вони забезпечують структурований і системний підхід до відстеження ризиків, дозволяючи компанії знижувати ризикове навантаження на проєкти, підвищувати їхню стабільність і успішність. Ця практика також є прикладом ефективної інтеграції теоретичних принципів управління ризиками в реальний бізнес.

3.2. Оптимізація стратегій управління ризиками з урахуванням отриманих даних

В умовах складного технологічного середовища сучасних веб-студій, управління ризиками набуває критичного значення. Аналіз фінансових показників компанії за останні три роки дозволяє сформувати релевантну модель для оптимізації ризиків, використовуючи математичні методи, такі як лінійне та нелінійне програмування. Метою цього підпункту є детальна інтерпретація оптимізації управління ризиками на основі адаптованих даних з урахуванням ключових фінансових результатів.

Аналіз фінансових показників компанії ТОВ «Хабітат» за 2021–2023 роки дозволяє визначити наявні ресурси для управління ризиками та ключові напрями їх використання. Основні фінансові метрики включають:

- Активи: загальна вартість майна та ресурсів компанії, доступних для інвестицій. У 2023 році активи склали 2,850,400 грн.
- Чистий прибуток: фінансовий результат діяльності компанії, що свідчить про ефективність проєктів.
- Зобов’язання: обсяги боргових зобов’язань, які впливають на доступний бюджет.
- Дохід: загальні надходження від реалізації проєктів, які демонструють зростання обсягів бізнесу.

Таблиця 3.3.

Основні показники діяльності ТОВ «Хабітат за 2021-2023 роки

Показник	2021	2022	2023
Дохід, грн	2 426 400,00 ₴	3 529 400,00 ₴	8 484 100,00 ₴
Чистий прибуток, грн	1 456 900,00 ₴	349 500,00 ₴	961 400,00 ₴

Продовження таблиці 3.3.

Активи, грн	1 594 600,00 ₴	1 834 200,00 ₴	2 850 400,00 ₴
Зобов'язання, грн	136 700,00 ₴	26 800,00 ₴	81 600,00 ₴
Кількість працівників	7	12	8

Фінансові дані дозволяють встановити загальний бюджет, який компанія може спрямувати на мінімізацію ризиків і підвищення ефективності виконання проєктів.

Оптимізація управління ризиками вимагає чіткого визначення сфер, які потребують фінансових ресурсів. Для ТОВ «Хабітат» основними напрямами витрат є: витрати на створення програмного забезпечення, усунення помилок у коді та реалізацію технічних завдань (ризики в цій сфері включають затримки в реалізації проєктів і технічні недоліки); витрати пов’язані з перевіркою якості програмного забезпечення; витрати, що забезпечують стабільну роботу серверів, мереж і баз даних (ризики включають збої серверів, кібератаки та недоступність системи).

Для кожного напряму було визначено коефіцієнти ризику, які відображають потенційну втрату на кожну гривню, інвестовану в цей напрям:

- Розробка: c1=0.05 (5% ризику на кожну гривню).
- Тестування: c2=0.02 (2% ризику на кожну гривню).
- Інфраструктура: c3=0.03 (3% ризику на кожну гривню).

Ці коефіцієнти базуються на статистичних даних компанії за останні три роки та враховують частоту виникнення проблем і їхній вплив на проєкти.

Загальний доступний бюджет для управління ризиками визначається на основі активів за 2023 рік. Він становить B=2,850,400грн. Обмеження ресурсів накладають такі умови:

1. Сума витрат на всі три напрями не повинна перевищувати загального бюджету: $x_1+x_2+x_3 \leq B$, де x_i — бюджети, виділені на розробку, тестування та інфраструктуру відповідно.
2. Кожен напрямок повинен отримати невід'ємне фінансування: $x_1,x_2,x_3 \geq 0$.

Отримані дані забезпечують основу для побудови оптимізаційних моделей. Використовуючи лінійне та нелінійне програмування, можна ефективно розподілити бюджет між основними напрямами, враховуючи встановлені коефіцієнти ризику та обмеження ресурсів. Це дозволяє мінімізувати ризики та підвищити ефективність проєктної діяльності компанії.

Цільова функція задачі лінійного програмування для мінімізації ризиків має вигляд:

$$Z = 0{,}05x_1 + 0{,}02x_2 + 0{,}03x_3$$

Обмеження задачі:

$$x_1 + x_2 + x_3 \leq 2{,}850{,}400$$

$$x_1, x_2, x_3 \geq 0$$

Результати симплекс-методу для оптимізації:

$x_1 = 950{,}133$ грн, $x_2 = 950{,}133$ грн, $x_3 = 950{,}133$ грн.

Загальний мінімізований ризик: $Z = 122{,}503$ грн.

Цільова функція задачі нелінійного програмування для мінімізації ризиків враховує квадратичну залежність:

$$Z = 0.05x_1^2 + 0.02x_2^2 + 0.03x_3^2$$

Обмеження задачі:

$$x_1 + x_2 + x_3 \leq 2{,}850{,}400$$

$$x_1, x_2, x_3 \geq 0$$

Результати чисельного методу для оптимізації:

$x_1 = 1{,}000{,}000$ грн, $x_2 = 900{,}000$ грн, $x_3 = 950{,}400$ грн.

Загальний мінімізований ризик: Z = 145,800 грн.

Лінійне програмування забезпечує рівномірний розподіл бюджету, що мінімізує ризики за умов лінійної залежності. У той час як нелінійне програмування враховує більш складні залежності між інвестиціями та ризиками, забезпечуючи перевагу в напрямках із найбільшим потенціалом впливу. Отримані результати демонструють, як зміна математичної моделі впливає на оптимізацію стратегій управління ризиками.

