МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Острозька академія»
Економічний факультет
Кафедра економіко-математичного моделювання та інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА
на здобуття освітнього ступеня магістра

на тему: «**Стратегічне управління ризиками в ІТ-компаніях: всебічний аналіз стратегій зменшення ризиків у розробці та розгортанні ІТ-додатків»**

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

Керівник: кандидат економічних наук, доцент
Новоселецький Олександр Миколайович

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

РОБОТА ДОПУЩЕНА ДО ЗАХИСТУ
Завідувач кафедри економіко-математичного моделювання та інформаційних технологій _____ (проф., д.е.н. Кривицька О.Р.)
Протокол № ____ від « ___ » _____ 2024 р.

Острог, 2024

Міністерство освіти і науки України
Національний університет «Острозька академія»

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

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

ЗАВДАННЯ
на кваліфікаційну роботу студента

_____Чернявського Андрія Володимировича _____

(прізвище, ім'я, по батькові)

1. Тема роботи «Стратегічне управління ризиками в ІТ-компаніях: всебічний аналіз стратегій зменшення ризиків у розробці та розгортанні ІТ-додатків»_____

керівник роботи ___кандидат економічних наук_____,

_____доцент Новоселецький Олександр Миколайович_____

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджено наказом ректора НаУОА від "_03__" __листопада_ 2023 року №_98__

2. Термін здачі студентом закінченої роботи: _____05.12.2024_____

3. Вихідні дані до роботи: наукові праці та нормативні документи стосовно керування ризиками, стратегії управління ризиками, моделі оцінки та аналізу ризиків.

4. Перелік завдань, які належить виконати: визначити теоретичні аспекти управління ризиками в ІТ-компаніях, провести дослідження ризиків у розробці та розгортанні ІТ-додатків, здійснити оцінку ризиків на реальному ІТ-проєкті, розробити стратегії управління ризиками, провести SWOT-аналіз, запропонувати стратегії вдосконалення. _____

5. Перелік графічного матеріалу: схематично відобразити механізм взаємодії замовника та виконавця ІТ-проекту.

6. Консультанти розділів роботи:

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

7. Дата видачі завдання: _____01.12.23_____

КАЛЕНДАРНИЙ ПЛАН

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

Студент: _____ _____

(підпис) (прізвище та ініціали)

Керівник кваліфікаційної роботи: _____ _____

(підпис) (прізвище та ініціали)

АНОТАЦІЯ

кваліфікаційної роботи на здобуття освітнього ступеня магістра за спеціальністю
122 Комп'ютерні науки ОПП
«Управління проєктами»
Національний університет «Острозька академія».
Кафедра економіко-математичного моделювання та інформаційних технологій.–
Острог, 2024

Тема: **Стратегічне управління ризиками в ІТ-компаніях: всебічний аналіз стратегій зменшення ризиків у розробці та розгортанні іт-додатків.**

Загальний обсяг роботи становить 129с., зокрема 10 таблиць, 1 рисунок та 53 джерела використаної літератури, три розділи, вступ і висновки.
Автор: Чернявський Андрій Володимирович
Науковий керівник: кандидат економічних наук, доцент
Новоселецький Олександр Миколайович
Захищена «_____»___ _____2024 року

Короткий зміст кваліфікаційної роботи.

Дана робота присвячена дослідженню ризиків, що виникають під час розробки та впровадження системи UMSystem, яка орієнтована на освітні установи. У роботі розглянуто основні теоретичні аспекти управління ризиками в ІТ-проектах. Проаналізовано основні ризики технічного, організаційного, бізнесового, безпекового та комунікаційного характеру. Окрему увагу приділено кіберзагрозам і фізичним загрозам, пов'язаним із військово-політичною ситуацією в Україні.

На основі проведеного SWOT-аналізу виявлено ключові сильні та слабкі сторони UMSystem, можливості для подальшого розвитку, а також загрози, які можуть вплинути на успішність впровадження та використання системи. У роботі надано рекомендації щодо мінімізації ризиків на кожному етапі розробки, зокрема шляхом впровадження сучасних методів управління, таких як Agile, DevOps, регулярне пентестування та багаторівневі заходи безпеки.

Результати дослідження можуть бути використані для підвищення ефективності роботи ІТ-компаній, що розробляють та впроваджують подібні системи, а також для забезпечення стабільності та безпеки інформаційних технологій в умовах сучасних викликів.

Ключові слова: ризик, управління, управління ризиками, інформаційні технології (ІТ).

ANNOTATION

qualifying work for obtaining a master's degree in the specialty
122 Computer Science EPP «Project Management»
The National University of Ostroh Academy
Department of Economic and Mathematical Modeling and Information Technology. – Ostroh, 2024

Topic: **Strategic risk management in IT companies: a comprehensive analysis of risk reduction strategies in the development and deployment of IT applications**

The total volume of the work is 129 pages, including 10 tables, 1 figure, and 53 references. The study consists of three chapters, an introduction, and conclusions.
Author: Andrii Volodymyrovych Cherniavskyi
Academic Supervisor: candidate of economic sciences, associate professor
Oleksandr Mykolayovych Novoseletskyi
Protected «_____», _____, 2024

Brief Summary of the Qualification Work

This research focuses on the study of risks associated with the development and implementation of the UMSystem, a platform designed for educational institutions. The work examines the fundamental theoretical aspects of risk management in IT projects and conducts an analysis based on contemporary models such as COSO ERM and FMEA. The research investigates key technical, organizational, business, security, and communication risks. Particular attention is given to cyber threats and physical risks arising from the ongoing military and political situation in Ukraine.

A SWOT analysis was conducted to identify the key strengths and weaknesses of UMSystem, opportunities for further development, and potential threats that may impact the success of the system's deployment and operation. The research provides recommendations for mitigating these risks at various stages of development, including the implementation of modern management methodologies such as Agile, DevOps, regular penetration testing, and multi-layered security strategies.

The findings of this research can be utilized to enhance the efficiency of IT companies involved in developing and implementing similar systems, while ensuring the stability and security of information technologies in the face of contemporary challenges.

Keywords: risk, management, risk management, information technology (IT).

ЗМІСТ

ВСТУП

Сучасний IT-сектор визначається високою динамікою змін та постійним розвитком. У цьому контексті стратегічне управління ризиками набуває особливого значення для IT-компаній, які зустрічаються зі складністю технологічних виробництв, підвищеною конкуренцією та швидкими темпами інновацій.

Актуальність. В умовах швидкого розвитку інформаційних технологій та високої динаміки змін на ринку, управління ризиками в IT-проектах стає не лише важливим, а й критичним елементом для забезпечення стабільності і надійності розроблених систем. Система UMSystem, орієнтована на освітні установи, є прикладом складного IT-проекту, що потребує ретельного підходу до оцінки та управління ризиками на всіх етапах її розробки та впровадження. Враховуючи поточні виклики, такі як економічна нестабільність, геополітична ситуація в Україні та розвиток нових технологій, ефективне управління ризиками допомагає не лише забезпечити стабільну роботу системи, але й запобігти можливим загрозам, що можуть вплинути на її успішну реалізацію.

Актуальність цієї теми також підкріплюється необхідністю підвищення надійності та безпеки IT-додатків у складних умовах, зокрема з урахуванням військових загроз, кібератак та проблем із персоналом через зовнішні обставини. Врахування таких чинників у системі управління ризиками є важливим для кожного етапу розробки, починаючи від ідеї до впровадження та супроводу. Оцінка ризиків дозволяє проактивно виявляти слабкі місця, своєчасно адаптувати стратегії та знижувати ймовірність негативних наслідків для проекту.

Стан наукової розробки даної теми підтверджує наявність численних досліджень у галузі управління ризиками та стратегічного управління. Це відображається у працях визнаних авторів. Роботи Гарольда Керзнера визначають стандартні практики управління проектами. У стратегічному управлінні важливий внесок зробили У. С. Кім та Р. Моборн з концепцією "Стратегії блакитного океану", а також Роберт С. Каплан та Девід П. Нортон. Девід Хіллсон досліджує аспекти управління ризиками в проектах. У галузі інновацій та Lean-підходів важливі внески внесли Ерік Ріс з концепцією Lean Startup та Джефф Сазерленд з методологією Scrum.

Ці автори створили основу для подальших наукових досліджень та практичного застосування стратегій у реальних проектних умовах. У своїх роботах автори також акцентують увагу на важливості адаптації цих методів до конкретних умов, таких як економічні або політичні зміни, що є надзвичайно важливим для оцінки ризиків у розробці складних IT-систем, таких як UMSystem. Ряд вітчизняних вчених, таких як І.В.Федулова, І.В. Макарчук, І.В. Данилюк, О.А. Лаговська, І.Л. Грабчук, К.Назарова [до кожної пункт в літ-рі] не припиняють досліджувати ці питання і в даний момент. Враховуючи швидкі темпи розвитку технологій та змін в бізнес-середовищі, важливо постійно адаптувати стратегії зменшення ризиків до нових реалій.

Метою даного дослідження є системний аналіз та розробка стратегій зменшення ризиків для IT-компаній, які здійснюють розробку та розгортання програмних продуктів, а також аналіз основних ризиків, що виникають при розробці та впровадженні IT-додатків та розробка рекомендацій щодо їх мінімізації шляхом впровадження сучасних моделей управління ризиками. Для досягнення цієї мети визначено наступні завдання:

- Дослідити існуючі моделі управління ризиками для IT-компаній;
- Оцінити вплив ризиків на ефективність роботи IT-додатків.
- Виявити основні ризики на етапах розробки та впровадження UMSystem;
- Запропонувати стратегії зменшення ризиків для UMSystem.

