Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет Комп'ютерних наук
(повна назва)

Кафедра Інформаційних управляючих систем
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

Дослідження методів та моделей управління ризиками в ІТ-проєктах

(тема)

Виконав:
здобувач 2 року навчання,
групи ІУСТм-23-1
Солодовников Максим Насирович
(прізвище, ім'я, по батькові)

Спеціальність 122 Комп'ютерні науки
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Інформаційні управляючі системи та технології
(повна назва освітньої програми)

Керівник: доц. Борисенко Т.І.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри ІУС _____ Петров К.Е.
(підпис) (прізвище, ініціали)

2025 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерних наук

Кафедра Інформаційних управляючих систем

Рівень вищої освіти другий (магістерський)

Спеціальність 122 Комп'ютерні науки
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Інформаційні управляючі системи та технології
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)

" 09 " грудня 2024 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Солодовникову Максиму Насировичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження методів та моделей управління ризиками в ІТ-проєктах

затверджена наказом по університету від " 27 " листопада 2024 р. № 1249Ст

2. Термін подання здобувачем роботи до екзаменаційної комісії " 18 " січня 2025 р.

3. Вихідні дані до роботи науково-технічні публікації та інтернет джерела з тематики дослідження методів та моделей управління ризиками в ІТ-проєктах, матеріали передатестаційної практики, нормативна документація та стандарти з управління ризиками в ІТ-проєктах.

4. Перелік питань, що потрібно опрацювати у роботі провести аналіз предметної області та виконати постановку задач дослідження; дослідити основні методи та етапи управління ризиками; виконати удосконалення методу аналізу ризиків в ІТ-проєктах; розробити програмну реалізацію управління ризиками; виконати експериментальну перевірку запропонованого методу управління ризиками на прикладі тестового ІТ-проєкту.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Аналіз предметної області	09.12.2024 - 15.12.2024	Виконано
2	Постановка задач дослідження	15.12.2024 – 16.12.2024	Виконано
3	Дослідження існуючих методів управління ризиками	16.12.2024 – 18.12.2024	Виконано
4	Розробка адаптивного методу управління ризиками	21.12.2024 – 24.12.2024	Виконано
5	Реалізація та тестування запропонованого методу	25.12.2024 – 30.12.2024	Виконано
6	Порівняння ефективності з стандартним варіантом	31.12.2024	Виконано
7	Аналіз результатів експериментальної перевірки	01.01.2025 – 12.01.2025	Виконано
8	Підготовка пояснювальної записки	01.01.2025 – 12.01.2025	Виконано
9	Підготовка презентації	13.01.2025	Виконано
10	Захист кваліфікаційної роботи	21.01.2025	Виконано

Дата видачі завдання 09 грудня 2024 р.

Здобувач _____
(підпис)

Керівник роботи _____ доц. Борисенко Т.І.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 87 с., 9 рис., 9 табл., 1 дод., 24 джерела.

АНАЛІЗ РИЗИКІВ, ІНФОРМАЦІЙНА СИСТЕМА, КОНТРОЛЬ РИЗИКІВ, МОДЕЛІ УПРАВЛІННЯ РИЗИКАМИ, ОЦІНКА РИЗИКІВ, УПРАВЛІННЯ РИЗИКАМИ В ІТ-ПРОЄКТАХ, ФАЗОВІ КОЕФІЦІЄНТИ.

Об’єктом дослідження кваліфікаційної роботи є процес управління ризиками в ІТ-проєктах.

Предметом дослідження є методи та моделі управління ризиками в ІТ-проєктах з використанням сучасних інформаційних технологій.

Метою кваліфікаційної роботи є дослідження та удосконалення процесу управління ризиками в ІТ-проєктах.

Робота містить таке: аналіз предметної області та постановку задач дослідження; результати дослідження та опис вибору основних методів управління ризиками для кожного етапу управління ризиками; опис удосконалення методу аналізу ризиків в ІТ-проєктах; опис програмної реалізації системи управління ризиками в ІТ-проєкті; експериментальну перевірку запропонованого підходу до управління ризиками.

Наукова новизна дослідження полягає у розробці удосконаленого підхода до оцінки (розрахунку ваги) ризиків завдяки впровадженню динамічних вагових коефіцієнтів, які дозволяють враховувати зміну значимості різних ризиків залежно від категорії ризику, етапу проєкту чи зовнішніх обставин.

Кваліфікаційну роботу виконано згідно методичних вказівок щодо розробки та оформлення кваліфікаційної роботи [1], ДСТУ 3008:2015 [2] та ДСТУ 8302:2015 [3].

ABSTRACT

Master’s thesis: 87 pages, 8figures, 9 tables, 1 appendices, 24 sources.

INFORMATION SYSTEM, PHASE COEFFICIENTS, RISK ANALYSIS, RISK ASSESSMENT, RISK CONTROL, RISK MANAGEMENT IN IT PROJECTS, RISK MANAGEMENT MODELS.

The object of the qualification research is the process of risk management in IT projects.

The subject of the research is the methods and models of risk management in IT projects using modern information technologies.

The aim of the qualification work is to study and improve the process of risk management in IT projects.

The work includes the following: an analysis of the subject area and formulation of research tasks; research results and a description of the selection of key risk management methods for each stage of risk management; a description of the improvement of the risk analysis method in IT projects; a description of the software implementation of the risk management system in an IT project; and an experimental verification of the proposed risk management approach.

The scientific novelty of the research lies in the development of an improved approach to risk assessment (weight calculation) through the introduction of dynamic weight coefficients. These coefficients enable consideration of the changing significance of various risks depending on the risk category, project stage, or external circumstances.

The qualification work was completed in accordance with the methodological guidelines for the development and design of qualification works [1], DSTU 3008:2015 [2], and DSTU 8302:2015 [3].

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

БД – база даних

ІС – інформаційна система

ІТ – інформаційні технології

КР – контроль ризиків

ПЗ – програмне забезпечення

СУР – система управління ризиками

API – Application Programming Interface

DFD – Data Flow Diagram

IDEF – Integrated DEFinition

PMBOK - Project Management Body of Knowledge

ВСТУП

У сучасному світі інформаційних технологій ризики стають невід'ємною частиною проєктної діяльності. В умовах динамічного розвитку індустрії, швидкої зміни технологій і високої конкуренції на ринку, управління ризиками в ІТ-проєктах стає критично важливим процесом. Це організовує проєктну діяльність таким чином, щоб мінімізувати вплив потенційних проблем і підвищити ймовірність досягнення поставлених цілей.

ІТ-проєкти мають свої унікальні особливості, що зумовлюють специфіку ризиків. Це можуть бути технічні ризики, пов'язані з вибором технологій і архітектури, організаційні ризики, такі як неефективна комунікація в команді, ризики дотримання строків та бюджету, а також зовнішні ризики, включаючи появу конкурентних продуктів чи зміни у регуляторних вимогах. Усе це створює складний ландшафт ризиків, який потребує глибокого аналізу та продуманого підходу до їхнього управління.

Ефективне управління ризиками в ІТ-проєктах передбачає систематичний підхід, який охоплює виявлення, аналіз, планування реагування, моніторинг і контроль ризиків. Це дозволяє команді передбачати потенційні проблеми, швидко реагувати на зміни й адаптувати свої стратегії відповідно до актуальної ситуації. Особливу роль відіграє інтеграція сучасних інформаційних технологій, які забезпечують автоматизацію процесів управління ризиками, підвищують точність аналізу даних і покращують комунікацію між учасниками проєкту.

Ця робота присвячена дослідженню методів та інструментів управління ризиками в ІТ-проєктах, із особливим акцентом на розробці та практичному застосуванні адаптивних підходів, які враховують динаміку проєктного середовища. Результати дослідження сприятимуть підвищенню ефективності управління ризиками та забезпеченню успішного виконання ІТ-проєктів.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧ ДОСЛІДЖЕННЯ

1.1 Аналіз основ предметної області управління ризиками в ІТ-проєктах

Управління ризиками — це складова частина загальної системи управління проєктами, яка займає важливе місце в сучасному бізнесі, зокрема в ІТ-сфері. Це пояснюється тим, що розробка програмного забезпечення, впровадження нових технологій або модернізація ІТ-інфраструктури пов'язані з високим рівнем невизначеності, що робить ризик-менеджмент критично важливим процесом.

ІТ-індустрія розвивається стрімкими темпами, і кожен проєкт має унікальні особливості, які потребують специфічного підходу до оцінки ризиків. У цьому контексті вивчення теоретичних основ управління ризиками допомагає зрозуміти, як формувати стратегічний підхід до мінімізації можливих загроз і забезпечення успіху проєкту.

В сучасному світі інформаційних технологій (ІТ) реалізація проєктів стикається з численними викликами. Одним із найважливіших аспектів ефективного виконання ІТ-проєкту є управління ризиками, адже саме від здатності правильно передбачати та реагувати на потенційні загрози залежить успіх проєкту.

Ризик у контексті ІТ-проєктів — це ймовірність виникнення подій або умов, які можуть негативно вплинути на вартість, терміни, якість або цілі проєкту.

Значення управління ризиками важко переоцінити, оскільки проєкти в галузі ІТ характеризуються високим рівнем невизначеності. Висока швидкість технологічного прогресу, складність програмного забезпечення, змінність вимог замовників та обмежені ресурси створюють умови для виникнення численних ризиків. Тому теоретичні основи управління ризиками є критично важливими для проєктних менеджерів, оскільки вони дозволяють ефективно

передбачати, оцінювати та мінімізувати загрози.

Поняття управління ризиками сформувалося в другій половині XX століття, коли виникла потреба стандартизувати підходи до управління великими проєктами. У 1970-х роках The National Aeronautics and Space Administration (NASA) активно використовувала ризик-менеджмент для реалізації своїх космічних програм. Цей досвід адаптували у сферу IT, що зростала паралельно з розвитком інформаційних технологій. Визначальними стали такі етапи: 1980-ті роки - стандартизація підходів до управління проєктами через створення PMBOK (Project Management Body of Knowledge) [4], 1990-ті роки - розвиток IT-індустрії та виникнення специфічних методів ризик-менеджменту в IT, 2000-ті роки - інтеграція ризик-менеджменту у гнучкі методології, такі як Agile та Scrum.

Управління ризиками починається з розуміння їх природи. У контексті IT-проєктів ризики можуть суттєво відрізнятися залежно від типу проєкту, його масштабів та складності. На рисунку 2.1 зображено приклад розподілення ризиків за їх типом:

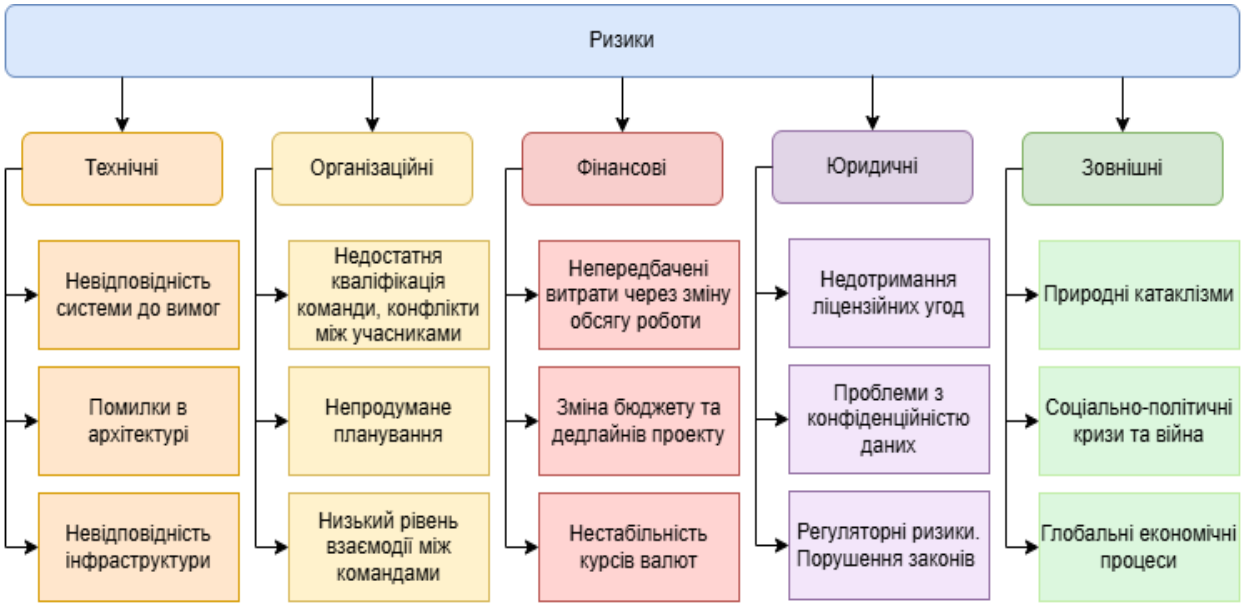

Рисунок 2.1 – Розподілення ризиків за їх типом

Детальніше розглянемо основні типи ризиків за джерелом виникненнях [5]:

а) технічні ризики:

1) невідповідність реальних можливостей системи до технічних вимог. Наприклад, під час розробки складних програмних систем може виникнути ситуація, коли обрані інструменти розробки не забезпечують потрібної продуктивності;

2) помилки в архітектурі, які стають очевидними лише на пізніх етапах реалізації. Це може призводити до переробок і значного збільшення витрат;

3) невідповідність інфраструктури потребам проєкту, наприклад, серверні ресурси не витримують навантаження після релізу.

б) організаційні ризики:

1) недостатня кваліфікація команди, конфлікти між учасниками, непродумане планування;

2) низький рівень взаємодії між командами: відсутність координації між відділом розробки та тестування часто призводить до затримок;

3) помилкове розподілення ролей: проєктний менеджер має володіти достатнім досвідом, щоб проєкт не втратив керованість.

в) фінансові ризики:

1) непередбачені витрати через зміну обсягу роботи (scope creep);

2) зміна бюджету та дедлайнів проекту;

3) курсові коливання, які впливають на бюджети міжнародних проєктів.