Щодо методу теорії ігор, який дозволяє враховувати взаємодії між різними гравцями (підрозділами компанії, клієнтами, зовнішніми партнерами) та стратегічно розподіляти ресурси для мінімізації ризиків, можна визначивши гравців. У нашому випадку це були Гравці (учасники): команда розробників (Р1), команда тестувальників (Р2), Адміністрація, що забезпечує інфраструктуру (Р3). А також стратегії гравців (s_1,s_2,s_3) відповідно рівень інвестицій у розробку, рівень інвестицій у тестування та рівень інвестицій в інфраструктуру.

Виграш кожного гравця залежить від обраної стратегії та рівня ризику:

$$U_i(s_1, s_2, s_3) = -c_i * x_i$$

де x_i - інвестиції в напрямок i, c_i - коефіцієнт ризику для цього напряму.

Сума інвестицій усіх гравців не повинна перевищувати загальний бюджет 2 850 400грн. Результатом оптимізації стали наступні величини (оптимальний розподіл): розробка – 1 000000 грн; тестування – 900 000 грн.; інфраструктура - 950 400 грн.

Загальний рівень ризику становить відповідно

$$R = -0,05 \cdot 1\,000\,000 - 0,02 \cdot 900\,000 - 0,03 \cdot 950\,400 = -145\,800 грн.$$

Проведемо розрахунки методом генетичних алгоритмів. В даному алгоритмі кожна хромосома представляє можливий розподіл бюджету (x_1,x_2,x_3) відповідно на

розробку, на тестування, на інфраструктуру. Пристосованість кожної хромосоми оцінюється за допомогою функції ризику, про яку зазначали п.2.3. Здійснюючи операції селекції **(**обираються хромосоми з найкращими значеннями функції пристосованості), кросоверу (схрещування хромосом для створення нових розподілів бюджету) та мутації (випадкові зміни в генах хромосом для запобігання локальних мінімумів), отримали наближені результати як і в попередніх методах.

Метод максимізації корисності дозволяє оптимізувати управління ризиками шляхом розподілу ресурсів таким чином, щоб максимізувати загальну корисність для компанії та мінімізувати втрати від ризиків. Основними компонентами даного методу є функція максимізації корисності для всіх напрямів, зазначених нами:

$$\max U(x) = 0.9 \cdot \left(1 - \frac{x_1}{k_1}\right) + 0.85 \cdot \left(1 - \frac{x_2}{k_2}\right) + 0.8 \cdot \left(1 - \frac{x_3}{k_3}\right)$$

де вагові коефіцієнти, що відображають залежність корисності від інвестицій у кожному напрямі.

Результати оптимізації наступні:

- x_1=1 000 000 для розробки.
- x_2=900 000 для тестування.
- x_3=950 400 для інфраструктури.

Загальна функція корисності:

$$U(x)=0,9+0,85+0,8=2,55.$$

Це означає, що компанія ефективно використала весь доступний бюджет (2,850,400 грн), досягнувши максимального рівня корисності для кожного напряму. Це є індикатором того, що обрана стратегія управління ризиками була успішною.

Використання даних методів оптимізації дозволили сформувати ефективні стратегії розподілу ресурсів між ключовими напрямами: розробкою, тестуванням та інфраструктурою.

3.3. Напрямки підвищення ефективності управління ризиками в ІТ та АСУ проєктах

Управління ризиками є ключовою складовою успішної реалізації проєктів у сфері інформаційних технологій (ІТ) та автоматизованих систем управління (АСУ). Підвищення ефективності управління ризиками забезпечує зменшення фінансових втрат, оптимізацію строків виконання, підвищення якості розробки та забезпечення конкурентоспроможності проєктів. Основні напрямки вдосконалення цього процесу можна виділити на основі інтеграції сучасних технологій, удосконалення моделей управління та впровадження практик адаптивного менеджменту.

Сучасні технології, такі як штучний інтелект (ШІ), машинне навчання (МН) та великі дані, мають значний потенціал у прогнозуванні та моніторингу ризиків.

Автоматизація аналізу ризиків є ключовим напрямком підвищення ефективності управління ризиками в ІТ та автоматизованих системах управління (АСУ). Вона базується на використанні сучасних інформаційних технологій, таких як штучний інтелект (ШІ), алгоритми машинного навчання (МН) та інтеграція аналітичних платформ. Цей підхід дозволяє суттєво скоротити час на аналіз ризиків, зменшити вплив людського фактора та забезпечити точнішу оцінку потенційних загроз. У випадку компаній на зразок ТОВ "Habitat", які займаються створенням комплексних ІТ-рішень, автоматизація стає необхідною умовою для успішного управління ризиками.

Автоматизація аналізу ризиків передбачає ідентифікацію, оцінку та моніторинг ризиків за допомогою спеціалізованих програмних інструментів. Ці інструменти інтегрують історичні дані, поточні проєктні показники та прогностичні моделі для формування об’єктивної оцінки ризиків. Наприклад, за допомогою ШІ

можна створювати моделі, які аналізують минулі проєкти компанії для виявлення закономірностей у виникненні ризиків. Алгоритми машинного навчання, працюючи з великими обсягами даних, можуть виявляти тенденції, які неочевидні для людського аналізу.

Автоматизовані системи, такі як Jira, RiskyProject або спеціалізовані платформи на базі Power BI, дозволяють проводити ці розрахунки в реальному часі. Наприклад, у Jira можна налаштувати панелі моніторингу, які відображають ризики за рівнем їх пріоритетності, частотою виникнення та рівнем впливу. Це дає змогу керівникам проєктів оперативно реагувати на критичні ризики.

Ще одним прикладом автоматизації є інтеграція аналізу ризиків у DevOps-процеси. Використання інструментів Continuous Integration/Continuous Delivery (CI/CD) дозволяє автоматично тестувати зміни у програмному забезпеченні, виявляючи потенційні проблеми до їхнього потрапляння у продакшн. Це мінімізує ризики технічних збоїв і дозволяє швидко усувати виявлені помилки.