Об'єктом дослідження є система управління ризиками в IT-проектах, на прикладі UMSystem.

Предметом дослідження є методи управління ризиками на етапах розробки та впровадження IT-додатків.

Методологічна база дослідження: визначається комплексом наукових та практичних підходів, що використовуються для системного аналізу та розробки стратегій управління ризиками в IT-компаніях. Основні методи та підходи включають:

1. Аналіз ризиків: Використання методів ідентифікації та оцінки ризиків на етапах розробки та розгортання IT-додатків. Застосування технік SWOT-аналізу для визначення сильних і слабких сторін, можливостей та загроз.

2. Стратегічне управління: Використання стратегічного аналізу для визначення ключових цілей, напрямків розвитку та вибору стратегій зменшення ризиків.

3. Оптимізація стратегій: Використання кількісних методів оптимізації для підбору ефективних стратегій зменшення ризиків при впровадженні IT-додатків.

4. Практичні дослідження: Реалізація аналізу ефективності розроблених стратегій на реальних проектах в IT-сфері з метою оцінки їхнього впливу на зменшення ризиків.

5. Літературний аналіз: Вивчення та аналіз наукових публікацій, книг, статей та методичних матеріалів з області управління ризиками, стратегічного управління та інших відповідних тем.

Ця методологічна база дозволяє здійснювати комплексний аналіз та розробку стратегій управління ризиками в IT-компаніях, враховуючи як теоретичні аспекти, так і практичний досвід реальних проектів.

Структура роботи. Робота складається зі вступу, трьох розділів, висновків та списку використаних джерел. У першому розділі розглянуто теоретичні аспекти управління ризиками в IT-компаніях. Другий розділ присвячений аналізу ризиків на різних етапах розробки IT-додатків. Третій розділ містить практичні рекомендації щодо зменшення ризиків для UMSystem.

Апробація. Результати дослідження були апробовані під час роботи над системою UMSystem. Практична частина дослідження, зокрема рекомендації щодо мінімізації ризиків, була обговорена та апробована командою розробників UMSystem, що підтверджує ефективність запропонованих заходів.

РОЗДІЛ 1.
ТЕОРЕТИЧНІ АСПЕКТИ УПРАВЛІННЯ РИЗИКАМИ В ІТ-КОМПАНІЯХ

1.1. Основні поняття та типи ризиків у сфері ІТ

Робота будь-якого підприємства завжди супроводжується наявністю невизначеності, яка виникає як через внутрішні, так і через зовнішні чинники. Зміни в таких сферах, як економіка, політика, соціальні процеси або технологічні інновації, можуть суттєво впливати на функціонування компанії, створюючи нові ризики. У зв'язку з цим постійно виникає потреба в аналізі цих ризиків і розробці ефективних стратегій для їх мінімізації. Управління ризиками, в свою чергу, є не лише важливим аспектом для підтримки ефективної діяльності підприємства, але й показником його здатності адаптуватися до змін, готовності до непередбачуваних подій та рівня стратегічної зрілості.

Термін «ризик» має багатий історичний контекст. Він походить від грецьких слів «ridsikon» та «ridsa», що в перекладі означають «стрімчак» або «скеля». Як зазначають мовознавці, це поняття має етимологічне коріння в Південній Америці, де місцеві народи використовували його для опису небезпек на морі, таких як можливість зіткнення з підводними скелями або потрапляння в шторм. У ширшому сенсі ризик почали розглядати як ситуацію, що містить потенційну небезпеку або невизначеність. З розвитком науки і філософії це поняття значно змінило своє тлумачення, ставши важливою категорією для вивчення людської діяльності в цілому.

З поширенням теорії ймовірностей розуміння ризику стало більш систематизованим і науково обґрунтованим. Ймовірність настання події і потенційні наслідки цих подій стали основними елементами для оцінки ризиків. У цьому контексті ризик визначається як ймовірність того, що певна подія відбудеться, а також можливі наслідки цього процесу. Тому управління ризиками стало невід'ємною частиною сучасного менеджменту.

У широкому вжитку термін «ризик» почав набувати особливої популярності в економічній літературі з початку XX століття. Однією з найбільш значущих праць,

яка сприяла цьому, є робота Френка Найта «Ризик, невизначеність та прибуток» [1]. У цій фундаментальній праці, що є основою його кандидатської дисертації, Найт запропонував чітке розмежування між поняттями «ризик» і «невизначеність». Він стверджував, що ризик проявляється в ситуаціях, де результати невідомі, але існує можливість передбачити розподіл ймовірностей для цих результатів. Отже, ризик можна розглядати як явище, яке піддається прогнозуванню та оцінці при прийнятті управлінських рішень.

Крім того, важливий вклад у розуміння концепції ризику зробив Дуглас Хаббард, який у своїй праці «Збій управління ризиками: чому він зламаний і як це виправити» [2, с. 146–164] представив власну інтерпретацію понять «ризик» та «невизначеність». Згідно з його концепцією, невизначеність – це стан, коли неможливо точно передбачити розвиток подій, і існує кілька можливих варіантів. Невизначеність можна виміряти за допомогою ймовірностей для кожного з можливих сценаріїв.

На думку Хаббарда, ризик є особливою формою невизначеності, коли деякі з можливих результатів включають серйозні наслідки, такі як фінансові втрати, травми чи катастрофи. Він підкреслює, що вимірювання ризику передбачає оцінку набору сценаріїв із відповідними ймовірностями та кількісною оцінкою можливих втрат. Тому управління ризиками виступає важливим інструментом у забезпеченні стабільності і безпеки підприємства, даючи можливість мінімізувати негативні наслідки та запобігти серйозним збиткам.

Сучасні методи управління ризиками включають інтеграцію кількісного та якісного аналізу, застосування інформаційних технологій для моделювання різних сценаріїв ризиків і розробку відповідних стратегій для зменшення ймовірності їхнього настання. Як наголошує Хаббард, ефективне управління ризиками не лише дозволяє компанії уникати катастрофічних наслідків, але й може істотно підвищити її конкурентоспроможність і забезпечити стабільність у довгостроковій перспективі.

Поняття «ризик» є одним з основних предметів дослідження в науці, оскільки воно служить важливим інструментом для оцінки і прогнозування невизначеностей у різних сферах діяльності людини. Цьому поняттю приділяють значну увагу як

вітчизняні, так і зарубіжні науковці, серед яких варто відзначити таких авторів, як В.Д. Базилевич, О.І. Барановський, Л. Бевер, В.В. Вітлінський, М.С. Горбач, Л.М. Гутко, М.І. Дорошенко та інших. Вони аналізують різні аспекти «ризику», зокрема його визначення, класифікацію та методи управління ним у різних сферах. Питання управління ризиками є також предметом досліджень таких науковців, як І.В. Федулова, В.В. Черкасов, А.О. Старостіна та інших.

З розширенням економічної діяльності та зростанням її різноманітності, поняття «ризик» почало активно застосовуватися в багатьох сферах економіки та бізнесу. Особливо важливе значення воно набуло у другій половині XX століття, коли з'явилися нові технології та методи управління великими проєктами. Розвиток проєктного менеджменту в США, що був обумовлений космічними програмами НАСА, дозволив поглибити розуміння ризиків у великих проєктах. В 1959 році в журналі Harvard Business Review [3] була опублікована стаття, в якій вперше згадується посада проєктного менеджера, що стало основою для систематизації управління проєктами. У 1969 році в США було засновано Інститут управління проєктами (PMI) [4, с. 42–54], який взяв на себе роль координатора та стандартизатора у галузі проєктного менеджменту, зокрема у розробці та поширенні практик управління ризиками.

На початку XXI століття проєктний підхід до управління бізнесом став основною стратегією для багатьох компаній, які прагнули досягти більшої ефективності та адаптивності. Це стало можливим завдяки успішному впровадженню проєктних методів, що зародилися під час промислової революції в Англії у середині XX століття, а також через швидкий розвиток інформаційних технологій. Сьогодні проєктний підхід застосовується не лише в інженерії та технології, але й у фінансах, маркетингу, консалтингу та багатьох інших сферах. Відповідно до ДСТУ ISO 73:2013 «Керування ризиком: словник термінів», ризик визначається як невизначеність щодо досягнення цілей [5], що підкреслює його сутність як управління в умовах невизначеності і змін.

Дослідження проєктних ризиків привертає особливу увагу, оскільки вони мають значний вплив на успішність проєктів в умовах глобалізації та швидкого

технологічного прогресу. Серед вітчизняних та зарубіжних дослідників, таких як Є. Верзух, Р. Брейлі, Дж. Бейлі, Ф. Кліффорд Грей, К. Редхед, У. Шарп та Д. Філліпс, є важливі роботи, що сприяють розробці методів мінімізації ризиків у рамках проєктного менеджменту. Українські науковці, серед яких Л.П. Батенко, І.І. Глущенко, В.І. Воропаєв, Р.М. Качалов, Б.А. Колтинюк, також суттєво доповнили наукову літературу, зокрема в частині управління ризиками в контексті національної економіки та бізнес-процесів.