г) юридичні ризики:

1) недотримання ліцензійних угод, використання неліцензованого програмного забезпечення;

2) проблеми з конфіденційністю даних, які можуть призводити до штрафів

Зовнішні ризики є одним із найбільш непередбачуваних чинників, які можуть вплинути на успішність ІТ-проєктів [6]. Ці ризики виникають через обставини, що перебувають поза контролем команди або організації, але можуть суттєво впливати на терміни, бюджет і якість результату. Розглянемо основні зовнішні ризики детальніше:

а) природні катаклізми: природні явища, такі як землетруси, повені, урагани або пожежі, можуть суттєво вплинути на перебіг ІТ-проєктів [7]. Вони можуть мати негативний вплив на інфраструктуру: пошкодження дата-центрів, офісних приміщень, обладнання чи комунікаційних ліній. Наприклад, землетрус може пошкодити сервери, що унеможливить доступ до критично важливих даних. Стихійні лиха можуть призвести до евакуації персоналу, затримки або припинення роботи команд;

б) соціально-політичні кризи та війна: ІТ-проєкти нерідко залежать від стабільності в регіоні, де розташовані команди або ключові партнери. До цього типу ризику належать:

1) військові конфлікти: у ситуації війни команди можуть бути евакуйовані, виникають перебої в електропостачанні, а також проблеми з комунікацією через перебої в роботі інтернету. Наприклад, війна в Україні 2022 року змусила багато ІТ-компаній переводити своїх працівників до безпечних регіонів чи за кордон;

2) протести та політична нестабільність: демонстрації або зміни влади можуть створювати бар’єри для реалізації проєктів, зокрема через правові або економічні зміни;

3) санкції: в умовах міжнародних санкцій компанії можуть втрачати доступ до необхідного програмного забезпечення чи апаратного забезпечення;

в) економічні ризики - глобальні економічні процеси впливають на всі сфери бізнесу, включаючи ІТ-проєкти:

1) коливання валютних курсів: особливо важливо для міжнародних проєктів, де команди в різних країнах отримують оплату в

різних валютах. Наприклад, різке падіння курсу валюти може призвести до збільшення витрат на оплату праці іноземних підрядників;

2) економічні кризи: зменшення фінансування проєктів через скорочення бюджетів компаній. У кризові періоди компанії скорочують витрати, що може спричинити замороження або припинення IT-проєктів;

г) правові та регуляторні ризики:

1) зміни законодавства: впровадження нових вимог до обробки даних, наприклад, загальний регламент захисту даних (GDPR) у ЄС, може вимагати від компаній перегляду проєктної документації або внесення змін до програмного забезпечення;

2) міжнародні правові бар'єри: обмеження на експорт технологій, програмного забезпечення або доступ до іноземних ринків;

За ступенем впливу ризики поділяються на:

– критичні ризики, які загрожують завершенню проєкту;

– помірні ризики, які можна компенсувати;

– незначні ризики, що незначно впливають на процеси.

За ймовірністю виникнення розрізняють такі ризики:

– високої ймовірності - ризики, які найімовірніше реалізуються;

– середньої ймовірності;

– низької ймовірності.

Приклади ризиків в IT-проєктах включають несвоєчасне надання ресурсів, відсутність зворотного зв’язку від замовника, а також зміни вимог на пізніх етапах реалізації. Наприклад, невраховані технічні обмеження при інтеграції системи можуть значно сповільнити процес розробки.

Управління ризиками в IT-проєктах передбачає систематичний процес, що включає кілька основних етапів [8]:

– ідентифікація ризиків: це перший крок, на якому визначають потенційні загрози. Інструменти, які використовуються на цьому етапі: брейнштормінг, аналіз подібних проєктів, SWOT-аналіз (виявлення сильних і

слабких сторін, можливостей і загроз);

– якісний та кількісний аналіз ризиків: оцінка ймовірності виникнення ризику та його впливу на проєкт, також цей етап включає розрахунки для оцінки вартісного впливу ризиків, використовуючи, наприклад, метод Монте-Карло чи дерев рішень;

– планування відповідей на ризики: розробка стратегій, які можуть включати один або одразу декілька результатів. До них можна віднести уникнення ризику (внесення змін у план для запобігання його виникненню), перенесення ризику (передача ризику на сторонні організації наприклад, страхування), зменшення ризику (впровадження дій для зниження його впливу), прийняття ризику (свідоме залишення ризику в плані);

– моніторинг і контроль: регулярний перегляд плану управління ризиками, внесення коригувань у відповідь на змінення умов проєкту.

Для ефективного управління ризиками широко використовуються такі інструменти, як матриця ризиків, яка дозволяє візуалізувати пріоритетність ризиків, та метод аналізу впливу для оцінки найбільш критичних загроз.

Існує кілька популярних моделей і підходів до управління ризиками, які широко застосовуються в галузі IT [9]:

– PMBOK (Project Management Body of Knowledge) – він пропонує детальний підхід до управління ризиками. Цей підхід включає такі шість процесів: планування управління ризиками, ідентифікація ризиків, виконання якісного та кількісного аналізу, розробка відповідей на ризики, контроль ризиків;

– PRINCE2 – ця методологія базується на принципах чіткого розподілу відповідальності та активного залучення замовників. Ризики оцінюються на кожному етапі життєвого циклу проєкту;

– Agile – в умовах Agile підходу управління ризиками відбувається інтерактивно протягом усього проєкту. Завдяки коротким ітераціям команда може швидко реагувати на зміни та адаптуватися до нових умов;

– Scrum – у Scrum ризики обговорюються під час спринт-планування, а

їхнє вирішення інтегрується в беклог.

Успішне впровадження управління ризиками вимагає дотримання кількох принципів:

– інтеграція ризик-менеджменту в загальний процес проєкту. Це дозволяє створити системний підхід;

– підвищення культури управління ризиками в команді. Регулярне навчання учасників команди допомагає вчасно ідентифікувати та усувати загрози;

– використання автоматизованих інструментів. Сучасні програми, такі як Jira, Trello, або Microsoft Project, мають інтегровані функції для управління ризиками;

Уявімо ситуацію, коли IT-компанія працює над створенням мобільного додатка. Один із ризиків полягає в можливому зриві дедлайнів через недостатню кваліфікацію команди. Для мінімізації ризику керівництво вирішує організувати додаткове навчання. Результат: дедлайни витримані, ризик усунутий.

Управління ризиками є важливим компонентом успішної реалізації IT-проєктів. Систематичний підхід до ідентифікації, аналізу, оцінки та мінімізації ризиків дозволяє підвищити ефективність роботи команди та забезпечити досягнення цілей проєкту. Завдяки впровадженню моделей управління ризиками, таких як PMBOK, PRINCE2 або Agile, IT-компанії отримують змогу адаптуватися до мінливих умов та знижувати вплив невизначеності. Перспективи розвитку цієї сфери пов’язані з активним використанням штучного інтелекту та автоматизації, що відкриває нові горизонти в мінімізації ризиків.

1.2 Аналіз методів і моделей для оцінки та управління ризиками

1.2.1 Аналіз моделей управління ризиками, які використовуються в IT-проєктах

Управління ризиками в IT-проєктах є одним із ключових напрямів діяльності проєктних менеджерів, адже саме здатність передбачити та ефективно реагувати на потенційні загрози часто визначає успішність реалізації проєкту. Для цього використовуються різноманітні моделі, кожна з яких пропонує певний набір методів і підходів, спрямованих на зменшення впливу невизначеності.

Найбільш поширеними моделями в IT-сфері є PMBOK, PRINCE2, Agile та інші, які були адаптовані для управління ризиками з урахуванням специфіки цієї галузі. Їх детальний аналіз дозволяє зрозуміти, які з них найбільш ефективні для конкретних типів проєктів.

Однією з найвідоміших моделей є PMBOK (Project Management Body of Knowledge), яка була розроблена Інститутом управління проєктами (PMI). Ця модель пропонує системний підхід до управління ризиками, який охоплює всі етапи життєвого циклу проєкту. Зокрема, вона включає процеси планування, ідентифікації, якісного та кількісного аналізу, а також розробки відповідей на ризики та їх подальшого моніторингу.

Планування управління ризиками, що є першим етапом у цій моделі, передбачає створення спеціального документа, який описує підходи, інструменти та методи, що будуть застосовуватися для роботи з ризиками. Цей етап забезпечує основи для подальшої діяльності та дозволяє команді підготуватися до майбутніх викликів.

Ідентифікація ризиків, яка є наступним кроком, базується на аналізі даних, зібраних із попередніх проєктів, використанні експертних оцінок та застосуванні таких інструментів, як SWOT-аналіз [10]. У процесі ідентифікації команда формує перелік можливих ризиків, які можуть виникнути в ході

реалізації проєкту. Це дозволяє проєктним менеджерам заздалегідь оцінити, які аспекти можуть потребувати додаткової уваги. Якісний аналіз ризиків, що слідує за цим, допомагає визначити пріоритетність ризиків шляхом оцінки ймовірності їх виникнення та рівня впливу на проєкт. У цьому контексті часто використовується матриця ризиків, яка дозволяє візуалізувати результати аналізу та виділити найбільш критичні ризики.

Кількісний аналіз ризиків, який є однією з найважливіших складових моделі PMBOK, спрямований на глибше розуміння потенційних загроз за допомогою математичних методів. Наприклад, використання методу Монте-Карло [11] дозволяє моделювати різні сценарії розвитку подій і визначити, як зміни у певних параметрах можуть вплинути на загальні результати проєкту. Це дає можливість краще підготуватися до ймовірних викликів і створити більш точний план реагування. Після цього розробляються конкретні стратегії роботи з ризиками. Серед таких стратегій можна виділити уникнення ризику, яке передбачає внесення змін до плану проєкту для запобігання його виникненню; зменшення впливу ризику за рахунок попереджувальних заходів; передачу ризику шляхом делегування відповідальності, наприклад, через страхування; і прийняття ризику, коли команда готова свідомо працювати з потенційною загрозою без додаткових змін.

Завершальним етапом управління ризиками в моделі PMBOK є моніторинг і контроль, які забезпечують постійне відстеження і коригування плану управління ризиками в процесі реалізації проєкту. Ця частина процесу є надзвичайно важливою, оскільки ризики можуть змінюватися впродовж життєвого циклу проєкту, а моніторинг дозволяє оперативно реагувати на нові загрози. Завдяки цьому модель PMBOK забезпечує систематичний та універсальний підхід, який можна адаптувати для роботи з різними типами проєктів у сфері інформаційних технологій.

PMBOK є надзвичайно популярною моделлю в IT-сфері через її гнучкість та універсальність. Вона дозволяє адаптувати методи управління ризиками до потреб конкретного проєкту, що особливо важливо в умовах

динамічного розвитку інформаційних технологій. Однак слід зазначити, що її застосування потребує значних зусиль на етапі планування та підготовки, а також високої кваліфікації команди, що може стати викликом для невеликих компаній або стартапів.

Загалом, аналіз моделі PMBOK показує, що вона є ефективним інструментом для управління ризиками в IT-проєктах, особливо в тих, що характеризуються високим рівнем складності та значними обсягами робіт. Її системний підхід дозволяє не лише мінімізувати вплив потенційних загроз, але й забезпечити загальну ефективність роботи команди, що робить її незамінним інструментом у сучасному управлінні проєктами.

1.2.2 Аналіз інструментів для управління ризиками

Управління ризиками є критично важливим етапом у процесі реалізації IT-проєктів, оскільки невизначеність і потенційні загрози можуть суттєво вплинути на успішність проєкту. Тому розуміння та правильний вибір інструментів для ефективного управління ризиками допомагає забезпечити стабільний розвиток проєкту, зменшити ймовірність виникнення непередбачених проблем і оптимізувати ресурси.

Управління ризиками в IT-проєктах є важливою складовою частиною процесу їхнього виконання. IT-проєкти часто характеризуються великою невизначеністю через технологічні складнощі, зміни у вимогах замовників, вплив зовнішніх факторів та багатозадачність. Зважаючи на ці особливості, управління ризиками набуває критичної значущості для успішної реалізації проєктів. Для ефективного управління ризиками існує безліч інструментів і методик, що можуть бути використані на різних етапах проєкту. Вибір інструментів для управління ризиками залежить від специфіки конкретного проєкту, його масштабу, а також доступних ресурсів і компетенцій команди.

Розглянемо детальніше основні інструменти та методи, що використовуються для аналізу та управління ризиками в ІТ-проєктах.

Управління ризиками в ІТ-проєктах можна здійснювати за допомогою кількох основних стратегій: уникнення, зменшення, перенесення та прийняття ризиків. Кожна з цих стратегій може бути реалізована за допомогою різних інструментів:

– уникнення ризиків передбачає запобігання ситуаціям, які можуть призвести до ризиків. Це може включати в себе зміну плану проєкту або вибір іншої технології для уникнення потенційних проблем. Для цього часто використовуються інструменти для прогнозування можливих загроз, такі як сценарне планування або метод Монте-Карло;

– зменшення ризиків полягає в тому, щоб знизити ймовірність виникнення ризиків або їхній вплив на проєкт. Застосовуються різні техніки, як от визначення резервних планів, створення буферів часу або використання контролів якості для зменшення ймовірності помилок. Для цього можна використовувати такі інструменти, як матриця ризиків або інші техніки моніторингу;

– перенесення ризиків означає переміщення ризиків на інші сторони, наприклад, за допомогою аутсорсингу або використання страхових механізмів. Інструменти для цього включають в себе договори про аутсорсинг або страхування ризиків;

– прийняття ризиків може бути доцільним, коли ймовірність ризику є дуже низькою, а його вплив не є значним. В цьому випадку інструменти можуть включати методи моніторингу, щоб своєчасно реагувати на зміни та коригувати план проєкту.

Сучасні програмні інструменти для управління ризиками є важливою складовою частиною успішного управління ІТ-проєктами. Вони дають змогу зібрати всі дані, пов'язані з ризиками, в одному місці, проводити їх аналіз, прогнозувати потенційні загрози та відстежувати прогрес у зменшенні ризиків. Деякі з популярних програмних засобів управління ризиками:

– Microsoft Project є одним з найбільш поширених інструментів для управління проєктами, що містить вбудовані функції для відстеження ризиків.

– Jira [12] дозволяє не лише відстежувати задачі, але й реалізовувати підхід до управління ризиками через створення спеціальних категорій для ризиків і їхніх статусів;

– Trello — інструмент, який підходить для візуалізації задачі, що стосуються ризиків, і на основі цих карток спільно з командою визначати стратегії їх зменшення або усунення;

– Risk Register та RiskWatch — спеціалізовані програмні платформи для управління ризиками. Вони дозволяють здійснювати реєстрацію ризиків, оцінювати їх ймовірність та вплив, створювати відповідні стратегії та відстежувати прогрес.

Методи аналізу ризиків є основою для вибору і застосування правильних інструментів в процесі управління ризиками. Існує кілька популярних методик, які широко використовуються для аналізу ризиків в IT-проєктах:

– SWOT-аналіз дозволяє виявити сильні та слабкі сторони проєкту, а також можливості і загрози, що допомагає сформулювати стратегію для управління ризиками. Цей інструмент дозволяє на ранніх етапах проєкту оцінити, де можуть виникнути потенційні проблеми і які заходи слід вжити для їх усунення;

– аналіз сценаріїв полягає в оцінці різних можливих варіантів розвитку подій у проєкті. Сценарії можуть бути оптимістичними, песимістичними або базовими, і це допомагає розробити план для кожного з них. Такий підхід дозволяє вчасно передбачити зміни і підготуватися до непередбачуваних ситуацій;

– метод Монте-Карло — це статистичний метод, що дозволяє оцінити ймовірність різних результатів, враховуючи невизначеність вхідних даних. Цей метод дозволяє моделювати ймовірність настання ризиків, розраховуючи їхні впливи на результати проєкту. Цей інструмент особливо корисний для великих і складних IT-проєктів.

Для того щоб управління ризиками було ефективним, необхідно розробити систему показників ефективності (KPI). Визначення таких показників дозволяє оцінювати, наскільки ефективно вжиті заходи щодо мінімізації або усунення ризиків. Основні KPI для управління ризиками в IT-проєктах можуть включати:

– час на виявлення ризиків — скільки часу потрібно для виявлення потенційної загрози для проєкту. Швидке виявлення ризиків дозволяє вжити заходів до того, як вони стануть критичними;

– вартість вирішення ризиків — скільки коштує мінімізувати або усунути ризик. Важливо порівнювати витрати на вирішення ризику з можливими втратами, які він може спричинити;

– ймовірність та вплив ризиків — визначення ймовірності виникнення ризику і його потенційного впливу на проєкт. Від цього залежить вибір стратегії управління;

– ефективність заходів щодо зменшення ризиків — оцінка того, наскільки успішно вжиті заходи для зменшення впливу ризиків. Цей показник дозволяє оцінити, чи правильно були обрані стратегії для управління ризиками.