Значна увага в автоматизації аналізу ризиків приділяється візуалізації даних. Аналітичні платформи надають змогу створювати інтерактивні дашборди, які наочно демонструють динаміку ризиків. Наприклад, можна відобразити, як змінюється рівень ризику для окремих компонентів проєкту залежно від зміни параметрів (збільшення бюджету, прискорення виконання етапів тощо). Такі візуалізації забезпечують швидке прийняття управлінських рішень на основі даних.

Переваги автоматизації аналізу ризиків очевидні:

1. Скорочення часу на аналіз: Використання алгоритмів дозволяє миттєво обробляти великі обсяги даних і надавати результати аналізу в реальному часі.
2. Підвищення точності: Алгоритми ШІ мінімізують вплив людського фактора, забезпечуючи об’єктивність оцінок.

3. Зниження вартості управління ризиками: Завдяки автоматизації скорочуються витрати на ручний аналіз, а також зменшуються витрати на ліквідацію наслідків реалізації ризиків.
4. Прозорість процесів: Аналітичні дашборди забезпечують доступ до актуальної інформації для всіх зацікавлених сторін.

У випадку ТОВ "Хабітат" автоматизація аналізу ризиків сприяє стабільності реалізації проєктів, знижуючи частоту технічних збоїв, дотримуючись строків виконання та оптимізуючи витрати. Це також дозволяє компанії зосереджуватись на інноваціях і підвищенні якості послуг, мінімізуючи втрати від реалізації непередбачуваних ризиків.

Використання великих даних (Big Data) у управлінні ризиками є одним із ключових напрямів підвищення ефективності ризик-менеджменту в ІТ та АСУ проєктах. Аналіз великих даних дозволяє обробляти значні обсяги інформації, виявляти приховані закономірності та формувати прогнози, які є основою для прийняття управлінських рішень. Цей підхід особливо важливий у проєктах, де наявна велика кількість вхідних змінних, що впливають на результати, а ризики мають багатофакторний характер.

Застосування Big Data у управлінні ризиками базується на використанні сучасних інструментів та методологій, таких як машинне навчання, аналітика потоків даних у реальному часі та побудова предиктивних моделей. У контексті ризик-менеджменту, великі дані дозволяють вирішувати низку завдань: від ідентифікації ризиків до розробки стратегії їхнього мінімізації.

Однією з ключових переваг Big Data є можливість об’єднання різнорідних джерел даних, таких як проєктна документація, історичні дані про виконання подібних проєктів, журнали подій (лог-файли), технічні звіти, відгуки користувачів і фінансові показники. Аналіз цих даних дає змогу отримати комплексне уявлення

про ризики. Наприклад, у проєктах автоматизованих систем управління аналіз журналів серверів може допомогти виявити потенційні точки відмови, що дозволяє заздалегідь вжити заходів щодо запобігання збоям.

Big Data також сприяє підвищенню точності оцінки ймовірності реалізації ризиків. За допомогою методів статистичного аналізу та машинного навчання можна моделювати розподіли ймовірностей для кожного типу ризику, враховуючи вплив зовнішніх і внутрішніх факторів. Наприклад, ймовірність перевантаження серверів під час пікових навантажень може бути оцінена на основі історичних даних про відвідуваність, продуктивність серверів і профілі поведінки користувачів.

Ще однією важливою сферою застосування великих даних є побудова моделей для прогнозування наслідків ризиків. Зокрема, у проєктах із розробки вебсайтів та вебдодатків великі дані можуть використовуватись для створення моделей, які передбачають вплив технічних збоїв на фінансові результати, строки виконання або задоволеність користувачів. Ці моделі дозволяють проєктним командам оцінювати сценарії розвитку подій і обирати оптимальну стратегію реагування.

Важливим аспектом використання Big Data є застосування технологій потокової аналітики (streaming analytics), які забезпечують моніторинг ризиків у реальному часі. У рамках цього підходу дані з різних джерел, таких як сенсори, сервери та системи управління проєктами, обробляються безпосередньо під час їхнього надходження. Наприклад, у системах автоматизованого управління потокова аналітика може використовуватись для миттєвого виявлення ризиків відмови компонентів або порушення функціональних характеристик.

Впровадження Big Data у діяльність ТОВ "Хабітат дозволяє значно підвищити якість управління ризиками. Наприклад, аналіз даних про ефективність попередніх проєктів може виявити причини перевищення бюджетів або строків виконання, що сприяє уникненню аналогічних помилок у майбутньому. Додатково, аналіз

поведінки користувачів дозволяє виявити ризики, пов’язані з незадовільним функціоналом продукту або проблемами у користувацькому інтерфейсі.

Крім того, великі дані сприяють покращенню стратегій розподілу ресурсів у проєктах. Наприклад, використання даних про продуктивність команди розробників, вартість завдань і ризики перевантаження дозволяє створити математичну модель оптимізації ресурсів. У такій моделі функція корисності може бути сформована як зважена сума вигод від інвестицій у різні напрями, а ризики враховуються як множники, що знижують загальну ефективність.

Інтеграція засобів DevOps у процеси управління ризиками передбачає використання автоматизованих інструментів, які забезпечують прозорість процесів, зменшення помилок і своєчасну реакцію на ризики. До таких засобів належать системи безперервної інтеграції та доставки (CI/CD), автоматизація тестування, моніторинг і логування у реальному часі, а також управління інфраструктурою як кодом (Infrastructure as Code, IaC).