Управління ризиками в проєктах із розробки та підтримки програмного забезпечення є особливо важливим в умовах швидких технологічних змін. Українські науковці, такі як І.О. Башинська, А.М. Акименко, Н.І. Галенко, зосереджують свою увагу на вивченні специфічних аспектів ризиків, пов'язаних з розробкою програмних продуктів, та на методах їх мінімізації в рамках проєктів, що мають високу ступінь невизначеності та технічної складності. Роботи зарубіжних вчених, зокрема Тома Де-Марко, Тімоті Лістера та Елані М. Хол, також активно сприяють розвитку теорії та практики управління ризиками в ІТ-проєктах, де акцент робиться на швидких змінах та необхідності своєчасної адаптації до нових умов.

Незважаючи на велике число публікацій, що присвячені визначенню «проєктного ризику», єдиної трактовки цього поняття серед науковців досі немає. В.О. Москаленко [6, с. 129–136] у своїй роботі визначає ризик проєкту як невизначену подію або умову, яка може вплинути як негативно, так і позитивно на одну з цілей проєкту. Це трактування дає змогу гнучко підходити до оцінки ризиків і враховувати як негативні, так і позитивні наслідки.

О.А. Гавриш [7, с. 50–51] у своїй роботі доповнює це визначення, розглядаючи проєктний ризик як набір ризиків, що можуть вплинути на економічну ефективність проєкту. Вона робить акцент на фінансових аспектах ризику, який виникає через внутрішні та зовнішні фактори, що впливають на бюджет проєкту під час його виконання. Такий підхід дозволяє краще оцінити фінансові ризики та розробити стратегії для їх мінімізації.

У спільній статті «Управління ризиками в проектному менеджменті», написаній Скопенко Н.С., Євсєєвою І.В. та Москаленком В.О. [8, с. 41–44],

акцентується увага на важливості розуміння причин і механізмів виникнення ризиків. Автори підкреслюють, що ефективність проєкту значною мірою залежить від того, наскільки вчасно були вжиті належні заходи для управління ризиками. Вони також відзначають, що ризик-менеджмент є важливим інструментом для мінімізації наслідків ризиків у нестабільному та швидко змінюваному середовищі.

Для проєктів, що стосуються розробки програмного забезпечення, доцільно уточнити трактування поняття проєктного ризику, визначивши, що ризик IT-проєкту включає не лише ймовірність виникнення подій, пов’язаних із технічними труднощами, перевищенням бюджету або затримками в розробці, але й ситуації, коли проєкт може зіштовхнутися з проблемами під час інтеграції нових технологій, виникненням непередбачених технічних труднощів або нестабільністю платформ розробки. Кожен з цих аспектів може суттєво вплинути на реалізацію проєкту, зокрема на своєчасність виконання робіт, виконання вимог зацікавлених сторін і на весь процес розробки програмного забезпечення. Оскільки IT-проєкти часто стикаються з численними технологічними та організаційними викликами, результати ризикових подій можуть бути як негативними, так і позитивними, що слід враховувати при розробці стратегій управління ризиками.

У зв'язку з тим, що проєктна діяльність підприємств здійснюється в умовах значної невизначеності, правильна оцінка та ефективне управління ризиками є критично важливими для успішного завершення проєкту. Оцінка ризиків на початкових етапах та вжиття заходів для їх мінімізації не лише знижує ймовірність виникнення проблем, але й дозволяє запобігти значним втратам, що можуть виникнути через неефективне управління ризиками. Таким чином, своєчасне виявлення ризиків і розробка чітких планів дій для їх зниження є одним із головних завдань та важливих аспектів проєктного менеджменту. Це дозволяє підвищити гнучкість проєкту і дає можливість швидше адаптуватися до змінюваних умов.

Одним з найважливіших етапів є точна ідентифікація ризиків, оскільки саме від цього залежить можливість ефективного планування стратегій для уникнення чи зниження наслідків можливих загроз. Ідентифікація ризиків є невід'ємною частиною стратегії управління ризиками. Основним документом, що визначає методи

ідентифікації ризиків, є міжнародний стандарт ISO/IEC 31010:2009 Risk management – Risk assessment techniques (Ризик-менеджмент – Техніки оцінювання ризиків), який надає перелік з 31 техніки ідентифікації ризиків. Цей стандарт дозволяє організаціям системно підходити до аналізу ризиків, використовуючи різноманітні методи для виявлення потенційних загроз.

У статті І.В. Федулової [9, с. 29–45] «Ідентифікація ризиків як складова ризик-менеджменту» докладно розглядаються 13 основних методів ідентифікації ризиків, які можна застосовувати в різних сферах проєктної діяльності. Серед них є як якісні методи, що базуються на експертних оцінках та аналізі можливих сценаріїв розвитку подій, так і кількісні методи, що дозволяють точніше вимірювати ймовірність виникнення ризиків і їх можливий вплив на проєкт. Проте слід зазначити, що IT-проєкти, особливо в сфері розробки програмного забезпечення, часто реалізуються в умовах високої невизначеності, оскільки існує велика кількість варіантів реалізації, зокрема через застосування різних мов програмування та інструментів розробки. У таких умовах вибір найефективнішої стратегії для реалізації проєкту може бути складним, а управління ризиками вимагає застосування більш гнучких і адаптивних підходів, що дозволяє постійно коригувати стратегію в залежності від змін у процесі розробки.

Зважаючи на численну кількість проєктних ризиків, правильна класифікація є ключовим аспектом у їх ефективному управлінні. Це дозволяє чітко визначити характер і потенційні наслідки кожного ризику, що, в свою чергу, сприяє прийняттю обґрунтованих рішень для мінімізації негативних впливів. Класифікація ризиків також допомагає зосередитися на найбільш значущих і критичних для проєкту загрозах, що забезпечує пріоритетність ресурсів і уваги. Вона є основою для подальшої оцінки та аналізу, що необхідно для прогнозування та розробки стратегії управління ризиками. Таким чином, правильна і чітка класифікація ризиків є фундаментом для успішного управління проєктами, особливо в умовах високої невизначеності та складності.

Наукові дослідження розглядають різноманітні підходи до класифікації ризиків, що залежать від конкретних об’єктів класифікації. Кожен підхід має свої

особливості та акценти, що дозволяє детальніше аналізувати різні аспекти ризиків. Зокрема, класифікація може базуватись на характеристиках, таких як ймовірність виникнення, ступінь впливу або етапи життєвого циклу проєкту. Вибір конкретного підходу до класифікації допомагає не лише систематизувати ризики, але й забезпечити ефективне управління ними. Таким чином, різноманітність підходів дозволяє створити більш гнучку та адаптовану модель для управління ризиками в залежності від умов конкретного проєкту.

Гавриш О.А. та Мельникова В.А. [10] пропонують таку класифікацію згідно об’єктів класифікування:

- за ймовірністю настання;
- за факторами;
- за фазами;
- за розміром можливих наслідків;
- за ступенем ризику.

Петренко О.Н. пропонує таку класифікацію проєктних ризиків, що базується на об’єкті класифікації. [11]:

1. за фазами (етапами) проєктної діяльності:
- ризики доінвестиційної фази;
- ризики інвестиційної фази;
- ризики експлуатаційної (виробничої) фази.
2. за можливістю впливу на виникнення ризиків:
- внутрішні (ендогенні);
- зовнішні (екзогенні).
3. за можливістю захисту від ризиків:
- ризики, які страхують;
- ризики, які не страхують.
4. За динамікою
- статичні;
- динамічні.

Ноздріна Л.В. [12, с. 211-274] пропонує декілька класифікацій проектних ризиків:

- в залежності від джерела виникнення: природно-кліматичні, технічні, виробничі, економічні, ринкові, ризики навмисних дій та інші;
- в залежності від місця виникнення: зовнішні та внутрішні;
- в залежності від тяжкості проявів: витрачена вигода, збитки, втрата, банкрутство;
- за ступенем передбачуваності: передбачувані з малою ймовірністю, непередбачувані;
- за можливістю страхування: ризики, що страхуються та ризики, що не страхуються;
- за критеріями ймовірності та наслідків ризику(«тигри» - висока ймовірність та вагомі наслідки, ці ризики є дуже небезпечними та мають бути негайно усунені; «алігатори» - низька ймовірність та вагомі наслідки - небезпечні ризики, котрих можна уникнути, якщо їх ретельно відслідковувати; «цуценята» - висока ймовірність та незначні наслідки; «кошенята» - низька ймовірність та незначні наслідки).

Бутко М.П. [13, с. 313-388] класифікує ризики відповідно до джерела виникнення:

1. технічні ризики:
- ризики, пов’язані зі змістом роботи;
- ризики визначення вимог до результатів роботи;
- ризики правильної оцінки, суб’єктивні судження;
- ризики технічних процесів;
- технологічні ризики;

2. управлінські ризики:
- ризики проектного менеджменту;
- ризики портфоліо/програмного менеджменту:
- операційні ризики;
- організаційні ризики;
- ресурсні ризики та інші.

3. комерційні ризики:

- ризики контрактних умов та термінів;
- закупівельні ризики;
- ризики по роботі з постачальниками та підрядниками;
- ризики по роботі з клієнтами та інші.

4. зовнішні ризики:

- ризики зміни законодавства;
- курсові ризики (валютні ризики);
- погодні ризики та інші.