З розвитком технологій з'являються нові інструменти і підходи до управління ризиками: інтернет речей (IoT), великий аналіз даних (Big Data), штучний інтелект (AI) — усі ці інновації відкривають нові можливості для виявлення та управління ризиками. Великий аналіз даних дозволяє аналізувати великі обсяги інформації про ризики, що виникають у процесі виконання IT-проєктів. За допомогою таких платформ, як Hadoop або Spark, можна виявляти закономірності і передбачати можливі загрози, штучний інтелект може допомогти автоматизувати процеси виявлення та управління ризиками. Наприклад, алгоритми машинного навчання можуть використовуватися для прогнозування ймовірності виникнення ризиків на основі попереднього досвіду.

1.3 Аналіз існуючих аналогів та рішень для управління ризиками

Сьогодні існує багато програмних продуктів, які пропонують інтерфейси та функціональність для комплексного управління ризиками в IT-проєктах. Вони дозволяють автоматизувати процеси і значно зменшити людський фактор в управлінні ризиками. Розглянемо основні програми, що найбільш часто використовуються в IT-сфері для управління ризиками.

Microsoft Project є одним з найпоширеніших інструментів для управління проєктами, що включає функції для управління ризиками. Він дозволяє визначати ймовірність ризиків, їхній вплив та пріоритизацію за допомогою графіків та таблиць, а також пропонує можливості для аналізу ресурсів і бюджетів проєкту. До переваг та недоліків використання цього продукту можна віднести:

– інтерфейс Microsoft Project добре інтегрується з іншими продуктами Microsoft (Excel, Power BI), що забезпечує зручний доступ до даних і звітів;

– можливість створення детальних планів і графіків проєктів з урахуванням усіх ризиків і змін;

– потужні інструменти для аналізу варіантів розвитку ситуацій і оцінки потенційних ризиків;

– підтримка роботи в команді, що дозволяє кільком користувачам одночасно працювати з проєктом та оновлювати дані;

– висока ціна ліцензії, що може бути не по кишені для малих компаній або стартапів;

– складність у навчанні і адаптації для нових користувачів, особливо для тих, хто не знайомий з програмами Microsoft;

– обмежена гнучкість в порівнянні з іншими інструментами, такими як Jira чи Trello, коли йдеться про швидке оновлення чи модифікацію планів в реальному часі.

Microsoft Project підходить для великих IT-проєктів з комплексними

ризиками, де важлива інтеграція з іншими інструментами Microsoft. Однак через високу вартість і складність програмного забезпечення, він може бути менш придатним для невеликих команд або проєктів.

Jira — популярний інструмент для управління проєктами в методології Agile, особливо в командах розробників програмного забезпечення. Jira дозволяє створювати завдання для вирішення ризиків, а також відстежувати їхній статус і пріоритетність. Вона підтримує роботу з ризиками в реальному часі, дозволяючи виявляти проблеми в процесі розробки й одразу призначати відповідальних осіб для їх вирішення. Можна виділити наступний список переваг та недоліків використання Jira:

– гнучкість і можливість налаштування під будь-яку специфіку проєкту;

– інтуїтивно зрозумілий інтерфейс і простота у використанні для команди розробників;

– вбудована підтримка методологій Scrum і Kanban для управління задачами і ризиками в рамках Agile;

– потужна інтеграція з іншими інструментами для моніторингу і автоматизації, такими як Bitbucket і Confluence;

– обмежена функціональність для управління більш складними або глобальними ризиками, що потребують комплексного планування;

– для початкових користувачів Jira може здаватися складною, особливо для тих, хто не знайомий із принципами Agile;

– вартість підписки на базовий пакет, який може бути досить дорогим для невеликих компаній або команд.

Jira ідеально підходить для середніх і великих IT-команд, що працюють за методологією Agile і мають потребу в постійному моніторингу ризиків на різних етапах розробки. Вона буде найбільш корисною для проєктів, де важливо працювати в режимі реального часу та швидко реагувати на зміни

Trello є простим у використанні інструментом для управління завданнями та рисками, який підходить для малих команд і проєктів. За допомогою візуальних дощок користувачі можуть організовувати завдання,

що стосуються ризиків, і виявляти потенційні проблеми на ранніх етапах. Переваги та недоліки:

– легкість у використанні та налаштуванні, що робить Trello ідеальним для невеликих команд або стартапів;

– можливість швидко змінювати статуси завдань, візуалізувати етапи роботи і ризики на дошках;

– безкоштовна версія, що підходить для команд з обмеженим бюджетом;

– вбудовані інструменти для комунікації та обміну інформацією між членами команди;

– обмежені функціональні можливості для складних і великих проєктів. Для складніших завдань потрібно інтегрувати Trello з іншими інструментами;

– немає потужних аналітичних функцій, таких як в Microsoft Project чи Jira;

– не підходить для великих команд з великою кількістю завдань та ризиків, що потребують більш складного управління.

RiskWatch — спеціалізоване програмне забезпечення для управління ризиками, яке дозволяє компаніям оцінювати, реєструвати і відслідковувати ризики на кожному етапі проєкту. RiskWatch включає функції для автоматичного оцінювання впливу ризиків, розрахунку їхнього впливу на бюджети та терміни виконання проєктів. Має наступні переваги та недоліки:

– система надає комплексний підхід до оцінки ризиків, включаючи фінансові та технологічні аспекти;

– інструменти для автоматизації і прогнозування ризиків дозволяють своєчасно реагувати на можливі проблеми;

– можливість інтеграції з іншими програмами для автоматизації процесів (наприклад, Microsoft Project або Jira);

– спеціалізація на управлінні ризиками, що дозволяє зосередитися виключно на цьому аспекті проєкту;

– висока вартість ліцензії та обмеження у функціях без додаткових

платних модулів;

– вимагає навчання для ефективного використання через свою складність і спеціалізацію;

– може бути надмірно складним для малих проєктів або команд.

RiskWatch — потужне рішення для великих компаній і проєктів, де потрібно детально управляти ризиками на різних етапах. Воно підходить для проєктів з високим рівнем складності, але може бути занадто дорогим і складним для малих компаній.

Існуючі програмні рішення для управління ризиками мають різні можливості та підходи. Вибір оптимального інструменту залежить від розміру проєкту, бюджету та специфіки роботи команди. Для великих і складних проєктів, де важливо здійснювати детальний аналіз і прогнозування є неймовірно важливим правильно віднестись до вибору програмного забезпечення по управлінню ризиками.

1.4 Постановка задач магістерської кваліфікаційної роботи

Об'єктом дослідження магістерської кваліфікаційної роботи є процес управління ризиками в ІТ-проектах.

Предметом дослідження є моделі та методи, які використовуються для ефективного управління ризиками в ІТ-проєктах

У процесі дослідження методів управління ризиками в ІТ-проєктах було виявлено кілька важливих проблем, які можуть значною мірою впливати на ефективність управління ризиками та успішність проєктів. Серед таких проблем можна виокремити невизначеність у визначенні та оцінці ризиків на різних етапах проєкту, що часто призводить до труднощів у прогнозуванні можливих загроз. Також спостерігається значне навантаження на ресурси і час, коли мова йде про складні багатофункціональні проєкти, що вимагають

постійного моніторингу ризиків та адаптації до змін. Крім того, існує проблема низької ефективності виявлення та моніторингу ризиків в умовах, коли проєкти розвиваються в реальному часі, а зміни можуть виникати швидко і без попередження. Одним із основних викликів є відсутність інтеграції між різними інструментами управління проєктами та управління ризиками, що ускладнює процеси оцінки та моніторингу ризиків, а також підвищує ймовірність упущення важливих аспектів.

Ураховуючи ці проблеми, стає очевидною необхідність створення нових підходів до управління ризиками, які були б ефективнішими та більш адаптованими до сучасних умов. Зокрема, важливо розробити методи і інструменти, що дозволяють більш точно і швидко оцінювати ризики, надавати чіткі рекомендації щодо їх мінімізації і забезпечувати інтеграцію різних етапів управлінської діяльності в рамках одного програмного середовища.

Таким чином, основною метою дослідження є аналіз існуючих підходів до управління ризиками в ІТ-проєктах, виявлення їхніх переваг і недоліків, а також розробка рекомендацій та нових рішень, що дозволяють підвищити ефективність цього процесу.

В ході виконання магістерської роботи необхідно буде вирішити такі задачі:

– провести детальний аналіз існуючих методів і моделей управління ризиками в ІТ-проєктах, вивчаючи їх застосування в різних типах проєктів і їхню здатність забезпечувати ефективне управління;

– дослідити ключові фактори, що впливають на ефективність управління ризиками, і визначити критерії, за якими оцінюється успішність таких процесів;

– розробити вдосконалений метод управління ризиками в ІТ-проєктах;

– розробити рішення з програмної реалізаціїї вдосконаленого метода управління ризиками в ІТ-проєктах;

– виконати експериментальну перевірку вдосконаленого методу.

Цей метод дозволить спростити процеси виявлення, оцінки та контролю ризиків, а також покращити взаємодію між керівниками проєктів, технічними фахівцями та іншими учасниками команди. Використання цього методу дозволить не тільки точніше оцінювати можливі ризики, але й своєчасно реагувати на їхні зміни, що значно підвищить ймовірність успішного завершення проєктів. Зокрема, завдяки інтеграції з іншими інструментами управління проєктами, це рішення забезпечить прозорість та ефективність управлінських процесів, зменшуючи час на виконання рутинних завдань.

2 МЕТОДИ ТА ЕТАПИ УПРАВЛІННЯ РИЗИКАМИ. УДОСКОНАЛЕННЯ АНАЛІЗУ РИЗИКІВ

2.1 Основні етапи управління ризиками в IT-проєктах

2.1.1 Виявлення внутрішніх та зовнішніх чинників впливу

Для успішного управління ризиками в IT-проєктах важливо визначити всі можливі чинники, які можуть впливати на реалізацію завдань, досягнення поставлених цілей та загальну успішність проєкту [14]. Ці чинники можна класифікувати на внутрішні, які залежать від самого проєкту та його учасників, та зовнішні, що залежать від навколишнього середовища. Розуміння їхньої природи та можливих впливів є важливим для ефективного управління ризиками та запобігання потенційним проблемам.

Внутрішні чинники безпосередньо пов'язані з організаційними, технічними та людськими аспектами проєкту. До основних внутрішніх чинників належать:

– людські ресурси – наявність кваліфікованої команди є ключовим аспектом успішного виконання проєкту. Недостатня кваліфікація або недосвідченість співробітників може спричинити затримки чи погіршення якості виконання завдань;

– матеріальні ресурси – відсутність необхідного апаратного чи програмного забезпечення, недостатній бюджет або обмеження в інфраструктурі можуть значно вплинути на реалізацію проєкту;

– організаційна структура – ефективність управління проєктом значною мірою залежить від комунікацій всередині команди, рівня підтримки менеджменту та наявності чіткої організаційної структури;

– якість планування – нереалістичні строки виконання, недостатньо детальний план чи неадекватний розподіл завдань можуть спричинити значні ризики на всіх етапах проєкту;

– поточний стан проєкту – виявлення проблем у ранній стадії

(наприклад, затримки в термінах або перевищення бюджету) допомагає оцінити поточний вплив ризиків і розробити відповідні коригувальні заходи.

Зовнішні чинники не залежать від внутрішніх процесів проєкту, проте можуть значно впливати на його результати [11]. Основними зовнішніми чинниками є:

– економічні – зміни у фінансових умовах, інфляція, нестабільність валютного курсу або скорочення інвестицій можуть обмежити доступ до фінансування;

– політичні – законодавчі зміни, регулювання галузі або політична нестабільність можуть створити додаткові перешкоди для виконання проєкту;

– технологічні – постійний розвиток технологій та поява нових стандартів можуть вимагати адаптації проєкту до нових умов;

– соціальні – зміни в уподобаннях споживачів, громадська думка чи тренди можуть вплинути на попит на кінцевий продукт;

– природні – форс-мажорні обставини, такі як стихійні лиха, можуть призводити до зривів у реалізації проєкту.

Таким чином, виявлення внутрішніх та зовнішніх чинників впливу є важливим етапом у процесі управління ризиками. Результати цього етапу забезпечують основу для ідентифікації ризиків, проведення їх аналізу та розробки плану реагування, що є важливим для підвищення ефективності реалізації ІТ-проєкту.

Далі у таблиці 2.1 буде наведено інформація, яка може бути використана для ідентифікації внутрішніх чинників впливу на ризики в ІТ-проєкті. У таблиці враховані ключові аспекти, які можуть впливати на проєкт.

Таблиця 2.1 – Внутрішні чинники впливу на ІТ-проєкт

Чинник	Вплив	Пріоритет
Організаційна структура	Уповільнення процесів ухвалення рішень через багаторівневу ієрархію.	Високий
Кваліфікація персоналу	Недостатній рівень навичок у команди для виконання ключових завдань.	Високий
Управління ресурсами	Дефіцит фінансування або перевантаження персоналу	Середній
Комунікація в команді	Непорозуміння між членами команди щодо вимог або термінів виконання	Високий
Технічна інфраструктура	Застаріле обладнання або недостатня потужність серверів	Середній
Культура управління ризиками	Відсутність чіткого плану роботи з ризиками або небажання визнавати ризики	Низький

У таблиці 2.2 наведено перелік зовнішніх чинників впливу та їх пріоритетність.

Таблиця 2.2 – Зовнішні чинники впливу на ІТ-проєкт

Чинник	Вплив	Пріоритет
Економічна ситуація	Зростання витрат на ресурси через інфляцію або коливання валютних курсів.	Високий
Політична стабільність	Ризики через зміну регуляторних вимог або політичну нестабільність у регіоні.	Середній
Соціокультурні аспекти	Бар’єри взаємодії через різницю у мовах або культурах в міжнародних командах	Середній
Технологічний прогрес	Швидка застарілість використовуваних технологій через інновації.	Високий

Продовження таблиці 2.1

Чинник	Вплив	Пріоритет
Екологічні умови	Перебої у роботі через стихійні лиха або природні катастрофи.	Низький
Конкуренція	Ризики втрати ринкової частки через вихід на ринок нових конкурентів або появу альтернативних рішень.	Середній

2.1.2 Ідентифікація ризиків: методи та інструменти

Ідентифікація ризиків є важливим етапом процесу управління ризиками [15], оскільки від її якості залежить ефективність усіх подальших дій. Головна мета цього етапу полягає у виявленні всіх потенційних ризиків, які можуть вплинути на проєкт, класифікації їх за джерелами та визначенні ступеня їх критичності для успішної реалізації проєкту.

Існує кілька методів ідентифікації ризиків, які можуть використовуватися залежно від специфіки проєкту. Одним із найпоширеніших є метод мозкового штурму, який передбачає залучення всієї команди проєкту для спільного обговорення можливих ризиків. Цей метод дозволяє генерувати велику кількість ідей, але потребує чіткої модерації для уникнення хаосу. Іншим ефективним підходом є метод номінальних груп, у якому задіюється група експертів, що формулюють ризики та обговорюють їх для подальшого ранжування. Цей метод забезпечує глибокий аналіз, але потребує більше часу та залежить від компетентності залучених експертів.