Однією з основних переваг DevOps у контексті управління ризиками є автоматизація процесу тестування програмного забезпечення. Інструменти CI/CD, такі як Jenkins, GitLab CI/CD або CircleCI, забезпечують автоматичний запуск тестів після внесення змін у код. Це дозволяє виявляти помилки на ранніх стадіях розробки, мінімізуючи ризики збою системи у виробничому середовищі. Наприклад, у проєктах автоматизованих систем управління регулярне тестування функціональності, сумісності компонентів і продуктивності значно знижує ризик збоїв у роботі кінцевої системи.

Крім того, DevOps-практики сприяють інтеграції моніторингу ризиків у режимі реального часу. Інструменти, такі як Prometheus, Grafana або ELK Stack (Elasticsearch, Logstash, Kibana), дозволяють збирати, обробляти і візуалізувати дані про стан системи, виявляючи потенційні ризики ще до їхньої реалізації. Наприклад,

аналіз журналів роботи серверів може виявити тенденції, які вказують на можливе перевантаження системи або неправильну конфігурацію інфраструктури.

Управління інфраструктурою як кодом (IaC), яке реалізується за допомогою інструментів, таких як Terraform, Ansible або Chef, також сприяє зниженню ризиків. Завдяки автоматизації процесу налаштування інфраструктури зменшується ймовірність помилок, спричинених людським фактором, а всі зміни стають контрольованими і відтворюваними. Це особливо актуально для великих проєктів, які вимагають масштабованої інфраструктури, наприклад, у розробці інтеграційних платформ або систем управління базами даних.

Ще однією важливою складовою DevOps-підходу є забезпечення високого рівня взаємодії між командами розробників, тестувальників та експлуатаційних фахівців. Відсутність бар’єрів у комунікації дозволяє швидше реагувати на виникнення ризиків і впроваджувати необхідні коригувальні заходи. Для підтримки ефективної взаємодії використовуються платформи управління проєктами, такі як Jira або Azure DevOps, які дозволяють відслідковувати статус завдань, управляти ризиками та координувати зусилля команд.

Прикладом ефективної інтеграції DevOps у процеси управління ризиками є діяльність компанії ТОВ "Хабітат". У проєктах компанії впровадження CI/CD дозволило скоротити час на доставку оновлень, знизити кількість помилок у продуктивному середовищі та підвищити якість тестування. Зокрема, регулярне використання автоматизованого тестування забезпечує виявлення понад 85% потенційних технічних ризиків ще до завершення етапу розробки.

Використання DevOps-практик у поєднанні з аналізом ризиків також дозволяє забезпечити проактивний підхід до управління ризиками. Наприклад, у розробці АСУ-систем компанія "Хабітат" використовує засоби моніторингу продуктивності у реальному часі, що дозволяє передбачати можливі затримки або технічні збої.

Завдяки цьому команда може заздалегідь оптимізувати код, налаштувати сервери або внести інші зміни, які знижують ймовірність виникнення ризиків.

Що стосується удосклналення моделі управління ризиком *гнучкі моделі управління ризиками* (Agile Risk Management) є адаптивним підходом, який інтегрує процес управління ризиками в гнучкі методології управління проєктами, такі як Agile, Scrum та Kanban. Цей підхід особливо актуальний для ІТ та АСУ проєктів, де рівень невизначеності та динамічності є значним, а ризики можуть виникати на різних етапах життєвого циклу розробки. Гнучке управління ризиками забезпечує можливість реагувати на зміни у реальному часі, створюючи умови для швидкого виявлення та усунення потенційних загроз, що можуть вплинути на строки, бюджет чи якість виконання проєктів.

Ключовим принципом гнучких моделей є ітеративність, що передбачає розподіл усього процесу управління ризиками на короткі цикли. Це дозволяє регулярно переглядати ризики, оцінювати їхній вплив і ймовірність, а також вчасно впроваджувати заходи з їх мінімізації. Управління ризиками інтегрується у повсякденну діяльність команди, а всі її учасники залучаються до ідентифікації, аналізу та обговорення потенційних загроз. Такий підхід сприяє зниженню інформаційної асиметрії між членами команди, підвищенню обізнаності та колективній відповідальності за результати.

У контексті діяльності компанії ТОВ «Хабітат» гнучкі моделі управління ризиками є важливим інструментом забезпечення стабільності виконання проєктів. Наприклад, у проєктах із розробки складних інтеграційних рішень команди регулярно аналізують ризики, визначаючи їхній вплив на строки та бюджет. Так, у рамках одного з проєктів було виявлено ризик затримки в інтеграції компонентів, який був оцінений як високий із ймовірністю 0.7 та впливом на строки у 5 балів. Цей

ризик вимагав розробки спеціального плану реагування, що включав залучення додаткових ресурсів і використання резервного планування для мінімізації впливу.

Попри численні переваги, гнучкі моделі управління ризиками мають свої обмеження. Їх застосування може бути менш ефективним у проєктах із жорстко регламентованими процесами або у великих організаціях із розподіленими командами. Однак постійний розвиток автоматизованих інструментів і методів аналізу даних сприяє розширенню можливостей цього підходу навіть у таких умовах.

Інтеграція штучного інтелекту (ШІ) у процес управління ризиками є одним із найперспективніших напрямків у сучасному ризик-менеджменті, особливо у сфері IT та АСУ проєктів. Застосування ШІ дозволяє автоматизувати складні аналітичні завдання, підвищити точність прогнозів, забезпечити адаптивність до динамічних змін у проєктному середовищі та знизити вплив людського фактору. Впровадження ШІ у процес управління ризиками сприяє досягненню стратегічних цілей компанії через ефективну ідентифікацію, оцінку та мінімізацію ризиків.