Грунтовне дослідження з даної тематики провів Макарчук Іван Віталійович [14], що дослідивши всі вищевказані підходи систематизував їх та об’єднав в наступну класифікацію:

1. Технологічні ризики:

- ризики використання неперевірених технологій;
- ризик технічних збоїв;
- ризик сумісності;
- ризик вразливості систем безпеки;
- ризик простою системи;
- ризик втрати даних;

2. Ризики недотримання плану-графіку реалізації ІТ-проекту:

- ризики розповзання охоплення проєкту;
- ризик нереалістичних термінів виконання;
- ризик неякісної оцінки завдання;
- ризик обмеження ресурсів в часі;
- ризик неочікуваних затримок;

3. Ризики бюджету ІТ-проєкту:

- ризик перевитрати бюджету;
- ризик несподіваних витрат;
- ризик неякісного фінансового управління;

4. Комунікаційні ризики:

- ризик слабкої комунікації в команді проєкту;
- ризик неякісної комунікації зі стейкхолдерами;
- ризик неоднозначності в заявлених вимогах ІТ-проекту;
- ризик неадекватного зворотного зв'язку;

5. Ризики якості продукту в рамках ІТ-проєкту:

- ризик отримання результату низької якості;
- ризик наявності дефектів програмного забезпечення;
- ризик неналежного тестування;

6. Ризик людських ресурсів ІТ проєкту:

- ризик недостатнього обсягу навчених людських ресурсів;
- ризик високої плинності кадрів поміж членів команди;
- ризик командного конфлікту;
- ризик вигорання членів команди;

7. Кон’юнктурні ризики ІТ-проєкту:

- ризик настання кризи на рівні глобальної або національної економіки;
- ризик настання кризи на рівні галузі, в рамках якої розробляється продукт;
- ризик настання кризи на рівні компанії-замовника ІТ-проекту;

8. Ризики регуляторного обмеження ІТ проєкту:

- ризик законодавчих і регуляторних змін;
- ризик посилення регуляторного поля в галузі виконання ІТ-проекту;
- ризик міжнародних регуляторних обмежень;
- ризик недотримання регуляторних вимог;
- ризик непередбачуваних регуляторних обмежень.

Оскільки дана класифікація є найновішою та включає діапазон всіх попередніх, то в подальшій роботі ми будемо використовувати саме її.

У результаті розгляду основних понять та типів ризиків у сфері ІТ можна зробити кілька важливих висновків. По-перше, управління ризиками в ІТ-сфері є ключовим елементом забезпечення стабільної та безпечної діяльності компаній, оскільки технологічні зміни, невизначеність та технічні складнощі можуть суттєво

впливати на результати проєктів. Ризики в ІТ-галузі мають різноманітні форми та джерела, що потребує комплексного підходу до їх ідентифікації, класифікації та оцінки. Поширення концепції ризику в бізнесі та науці сприяло розвитку нових методів управління ризиками, що поєднують як кількісні, так і якісні підходи, дозволяючи ефективно прогнозувати можливі загрози та зменшувати їхні наслідки.

Зокрема, в ІТ-проєктах, що часто стикаються з високою невизначеністю, особливу важливість набувають методи адаптивного управління ризиками. Це дозволяє не тільки мінімізувати можливі негативні наслідки, але й відкриває нові можливості для оптимізації проєктів і досягнення кращих результатів. Підходи до класифікації ризиків, розроблені різними дослідниками, надають чітке уявлення про їхню природу та ступінь впливу, що дозволяє зосередити зусилля на найбільш критичних загрозах.

Отже, ефективне управління ризиками в ІТ є не тільки важливим інструментом для забезпечення безпеки та стабільності проєктів, але й важливою складовою стратегічної зрілості компаній, що прагнуть успішно адаптуватися до швидко змінюваного технологічного середовища.

1.2. Стратегії управління ризиками в ІТ-проектах

Управління ризиками є ключовим елементом успішного виконання будь-якого ІТ-проєкту, оскільки сучасне інформаційне середовище характеризується високою швидкістю змін, складністю технологій та непередбачуваністю зовнішніх факторів. ІТ-проєкти, як правило, мають великий масштаб і багатокомпонентну структуру, що робить їх вразливими до різноманітних ризиків, включаючи технологічні, організаційні, фінансові, а також ризики, пов'язані з людським фактором і зовнішніми умовами, такими як зміни в законодавстві чи економічних умовах.

Особливістю ІТ-проєктів є їхня швидка адаптація до нових вимог та можливість значних коригувань на будь-якій стадії реалізації, але це також означає, що ризики можуть виникати на будь-якому етапі — від початкового планування до стадії експлуатації та підтримки. Без належного управління ризиками, проєкти

можуть стикатися з непередбаченими труднощами, які призводять до збільшення витрат, затримок у термінах виконання, погіршення якості результату або навіть до повного зриву проєкту.

Один із основних підходів до успішного управління ризиками полягає в їх проактивному виявленні, оцінці та плануванні заходів, спрямованих на зменшення ймовірності негативних наслідків. Це включає в себе використання різноманітних стратегій, таких як уникнення, зниження, передача або прийняття ризиків, що дозволяють ефективно мінімізувати можливі загрози для проєкту. Ключовим є вміння вибрати правильну стратегію в залежності від характеру ризику та специфіки проєкту, зокрема його масштабу, складності та термінів виконання.

Ризики, як правило, не можуть бути усунені повністю, однак їх можна зменшити до прийнятного рівня шляхом обґрунтованого управлінського підходу. Таким чином, стратегії управління ризиками допомагають не лише мінімізувати негативні наслідки, але й сприяють створенню умов для максимально ефективної реалізації проєкту, підтримання бюджету та дотримання термінів.

У цьому підрозділі розглядатиметься комплекс основних стратегій управління ризиками в ІТ-проєктах, їх застосування в різних ситуаціях, а також методи, які дозволяють проактивно реагувати на потенційні загрози. Оцінка та вибір відповідних стратегій на різних етапах проєкту є важливим елементом для забезпечення його успішного виконання в умовах постійних змін та непередбачуваних ситуацій.

Так само як і з класифікацією існують різні підходи і до стратегій управління ризиками. Так автори Грабіна К. В. і Шендрик В. В. в своїй роботі “Метод управління ризиками ІТ-проєктів з врахуванням загроз та можливостей”[15] розглядають стратегії з точки зору реагування на невизначеність, загрозу та можливості.

Усі проєкти піддаються ризикам, оскільки є унікальними системами з різною складністю, що здійснюються з метою отримання вигоди для стейкхолдерів. Вони реалізуються в умовах обмежень, припущень і різних, часом суперечливих, очікувань стейкхолдерів, які можуть змінюватися. Команда проєкту повинна свідомо та контрольовано брати на себе ризики в процесі виконання проєкту, щоб забезпечити створення цінності, враховуючи як ризики, так і вигоди [16;17;18].

Це означає, що проєкти функціонують у середовищі, яке характеризується різними рівнями невизначеності, де можуть приховуватися як можливості, так і загрози. Тому команди проєктів повинні активно вивчати, оцінювати та вирішувати, як реагувати на них.

Основною метою управління ризиками є виявлення ризиків та ефективне їх управління, які не охоплюються іншими процесами проєктного управління. Якщо ризики залишаються неконтрольованими, це може призвести до відхилення від запланованих цілей і неуспішного завершення проєкту. Тому ефективність управління ризиками безпосередньо впливає на ймовірність успіху проєкту.

Невизначеність загалом означає стан, коли майбутні події або наслідки не можуть бути точно передбачені. Вона включає різні аспекти:

- ризик, пов'язаний із незнанням майбутніх подій;
- неоднозначність, що виникає через невизначеність поточних або майбутніх умов;
- складність, зумовлена динамічними системами, які швидко змінюють свої характеристики і можуть мати непередбачувані результати.

Для успішного подолання невизначеності важливо розуміти середовище, в якому функціонує проєкт. Серед факторів, які впливають на невизначеність проєкту, можна виділити:

- Економічні фактори: доступність ресурсів, умови кредитування, інфляція;
- Технічні фактори: нові або перспективні технології, складність систем, інтерфейси;
- Юридичні та законодавчі обмеження і вимоги;
- Фізичне середовище: умови праці, безпека, кліматичні умови;
- Соціальні впливи, зокрема громадська думка;
- Політичні впливи, як внутрішні, так і зовнішні.

Невизначеність є невід'ємною характеристикою будь-якого проєкту, що ускладнює прогнозування наслідків діяльності та створює різноманітні кінцеві результати — як можливості, так і загрози. Можливість — це подія, що приносить вигоду цілям проєкту, а загроза — подія, яка має негативний вплив. Вони разом

формують ризики проєкту, на які можна реагувати різними стратегіями (див. табл. 1.1).

Таблиця 1.1

Стратегії реагування на невизначеність

№	Стратегія реагування	Опис стратегії реагування
1	Збирання інформації	У деяких випадках невизначеність можна зменшити за рахунок отримання додаткової інформації, зокрема проведення досліджень, залучення експертів або аналізу ринку.
2	Підготовка до декількох кінцевих результатів	За допомогою цієї стратегії реагування команда проєкту повинна мати окрім основного рішення, ще й резервний план на випадок надзвичайних ситуацій.
3	Проєктування на основі набору	Кілька варіантів проєктування або альтернатив команда проєкту може дослідити на початковому етапі. Це допоможе знайти компроміс, зокрема: між часом та вартістю, якістю та вартістю, ризиком та розкладом, розкладом та якістю.
4	Розвиток стійкості	Команда проєкту повинна мати можливість навчатися, адаптуватися та швидко реагувати на несподівані зміни [15].