SWOT-аналіз є ще одним ефективним методом, який дозволяє оцінити сильні та слабкі сторони проєкту, а також виявити можливості та загрози [16]. Це сприяє не тільки ідентифікації ризиків, але й розумінню їхнього впливу на проєкт. Аналіз уроків минулого також заслуговує на увагу, оскільки

використовує історичні дані про ризики з аналогічних проєктів, що дає змогу робити прогнози на основі реального досвіду. Однак важливо враховувати, що застарілі дані можуть бути непридатними для нових умов.

Інтерв'ю з зацікавленими сторонами є корисним інструментом для отримання інформації про ризики від клієнтів, спонсорів або інших стейкхолдерів [17]. Це дає змогу врахувати специфіку проєкту, але вимагає обережного підходу через можливість суб'єктивності відповідей. Аналіз сценаріїв також є популярним методом, який передбачає моделювання можливих сценаріїв розвитку подій та визначення ризиків, що можуть виникнути у кожному сценарії. Цей підхід забезпечує деталізований аналіз, але є більш складним та трудомістким.

Інструменти ідентифікації ризиків допомагають структурувати інформацію. Матриця ризиків, наприклад, є зручним візуальним засобом для визначення ймовірності та впливу ризику. Вона полегшує пріоритизацію ризиків і сприяє ухваленню зважених рішень. Також можуть використовуватися шаблони чек-листів, які включають попередньо визначені категорії ризиків та запитання, що допомагають не пропустити важливі аспекти під час ідентифікації.

Таким чином, використання різноманітних методів і інструментів у процесі ідентифікації ризиків дозволяє підвищити її якість, забезпечуючи точність і повноту отриманих даних. Це створює основу для подальшого якісного аналізу та управління ризиками.

У нашому випадку для ідентифікації ризиків у IT-проєкті ми обрали метод спілкування з експертами як найбільш надійний та безпечний варіант. Цей підхід передбачає проведення консультацій з фахівцями, які мають багатий досвід у сфері управління проєктами, розробки програмного забезпечення та аналізу ризиків. Залучення експертів дозволяє виявити широкий спектр ризиків, включаючи специфічні для конкретного проєкту чи галузі, які могли б залишитися непоміченими при використанні інших методів.

Основною перевагою цього методу є можливість отримати глибокий і

детальний аналіз ризиків завдяки залученню професіоналів із практичним досвідом. Експерти можуть не лише ідентифікувати ризики, але й оцінити їхню ймовірність та вплив, базуючись на своїх знаннях та аналізі попередніх проєктів. Це знижує ймовірність суб'єктивних помилок, які можуть виникнути при використанні автоматизованих чи шаблонних підходів.

Метод спілкування з експертами також дозволяє враховувати поточні тренди, зміни у технологіях, нормативному середовищі чи ринку, що робить аналіз більш актуальним [18]. Окрім того, він сприяє розвитку командного підходу, оскільки експерти можуть поділитися своїми знаннями з командою проєкту, підвищуючи її загальний рівень компетенції у сфері управління ризиками.

Застосування цього методу у нашому дослідженні забезпечить точну ідентифікацію ризиків і створить основу для подальшого їх якісного та кількісного аналізу. Це дозволить розробити ефективний план реагування та мінімізувати негативний вплив ризиків на реалізацію проєкту.

2.1.3 Якісний та кількісний аналіз ризиків

Аналіз ризиків є одним з ключових етапів управління ризиками, що дозволяє не лише ідентифікувати потенційні загрози, але й оцінити їхню вагомість та вплив на проєкт. Якісний та кількісний аналіз ризиків забезпечує основу для прийняття обґрунтованих управлінських рішень, спрямованих на зменшення впливу ризиків або їх повне усунення.

Метою якісного аналізу є систематизація ризиків, оцінка їхньої ймовірності та потенційного впливу на виконання проєкту. Основні аспекти якісного аналізу включають:

– класифікація ризиків – ідентифіковані ризики групуються за категоріями, такими як фінансові, технічні, організаційні чи зовнішні. Це

дозволяє структурувати дані та зосередитися на найбільш критичних аспектах;

– оцінка ймовірності ризиків – для кожного ризику визначає ступінь його ймовірності. Для цього можуть використовуватися експертні оцінки, які розділяють ризики на категорії, наприклад: низька, середня, висока ймовірність;

– оцінка впливу ризиків – вплив ризиків на проєкт оцінюється за шкалою, наприклад: незначний, помірний, значний, критичний. Ця оцінка базується на потенційних наслідках для строків, бюджету, якості чи ресурсів проєкту;

– матриця ризиків – використовується для візуалізації результатів аналізу. Матриця складається з двох осей: ймовірності виникнення ризиків та їхнього впливу [19]. Вона дозволяє ідентифікувати ризики, які потребують першочергової уваги.

Кількісний аналіз поглиблює результати якісного аналізу, надаючи числову оцінку ймовірності та впливу ризиків. У нашому випадку буде використано такі підходи:

– розрахунок вагових коефіцієнтів ризиків – вагові коефіцієнти визначаються на основі значущості ризику для проєкту. Цей підхід враховує зміну впливу ризику залежно від фази проєкту та зовнішніх чинників;

– адаптивна модель аналізу ризиків – ми використовуватимемо модель, яка враховує динамічні зміни ваги ризиків на різних етапах проєкту. Наприклад, ризики, пов'язані з технологічними складнощами, можуть мати більший вплив на початкових етапах, тоді як фінансові ризики стають критичними ближче до завершення;

– сценарний аналіз – моделювання можливих сценаріїв розвитку подій допомагає оцінити, як різні ризики можуть вплинути на проєкт у разі їх виникнення. Наприклад, можна оцінити фінансові втрати за сценарієм затримки виконання ключових етапів проєкту.

Для проведення якісного та кількісного аналізу ризиків буде використано дані, отримані на етапі їхньої ідентифікації. Зібрані дані будуть

класифіковані, проаналізовані та внесені до матриці ризиків. Надалі, із застосуванням адаптивної моделі, будуть розраховані вагові коефіцієнти ризиків для кожного сценарію, після чого результати аналізу використовуватимуться для розробки плану реагування.

Цей підхід забезпечить практичну цінність у рамках експериментальної перевірки, дозволяючи оцінити ефективність запропонованого методу управління ризиками у реальних умовах.

2.2 Удосконалення підходу до аналізу ризиків

Класична матриця ризиків є популярним інструментом для оцінки й управління ризиками в проєктах [19]. Вона зазвичай складається з двовимірної таблиці, де одна вісь представляє ймовірність виникнення ризику (наприклад, низька, середня, висока), а інша – вплив цього ризику на проєкт (наприклад, незначний, помірний, критичний). Кожен ризик класифікується за цими двома параметрами, що дозволяє розмістити його в одній із клітинок матриці. Далі на рисунку 2.1 наведено приклад матриці ризиків, яка може бути використана у проєкті.

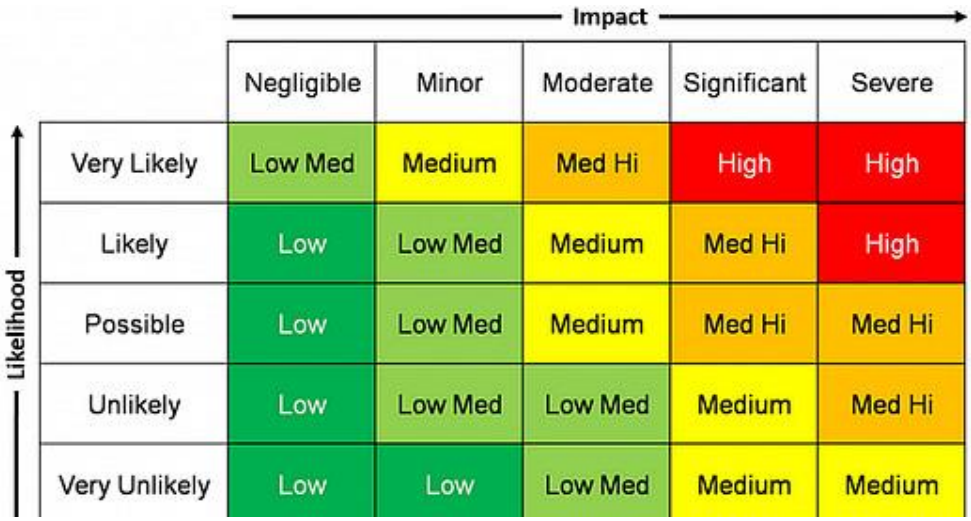

Рисунок 2.1 – Приклад матриці ризиків

Важливою характеристикою ризику є його вага. Вона використовується щоб структуровано підходити до управління ризиками, забезпечувати кількісну оцінку ризиків для прийняття зважених рішень, а саме виділення додаткових ресурсів, планування дій, аналізу впливу змін або пріоритизації завдань у рамках проєкту. Вага ризику дає змогу структурно та прозоро підходити до таких рішень, визначаючи найкритичніші аспекти, які потребують першочергової уваги.

Для визначення ваги ризику використовується формула (2.1):

$$R = P \times I \tag{2.1}$$

де P – ймовірність виникнення ризику;

I – вплив ризику за рейтинговою шкалою, де 1 – низький вплив на строки виконання проекту, якість або вартість, 5 – високий вплив.

Ця формула дозволяє визначити базову вагу ризику (R), який є показником важливості ризику. Чим більший результат, тим серйозніший ризик і тим більше уваги він потребує.

Для вдосконалення аналізу ризиків в IT-проєктах пропонується модифікація формули розрахунку ваги ризика, яка спрямована на підвищення точності й адаптивності до умов проєкту та зовнішнього середовища, що змінюється. Це досягається завдяки впровадженню динамічних вагових коефіцієнтів, які дозволяють враховувати зміну значимості різних ризиків залежно від категорії ризику, етапу проєкту чи зовнішніх обставин.

Також пропонується використати метод аналізу сценаріїв, який дозволяє прогнозувати ймовірність виникнення ризиків і оцінювати їхній потенційний вплив за різних умов. Це допомагає побудувати більш детальну і реалістичну картину можливих ситуацій, визначити, які ризики потребують негайного реагування, а які – можуть бути відкладені.

З врахуванням динамічних вагових коефіцієнтів вага ризику (R_{score}) розраховується за формулою (2.2):

$$R_{score} = F_{phase} \times W \times P \times I \quad (2.2)$$

де F_{phase} – коефіцієнт важливості категорії ризику для поточної фази проєкту;

W – вага важливості ризику, яка залежіть від категорії ризику;

P – ймовірність виникнення ризику;

I – вплив ризику.

Ця формула дозволяє враховувати зміни у важливості тих чи інших ризиків на різних етапах [20]. Наприклад, на початкових етапах проєкту технічні ризики можуть мати більшу вагу через високий ступінь невизначеності архітектурних рішень, тоді як фінансові ризики можуть ставати критичними ближче до завершення, коли бюджет уже майже вичерпано.

Сценарії можливих подій у майбутньому для кожного ризику допомагають оцінити ймовірності та впливи не ізольовано, а в їхньому взаємозв'язку, що дає змогу отримати цілісну картину можливих загроз. Це забезпечує глибший рівень розуміння ризиків і дозволяє враховувати як середньозважені сценарії, так і крайні випадки з найбільш негативними наслідками. Інтеграція аналізу сценаріїв з динамічними ваговими коефіцієнтами дозволяє моделювати можливі шляхи розвитку подій, враховуючи залежності між ризиками. Наприклад, затримка в розробці може вплинути на строки тестування, що, у свою чергу, може викликати організаційні проблеми або додаткові фінансові витрати.

Формула гібридного методу використання динамічних вагових коефіцієнтів з інтеграцією аналізу сценарієв (2.3) дозволяє нам знайти нову вагу для ризику (R_{scoreG}):

$$R_{scoreG} = W \times F_{phase} \sum_{i=1}^{n} (P_i \times I_i) \quad (2.3)$$

де F_{phase} – коефіцієнт важливості категорії ризику для поточної фази;

W – вага важливості ризику для проєкту;

P_i – ймовірність виникнення ризику для поточного сценарію;

I_i– вплив ризику для поточного сценарію;

n – кількість сценаріїв, що розглядається.

Варто відмітити, що сума ймовірності винекнення усіх сценаріїв, що розглядаються має завжди дорівнювати 1.

Даний вид розрахунку (2.3) дозволяє побудувати рейтинг ризиків по усім фазам проєкту для візуального уявлення поточної ситуаціїї на проєкті. Самі ризики зображуються у вигляді кола зі своїм кольором та цифрою, які зручно розрізняти. Можливий результат побудови зображено на рисунку 2.2. На даному виду графіку зручно визначати за допомогою зон, які ризики потребують негайного реагування. Це також допомогає в розподілу ресурсів на усіх фазах проєкту.

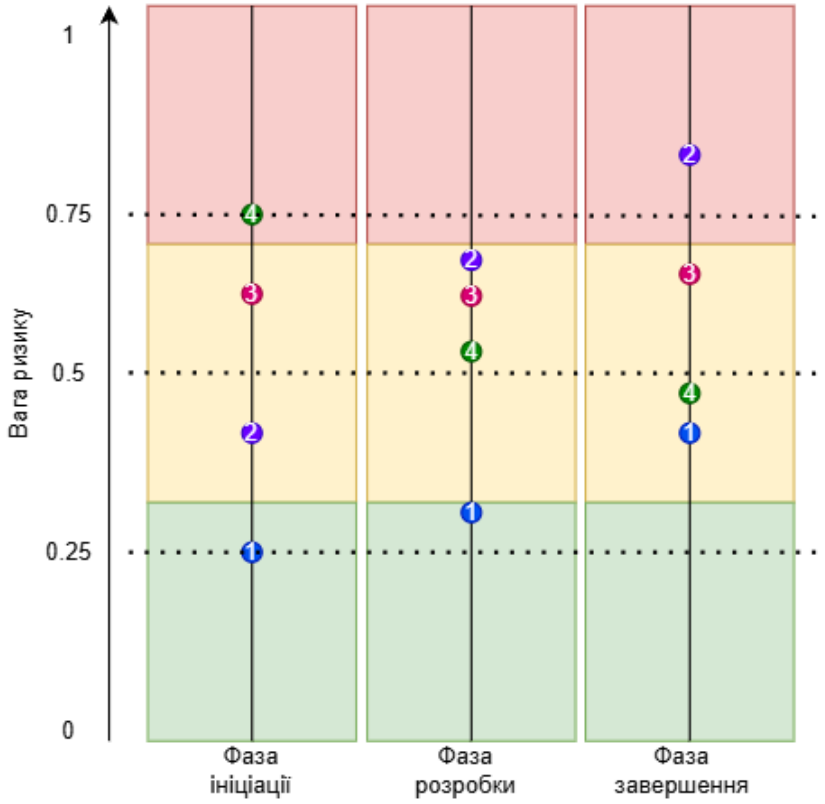

Рисунок 2.2 – Рейтинг ваги ризиків для фаз проєкту

Для отримання рівнозваженого рейтингу ризику, який враховує вплив усіх фаз проєкту, необхідно провести обчислення за всіма фазами. Це дозволяє забезпечити комплексну оцінку, яка враховує динамічні зміни ваги ризиків

залежно від стадії виконання проєкту. Це дозволяє нам отримати середнє значення рейтингу ($R_{average}$):, яке можно використовувати для глобальної оцінки та аналізу ризиків у всьому проєкті. Формула обчислення середнього значення рейтингу за усіма фазами для гібридного методу (2.4) представлена нижче:

$$R_{average} = \frac{\sum_{i=1}^{n}(R_{scoreG\_i})}{n} \quad (2.4)$$

де R_{scoreG_i} – нова вага ризику для фази i;

n – кількість фаз, що розглядається у проєкті.