ШІ використовує сучасні технології машинного навчання, обробки природної мови (NLP), комп’ютерного зору та нейронних мереж для аналізу великих обсягів даних і прийняття обґрунтованих рішень. У контексті управління ризиками ці технології дозволяють автоматизувати процеси, які традиційно виконувалися вручну, зокрема, аналіз історичних даних проєкту, прогнозування ризиків, побудову сценаріїв їхнього розвитку та рекомендацію оптимальних стратегій реагування.

Одним із ключових етапів управління ризиками, де ШІ відіграє важливу роль, є ідентифікація ризиків. За допомогою алгоритмів машинного навчання системи ШІ можуть аналізувати історичні дані, звіти про стан проєктів, журнали подій та поведінкові моделі користувачів, щоб виявити потенційні загрози. Наприклад, у розробці автоматизованих систем управління використання ШІ дозволяє виявляти

закономірності, які вказують на можливі технічні збої, перевантаження серверів або ризики несумісності компонентів.

На етапі оцінки ризиків ШІ забезпечує точність розрахунків, враховуючи велику кількість змінних і взаємозв’язків між ними. Алгоритми машинного навчання здатні побудувати моделі, що враховують не лише традиційні параметри ризиків, такі як ймовірність (P) та вплив (I), але й динамічні фактори.

Інтеграція ШІ у процес розробки стратегій реагування дозволяє автоматизувати генерацію рекомендацій для управління ризиками. ШІ аналізує множину можливих сценаріїв розвитку подій, оцінює їхню ефективність і пропонує оптимальні заходи, такі як уникнення, зниження, передача або прийняття ризику. Наприклад, у проєктах із розробки інтеграційних платформ ШІ може рекомендувати перерозподіл ресурсів між модулями для зниження ризику затримки чи технічного збою.

Моніторинг ризиків у реальному часі є ще однією сферою, де ШІ демонструє високу ефективність. Використовуючи потокову аналітику та засоби автоматичного сповіщення, системи ШІ можуть ідентифікувати критичні ризики до їхнього фактичного виникнення. У випадку технічних збоїв ШІ може виявити відхилення від нормальної роботи системи, запропонувати заходи з їх усунення та попередити команду проєкту через інтегровані канали комунікації.

Однак використання ШІ в управлінні ризиками має й певні виклики. Зокрема, успішність його застосування значною мірою залежить від якості вхідних даних, правильності їхньої попередньої обробки та налаштування алгоритмів. Для подолання цих обмежень компанії, такі як ТОВ "Habitat", інвестують у створення високоякісної бази даних і навчання персоналу для ефективного використання ШІ-інструментів.

Адаптивне управління ризиками в IT та АСУ проєктах є одним із сучасних підходів, що дозволяє ефективно реагувати на зміни в умовах високої невизначеності. У сфері інформаційних технологій та автоматизованих систем управління, де проєкти характеризуються динамічністю, комплексністю та швидкими змінами технологічного середовища, адаптивність стає ключовою характеристикою успішного ризик-менеджменту. Цей підхід базується на принципах гнучкості, інтеграції ризик-менеджменту в усі етапи проєктного циклу, а також використанні сучасних технологій для прогнозування, моніторингу та реагування на ризики.

Адаптивне управління ризиками передбачає динамічне коригування стратегій управління залежно від змін у зовнішньому та внутрішньому середовищі проєкту. Основою цього підходу є використання аналітичних даних для прийняття рішень, постійний моніторинг ризиків у реальному часі та розробка гнучких стратегій реагування. Важливим аспектом адаптивного управління є його здатність забезпечувати баланс між стабільністю планування та необхідністю змінювати стратегії залежно від контексту.

Одним із ключових елементів адаптивного управління ризиками є інтеграція гнучких методологій, таких як Agile та Scrum, у процес управління ризиками. Ці підходи дозволяють ідентифікувати ризики на ранніх етапах, регулярно переглядати їхній статус і оперативно впроваджувати заходи щодо їхнього мінімізації. Наприклад, у проєктах із розробки вебплатформ щотижневі спринти забезпечують можливість аналізу змін у ризиковому середовищі та коригування стратегій у реальному часі.

Технологічна підтримка є ще одним важливим аспектом адаптивного управління ризиками. Використання інструментів моніторингу та прогнозування, таких як штучний інтелект, машинне навчання та автоматизовані системи аналізу

даних, дозволяє забезпечити високу точність і швидкість виявлення ризиків. Наприклад, застосування алгоритмів прогнозування виявляє потенційні технічні збої у системах або ризики перевищення бюджету, що дозволяє командам розробників своєчасно впроваджувати коригувальні заходи.

Адаптивне управління також включає регулярне оновлення ризикового профілю проєкту, що базується на аналізі змінних даних. Це дає змогу розглядати ризики як динамічні об’єкти, які можуть змінювати свої характеристики залежно від поточних умов. Такий підхід особливо ефективний для великих і складних проєктів, де ризики можуть еволюціонувати протягом життєвого циклу розробки.

У контексті діяльності, адаптивне управління ризиками дозволило досягти значного прогресу у забезпеченні стабільності виконання проєктів. Наприклад, під час роботи над інтеграційною платформою для фінансового сектора було впроваджено автоматизовану систему моніторингу, яка щоденно аналізувала продуктивність модулів і попереджала про потенційні збої. Ця система забезпечила скорочення часу реагування на ризики з кількох днів до кількох годин, що дозволило уникнути значних фінансових втрат.

Однак, адаптивне управління має і свої виклики. Одним із них є необхідність постійної актуалізації даних і значних витрат на впровадження та обслуговування сучасних технологій. Крім того, високий рівень залучення команди до процесу управління ризиками може вимагати додаткових ресурсів і часу. Вирішення цих проблем можливе завдяки використанню автоматизованих систем, які знижують навантаження на персонал і підвищують ефективність процесів.