Таким чином, ризики є невід’ємною частиною невизначеності. Ризик визначається як подія чи умова, яка має невизначений характер і, якщо відбудеться, може вплинути на одну або більше цілей проєкту, як позитивно, так і негативно.

Члени команди проєкту повинні постійно виявляти ризики протягом всього життєвого циклу проєкту, щоб мінімізувати негативний вплив загроз і максимально використовувати можливості. Як загрози, так і можливості мають конкретні стратегії реагування, які повинні бути заздалегідь заплановані для реалізації у разі виникнення ризику.

Загроза – це подія або умова, яка у випадку настання негативно впливає на одну або кілька цілей. Для боротьби із загрозами можна використовувати будь-яку із п’яти альтернативних стратегій (табл. 1.2).

Таблиця 1.2

Стратегії реагування на загрозу

№	Стратегія реагування	Опис стратегії реагування
1	Уникнення	Команда проєкту діє з метою усунути загрозу або захистити проєкт від її впливу
2	Ескалація	Команда або спонсор проєкту погоджуються, що загроза виходить за межі проєкту або запропонована реакція перевищить повноваження керівника проєкту
3	Передача	Це перехід володіння загрозою третій стороні для управління ризиком та прийняття наслідків у разі виникнення загрози
4	Пом’якшення	Здійснюються заходи щодо зменшення ймовірності виникнення та/або впливу загрози
5	Прийняття	Ця стратегія передбачає визнання загрози без планування жодних активних заходів [15].

Можливість – це подія або умова, яка у випадку настання позитивно впливає на одну або декілька цілей проєкту. Для роботи із можливостями можна розглянути п’ять альтернативних стратегій (табл. 1.3)

Таблиця 1.3

Стратегії реагування на можливості

№	Стратегія реагування	Опис стратегії реагування
1	Використання	Команда проєкту діє з метою забезпечення настання можливості
2	Ескалація	Команда або спонсор проєкту погоджуються, що можливість виходить за межі проєкту або запропонована реакція перевищить повноваження керівника проєкту.
3	Розподіл	Спільне використання можливостей передбачає передачу володіння можливістю третій стороні, яка може найкраще скористатися вигодою від цієї можливості.
4	Посилення	Здійснюються заходи щодо збільшення ймовірності настання та/або впливу можливості.

5	Прийняття	Ця стратегія передбачає визнання існування нагоди без планування жодних активних заходів [15].

Для зменшення загроз і посилення впливу можливостей під час реалізації проєкту пропонується використовувати профілактичні підходи.

Індивідуальні – заходи, спрямовані на окремі завдання або конкретних учасників команди чи проєкту.

Групові – дії, що охоплюють групи завдань або учасників із подібними причинами виникнення ризиків та можливостей.

Масові – комплексні заходи, які охоплюють усіх учасників та всі завдання проєкту.

Для покращення ефективності управління ризиками в ІТ-проєктах слід удосконалювати чинні процеси з урахуванням як можливостей, так і загроз, а також впроваджувати нові, ще не реалізовані. Досягти цього можна шляхом створення та впровадження інформаційної технології управління ризиками, яка враховуватиме всі аспекти ризиків і можливостей.

Натомість Журан О.А. та Глава М.Г. в своїй роботі “Управління ризиками в ІТ-проєктах” [19] рекомендує здійснювати управління ризиками проєктів за чотирма етапами:

1. Ідентифікація. На цьому етапі виявляються ризики, які можуть завадити досягненню цілей проєкту. Найчастіше зустрічаються технічні ризики, що є типовими для ІТ-проєктів і зазвичай легше піддаються вирішенню. Складнішими є ризики, пов’язані з "політичними інтригами"; "браком підтримки з боку керівництва"; "опором користувачів або підрядників"; "недостатнім фінансуванням".
2. Аналіз. Метою цього етапу є визначення найбільш критичних ризиків, оскільки намагатися боротися з усіма ризиками одночасно є як неефективним, так і економічно невиправданим.
3. Планування. На цьому етапі розробляються стратегії реагування на кожен із критичних ризиків. Найпоширенішими є три підходи:

- Transfer – передача відповідальності за ризик іншій стороні (наприклад, замовнику, партнеру або страховій компанії). Застосовується у випадках, коли самостійно вплинути на ризик неможливо.
- Accept – прийняття ризику без додаткових заходів. Використовується, коли усунути ризик неможливо, а передача відповідальності є надто витратною.
- Mitigate – активне управління ризиком. Передбачає створення основного плану для мінімізації ризику та резервного плану на випадок його реалізації.

4. Моніторинг і контроль. Постійне оновлення плану проєкту та списку ризиків із застосуванням методів прогнозування, серед яких:

- Buffer time – резервування додаткового часу (зазвичай 30% від тривалості задач).
- Load Factor – використання статистичних коефіцієнтів для уточнення строків задач залежно від їх складності та унікальності.
- PERT – розрахунок строків із врахуванням оптимістичного, очікуваного та песимістичного сценаріїв.
- Метод Монте-Карло – моделювання ризиків із високою точністю та можливістю оцінки їхнього рівня в проєкті.

IT-компанії часто страхують ризики та відповідальність через договори із замовниками або фінансові гарантії. Одним із поширених підходів є SLA (Service Level Agreement), який активно застосовується для підтримки програмного забезпечення та аутсорсингових проєктів. Цей підхід забезпечує управління нестандартними ситуаціями, проблемами та рівнем сервісу.

У світовій практиці популярним є страхування професійної відповідальності для захисту від помилок або упущень у розробці та впровадженні IT-систем. Однак в Україні такі страхові послуги наразі не надаються[19].

Управління ризиками є критично важливим для успішної реалізації IT-проєктів, оскільки навіть невеликі непередбачувані події можуть значно вплинути на результат. Ризики можуть виникати на будь-якому етапі життєвого циклу проєкту, починаючи з планування та розробки до впровадження та підтримки. Ризики можуть бути викликані зовнішніми чинниками, такими як зміни в економічному середовищі

або політичні зміни, а також внутрішніми проблемами, зокрема через зміни технологій або невизначеність в бізнес-вимогах. Однак завдяки стратегічному підходу до управління ризиками, проєкти можуть мінімізувати негативний вплив цих ризиків.

Світова практика виділяє наступний ряд стратегій як основні, зокрема це:

- стратегія уникнення ризику;
- стратегія передачі ризику;
- стратегія прийняття ризику;
- стратегія реагування на ризик;
- стратегія гнучкості та адаптації.

Уникнення ризику є однією з найефективніших стратегій для зниження небезпеки для проєкту, оскільки передбачає вжиття заходів для повного усунення можливості виникнення ризику. Це може включати як зміни на етапі планування, так і вибір більш надійних, перевірених технологій. Наприклад, організація може вибрати стабільніші технологічні рішення, замість нових чи експериментальних платформ, що мінімізує технічні ризики. Крім того, до уникнення можна віднести коригування вимог або вибір альтернативних рішень, які знижують ймовірність небажаних подій. Це особливо важливо на етапах аналізу та проектування, коли можна змінити підхід або технології, щоб уникнути потенційних загроз, таких як недостатня масштабованість, низька надійність або відсутність підтримки.

Уникнення ризиків дає можливість контролювати ситуацію на ранніх етапах проєкту, що знижує ймовірність виникнення значних проблем у майбутньому. Однак, важливо пам'ятати, що цей підхід не завжди є можливим для всіх типів ризиків, особливо якщо їхні джерела знаходяться поза межами контролю проєктної команди. Тому ця стратегія, хоч і ефективна, застосовується лише тоді, коли існують об'єктивні можливості для її впровадження[20].

Зниження ризику орієнтоване на зменшення ймовірності виникнення небажаних подій або на зменшення їхніх наслідків. У IT-проєктах ця стратегія є надзвичайно важливою, оскільки багато технічних проблем можуть бути прогнозованими і передбаченими. Застосування цієї стратегії включає використання

резервних копій даних, дублювання інфраструктури, перевірку коду через додаткові тести і застосування надійних технологій, що дозволяє знижувати ймовірність несправностей або збоїв. Це також включає використання методів автоматизації для моніторингу і виявлення проблем на ранніх етапах.

Одним із прикладів зниження ризику є впровадження систем високої доступності та відмовостійкості, таких як резервування сервісів або дублювання критичних компонентів системи. За допомогою таких заходів можна зменшити ймовірність відмови системи і запобігти можливим фінансовим збиткам або шкоді для репутації компанії. Застосування інструментів автоматичного тестування, перевірки коду та систем моніторингу дозволяє своєчасно виявляти недоліки та усувати їх ще до того, як вони переростуть у серйозні проблеми.

Крім того, у випадку ризиків, пов'язаних із людським фактором, використання додаткових навчальних програм для співробітників і створення систем підтримки також дозволяє знижувати ймовірність помилок, що можуть призвести до негативних наслідків. Впровадження стратегії зниження ризиків допомагає ефективно реагувати на можливі загрози ще до їх виникнення.

Передача ризику включає в себе перенесення частини відповідальності за можливі ризики на третіх осіб або організації, такі як аутсорсинг певних задач або укладання контрактів зі страховими компаніями. Це може бути корисно для зменшення фінансових витрат у разі виникнення непередбачених подій або для зниження навантаження на внутрішні ресурси компанії. Наприклад, організація може передати частину своїх ризиків на постачальників або підрядників, які можуть забезпечити високий рівень безпеки, тестування або навіть обслуговування серверів, таким чином зменшуючи ймовірність серйозних проблем для основного проєкту.