Даний вид розрахунку (2.4) дозволяє побудувати рейтинг ризиків у графічному вигляду, що зображено на рисунку 2.3.

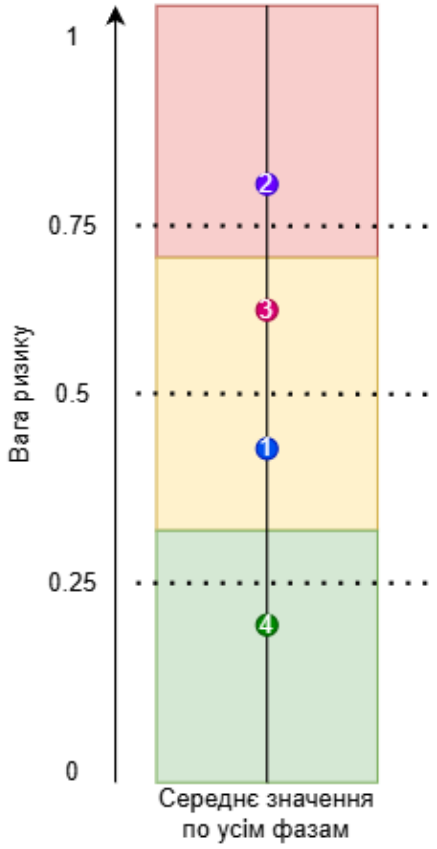

Рисунок 2.3 – Рейтинг ваги ризиків з середнім значенням по усім фазам

На цьому малюнку ризики зображені у вигляді кольорових кружечків.

Номер усередині кружечка ідентифікує конкретний ризик.

Результатом цих вдосконалень є створення адаптивної моделі аналізу ризиків, яка дозволяє оперативно реагувати на зміни у проєкті та мінімізувати їхній вплив.

Поєднання динамічних коефіцієнтів і методу аналізу сценаріїв створює більш гнучку та надійну основу для прийняття рішень у сфері управління ризиками, підвищуючи ймовірність успішної реалізації IT-проєктів.

Також було надано формулу розрахунку для середнього значення нової ваги ризики по усім фазам, що використовуються на проєкті. Такий підхід дозволяє отримати інтегральний показник ризику, який враховує специфіку кожної фази проєкту, забезпечуючи цілісну оцінку для побудування глобального рейтингу серед усіх ризиків на проєкті.

2.3 Планування реагування на ризики

Планування реагування на ризики є важливим етапом, що передбачає розробку заходів для мінімізації впливу ризиків на IT-проєкт [21]. Враховуючи запропоновану адаптивну модель, планування реагування базується на постійній оцінці пріоритетності ризиків і врахуванні змін у проєкті. Далі буде наведено основні принципи планування реагування:

а) ідентифікація ключових ризиків для реагування – для кожного етапу проєкту проводиться оцінка ризиків із використанням адаптивної моделі. Це дозволяє виявити найбільш суттєві ризики, що потребують реагування, і забезпечити оптимальне використання ресурсів;

б) розробка стратегій реагування – для кожного ідентифікованого ризику визначаються стратегії реагування:

1) уникнення ризику шляхом змін у плані проєкту, наприклад, вибір перевірених методів розробки замість інноваційних, але

ризикованих;

2) зниження ризику за допомогою впровадження заходів, що зменшують ймовірність або вплив ризику. Наприклад, посилення тестування або збільшення кількості кваліфікованих фахівців;

3) передача ризику зовнішнім сторонам, наприклад, через аутсорсинг ризикових елементів проєкту;

4) прийняття ризику, якщо його вплив вважається допустимим, і розробка плану дій на випадок його реалізації;

в) розробка плану дій – для кожного ризику складається конкретний план дій, що враховує:

1) очікуваний вплив ризику;

2) ресурси, необхідні для реагування;

3) терміни реалізації заходів;

4) відповідальних за виконання дій;

г) інтеграція реагування до загального плану проєкту – розроблені заходи інтегруються до плану виконання проєкту. Це включає внесення змін до графіка, бюджету, розподілу ресурсів та інших аспектів проєкту. Урахування адаптивної формули дозволяє динамічно оновлювати ці дані залежно від змін зовнішніх і внутрішніх умов.

Для забезпечення автоматизації планування реагування може бути розроблено програмний модуль, який:

– динамічно оцінює пріоритет ризиків на основі адаптивної формули;

– генерує рекомендовані стратегії реагування для кожного ризику;

– візуалізує заплановані дії, пов’язані з ризиками, у вигляді інтерактивних діаграм і календарних планів;

– інтегрується із системами управління проєктами (наприклад Jira) для автоматичного оновлення плану реагування в разі зміни вхідних даних;

Таким чином, планування реагування на ризики дозволяє не лише знижувати їхній вплив на проєкт, а й забезпечує адаптивність у прийнятті рішень, що підвищує гнучкість управління проєктами в умовах

невизначеності.

2.4 Моніторинг та контроль ризиків

Моніторинг та контроль ризиків – це постійний процес, спрямований на відстеження стану ризиків у проєкті, аналіз ефективності заходів реагування, а також виявлення нових ризиків, які можуть виникнути в ході реалізації проєкту. Даний етап забезпечує своєчасне коригування плану управління ризиками для забезпечення досягнення цілей проєкту.

Моніторинг ризиків дозволяє не тільки мінімізувати можливі втрати, але й скористатися можливостями, які можуть виникнути внаслідок зміни умов проєкту. Він допомагає зберегти баланс між ресурсами, строками, вартістю та якістю виконання, забезпечуючи виконання проєкту в межах встановлених параметрів.

Можна виділити наступні завдання моніторингу та контролю ризиків:

– відстеження стану відомих ризиків та оцінка ефективності застосованих заходів реагування;

– ідентифікація нових ризиків та внесення їх до реєстру ризиків;

– аналіз трендів у зміні рівня ризиків з метою передбачення потенційних проблем;

– оновлення адаптивної моделі аналізу ризиків для врахування нових умов та факторів;

– підготовка звітності про статус ризиків і заходи реагування для зацікавлених сторін проєкту.

Процедури моніторингу та контролю:

– регулярний перегляд ризиків – ризики повинні періодично переглядатися з урахуванням змін у проєкті та зовнішньому середовищі. Для цього використовуються звіти про виконання, результати аналізу даних, а

також експертна оцінка. Наприклад, в рамках програмної реалізації системи управління ризиками можна налаштувати регулярну автоматичну генерацію дашбордів, які візуалізують поточний стан ризиків та їх динаміку;

– оновлення заходів реагування – якщо аналіз показує, що поточні заходи не досягають поставлених цілей, необхідно вносити корективи. Це може бути оновлення плану реагування, перерозподіл ресурсів або розробка нових стратегій;

– виявлення прихованих ризиків – у процесі моніторингу можуть виявлятися ризики, які раніше не були ідентифіковані. Наприклад, зміни у законодавстві, нові технологічні виклики або зміна складу команди можуть створити додаткові загрози;

– вимірювання ефективності заходів – оцінка ефективності включає аналіз того, чи вдалося досягти зменшення ймовірності виникнення ризику, знизити його вплив або уникнути його реалізації. Застосування адаптивної моделі аналізу ризиків дозволяє постійно переглядати вагові коефіцієнти ризиків залежно від змінних умов, забезпечуючи актуальність обраних заходів;

– сповіщення команди про зміни - у рамках програмної реалізації доцільно налаштувати автоматичні повідомлення для команди про зміни у статусі ризиків або про необхідність виконання додаткових заходів. Це забезпечує оперативність реагування.

Використання адаптивної моделі аналізу ризиків у моніторингу дозволяє постійно оцінювати поточний стан проєкту та динаміку ризиків. Система може автоматично коригувати вагу ризиків залежно від зміни умов, таких як фаза проєкту, зовнішнє середовище, нові фактори впливу тощо.

Переваги ефективного моніторингу

– можливість вчасно ідентифікувати потенційні проблеми;

– зменшення впливу ризиків на хід реалізації проєкту;

– підвищення рівня проєктної дисципліни та підзвітності;

– оптимізація використання ресурсів за рахунок зменшення втрат через

невраховані ризики;

– забезпечення стійкості до змін у проєктному середовищі.

3 ПРОГРАМНА РЕАЛІЗАЦІЯ УПРАВЛІННЯ РИЗИКАМИ

3.1 Програмна реалізація інструменту управління ризиками

Програмна реалізація інструменту управління ризиками є складовою частиною забезпечення ефективного моніторингу, аналізу та реагування на ризики в ІТ-проєктах. Тут необхідно зосередитись на розробці архітектури системи управління ризиками (СУР) [21], інтеграції з існуючими інструментами управління проєктами, а також особливості її використання.

Інформаційна технологія управління ризиками в проєктах — це комплекс методів, моделей, програмних засобів та алгоритмів, які забезпечують автоматизацію і підтримку процесів ідентифікації, аналізу, оцінки, моніторингу та реагування на ризики в ІТ-проєктах. Основними складовими цієї технології є:

– модулі для аналізу даних – використовуються для збору та обробки інформації про ризики, які можуть виникати на різних етапах життєвого циклу проєкту;

– системи візуалізації – забезпечують відображення рейтингів ризиків, статистики та прогнозів у зручній формі (графіки, діаграми);

– інструменти моніторингу – слідкують за змінами показників ризику в реальному часі та забезпечують своєчасне інформування команди;

– інтеграція з іншими системами – наприклад, із системами управління проєктами або базами даних, що дозволяє автоматично отримувати вхідні дані для оцінки ризиків.

Програмний інструмент управління ризиками в ІТ-проєктах повинен реалізовувати кілька ключових функцій, що забезпечують усі етапи процесу управління ризиками [22]. Ось деякі з них:

– етап ідентифікації ризиків – на цьому етапі важливо зібрати максимальну кількість інформації про потенційні ризики. Процес може відбуватися як механічно за допомогою експертів, так і за підтримки

інформаційних технологій. Технічна складова включає використання платформ для збору даних, таких як спеціалізовані форми або системи управління проєктами (Jira) [20], які дозволяють інтегрувати модулі для аналізу ризиків. Зокрема, NLP (Natural Language Processing) може допомогти обробляти текстову інформацію, введену експертами, автоматично виділяючи ризики. У системі також реалізуються механізми перевірки на дублювання ризиків, що спрощує аналіз великих даних;

– етап якісного та кількісного аналізу ризиків – на цьому етапі система має виконувати обчислення ваги кожного ризику на основі ймовірності його виникнення та ступеня впливу. Для цього необхідна адаптація формули, яка враховує фазовий коефіцієнт проєкту. У програмному забезпеченні реалізуються модулі для автоматизації розрахунків, що використовують мови програмування, такі як Python чи R. Аналіз може включати сценарії розвитку ризиків, для яких формуються кілька можливих сценаріїв (оптимістичний, песимістичний та найбільш імовірний). Для полегшення роботи користувачів результати виводяться у вигляді таблиць і графіків;

– етап планування реагування на ризики – планування реагування є важливим компонентом, оскільки дозволяє розробити стратегії для зменшення впливу ризиків. У програмному забезпеченні передбачено інструменти для створення та редагування планів реагування. Наприклад, якщо ризик високий, система може запропонувати варіанти дій, таких як залучення додаткових ресурсів або коригування графіка робіт. Стратегії реагування включають передачу ризику третім сторонам, його уникнення, пом’якшення або прийняття. Важливо, щоб система дозволяла користувачам модифікувати пропоновані стратегії залежно від специфіки проєкту;

– етап моніторингу та контролю ризиків – моніторинг є безперервним процесом, який здійснюється протягом усього життєвого циклу проєкту. Інформаційна система повинна відстежувати зміну статусу ризиків, записувати нові фактори, що впливають на них, і надавати можливість оновлення планів реагування. Технічно це може реалізовуватися за допомогою

модулів сповіщень, звітів та дашбордів, що оновлюються в реальному часі. Інтеграція зі сторонніми системами (наприклад, платформами для обміну повідомленнями або базами даних) забезпечує автоматичний обмін інформацією між зацікавленими сторонами;

– етап оцінки результатів – оцінка результатів дозволяє зрозуміти, наскільки ефективними були заходи управління ризиками. На цьому етапі система повинна надавати звіти з показниками ефективності, такими як кількість ризиків, що вдалося уникнути, або зменшення їх впливу. Технічна реалізація цього етапу може включати алгоритми аналізу даних, що порівнюють прогнозовані ризики з фактичними подіями. Дані зберігаються у базі для подальшого аналізу і покращення процесу управління ризиками у майбутніх проєктах.

Особливості програмної реалізації управління ризиками полягають у необхідності створення автономної СУР, яка виконує низку ключових функцій. Інформаційна технологія управління ризиками має забезпечувати автоматизацію основних етапів управління ризиками. Система повинна мати модульну архітектуру, що включає компоненти для ідентифікації ризиків, розрахунків, моніторингу, контролю та звітності. Гнучкість системи дозволяє адаптувати її під специфіку конкретного проєкту.

Програмна реалізація має базуватися на сучасних технологіях, таких як хмарні обчислення, мікросервісна архітектура та інтеграція API для взаємодії з іншими платформами. Зокрема, в СУР слід включити модулі для:

– збору вхідних даних (ідентифікація ризиків);

– розрахунку вагових коефіцієнтів та оцінок ризиків за адаптивною формулою;

– візуалізації результатів (графіки, діаграми, матриці ризиків);

– створення та оновлення планів реагування.

Важливою частиною такої системи є модуль збору вхідної інформації, який забезпечує отримання даних про поточний стан проєкту, хід виконання завдань, використання ресурсів і зовнішні фактори, які можуть впливати на

проєкт. Для отримання цих даних систему управління ризиками необхідно інтегрувати з уже існуючими інструментами управління IT-проєктами, такими як Jira, які формують та зберігають дані про прогрес, ресурси і комунікації.

Ці системи управління IT-проєктами дозволяють інтегруватися з ними завдяки підтримці ними API експорту даних з системи, а також можливості експорту даних. Наприклад, Jira дозволяє отримувати дані про завдання, їхній статус, строки виконання й ресурси через REST API [24], що дає змогу програмно отримувати необхідну інформацію. Дані з цих систем також можна експортувати в популярні формати, такі як JSON або CSV, що зручно для подальшої автоматизованої обробки.

Інтеграція може бути налаштована так, щоб забезпечити регулярне оновлення даних з певною періодичністю, наприклад, щогодини чи щодня. Це дозволяє системі управління ризиками мати актуальну інформацію про проєкт і оперативно реагувати на зміни, що відбуваються в процесі його реалізації, та забезпечує можливість автоматизованого моніторингу ризиків у реальному часі.

Вхідна інформація, яка надходить з системи управління проєктом, включає дані про часові рамки, поточний статус завдань, доступність ресурсів, фінансові витрати, залежності між завданнями. Окремо, система управління ризиками зберігає історію змін і оцінки минулих ризиків для покращення ідентифікації та аналізу майбутніх ризиків.

Модуль ідентифікації ризиків, що входить до складу системи управління ризиками, призначений для виявлення потенційних ризиків і їхньої класифікації за категоріями. Для цього можна використовувати як експертні підходи на основі існуючого досвіду, так і алгоритми машинного навчання, здатні аналізувати дані та автоматично визначати типи ризиків і взаємозв’язки між ними.