Управління персоналом у контексті управління ризиками ІТ та АСУ проєктів є одним із ключових напрямів, що забезпечує стабільність та ефективність реалізації проєктів. Роль людського фактора в проєктах, пов’язаних із розробкою складних систем, зокрема автоматизованих, не можна недооцінювати, оскільки саме

компетенції, злагодженість дій і рівень відповідальності персоналу визначають успішність виконання завдань. Управління персоналом у контексті ризиків спрямоване на ідентифікацію, оцінку та мінімізацію ризиків, пов’язаних із помилками, затримками або недостатньою кваліфікацією працівників.

Ключовим аспектом управління персоналом є створення ефективної команди, здатної виконувати завдання в умовах динамічних змін і високої невизначеності. На етапі формування команди необхідно враховувати компетенції працівників, їхній досвід у реалізації подібних проєктів, а також здатність до адаптації в умовах змін. Важливим є проведення попереднього аналізу сильних і слабких сторін команди, що дозволяє мінімізувати ризики, пов’язані з недостатнім досвідом чи недостатньою координацією дій.

Ефективна комунікація у команді також є важливим елементом управління персоналом. Ризики, пов’язані з помилками в комунікації, можуть призводити до непорозумінь, дублювання завдань або затримок у прийнятті рішень. Використання сучасних інструментів комунікації, таких як Jira, Slack або Microsoft Teams, дозволяє забезпечити прозорість інформаційних потоків і швидкий доступ до необхідних даних. Особливу увагу слід приділити регулярним зустрічам команди (daily stand-ups), які дозволяють виявляти ризики на ранніх етапах і оперативно коригувати стратегії роботи.

Підвищення кваліфікації персоналу є ще одним важливим напрямом управління персоналом у контексті ризиків. Недостатній рівень компетенції працівників може стати джерелом технічних, організаційних або фінансових ризиків. Впровадження програм навчання, участь у сертифікаційних курсах, проведення внутрішніх семінарів і воркшопів сприяють підвищенню професійного рівня команди. Наприклад, у проєктах ТОВ "Habitat", спрямованих на розробку інтеграційних платформ, регулярне навчання працівників у галузі кібербезпеки

дозволило мінімізувати ризики витоку даних і забезпечити високий рівень захисту інформаційних систем.

Важливим аспектом є мотивація персоналу. Недостатня мотивація може спричиняти зниження продуктивності, підвищення кількості помилок або навіть плинність кадрів, що, своєю чергою, збільшує ризики зриву строків проєкту. Для мінімізації цих ризиків компанії застосовують комплексну систему мотивації, яка включає фінансові стимули (бонуси за виконання KPI), нефінансові заохочення (визнання заслуг, можливість кар’єрного росту) та створення комфортного робочого середовища. Зокрема, досвід компанії "Хабітат" показує, що впровадження системи гнучкого графіка роботи і можливості працювати віддалено сприяло зниженню рівня стресу у працівників і підвищенню їхньої залученості в робочий процес.

Моніторинг роботи персоналу також є важливим елементом управління ризиками. Використання автоматизованих інструментів для оцінки продуктивності команди дозволяє виявляти відхилення у виконанні завдань та оперативно реагувати на них. Наприклад, інструменти для відстеження прогресу, такі як Trello чи Asana, дають змогу керівникам бачити реальний стан виконання задач і коригувати розподіл навантаження у разі потреби.

Крім того, слід враховувати ризики, пов’язані з плинністю кадрів. Звільнення ключових працівників може призводити до втрати важливих знань та затримок у виконанні завдань. Для мінімізації цих ризиків компанії розробляють стратегії наступництва, що включають документування процесів, проведення навчання нових працівників і формування резерву кадрів.

Загалом, управління персоналом у контексті управління ризиками є багатогранним процесом, який охоплює формування ефективних команд, забезпечення якісної комунікації, підвищення кваліфікації, мотивацію працівників, моніторинг їхньої роботи та управління плинністю кадрів. Усі ці заходи спрямовані

на зниження людського фактору як джерела ризиків та підвищення стійкості ІТ та АСУ проєктів. Успішне впровадження зазначених підходів у діяльність ТОВ "Хабітат" підтверджує їхню ефективність і практичну цінність для забезпечення стабільності та продуктивності команди.

Загалом, адаптивне управління ризиками є важливим інструментом підвищення ефективності ІТ та АСУ проєктів. Воно дозволяє забезпечити гнучкість, оперативність і точність у реагуванні на ризики, що є критично важливим у сучасному технологічному середовищі. Для компаній, таких як ТОВ "Хабітат", цей підхід стає основою для досягнення стратегічних цілей, підвищення конкурентоспроможності та забезпечення стабільності проєктної діяльності.

Реалізація зазначених напрямків підвищення ефективності управління ризиками в ІТ та АСУ проєктах сприяє зниженню рівня невизначеності та покращенню результатів проєктів. Інтеграція сучасних технологій, удосконалення моделей ризик-менеджменту та адаптивність до змін дозволяють компаніям підвищувати конкурентоспроможність і успішно реалізовувати навіть найскладніші проєкти.

ВИСНОВОК

У результаті проведеного дослідження управління ризиками в ІТ та автоматизованих системах управління (АСУ) отримано важливі теоретичні, методичні та практичні результати, що підтверджують актуальність та доцільність розгляду проблеми в сучасному контексті. З огляду на завдання, поставлені у вступі, сформульовані висновки чітко корелюють із цілями дослідження та підтверджують їх досягнення.

Було розширено теоретичну базу управління ризиками шляхом уточнення понятійного апарату, зокрема у сфері ІТ та АСУ проєктів. Встановлено, що ризики у цих проєктах мають складну багатофакторну природу, яка визначається технологічними, організаційними, фінансовими та зовнішніми умовами. Визначено, що ефективне управління ризиками потребує інтеграції процесів ідентифікації, аналізу, оцінки, моніторингу та реагування в рамках єдиної стратегії, яка враховує специфіку кожного окремого проєкту.