Важливим елементом стратегії передачі ризику є правильне формулювання контрактів і угод, що чітко визначають межі відповідальності і правила у разі виникнення проблем. У таких випадках важливо ретельно вибирати постачальників та партнерів, перевіряючи їхній досвід і надійність. Також необхідно враховувати можливі зміни в зовнішньому середовищі, які можуть вплинути на успішність передачі ризику, такі як зміни в законодавстві чи економічних умовах .

Стратегія передачі ризику також включає використання страхування як одного з методів для покриття фінансових ризиків. Це дозволяє організації зменшити своє фінансове навантаження у разі виникнення непередбачених обставин, наприклад, втрат даних або технологічних збоїв[21].

Прийняття ризику є стратегією, що використовується, коли ймовірність негативного впливу ризику є низькою або його наслідки не мають значного впливу на кінцевий результат проєкту. У такому випадку організація може вирішити не вжити додаткових заходів для усунення або зменшення ризику, якщо витрати на це перевищують можливі збитки. Цей підхід може бути виправданим, коли ймовірність настання негативних подій незначна, і витрати на їх запобігання будуть надмірними.

Прийняття ризику передбачає, що компанія погоджується з тим, що певні загрози можуть реалізуватися, але для цього буде підготовлена відповідна стратегії реакції. Це може включати планування резервних фондів або створення спеціальних команд для оперативного вирішення проблем у разі їх виникнення. Зазвичай така стратегія застосовується до менш критичних або малоймовірних ризиків, які не призведуть до серйозних фінансових чи репутаційних втрат[22].

Це дозволяє організації зберігати ресурси і зосередитися на інших важливих аспектах проєкту, таких як інновації або оптимізація процесів. Однак навіть при прийнятті ризику важливо мати план для його швидкого вирішення, щоб зменшити наслідки в разі його реалізації.

Стратегія реагування на ризик включає в себе підготовку до можливих непередбачуваних ситуацій і розробку планів дій для швидкого реагування на ризикові події, коли вони все ж таки реалізуються. Це вимагає створення чітких алгоритмів для обробки інцидентів і визначення відповідальних осіб та ресурсів для вирішення проблем. Наприклад, для технічних збоїв можуть бути розроблені плани відновлення після аварії, які включають в себе чіткі процедури для швидкого відновлення функціональності критичних систем, таких як сервери або бази даних.

Крім того, важливими складовими цієї стратегії є створення спеціальних команд для швидкої реакції на виникнення непередбачених ситуацій. Ці команди повинні бути добре підготовлені і мати чітке уявлення про процеси відновлення.

Наприклад, у випадку збоїв у роботі серверів або програмного забезпечення, компанія може призначити інженерів і технічних експертів, які негайно візьмуть на себе відповідальність за виправлення ситуації, щоб забезпечити мінімальний час простою.

Додатково важливо мати систему моніторингу, яка дозволяє виявляти потенційно небезпечні ситуації на ранніх етапах. Це дозволяє вжити необхідних заходів ще до того, як ризик перерасте в серйозну проблему, зменшуючи таким чином втрати або тривалість інцидентів.

Реагування на ризик також включає в себе відновлення даних після технічних проблем і надання консультаційної підтримки користувачам у разі виникнення проблем у взаємодії з програмним забезпеченням або інфраструктурою. Це дозволяє не лише вирішити проблему, але й зберегти довіру до компанії, продемонструвавши її здатність оперативно вирішувати складні ситуації.

Гнучкість і адаптація є важливими стратегіями в умовах швидко змінюваного середовища, характерного для IT-проєктів. Оскільки технології і вимоги користувачів можуть змінюватися під час реалізації проєкту, організації повинні бути готові швидко адаптувати свої плани і підходи до нових обставин. Одним із основних способів забезпечення такої гнучкості є використання методології Agile, яка дозволяє командам адаптуватися до змін і оперативно виявляти нові ризики.

Застосування Agile-підходу дозволяє швидко реагувати на зміни у вимогах або в умовах ринку, що робить проєкти більш стійкими до зовнішніх впливів. Наприклад, якщо нові технології починають набувати популярності або з'являються нові вимоги до функціональності продукту, команда може швидко адаптувати плани розробки, не порушуючи основний графік або бюджет проєкту.

Гнучкість також передбачає використання інструментів і технологій, які дозволяють зменшити залежність від конкретних рішень або постачальників. Це може включати використання відкритих стандартів, мікросервісної архітектури та інших технологій, які дозволяють легко вносити зміни без значних витрат часу чи ресурсів. Гнучкий підхід дозволяє адаптуватися не тільки до нових технологій, але й до зміни умов зовнішнього середовища, таких як економічні чи політичні зміни, що можуть вплинути на проєкт.

Ця стратегія дозволяє не тільки зменшити ймовірність появи нових ризиків, але й дає можливість ефективно керувати існуючими ризиками, адаптуючи їхнє управління в залежності від змінюваних обставин. Вона також сприяє постійному вдосконаленню процесів управління ризиками, оскільки команди можуть вивчати нові проблеми і використовувати отримані уроки для покращення майбутніх проєктів[23].

Управління ризиками в ІТ-проєктах є невід'ємною частиною їх успішної реалізації, оскільки на кожному етапі проєкту існує безліч потенційних загроз і можливостей, що можуть вплинути на його результат. Важливість правильного вибору стратегії управління ризиками, яка відповідає характеру проєкту, масштабу, складності та специфічним умовам, не можна недооцінювати. Враховуючи швидкість технологічних змін та динамічність зовнішнього середовища, проактивне виявлення, оцінка та зменшення ризиків є ключем до успіху.

Загалом, ефективне застосування стратегій управління ризиками дозволяє зберігати стабільність проєкту в умовах невизначеності, покращувати якість результату та забезпечувати успішне досягнення цілей. Урахування як загроз, так і можливостей дозволяє командам проєктів не тільки уникати негативних наслідків, але й активніше використовувати потенційні вигоди для забезпечення конкурентоспроможності та успіху проєкту в довгостроковій перспективі.

1.3.Роль стратегічного планування в управлінні ризиками ІТ-компаній

Стратегічне планування відіграє важливу роль в управлінні ризиками в ІТ-компаніях, оскільки дозволяє організаціям передбачати й оцінювати потенційні загрози та можливості, а також розробляти заходи для їх мінімізації. Розглянемо кілька ключових аспектів, через які стратегічне планування впливає на управління ризиками в ІТ-сфері.

Стратегічне планування дозволяє ІТ-компаніям оцінювати можливі ризики на різних етапах розвитку бізнесу. Це включає в себе як зовнішні ризики, такі як зміни

в ринковій ситуації чи технологічні інновації, так і внутрішні, наприклад, неефективність операційних процесів або слабкість у забезпеченні безпеки даних.

Прогнозування ризиків на різних етапах розвитку IT-компанії є важливою складовою стратегії управління ризиками, оскільки дає можливість компанії своєчасно виявити потенційні загрози та прийняти відповідні заходи для їх мінімізації або уникнення. Воно дозволяє організації не лише підготуватися до непередбачених ситуацій, але й забезпечити належний рівень стабільності та гнучкості в умовах постійних змін технологічного середовища. Прогнозування ризиків є особливо важливим для забезпечення довгострокового розвитку компанії, ефективного використання ресурсів і досягнення стратегічних цілей. Воно дозволяє спрогнозувати як технічні, так і економічні та організаційні ризики, а також дає змогу адаптувати стратегії розвитку компанії до зовнішніх змін, знижуючи ймовірність виникнення великих проблем у майбутньому[23].

На етапі стартапу (заснування компанії): На початкових етапах розвитку IT-компанії прогнозування ризиків є критичним для визначення потенційних загроз і уникнення непередбачуваних ситуацій. Саме в цей період компанія стикається з найбільшими фінансовими, організаційними та технологічними труднощами. Ризики, пов'язані з нестачею фінансування, можуть негативно вплинути на здатність компанії залучати інвестиції та створювати конкурентоспроможний продукт. Крім того, на початкових етапах можливі труднощі з формуванням стабільної команди та ефективного управління проектами. Прогнозування допомагає визначити, чи достатньо ресурсів для реалізації ідеї, а також дає змогу врахувати ризики, пов'язані з юридичними питаннями, такими як права на інтелектуальну власність, патенти та інші аспекти захисту технологій. Важливим є також врахування ризиків з боку ринку, таких як невизначеність попиту на продукт або високий рівень конкуренції в обраній ніші.

На етапі росту і розширення: Коли IT-компанія починає масштабувати свої операції та розширювати ринок збуту, прогнозування ризиків стає ще більш важливим. У цей час компанія стикається з новими викликами, які потребують адаптації стратегії і розширення операцій. Ризики, пов'язані з інтеграцією нових

технологій або масштабуванням бізнесу, можуть суттєво вплинути на стабільність компанії. Також на цьому етапі є загроза виникнення управлінських проблем, коли необхідно забезпечити ефективне управління збільшеною командою та новими проектами. Прогнозування допомагає передбачити проблеми, пов'язані з відсутністю необхідних ресурсів для масштабування, включаючи людські, технологічні та фінансові ресурси. Крім того, компанії необхідно бути готовою до змін на ринку, таких як нові регуляції або зміни у вимогах споживачів. Це дозволяє своєчасно реагувати на нові виклики, що можуть виникнути під час розширення компанії.