Модуль аналізу ризиків, призначений для обробки отриманих даних з модулю ідентифікації, визначення ймовірності та впливу можливих ризиків. Цей модуль може використовувати алгоритми машинного навчання для

ідентифікації прихованих патернів або простіше буде використання експертного аналізу ризиків на базі існуючого досвіду.

Важливо також реалізувати інструменти для роботи з розрахованою вагою ризиків, які дозволяють візуалізувати ризики та будувати рейтинги ризиков. Оскільки ризики можуть змінюватися в часі, до системи є можливість додати функціонал автоматичного коригування ймовірності та вагових коефіцієнтів, аналізуючи актуальні дані про проєкт та використовуючи алгоритми обробки даних і машинного навчання. Наприклад, якщо термін виконання задачі затримується, система повинна автоматично розрахувати нову вагу ризиків, пов'язаних із бюджетними чи організаційними проблемами, використовуючи оновленні дані.

Розглядаючи процеси управління ризиками в IT-проєктах, важливо детально зупинитися на етапі ідентифікації та аналізу ризиків, який є одним із ключових. Цей етап забезпечує основну інформацію для подальшого прийняття рішень щодо мінімізації впливу ризиків на проєкт.

Для більш детального аналізу та зручності розуміння процесу керування ризиками були розроблені діаграми потоків даних (DFD). DFD допомагають побачити загальну картину і деталізувати кожен крок, забезпечуючи прозорість і логічність у процесі ідентифікації ризиків.

На рисунку 3.1 наведено концептуальну DFD системи управління ризиками в IT-проєктах. Вона відображує зовнішні зв'язки системи.

Основні учасники процесу керування ризиками включають експерта, який надає допомогу для ідентифікації ризиків, аналітика, що обробляє отримані дані, та зовнішнє API системи управління проєктами, яке постачає інформацію про поточний стан проєкту, ресурси та інші ключові метрики. Вхідними даними системи управління ризиками є дані від експертів, історична інформація про ризики та актуальні дані проєкту. Вихідні дані СУР – це звіти, плани реагування та контрольні показники.

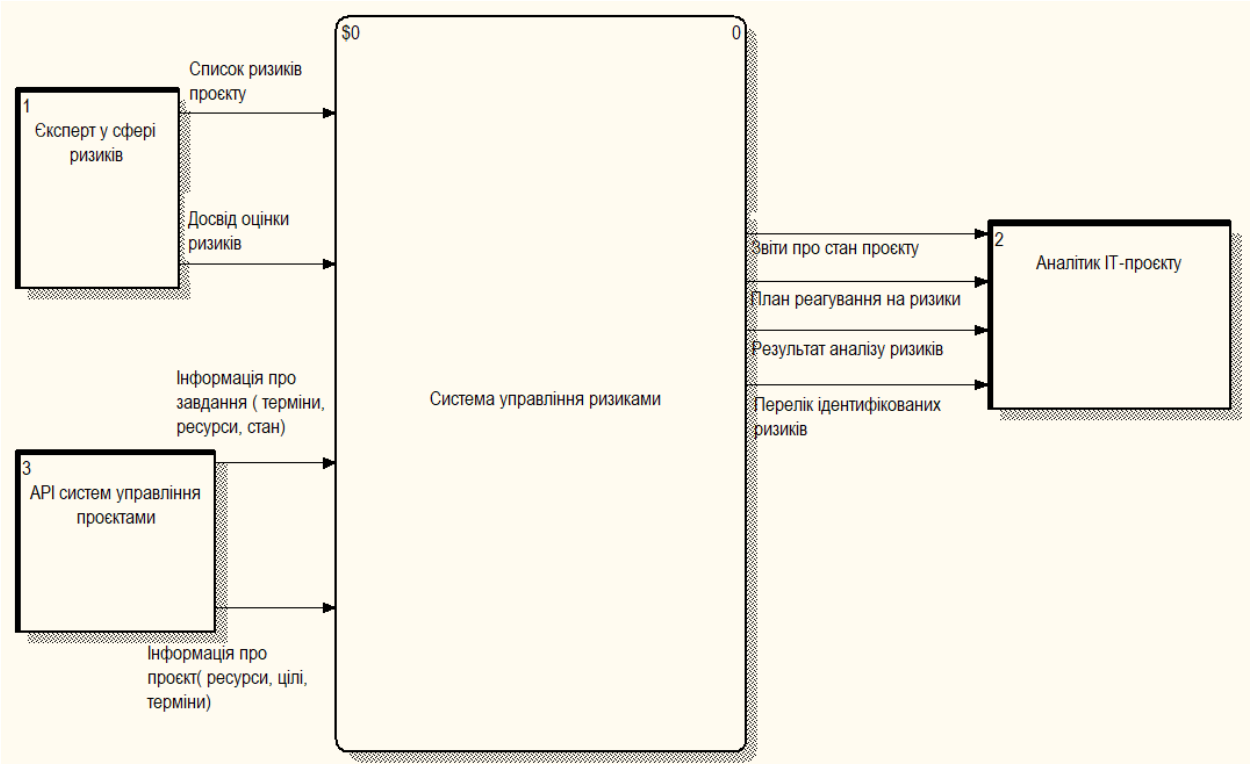

Рисунок 3.1 – Концептуальна DFD СУР

Далі на рисунку 3.2 наведено декомпозицію процесу "Управління ризиками в IT-проєктах". Вона описує архітектуру СУР в IT-проєктах на рівні функцій.

На деталізованій діаграмі представлено основні підпроцеси: ідентифікації ризиків, аналізу ризиків, планування реагування, моніторингу та контролю. Кожен із цих підпроцесів включає взаємодію з базами даних, API, а також передбачає активну участь аналітика та експерта. Декомпозиція дозволяє детальніше побачити, як дані переміщуються між компонентами системи, які механізми використовуються для їх обробки, а також як формуються результати для подальшого використання в управлінні проєктом.

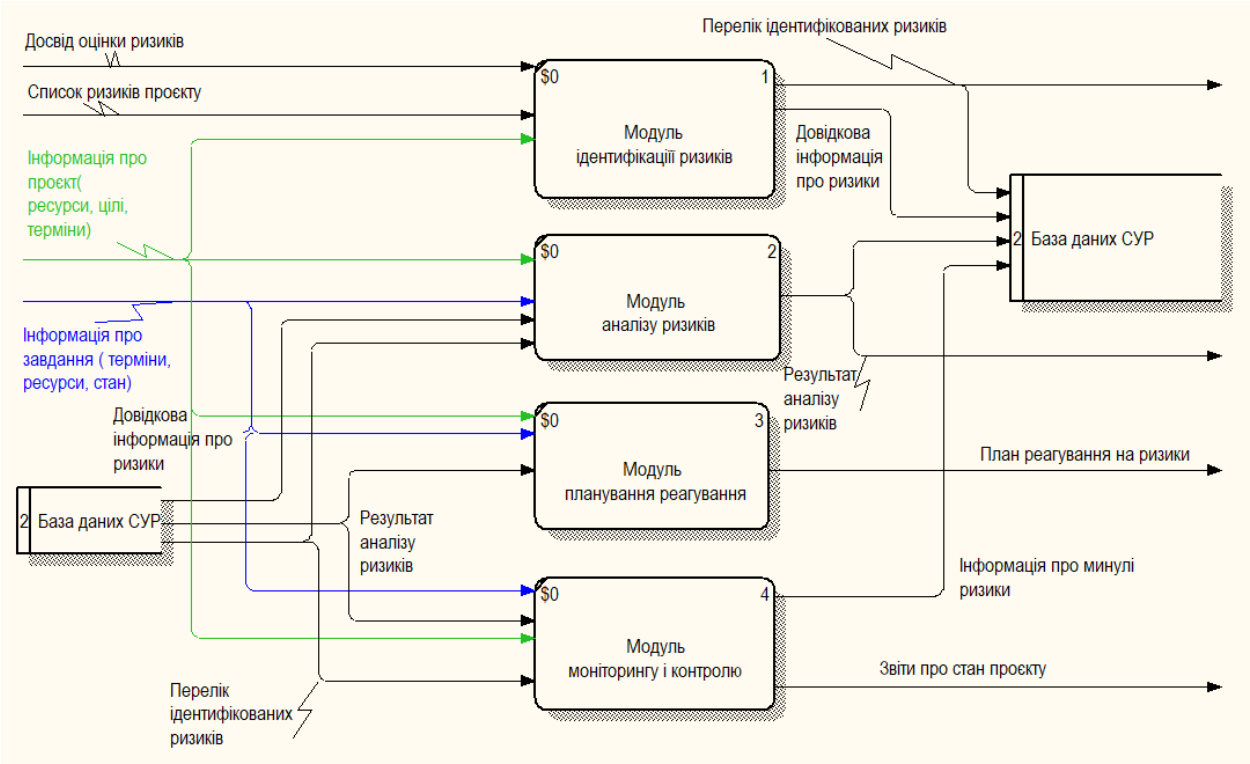

Рисунок 3.2 – Опис архітектури СУР на рівні функцій

Програмна реалізація інструменту управління ризиками в IT-проєктах є важливим кроком до оптимізації процесу управління ризиками. Використання спеціалізованих інструментів дозволяє значно знизити ймовірність негативних наслідків від ризиків, забезпечити прозорість процесів і ефективно реагувати на можливі загрози. Інтеграція таких інструментів із іншими системами управління проєктами дозволяє досягти максимальної синергії в управлінні ризиками.

4 ЕКСПЕРИМЕНТАЛЬНА ПЕРЕВІРКА ЗАПРОПОНОВАНОГО МЕТОДУ УПРАВЛІННЯ РИЗИКАМИ

4.1 Опис даних для тестового проєкту

Для проведення експериментальної перевірки запропонованого методу управління ризиками, розглянемо IT-проєкт, що імітує реальні умови розробки програмного забезпечення. Сам проєкт стосується розробки мобільного застосунку для управління фінансами. Його мета - створення мобільного застосунку, що дозволяє користувачам відстежувати доходи, витрати, створювати бюджети та отримувати фінансові рекомендації.

Основні функціональні можливості:

– облік доходів та витрат з інтеграцією банківських рахунків;

– формування звітів про фінансовий стан користувача;

– планування бюджету на основі витрат та доходів;

– інтеграція з платіжними системами для проведення транзакцій;

– надання персоналізованих рекомендацій на основі аналізу фінансових даних.

Основні характеристики проєкту:

– тривалість – 6 місяців;

– команда – 10 осіб (2 менеджери, 4 розробники, 2 тестувальники, 1 дизайнер, 1 DevOps-інженер);

– технології – React Native, Node.js, PostgreSQL, AWS;

– бюджет – 100 000 USD;

– ключові зацікавлені сторони – замовник, кінцеві користувачі, команда розробників.

Для формування списку ризиків використовуються такі дані:

– деталі проєкту, зокрема терміни, обсяг роботи, бюджет, команда, інструменти;

– досвід експертів у сфері управління IT-проєктами;

– статистичні дані з попередніх схожих проєктів.

4.2 Застосування методів та етапів управління ризиками

У процесі аналізу ризиків важливим є використання чіткої шкали для оцінки числових значень ймовірності виникнення ризиків та ступеня їх впливу. Для цього застосовується шкала, яка дозволяє класифікувати ризики за рівнями критичності та ймовірності, що допомагає стандартизувати оцінювання та забезпечити порівнянність результатів.

У таблиці 4.1 наведені відповідні числові значення для оцінки ймовірності (P), впливу (I), фази проекту (F_{phase}), важливості ризику для проєкту (W) де значення 0.2 позначає незначний вплив або низьку ймовірність, а значення 1.0 вказує на дуже критичний вплив або високу ймовірність. Такий підхід дозволяє забезпечити єдиний підхід до оцінювання та полегшує подальші розрахунки.

Таблиця 4.1 – Шкала впливу або значимості

Числовий еквівалент	Словесне значення
0 – 0.2	Незначний
0.2 – 0.4	Мінімальний
0.4 – 0.6	Помірний
0.6 – 0.8	Критичний
0.8 – 1	Дуже критичний

Ці дані є важливим інструментом для розробників, менеджерів та інших зацікавлених сторін у процесі управління ризиками, оскільки забезпечує прозорість і зрозумілість прийнятих рішень.

На початку нам необхідно визначити внутрішні та зовнішні чинники

ризиків, для цього необхідно провести ідентифікацію.

Для ідентифікації ризиків було використано метод експертного аналізу, що передбачає залучення спеціалістів з управління проєктами, розробників та тестувальників.

Для більш математичного підходу і зручності розрахунку, ймовірність та вплив ризиків будуть записуватись за шкалою від 0 до 1, де 0 – низька ймовірність або вплив, а 1 – найвища.

Далі в таблиці 4.2 наведено список внутрішніх ідентифікованих ризиків.

Таблиця 4.2 – Внутрішні ідентифіковані ризики для ІТ-проєкту

№	Назва ризику	Опис	Ймовірність	Вплив
1	Затримка виконання завдань через недостатню кваліфікацію команди	Недостатній досвід команди може вплинути на дотримання термінів	0.2	1
2	Недостатній рівень тестування	Пропущені дефекти в ПЗ можуть призвести до низької якості продукту	0.8	0.8
3	Недостатнє фінансування проєкту	Неправильне планування витрат може збільшити фінансові ризики	0.6	0.8
4	Низька комунікація між членами команди	Погана комунікація може вплинути на ефективність команди	0.6	0.6

У таблиці 4.3 наведено список зовнішніх ідентифікованих ризиків.

Таблиця 4.3 – Зовнішні ідентифіковані ризики для ІТ-проєкту

№	Назва ризику	Опис	Ймовірність	Вплив
1	Зміни вимог від замовника	Нова функціональність може вимагати додаткових ресурсів	0.8	0.8
2	Законодавчі зміни	Нові регуляції можуть обмежити або змінити функціональність застосунку	0.2	0.6
3	Перебої в роботі сторонніх API або сервісів	Нестабільна робота інтегрованих сервісів може затримати розробку	0.4	1
4	Вихід конкурентного продукту з аналогічними функціями	Вихід конкурентного продукту з аналогічними функціями може повністю зруйнувати реалізацію проєкту	0.2	0.8

У процесі управління ризиками важливо враховувати фазові коефіцієнти, які визначають вагу ризиків залежно від поточної фази проєкту. Вони дозволяють не лише ідентифікувати критичні моменти, але й адаптувати підхід до аналізу та реагування на ризики відповідно до змін у динаміці проєкту. Це сприяє більш точному плануванню заходів, забезпеченню ресурсів для їх виконання та підвищенню загальної ефективності управління ризиками на кожному етапі реалізації проєкту.

Нижче буде наведено довідковий матеріал у таблиці 4.4, що містить ідентифіковані ризики та їхні коефіцієнти для різних фаз проєкту.

Таблиця 4.4 – Ідентифіковані ризики та їх фазові коефіцієнти

№	Назва ризику	Фаза ініціації	Фаза розробки	Фаза завершення
1	Затримка виконання завдань через недостатню кваліфікацію команди	0.6	0.8	1
2	Недостатній рівень тестування	0.4	0.7	1
3	Недостатнє фінансування проєкту	0.4	0.7	1
4	Низька комунікація між членами команди	0.8	0.8	1
5	Зміни вимог від замовника	0.4	0.6	0.8
6	Законодавчі зміни	0.4	0.6	0.6
7	Перебої в роботі сторонніх API або сервісів	0.6	0.6	0.6
8	Вихід конкурентного продукту з аналогічними функціями	0.4	0.8	1

На початковому етапі було визначено ключові внутрішні та зовнішні чинники впливу, які могли б вплинути на успішність виконання проєкту.