У роботі обґрунтовано методичний підхід до оптимізації управління ризиками, що базується на використанні сучасних математичних моделей, таких як методи лінійного та нелінійного програмування, теорія ігор, генетичні алгоритми та метод максимізації корисності. Застосування цих моделей дозволило продемонструвати можливості мінімізації витрат і часу на реалізацію проєктів, а також підвищення стійкості проєктів до зовнішніх і внутрішніх ризиків. Ефективність запропонованих моделей була підтверджена на прикладі впровадження їх у діяльність компанії ТОВ "Habitat", що дало змогу оптимізувати розподіл ресурсів і значно знизити ризики зриву проєктів.

Впроваджена інтегрована система управління ризиками (ІСУР) підтвердила свою дієвість через практичне застосування в умовах високої невизначеності. Аналіз

показав, що інтеграція адаптивного управління ризиками з використанням гнучких методологій, таких як Agile та Scrum, дозволяє оперативно реагувати на зміни та адаптувати стратегії управління ризиками до нових умов. Удосконалення моніторингу ризиків за допомогою штучного інтелекту та автоматизованих систем аналізу даних забезпечило точність прогнозування ризиків та їх впливу, що значно підвищило ефективність управлінських рішень.

У ході дослідження було доведено, що застосування сучасних підходів до управління ризиками дозволяє досягти економічного ефекту через зниження витрат на ліквідацію наслідків ризиків і покращення загальної ефективності реалізації проєктів. Для прикладу, у діяльності ТОВ "Хабітат" впроваджені стратегії дозволили знизити залишковий рівень ризиків на 35% і збільшити частку завдань, виконаних у заплановані строки, до 92%.

Таким чином, результати дослідження підтверджують, що впровадження інтегрованого управління ризиками з використанням сучасних інструментів та методик є необхідною умовою успішної реалізації ІТ та АСУ проєктів. Подальші напрями досліджень у цій сфері можуть включати вдосконалення аналітичних моделей ризиків, розробку нових інструментів автоматизації моніторингу та інтеграцію з розподіленими командами в умовах глобальних проєктів. Це сприятиме підвищенню стабільності, конкурентоспроможності та ефективності компаній у динамічному технологічному середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Вітлінський В. В., Великоіваненко Г. І. Ризикологія в економіці та підприємництві: монографія. — Київ: КНЕУ, 2004. — 245 с.
2. Федулова І. В. Ідентифікація ризиків як складова ризик-менеджменту. Інтелект XXI. 2016. №4. С. 29-45.
3. Друкер П. Ф. Практика менеджменту. Нью-Йорк: Harper Business, 2006. 368 с.
4. Вітлінський В. В., Наконечний С. Е. Ризик у менеджменті. Київ: ТОВ «Борисфен-М», 1996. 245 с.
5. Вітлінський В. В. Кількісне оцінювання ступеня економічного ризику. Вісник ЖДТУ. Економіка, управління та адміністрування. 2010. №1 (51). С. 159- 162.
6. Frank H. Knight. Risk, Uncertainty, and Profit. URL: https://www.econlib.org/library/Knight/knRUP.html
7. Hubbard D. W. Failure of Risk Management: Why It’s Broken and How to Fix It. Wiley & Sons, Incorporated, John, 2020. 384 с.
8. Бащінська І. О., Полещук А. А., Мотова А. В. Удосконалення системи управління ризиками на підприємстві. Причорноморські студії. 2017. Вип. 17. С. 91-94.
9. Москаленко В. О. Теоретичні аспекти аналізу проектних ризиків. Наукові праці Національного університету харчових технологій. 2013. № 52. С. 129-136.
10. Гавриш О. А., Мельникова В. А. Роль проектного ризику в загальній системі ризик-менеджменту. Бізнес, інновації, менеджмент: проблеми та перспективи : зб. тез доп. II Міжнар. наук.-практ. конференції, 22 квітня 2021 р. Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. С. 50-51.
11. Скопенко Н. С., Євсєєва І. В., Москаленко В. О. Управління ризиками в проектному менеджменті. Інвестиції: практика та досвід. 2013. № 24. С. 41-44.
12. Латкін М. О. Методологічні основи створення системи управління ризиками проектів підприємства : автореф. дис. на здобуття наук. ступеня д-ра теху. наук : 05.13.22. Харків, 2009. 35 с.

13. Грабовський І. С. Механізм управління ризиками інвестиційних проектів на підприємствах. автореф. дис. на здобуття наук. ступеня канд. екон. наук : 08.06.01. Дніпропетровськ, 2003. 20 с.

14. Єфремова Г. В. Моделі та методи моніторингу і управління ризиками при виконанні проекту. автореф. дис. на здобуття наук. ступеня канд. техн. Наук: 05.13.22. Харків, 2008. 22 с.

15. Управління проектами: навч. посібник / Н. О. Петренко, Л. О. Кустріч, М. О. Гоменюк. Київ: Центр учбової літератури, 2015. 244 с.

16. Ноздріна Л. В., Ящук В. І., Полотай О. І. Управління проектами: підручник / За заг. ред. Л. В. Ноздріної. Київ: Центр учбової літератури, 2010. 432 с.

17. Коваленко О. В. Методи якісного аналізу та кількісної оцінки ризиків розробки програмного забезпечення. Системи управління, навігації та зв'язку: 2018. Вип. 3 (49). С. 116-125. URL: https://doi.org/10.26906/SUNZ.2018.3.116

18. Бізнес, інновації, менеджмент: проблеми та перспективи : зб. тез доп. II Міжнар. наук.-практ. конф., 22 квітня 2021 р. / КПІ ім. Ігоря Сікорського. Київ : Вид-во «Політехніка», 2021. 288 с. URL: http://confmanagement.kpi.ua/2021

19. Сливоцький А. Дж. Прорив: навч. посіб. Львів: Український Католицький Університет, 2010. 327 с.