На етапі стабільності та зрілості: Коли компанія досягає певного рівня стабільності, прогнозування ризиків дає змогу компанії підтримувати і навіть покращувати свою конкурентоспроможність. Це час, коли компанія повинна уникати команди старіння технологій і постійно інвестувати в інновації. Ризики, пов’язані з технічними змінами, такими як швидке застарівання продуктів або технологій, можуть стати серйозними загрозами. Водночас, ІТ-компанія, що знаходиться на стадії зрілості, повинна постійно стежити за змінами на ринку, оскільки зростає ймовірність появи нових конкурентів або технологічних проривів, які можуть змінити умови ведення бізнесу. Прогнозування дозволяє вчасно виявити загрози для сталого розвитку, включаючи зниження ефективності менеджменту, неефективне використання ресурсів або відсутність гнучкості в адаптації до змінюваних вимог ринку. У цей період особливо важливим є планування ризиків, пов'язаних з безпекою даних і дотриманням нових регуляторних вимог, що стають дедалі важливішими для компаній, які працюють на глобальному ринку.

На етапі трансформації або виведення продукту на нові ринки: ІТ-компанії, що знаходяться на етапі трансформації, повинні особливо уважно прогнозувати ризики, пов’язані з виходом на нові ринки або запуском інноваційних продуктів. Вони можуть зіткнутися з труднощами в адаптації свого програмного забезпечення або послуг до нових технологічних вимог, що можуть бути специфічними для нових ринків. Зокрема, ризики, пов'язані з культурними або юридичними відмінностями, можуть істотно вплинути на успіх цієї стратегії. Крім того, компанія може зіткнутися з непередбачуваними труднощами при інтеграції продуктів на нових ринках, оскільки

вимоги до продуктів і ринкові умови можуть бути значно відмінними. Прогнозування дозволяє врахувати такі фактори, як можливість локалізації продукту, зміни в структурі попиту, а також швидкість адаптації до змін у законодавстві[24].

Стратегічне планування відіграє ключову роль у процесі оцінки потенційних загроз і можливостей для ІТ-компаній, оскільки дає змогу системно передбачати зміни, адаптуватися до них та мінімізувати ризики. Застосування стратегічного планування дозволяє компанії ретельно оцінювати як зовнішні, так і внутрішні фактори, що можуть вплинути на її діяльність, і, на основі цього аналізу, розробляти відповідні стратегії. Розглянемо кілька розширених аспектів, як стратегічне планування допомагає оцінювати ці загрози та можливості.

Аналіз зовнішнього середовища через PESTEL. Одним із основних етапів стратегічного планування є всебічний аналіз зовнішнього середовища, що дозволяє виявити основні тренди та впливи, здатні вплинути на розвиток ІТ-компанії. Метод PESTEL (Політичний, Економічний, Соціальний, Технологічний, Екологічний, Легальний) є потужним інструментом, що дає змогу виявити різноманітні загрози та можливості. Наприклад, політичні зміни, як-от нові закони або зміни у регулюванні, можуть спричинити нові вимоги для ІТ-сектору, що потребує негайної адаптації стратегії. Технологічні інновації, такі як розповсюдження нових алгоритмів штучного інтелекту або блокчейн-технологій, можуть створювати нові можливості для розробки продуктів, але водночас становлять загрози через появу нових конкурентів чи зміну вимог користувачів. Економічні кризи або коливання валют можуть мати серйозний вплив на фінансову стабільність компанії, що теж треба враховувати при стратегічному плануванні.

SWOT-аналіз для комплексної оцінки внутрішніх і зовнішніх факторів. SWOT-аналіз (Сили, Слабкості, Можливості, Загрози) є ще одним важливим інструментом, що допомагає ІТ-компаніям оцінити, які внутрішні сильні та слабкі сторони, а також зовнішні можливості та загрози можуть впливати на їх діяльність. Аналіз сильних сторін дозволяє компанії визначити, в яких аспектах вона перевершує конкурентів, наприклад, у технічній експертизі чи наявності патентів. Однак, це також допомагає виявити слабкі сторони, такі як обмеження в ресурсах чи недостатня

адаптація до змін у ринку. Зовнішні можливості можуть бути пов'язані з новими ринками або партнерствами, а загрози – з підвищеною конкуренцією або змінами в законодавстві. SWOT-аналіз дозволяє приймати зважені рішення щодо оптимізації бізнес-процесів і уникнення можливих ризиків.

Оцінка ризиків та їх вплив на проєкти. Оцінка ризиків є важливою складовою стратегічного планування, оскільки ІТ-компанії часто стикаються з непередбаченими ситуаціями, такими як затримки в проєктах, технічні помилки, зміни в вимогах замовників чи втрати важливих співробітників. Стратегічне планування допомагає не тільки передбачити можливі проблеми, але й виявити критичні точки ризику, що можуть серйозно зашкодити компанії. Наприклад, нестабільність в ІТ-інфраструктурі або відсутність кваліфікованих розробників можуть стати серйозними бар'єрами для реалізації проєктів. Оцінка цих ризиків дозволяє створити заходи з їх мінімізації або нейтралізації. Це може включати стратегічні інвестиції в нові технології, підвищення кваліфікації персоналу або страхування від технічних неполадок[25].

Планування можливостей через інновації та розвиток ресурсів. Пошук нових можливостей через інновації є важливою частиною стратегічного планування для ІТ-компаній. Це включає в себе аналіз нових технологічних трендів, таких як великий обсяг даних, автоматизація та інші передові технології. Завдяки стратегічному плануванню компанія може своєчасно розпізнати ці зміни та адаптуватися до них, втілюючи нові технології або створюючи нові бізнес-моделі. Крім того, стратегічне планування допомагає оцінити доступні ресурси та забезпечити їх ефективне використання. Це включає в себе людські ресурси, фінансові можливості, інтелектуальну власність і технологічну базу, що дозволяє компанії використовувати ці фактори для досягнення конкурентних переваг.

Адаптація до змін через постійний моніторинг та коригування стратегії. Оскільки ІТ-сектор є надзвичайно динамічним, стратегічне планування дозволяє компаніям гнучко адаптувати свої стратегії до змін. Постійний моніторинг зовнішніх і внутрішніх факторів допомагає своєчасно коригувати стратегію, щоб залишатися конкурентоспроможними на ринку. Наприклад, коли компанія стикається з новими викликами, такими як зміни в уподобаннях клієнтів або зміна економічної ситуації,

стратегічне планування дає можливість швидко переналаштувати бізнес-процеси, інвестувати в нові технології чи навіть змінювати бізнес-моделі. Таким чином, постійна адаптація та коригування стратегії є необхідними для забезпечення довгострокового успіху компанії в умовах швидких змін.

У результаті, стратегічне планування допомагає ІТ-компаніям не лише ефективно оцінювати потенційні загрози та можливості, але й створює систему для реагування на зміни, що дає можливість бути гнучкими і адаптивними в умовах високої невизначеності. Цей процес дозволяє забезпечити стабільний розвиток компанії, зберігаючи її конкурентоспроможність та гнучкість перед змінами на ринку і в технологіях.

Загалом, прогнозування ризиків на кожному з етапів розвитку ІТ-компанії є надзвичайно важливим інструментом для забезпечення її стабільного та успішного розвитку. Воно дає можливість знизити вплив негативних факторів, оптимізувати ресурси та зберігати конкурентоспроможність у змінюваних умовах. Своєчасне виявлення і оцінка потенційних ризиків допомагає компанії бути більш гнучкою і готовою до змін, а також дозволяє ефективно реагувати на будь-які виклики, що можуть виникнути на кожному етапі її розвитку.

Визначення пріоритетів для управління ризиками. Здійснення стратегічного планування допомагає компанії визначити найважливіші напрямки для управління ризиками. Це включає в себе визначення пріоритетних аспектів безпеки, фінансової стабільності та технологічних інновацій, що є найбільш критичними для довгострокового розвитку компанії. Це процес, за допомогою якого організація може ідентифікувати ризики, що мають найбільший потенціал для впливу на її діяльність, і сформулювати стратегії для їх зниження чи нейтралізації[25].

Стратегічне планування дозволяє ІТ-компаніям здійснювати ретельний аналіз усіх можливих загроз, щоб зрозуміти, які з них є найбільш критичними для бізнесу. Цей процес включає в себе наступні етапи: аналіз внутрішніх і зовнішніх факторів; оцінка ймовірності і впливу; ресурси для управління ризиками.

Стратегічне планування дає змогу оцінити як зовнішні, так і внутрішні фактори, що можуть спричинити ризики. Зовнішні ризики можуть бути пов'язані зі

змінами в законодавстві, економічними коливаннями чи технологічними інноваціями. Внутрішні ризики, у свою чергу, можуть стосуватися нестабільності фінансових потоків, проблем з кадрами або технологічними ресурсами. Оцінка та аналіз цих факторів на етапі стратегічного планування дозволяє з'ясувати, які з них найбільш ймовірно будуть впливати на виконання проєктів і на загальну ефективність компанії.

Для визначення основних ризиків важливо оцінити не тільки ймовірність їх виникнення, а й рівень впливу на компанію. Цей етап включає застосування різних методів, зокрема SWOT-аналізу, аналізу ймовірностей та оцінки впливу, що дозволяють виявити найбільш критичні загрози. Наприклад, якщо ймовірність кіберзагрози висока, а вплив на репутацію та фінанси компанії значний, такий ризик потребує пріоритетної уваги.