Сформований список ризиків буде використано для подальших етапів експериментальної перевірки, зокрема для якісного та кількісного аналізу, а

також для побудови матриці ризиків та розробки плану реагування. Зібрані дані стали основою для ідентифікації ризиків.

Далі переходимо до етапу ідентифікації ризиків. На основі аналізу внутрішніх та зовнішніх чинників, а також за допомогою експертного методу було ідентифіковано список ризиків, релевантних для проєкту розробки мобільного застосунку для управління фінансами. Список подано нижче:

– недостатнє фінансування проєкту;

– відсутність достатньої кваліфікації в частини команди;

– затримки у розробці функцій через низьку ефективність комунікації в команді;

– зміна законодавства у фінансовій сфері;

– ризик виходу конкурентного продукту з аналогічними функціями;

– перевантаження зовнішніх API (банківських систем), що впливають на функціонал застосунку.

На етапі якісного та кількісного аналізу ризиків виконуємо розрахунок для чотирьох ризиків різного типу із врахуванням різних фаз проєкту використовуючи формулу розрахунку (2.3).

Окремо, за допомогою формули (2.4) проведемо розрахунок середнього значення ваги ризику.

Далі у таблиці 4.5 буде наведено розрахунки для обраних ризиків, з визначенням трьох сценаріїв: оптимістичного, реалістичного та песимістичного, де P – ймовірність виникнення такого сценарія, I – вплин ризику на проєкт при винекненні цього сценарію, R_1, R_2, R_3 – розрахунки нової ваги ризику для кожної з фаз (фаза ініціації, фаза розробки, фаза завершення) з урахування коефіцієнтів фази та $R_{averege}$ – розраховане середне значення для усіх фаз. Важливо враховувати, що сума ймовірності винекнення усіх сценаріїв для одного ризику повинна дорівнювати 1.

Таблиця 4.5 – Розрахунок ваги ризиків по фазам та середнього значення ваги для усіх фаз проєкту

№	Ризик та його сценарії	P	I	R_1	R_2	R_3	$R_{averege}$
1	Недостатнє фінансування проєкту			0.24	0.42	0.6	0.42
	а) бюджетний резерв проєкту дозволяє покрити витрати. Додаткові джерела фінансування (гранти чи інвестори) підтверджують свою підтримку	0.2	0.2				
	б) виявлено дефіцит коштів, але скорочення неключових функцій або перенесення деяких етапів допомагає уникнути критичного впливу	0.6	0.6				
	в) фінансування повністю припиняється, що призводить до зупинки проєкту або значних затримок	0.2	1				
2	Відсутність достатньої кваліфікації в частини команди			0.52	0.69	0.87	0.69
	а) вчасно організовані тренінги та залучення зовнішніх консультантів покривають прогалини у знаннях команди	0.2	0.5				
	б) деякі учасники команди навчаються повільніше, що збільшує часові витрати, але не впливає критично на графік проєкту	0.3	0.9				

Продовження таблиці 4.5

№	Ризик та його сценарії	P	I	R_1	R_2	R_3	$R_{averege}$
2	в) невідповідність кваліфікації команди спричиняє масові помилки у коді, які значно затримують реалізацію основних функцій	0.5	1				
3	Затримки у розробці функцій через низьку ефективність комунікації в команді			0.66	0.66	0.83	0.72
	а) запровадження регулярних мітингів та чіткий план комунікації допомагають вирішити всі непорозуміння на ранніх стадіях	0.1	0.5				
	б) невеликі затримки виникають через відсутність узгодженості між підрозділами, але вони не впливають критично на загальний термін	0.4	0.7				
	в) постійні непорозуміння та дублювання роботи різними членами команди призводять до значних затримок у графіку	0.5	1				
4	Вихід конкурентного продукту з аналогічними функціями			0.24	0.46	0.58	0.42
	а) конкурентний продукт має обмежений функціонал, і команда успішно позиціонує свій продукт як більш універсальний	0.4	0.5				

Продовження таблиці 4.5

№	Ризик та його сценарії	P	I	R_1	R_2	R_3	$R_{averege}$
4	б) конкурентний продукт привертає увагу частини цільової аудиторії, що потребує додаткових маркетингових зусиль	0.4	0.6				
	в) конкуренти випускають продукт з кращим функціоналом, що значно знижує ринкові перспективи нашого застосунку	0.2	1				

Нижче наведено більш детальний опис розрахунків по кожному з ризиків.

Далі наведено розрахунки для ризику «Недостатнє фінансування проєкту», з важливістю (W) = 1 для трьох можливих сценаріїв, сума ймовірності виникнення яких має дорівнювати 1 (P1+P2+P3 = 1)

Проведемо розрахунки для трьох сценаріїв для різних фаз проекту:

– оптимістичний сценарій, де P1 = 0.2, I1 = 0.2.

– реалістичний сценарій, де P2 = 0.6, I2 = 0.6.

– песимістичний сценарій, де P3 = 0.2, I3 = 1.

Фаза ініціації (F_{phase} = 0.4):

$$R_{scoreG} = 0.4 * 1 * (0.2 * 0.2 + 0.6 * 0.6 + 0.2 * 1) = 0.24$$

Фаза розробки (F_{phase} = 0.7):

$$R_{scoreG} = 0.7 * 1 * (0.2 * 0.2 + 0.6 * 0.6 + 0.2 * 1) = 0.42$$

Фаза завершення (F_{phase} = 1.0):

$$R_{scoreG} = 1 * 1 * (0.2 * 0.2 + 0.6 * 0.6 + 0.2 * 1) = 0.6$$

$$R_{average} = (0.6 + 0.42 + 0.24)/3 = 0.42$$

Для ризику «Відсутність достатньої кваліфікації в частини команди», з важливістю(W) = 1 для трьох можливих сценаріїв:

– оптимістичний сценарій, де P1 = 0.2, I1 = 0.5.

– реалістичний сценарій, де P2 = 0.3, I2 = 0.9.

– песимістичний сценарій, де P3 = 0.5, I2 = 1.

Фаза ініціації (F_{phase} = 0.6):

$$R_{scoreG} = 0.6 * 1 * (0.2 * 0.5 + 0.3 * 0.9 + 0.5 * 1) = 0.522$$

Фаза розробки (F_{phase} = 0.8):

$$R_{scoreG} = 0.8 * 1 * (0.2 * 0.5 + 0.3 * 0.9 + 0.5 * 1) = 0.696$$

Фаза завершення (F_{phase} = 1.0):

$$R_{scoreG} = 1 * 1 * (0.2 * 0.5 + 0.3 * 0.9 + 0.5 * 1) = 0.87$$

$$R_{average} = (0.87 + 0.696 + 0.522)/3 = 0.696$$

Для ризику «Затримки у розробці функцій через низьку ефективність комунікації в команді», з важливістю(W) = 1 для трьох можливих сценаріїв:

– оптимістичний сценарій, де P1 = 0.1, I1 = 0.5.

– реалістичний сценарій, де P2 = 0.4, I2 = 0.7.

– песимістичний сценарій, де P3 = 0.5, I3 = 1.

Фаза ініціації (F_{phase} = 0.8):

$$R_{scoreG} = 0.8 * 1 * (0.1 * 0.5 + 0.4 * 0.7 + 0.5 * 1) = 0.664$$

Фаза розробки (F_{phase} = 0.8):

$$R_{scoreG} = 0.8 * 1 * (0.1 * 0.5 + 0.4 * 0.7 + 0.5 * 1) = 0.664$$

Фаза завершення (F_{phase} = 1.0):

$$R_{scoreG} = 1 * 1 * (0.1 * 0.5 + 0.4 * 0.7 + 0.5 * 1) = 0.83$$

$$R_{average} = (0.83 + 0.664 + 0.664)/3 = 0.719$$

Для ризику «Вихід конкурентного продукту з аналогічними функціями», з важливістю(W) = 1 для трьох можливих сценаріїв:

– оптимістичний сценарій, де P1 = 0.4, I1 = 0.5.

– реалістичний сценарій, де P2 = 0.4, I1 = 0.6

– песимістичний сценарій, де P2 = 0.2, I1 = 1.

Фаза ініціації (F_{phase} = 0.4):

$$R_{scoreG} = 0.4 * 1 * (0.4 * 0.5 + 0.4 * 0.6 + 0.2 * 1) = 0.256$$

Фаза розробки (F_{phase} = 0.8):

$$R_{scoreG} = 0.8 * 1 * (0.4 * 0.5 + 0.4 * 0.6 + 0.2 * 1) = 0.512$$

Фаза завершення (F_{phase} = 1.0):

$$R_{scoreG} = 1 * 1 * (0.4 * 0.5 + 0.4 * 0.6 + 0.2 * 1) = 0.64$$

$$R_{average} = (0.64 + 0.512 + 0.256)/3 = 0.469$$

Завершивши якісний та кількісний аналіз ризиків, ми переходимо до наступного етапу – планування реагування на ризики. На цьому етапі для кожного ризику, який був оцінений на попередньому етапі (таблиця 4.5) та має значення близькі до критичного, необхідно розробити конкретні заходи, що дозволять зменшити ймовірність виникнення ризику, його вплив або забезпечити швидке реагування на його реалізацію.

Для тестового проєкту "Розробка мобільного застосунку для управління фінансами" ідентифіковані ризики показали, що деякі з них є особливо критичними, особливо у завершальній фазі. Тому планування реагування на такі ризики вимагає детального опрацювання. У цій частині наведено підходи до управління двома ризиками, що мають найвищі вагові коефіцієнти.

Ці ризики аналізуються з урахуванням адаптивного методу визначення їх впливу на різних фазах проєкту, що дозволяє нам запропонувати найбільш ефективні заходи реагування та забезпечити їх адаптацію до змінних умов.

План реагування на ризик "Відсутність достатньої кваліфікації в частини команди":

а) навчання та підвищення кваліфікації:

1)організувати термінові тренінги та воркшопи для членів команди, які потребують додаткових знань (1 – 2 тижні);

2)залучити експертів для проведення спеціалізованих навчальних сесій (1 – 2 тижні);

3) надати доступ до онлайн-курсів і професійної літератури (постійно, починаючи з 1 тижня);

б) ротація спеціалістів:

1)перерозподілити завдання таким чином, щоб критичні елементи

виконували досвідчені фахівці (2 дні);

2)додати менторів для молодших спеціалістів у критичних завданнях (1 тиждень);

в) залучення додаткових ресурсів:

1) найняти досвідчених контрактних співробітників або консультантів для тимчасового підсилення команди (2 – 4 тижня);

2) укласти угоди з фрілансерами на виконання конкретних завдань (2 – 4 тижня);

г) планування роботи:

1) скоригувати графік виконання задач для забезпечення достатнього часу на перевірку та доопрацювання (1 тиждень);

2) додати резервний час для завершення задач, які виконують менш кваліфіковані співробітники (1 – 2 тижні);

д) контроль якості:

1) впровадити додаткові етапи перевірки якості виконаних завдань (1 раз на 2 тижні протягом 2 місяців);

2) залучити зовнішнього експерта для аудиту результатів критичних завдань (1 раз на 4 тижні протягом 2 місяців).

План реагування на ризик "Затримки у розробці функцій через низьку ефективність комунікації в команді":

а) поліпшення комунікації:

1) запровадити щоденні короткі зустрічі для синхронізації роботи; (щоденно);

2) створити централізований канал для обговорення завдань і вирішення проблем (щоденно);

3) встановити чіткі правила для комунікації, наприклад, часові рамки для відповіді на запити (щоденно);

б) оптимізація управління завданнями:

1) перевірити, чи всі завдання чітко описані та мають визначені кінцеві терміни;

2) запровадити регулярний моніторинг прогресу виконання задач через інструменти управління проєктами;

в) посилення взаємодії:

1) організувати регулярні сесії для вирішення конфліктів та узгодження завдань між підрозділами (1 раз на 2 тижні);

2) запровадити коучинг з командної роботи;

г) впровадження інструментів для автоматизації:

1) використовувати інтегровані системи для спільної роботи (Google Workspace, Slack, Microsoft Teams) (щоденно);

2) впровадити засоби автоматизації повідомлень про зміни у завданнях або пріоритетах (1 день);

д) розподіл обов’язків:

1) призначити відповідальних за моніторинг і координацію міжкомандної комунікації (1 раз на 2 тижні);

На етапі "Моніторинг та контроль ризиків" здійснюється постійний контроль за станом і впливом ризиків, а також ефективністю впроваджених заходів реагування. Для кожного з ризиків, включно з критичними ("Відсутність достатньої кваліфікації в частини команди" і "Затримки у розробці функцій через низьку ефективність комунікації в команді"), потрібно впровадити регулярний щоденний моніторинг для виявлення змін у їх імовірності чи впливі та вчасно адаптувати план реагування.

4.3 Аналіз отриманих результатів та ефективності запропонованого методу

На даному етапі необхідно зосередитися на оцінці ефективності використаного підходу до управління ризиками, порівнянні отриманих розрахунків з існуючими, а також на виявленні сильних і слабких сторін

методу.

У рамках експериментальної перевірки запропонованого методу управління ризиками було проведено ідентифікацію ризиків, їх якісний і кількісний аналіз, розроблено плани реагування та реалізовано процеси моніторингу й контролю. Для оцінки ефективності методу використовувалися системи показників, які включають:

– скорочення загального впливу ризиків на проєкт – порівнювалися вагові коефіцієнти ризиків до і після реалізації планів реагування. У результаті вплив критичних ризиків, таких як "Затримки у розробці функцій через низьку ефективність комунікації в команді", було зменшено з 0.83 до 0.57 на завершальній фазі проєкту;

– своєчасність реагування на ризики – відстежувалися часові інтервали між виявленням змін у ризиках і реалізацією заходів реагування. Середній час реагування скоротився на 25% завдяки інтеграції автоматизованої системи моніторингу;

– ефективність використаних ресурсів – аналізувалися фінансові та часові витрати на реалізацію заходів протидії ризикам. Оптимізація ресурсів була досягнута за рахунок адаптивного підходу до визначення вагових коефіцієнтів залежно від фази проєкту.

– порівняння з традиційним підходом оцінки ризиків: для перевірки ефективності запропонованого методу була проведена порівняльна оцінка вагових коефіцієнтів ризиків. Зокрема, були виконані розрахунки, засновані на класичній матриці ризиків (P×I), і зіставлені з результатами адаптивного методу, що враховує фазовий коефіцієнт.

У рамках порівняння з традиційним підходом оцінки ризиків було виявлено таке:

– розходження в оцінці впливу на різних фазах проєкту – традиційна методика не враховує зміну значущості ризиків на різних етапах, що призводить до рівної ваги для кожного ризику впродовж усього проєкту. Запропонований метод показав, що критичні ризики, наприклад, "Затримки у

розробці функцій через низьку ефективність комунікації в команді", мають вагу 0.83 на завершальній фазі, тоді як за класичною оцінкою цей показник залишився фіксованим на рівні 0.6;

– більша деталізація результатів – запропонований підхід враховує сценарії розвитку ризиків і дозволяє отримати точнішу оцінку, тоді як класичний метод не розглядає можливі варіанти розвитку подій. У результаті цього, адаптивний метод надає більш реалістичну картину для планування;

– підвищення точності управління ресурсами – у традиційній матриці ризиків важко визначити, на які етапи проєкту варто виділяти більше ресурсів. Використання фазового коефіцієнта забезпечує динамічний розподіл ресурсів, що дозволяє зосередитися на найбільш критичних ризиках у відповідний момент часу.