20. Проектний менеджмент: регіональний зріз: навч. посіб. / М. П. Бутко та ін. / За заг. ред. Бутка М.П. Київ: Центр учбової літератури, 2016. 416 с.

21. Krane H. P., Rolstadås A., Olsson, N. O. E. Categorizing Risks in Seven Large Projects – Which Risks Do the Projects Focus On? Project Management Journal. 2010. Vol. 41(1). P. 81-86. https://doi.org/10.1002/pmj.20154

22. Когут І. В., Сачук С. В. Методології управління проєктами в інформаційних технологіях, їх переваги та недоліки // Міжнародний науковий журнал "Інтернаука". Серія: "Економічні науки". - 2022. - №4. https://doi.org/10.25313/2520-2294-2022-4-7957

23. Вавіленкова А. І. Аналіз гнучких методологій розробки програмного забезпечення для реалізації у командних проєктах / А. І. Вавіленкова // Вісник Національного технічного університету "ХПІ". Сер.: Нові рішення в сучасних

технологіях: зб. наук. пр. Bulletin of the National Technical University "KhPI". Ser.: New solutions in modern technology: col. of sci. papers. – Харків : НТУ "ХПІ", 2021. – № 1 (7). – С. 39-46.

24. ДеМарко Т., Лістер Т. Вальсуючи з ведмедями: управління ризиками в проектах по розробці програмного забезпечення. Пер. з англ. Київ: Вид-во "Альпіна Паблішер", 2019. 256 с.

25. Соловко Я.Т. Теорія ймовірностей та математична: навчальний посібник/ Я.Т. Соловко, П.Г. Остафійчук, О.З. Гарпуль, С.А. Войтик. – Івано- Франківськ: Симфонія форте, 2015. – 152 с.

26. Барановський О. І. Фінансові кризи: передумови, наслідки і шляхи запобігання: монографія. — К., 2009. — 220 с.

27. Гутко Л. М. Класифікація ризиків виробничо-економічної діяльності суб'єктів господарювання // Вісник БДАУ. — 2006. — Вип. 44. — С. 98–102.

28. Agile vs. waterfall project management. URL: https://www.atlassian.com/agile/project-management/project-management-intro

29. ДСТУ IEC/ISO 31010:2013. Керування ризиком. Методи загального оцінювання ризику (IEC/ІБО 31010:2009, ЮТ). [Чинний від 2013-12-11]. Київ, 2015. 79 с. (Національний стандарт України). URL: https://zakon.isu.net.ua/sites/default/files/normdocs/iso_31010.pdf

30. Federation of European Risk Management Associations. URL: https://www.ferma.eu/

31. Гонтарева І. В. Управління проектами: підручник. — Харків: ХНЕУ, 2011. — 444 с.

32. Ілляшенко С. М. Економічний ризик. Вид. 2-ге, доп. і перероб. — Київ, 2004. — 217 с.

33. Матвіїшин Є. Г. Планування проєктних дій: навч. посіб. — Київ: Хай-Тек Прес, 2008. — 216 с.

34. Башинська І. О., Новак Н. Г. Ефективне управління проектами підприємства // Інфраструктура ринку: електронний науково-практичний журнал. — 2017. — № 6. — С. 113–117.

35. Комишова Г. І., Петрова В. Ф., Соколов С. І. Методи оцінки ризиків у проєкті // Управління проектами та розвиток виробництва: зб. наук. пр. — Луганськ: СНУ ім. В. Даля, 2010. — № 3 (35). — С. 94–97.

36. Буріменко Ю. І., Галан Л. В., Лебедєва І. Ю. та ін. Управління проєктами: навч. посіб. / за ред. Ю. І. Буріменко. — Одеса: ОНАЗ ім. О. С. Попова, 2017. — 208 с.

37. Опанасюк В. А., Лебедовський В., Жарлінська Р. Г., Лісницька О. В. Дослідження ефективності системи управління ризиками // Без коріння саду не цвісти: зб. наук. пр. — Житомир: Поліський національний університет, 2022. — С. 162–164.

38. Приказюк Н. В., Мендрик Д. Є. Модель управління ризиками: еволюція та трансформація // Економіка та суспільство. — 2020. — Вип. 22. URL: https://economyandsociety.in.ua/index.php/journal/article/view/90/85 (дата звернення: 28.10.2023).

39. Рішняк І. В. Моделювання процесу управління ризиками у мультипроектному середовищі. *Вісник Національного університету «Львівська політехніка». Інформаційні системи та мережі*. 2014. № 783. С. 446–473.

40. Скопенко Н. С., Євсєєв І. В., Москаленко В. О. Управління ризиками в проєктному менеджменті. *Інвестиції: практика та досвід*. 2013. № 24. С. 41–42.

41. Вітлінський В.В. Ризикологія в економіці та підприємництві : монографія. Київ, 2004. 480 с.

42. Comparison of risk management analysis between PMBOK, ISO 31000, AS/NZS / Sari E. M., Simanjuntak M. A., Wibowo M. A., Sinaga O. // PalArch’s Journal of Archaeology of Egypt/Egyptology. 2020. No 17 (10). P. 1439–1451.

43. Power BI Documentation. Microsoft Learn. URL: https://learn.microsoft.com/en-us/power-bi/.

44. Jira Software Documentation. Atlassian. URL: https://www.atlassian.com/software/jira.

45. RiskyProject Documentation. Intaver Institute Inc. URL: https://www.intaver.com.