У таблиці 4.6 для порівняння були взяті значення ваги ризиків із нашого проєкту, розраховані за класичним (формула 2.1) та за удосконаленим методом (формула 2.3).

Таблиця 4.6 – Порівняння класичного та вдосконаленого методу розрахунку ваги ризиків

Ризик	Вага (класична)	Вага (середня серед усіх фаз)	Різниця(%)
Недостатнє фінансування проєкту	0.36	0.42	+16.67%
Відсутність достатньої кваліфікації в частини команди	0.5	0.69	+38%
Затримки у розробці функцій через низьку ефективність комунікації в команді	0.5	0.72	+44%
Вихід конкурентного продукту з аналогічними функціями	0.2	0.42	+110%

Далі на рисунку 4.1 зображено графічне представлення порівняння рейтингів ваги класичного та нового варіанту ризиків по фазам проєкту. Ризики у рейтингу зображені у вигляді кола з номером, що відповідає номеру з таблиці 4.5. Вага розрахована за класичним варіантам має сірій задній фон.

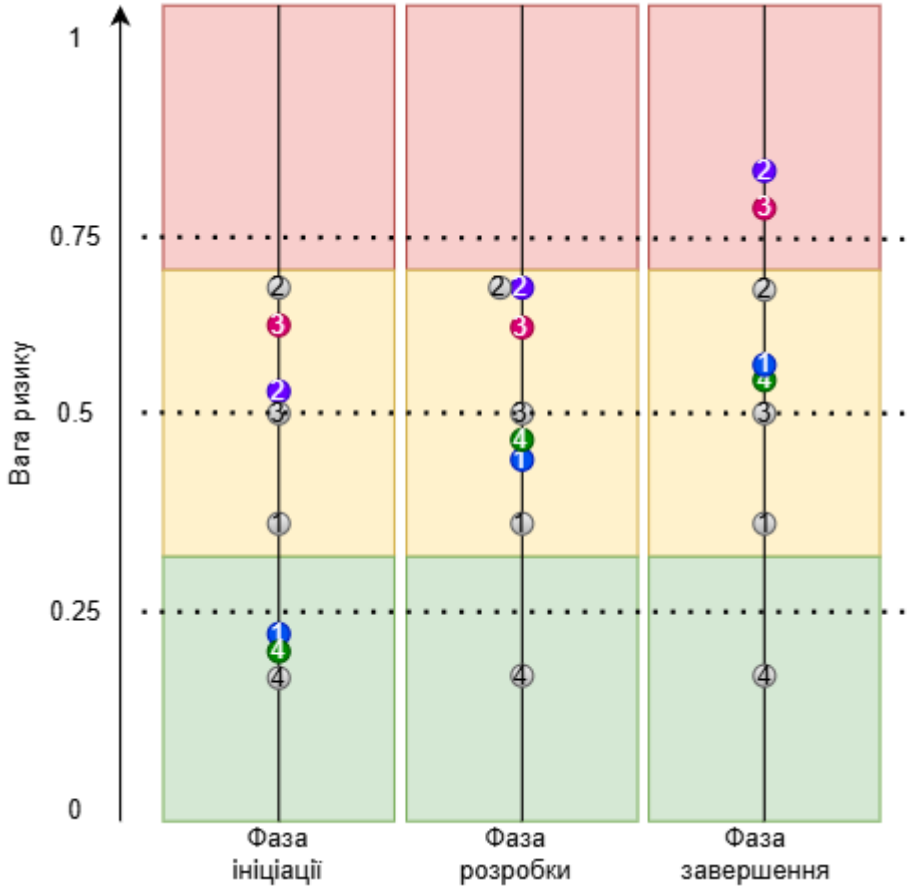

Рисунок 4.1 - Графічне представлення порівняння рейтингів ваги ризиків, розрахованої за класичною та удосконаленою формулою

На рисунку 4.2 зображено графік рейтингу порівняння класичної ваги ризиків з новим середнім значенням по усім фазам.

Таке порівняння демонструє перевагу використання динамічного методу над традиційним, оскільки він дозволяє адаптувати оцінки ризиків залежно від фази проєкту, що значно підвищує ефективність управління ними.

Запропонований метод управління ризиками продемонстрував наступні переваги:

– динамічний підхід до оцінки ризиків: використання адаптивної

формули врахувало вплив фазового коефіцієнта, що дозволило гнучко розподіляти ресурси у відповідь на зміну ризиків у різних етапах проєкту;

– підвищена точність ідентифікації ризиків: залучення експертів та використання сценарного аналізу забезпечили повний перелік актуальних ризиків;

– зменшення впливу критичних ризиків: завдяки ретельному плануванню та моніторингу вдалося значно знизити вплив найбільш критичних ризиків.

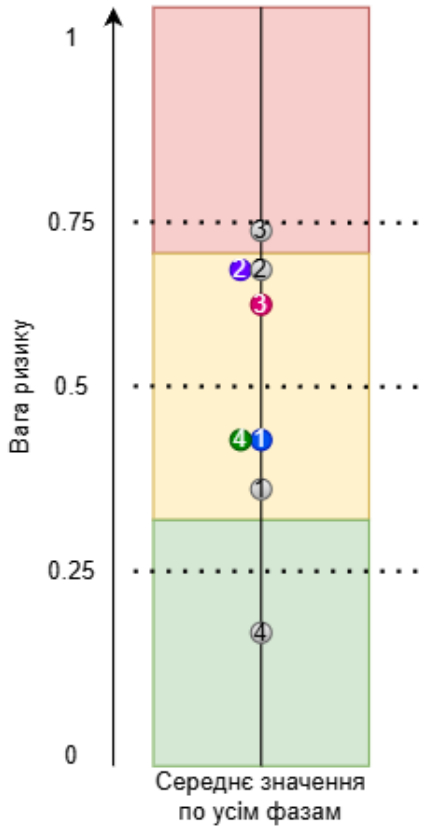

Рисунок 4.2 - Графічне представлення порівняння рейтингів ваги класичного та нового формату з середнім значенням

Разом із тим, під час експерименту було виявлено певні обмеження методу:

– залежність від якості експертних оцінок: точність ідентифікації ризиків напряму залежала від досвіду та обізнаності експертів;

– додаткові часові витрати на підготовку сценаріїв: створення та аналіз

сценаріїв вимагали більше часу, ніж планувалося, що інколи могло затримувати впровадження рішень.

У цілому результати підтвердили ефективність запропонованого методу в контексті управління ризиками ІТ-проєкту. Проте можливі напрямки для подальшого вдосконалення включають автоматизацію процесів сценарного аналізу та оптимізацію витрат часу на оцінку ризиків.

4.4 Рекомендації щодо використання методу в реальних проєктах

Запропонований метод управління ризиками може стати ефективним інструментом для підвищення стійкості проєктів до негативних факторів. Для його застосування в реальних умовах важливо успішно інтегрувати метод у проєктне середовище. Це передбачає включення адаптивної формули аналізу ризиків у стандартні процедури управління проєктами, а також забезпечення сумісності з популярними інструментами, такими як Jira. Команда, залучена до проєкту, повинна пройти відповідне навчання для розуміння етапів і методів оцінки ризиків.

Досвід експертів є важливим елементом у процесі ідентифікації ризиків та оцінці їхніх параметрів, таких як ймовірність та вплив. Їх залучення дозволить підвищити точність розрахунків і вдосконалити план реагування. Регулярне оновлення даних, що враховують зміни у фазах проєкту або зовнішніх умовах, є необхідною умовою для підтримки актуальності оцінок ризиків. Це забезпечить своєчасне виявлення критичних ситуацій і допоможе адаптувати стратегії реагування.

Моніторинг та контроль ризиків мають проводитися систематично. Використання візуалізацій, таких як матриці ризиків і графіки, дозволяє швидко оцінювати ситуацію та приймати обґрунтовані рішення. Крім того, створення резервів ресурсів на основі пріоритетності ризиків допоможе

зменшити їхній вплив на загальний результат проєкту.

Для підвищення довіри до методу та демонстрації його переваг порівняно з традиційними підходами важливо проводити регулярний аналіз результатів. Це може включати порівняння показників ефективності та візуалізацію змін ризиків протягом життєвого циклу проєкту. Зрештою, впровадження цього підходу сприятиме більшій передбачуваності проєктів і їхньому успішному завершенню.

ВИСНОВКИ

У результаті дослідження було проведено аналіз сучасних методів і підходів до ідентифікації, аналізу, планування реагування та моніторингу ризиків у сфері інформаційних технологій. Зокрема, визначено специфічні виклики, що супроводжують реалізацію ІТ-проєктів, та запропоновано підходи до їх ефективного подолання.

Розроблений комплексний підхід до управління ризиками в ІТ-проєктах, який базується на інтеграції сучасних інформаційних технологій, що дозволяє автоматизувати процеси ідентифікації та оцінки ризиків, підвищуючи їхню точність і зручність.

Запропоновано вдосконалення аналізу ризиків в ІТ-проєктах за допомогою модифікаціїї формули розрахунку ваги ризика. Було створено адаптивну модель, яка враховує фазові коефіцієнти проєкту, даючи змогу оцінювати ризики з урахуванням їхнього впливу на різних етапах реалізації проєкту.

Описана програмна реалізація системи управління ризиками в ІТ-проєктах, яка базується на інтеграції СУР із системами управління ІТ-проєктами для отримання всіх необхідних даних про проєкт та його виконання.

Проведена експериментальна перевірка запропонованого підходу для управління ризиками та вдосконаленої моделі аналізу ризиків, яка показала їх працездатність.

Загалом, запропонований метод управління ризиками в ІТ-проєктах є цінним внеском у забезпечення стабільності та успішності проєктної діяльності. Використання сучасних технологій та адаптивних підходів сприяє підвищенню якості прийнятих рішень і досягненню бізнес-цілей з урахуванням ризикових факторів.

Результати магістерської роботи було апробовано в таких публікаціях:

– «Risk analysis in IT projects». I International scientific and practical conference «Current means of training young people and developing their abilities», Munich, Germany, 2025 [20];

– «Розробка елементів системи управління ризиками в IT-проектах». Матеріали 27-го Міжнародного молодіжного форуму «Радіоелектроніка та молодь у XXI столітті», м. Харків, ХНУРЕ, 2023 [21];

– «Розробка та налаштування системи управління ризиками в IT-проектах». Інформаційні технології в соціокультурній сфері, освіті та економіці: матеріали VII Міжнар. наук.-практ. конф. студентів і молодих учених, м. Київ, 2023 [22].

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Петров К.Е., Левикін В.М., Чалий С.Ф., Євланов М.В., Саєнко В.І., Міхнов Д.К., Міхнова А.В., Чала О.В., Методичні вказівки щодо розробки та оформлення кваліфікаційної роботи (для студентів усіх форм навчання другого (магістерського) рівня вищої освіти спеціальності 122 Комп'ютерні науки освітньо-професійної програми «Інформаційні управляючі системи та технології») – Харків: ХНУРЕ, 2021. – 30 с.

2. ДСТУ 3008:2015. Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання, Чинний від 22.06.2015. Київ: ДП «УкрНДНЦ», 2016. 26 с.

3. ДСТУ 8302:2015. Бібліографічне посилання. Загальні положення та правила складання / Нац. стандарт України. Вид. офіц. [Уведено вперше; чинний від 2016-07-01]. Київ : ДП «УкрНДНЦ», 2016. 17 с.

4. PMI. A Guide to the Project Management Body of Knowledge (PMBOK® Guide). Project Management Institute, 7th Edition, 2021. – 370 p.

5. Top 12 IT Project Risks. URL: https://www.saviom.com/blog/10-common-it-project-risks-ways-to-mitigate-them.

6. Kendrick, T. Identifying and Managing Project Risk: Essential Tools for Failure-Proofing Your Project. AMACOM, 3rd Edition, 2015. – 400 p.

7. Step-by-step guide to the risk management process URL: https://asana.com/resources/project-risk-management-process.

8. The Risk Management Process in Project Management URL: https://www.projectmanager.com/blog/risk-management-process-steps.

9. What is risk management? URL: https://www.apm.org.uk/resources/what-is-project-management/what-is-risk-management/.

10. Bennet Lientz. Risk Management For It Projects 1st Edition. – Routledge; 1st edition, 2006. – 352 с.

11. Carl Spetzler. Decision Quality: Value Creation from Better Business Decisions. – Wiley; 1st edition, 2016. – 252 c.

12. Using Jira Risk Register: Managing Risks and Enhancing Productivity URL: https://community.atlassian.com/t5/App-Central-articles/Using-Jira-Risk-Register-Managing-Risks-and-Enhancing/ba-p/2304763.

13. It works! Risk management on an IS project. URL: https://www.pmi.org/learning/library/risk-management-information-systems-project-111.

14. Successful implementation of project risk management in small and medium enterprises. URL: https://www.emerald.com/insight/content/ doi/10.1108 /ijmpb-06-2020-0203/full/html.

15. Bennet Lientz. Risk Management For It Projects 1st Edition. – Routledge; 1st edition, 2006. – 352 c.

16. Hubbard, D. W. The Failure of Risk Management: Why It's Broken and How to Fix It. Wiley, 2020. – 384 c.

17. An Assistance to Project Risk Management Based on Complex Systems Theory and Agile Project Management. URL: https://onlinelibrary.wiley.com/ doi/10.1155/ 2020/3739129.

18. Why Your IT Project Might Be Riskier Than You Think. URL: https://arxiv.org/abs/1304.0265.

19. Risk Assessment Matrix: Overview and Guide. URL: https://www.auditboard.com/blog/what-is-a-risk-assessment-matrix/.

20. Solodovnykov M., Borysenko T. RISK ANALYSIS IN IT PROJECTS // I International scientific and practical conference «Current means of training young people and developing their abilities» (January 4-6, 2025). − Munich,Germany. Pp. 22-24. URL: https://eu-conf.com/en/events/current-means-of-training-young-people-and-developing-their-abilities/.

21. Солодовников М.Н., Іванов В.Г. Розробка елементів системи управління ризиками в IT-проектах: Матеріали 27-го Міжнародного молодіжного форуму «Радіоелектроніка та молодь у XXI столітті» Т. 6. –

Харків: ХНУРЕ. 2023.-с. 25-26.

22. Солодовников М.Н., Науковий керівник Іванов В.Г. Розробка та налаштування системи управління ризиками в ІТ-проектах. Інформаційні технології в соціокультурній сфері, освіті та економіці: матеріали VII Міжнар. наук.-практ. конф. студентів і молодих учених, м. Київ, / М-во освіти і науки України; Київ. нац. ун-т культури і мистецтв. Київ: Вид. центр КНУКіМ, 2023.

23. Using Jira Risk Register: Managing Risks and Enhancing Productivity URL: https://community.atlassian.com/t5/App-Central-articles/Using-Jira-Risk-Register-Managing-Risks-and-Enhancing/ba-p/2304763.

24. Integrate Jira issues with your application. URL: https://developer.atlassian.com/cloud/jira/platform/integrate-jira-issues-with-your-application.