Стратегічне планування дозволяє визначити, які ресурси будуть необхідні для управління різними типами ризиків. Це дозволяє зосередити зусилля на найбільш важливих аспектах і забезпечити правильний розподіл ресурсів для мінімізації найбільших загроз. Наприклад, якщо компанія має обмежений бюджет, вона повинна спрямувати більшу частину фінансових ресурсів на захист від ризиків, які можуть призвести до значних збитків, таких як кіберзагрози або порушення в законодавчій сфері[26].

Після ідентифікації основних ризиків стратегічне планування допомагає компанії зосередити увагу на найважливіших аспектах діяльності, які потребують першочергового управління. Розглянемо кілька ключових напрямів, де стратегічне планування має особливе значення:

Безпека (кібербезпека). Кіберзагрози є одними з найбільших викликів для IT-компаній. Стратегічне планування дає змогу зосередитися на питаннях захисту інформації та захисту від кібератак, що може включати впровадження заходів щодо шифрування даних, моніторингу мереж та безпеки серверів. Зокрема, стратегічний аналіз дозволяє компанії оцінити, які кіберзагрози найбільше підривають її діяльність і розробити пріоритетні заходи для їх мінімізації, такі як регулярне оновлення програмного забезпечення, навчання персоналу та створення планів реагування на інциденти.

Фінансові ризики. Фінансові аспекти завжди є важливими в управлінні будь-яким бізнесом, і ІТ-компанії не є винятком. Стратегічне планування допомагає визначити потенційні фінансові ризики, зокрема ризики, пов'язані з неплатоспроможністю клієнтів, змінами у валютних курсах або підвищенням вартості ресурсів. Це дозволяє компанії зосередитися на створенні фінансових резервів або використовувати страхування для захисту від можливих втрат. Крім того, стратегічне планування дозволяє спрогнозувати фінансові потреби компанії для підтримки стабільної роботи, навіть в умовах економічної нестабільності[27].

Технологічні ризики. Оскільки ІТ-компанії залежать від постійного оновлення технологій і інновацій, важливо передбачити технологічні ризики, які можуть виникнути в результаті швидкого розвитку технологічних змін або невідповідності технологічних рішень потребам ринку. Стратегічне планування дозволяє зосередити увагу на виявленні технологічних загроз, таких як швидке старіння обладнання чи невідповідність програмного забезпечення новим вимогам. Це допомагає не тільки уникати ризиків, пов’язаних із застарілими технологіями, але й дає змогу компанії активно інвестувати в новітні розробки та інновації.

Регуляторні та правові ризики. Стратегічне планування допомагає визначити ризики, що виникають через зміни в законодавстві або нормативних актах. Це особливо важливо для ІТ-компаній, що працюють у різних юрисдикціях або мають справу з персональними даними. Визначення таких ризиків дозволяє компанії своєчасно адаптувати свою діяльність до змін у законодавстві, наприклад, щодо захисту даних або вимог до звітності. Стратегічне планування забезпечує необхідні ресурси для своєчасного оновлення політик і процедур, що дозволяє знизити ймовірність порушення законодавчих норм і пов'язаних з цим штрафів[28].

Таким чином, стратегічне планування дозволяє ІТ-компаніям не лише виявити найважливіші ризики, але й на основі аналізу цих ризиків визначити пріоритети для управління ними. Це дає змогу зосередити ресурси на найбільш критичних аспектах бізнесу, таких як безпека, фінанси та технології, що дозволяє значно знизити ймовірність негативних наслідків і підвищити стійкість компанії до різноманітних загроз.

Гнучкість і адаптація до змін: стратегічне планування відіграє вирішальну роль у здатності компаній оперативно адаптуватися до змін у технологічному середовищі чи ринкових умовах. Особливо це актуально для IT-компаній, де інновації, нові технології та зміни в поведінці клієнтів відбуваються з надзвичайною швидкістю. Завдяки стратегічному плануванню компанія може передбачати можливі зміни в технологічному середовищі, такі як поява нових мов програмування, платформ чи інструментів автоматизації. Це дозволяє заздалегідь планувати перехід на сучасні технології, не ризикуючи втратити конкурентоспроможність.

Крім того, стратегічне планування дозволяє компаніям передбачати зміни у ринкових умовах, таких як змінення попиту, поява нових гравців на ринку або зміна економічної ситуації. Завдяки цьому компанії можуть не лише швидко адаптувати свою продукцію чи послуги до нових умов, але й зберігати ефективність навіть у кризових ситуаціях. Наприклад, компанія, яка використовує стратегічне планування, може передбачити можливі ринкові тренди, такі як зростання попиту на хмарні послуги чи впровадження штучного інтелекту, і заздалегідь розробити відповідні рішення.

Сценарне планування є одним із важливих інструментів у цьому процесі. Завдяки йому компанії можуть розробити кілька можливих сценаріїв розвитку подій і мати готові плани дій для кожного з них. Скажімо, якщо на ринку з’являється новий конкурент із агресивною стратегією ціноутворення, компанія може швидко реалізувати підготовлені дії, щоб зберегти свої позиції.

Гнучкість у стратегічному плануванні полягає в здатності компанії змінювати свої плани, стратегії чи розподіл ресурсів залежно від змін зовнішнього чи внутрішнього середовища. Це забезпечує компанії стійкість до впливу непередбачуваних обставин. Приміром, у разі раптової зміни регуляторних вимог стратегічно орієнтована компанія може швидко внести необхідні корективи в свої процеси, уникнувши штрафів чи затримок.

Гнучкість також дозволяє компаніям більш ефективно розподіляти ресурси у разі зміни пріоритетів. Як варіант, якщо під час розробки нового продукту виникають ризики, пов’язані з безпекою даних, компанія може швидко спрямувати додаткові

ресурси для їх усунення, зменшуючи можливість виникнення негативних наслідків[29].

Ще одним аспектом гнучкого планування є можливість швидко адаптувати бізнес-модель до нових умов. Зокрема, пандемія COVID-19 змусила багато компаній переходити на віддалену роботу чи розробляти онлайн-продукти. Ті компанії, які мали гнучкі стратегії, змогли швидше адаптуватися до нових реалій і навіть отримати переваги від змін.

Окрім того, гнучке планування сприяє зменшенню ризиків, пов’язаних із управлінням людськими ресурсами. На зразок, стратегічно мислячі компанії інвестують у навчання та перекваліфікацію своїх співробітників, що дозволяє їм швидко освоювати нові інструменти чи технології. Це важливо для IT-сфери, де швидкість змін у технологіях потребує від фахівців постійного оновлення знань.

Гнучкість у стратегічному плануванні допомагає компаніям не лише зменшувати ризики, але й використовувати зміни як можливості для зростання. Наприклад, швидке реагування на нові ринкові можливості дозволяє компанії бути першопрохідцем у впровадженні нових технологій чи послуг. Це може включати розширення на нові ринки, запуск інноваційного продукту чи оптимізацію існуючих процесів.

Таким чином, гнучкість і адаптація до змін через стратегічне планування є ключовими чинниками довгострокового успіху компаній, особливо у сфері IT, де непередбачуваність і швидкість змін є нормою. Це дозволяє не лише уникати ризиків, але й створювати умови для розвитку навіть у нестабільних умовах.

Стратегічне планування забезпечує основу для інтеграції ризик-менеджменту в корпоративну стратегію, створюючи узгоджений підхід до управління всіма аспектами діяльності компанії. Це дозволяє організаціям розглядати ризики в контексті їх впливу на досягнення стратегічних цілей, а не ізольовано. Завдяки цьому ризик-менеджмент стає невід’ємною частиною загальної стратегії, допомагаючи адаптувати процеси, ресурси та рішення для забезпечення стійкості компанії. Наприклад, під час стратегічного планування виходу на новий ринок враховуються можливі ризики, такі як регуляторні обмеження, культурні відмінності, економічна

нестабільність або специфіка споживчої поведінки. Інтеграція ризиків у стратегію дозволяє враховувати всі ці аспекти вже на етапі планування[30].

Інтеграція управління ризиками передбачає, що аналіз ризиків є невід'ємною частиною процесу прийняття стратегічних рішень на всіх рівнях компанії. Кожне значуще рішення, пов'язане зі стратегією, супроводжується оцінкою потенційних загроз і можливостей, які можуть вплинути на його реалізацію. Завдяки стратегічному плануванню ризики не тільки ідентифікуються, але й пріоритизуються залежно від їхнього впливу на стратегічні цілі. Наприклад, якщо компанія розробляє новий продукт, ризики, пов'язані із затримками постачання компонентів, технічними проблемами або невідповідністю вимогам ринку, аналізуються заздалегідь. Це дозволяє розробити альтернативні плани дій і знизити ймовірність виникнення кризових ситуацій.

Матриця ризиків та інші стратегічні інструменти відіграють ключову роль у забезпеченні інтеграції ризик-менеджменту. Застосування матриці дозволяє систематизувати та оцінити ризики за їх імовірністю і можливим впливом на компанію. Цей підхід допомагає ідентифікувати найбільш критичні ризики та зосередити ресурси на їхньому зниженні. Завдяки цьому компанія може планувати свою діяльність з урахуванням ризиків, які матимуть найбільший вплив на її довгострокові цілі. Крім того, стратегічне планування сприяє впровадженню механізмів постійного моніторингу ризиків у режимі реального часу. Це особливо важливо для IT-компаній, які працюють у динамічному середовищі, де зміни можуть відбуватися миттєво.

Корпоративна культура також є важливим фактором у забезпеченні інтеграції ризик-менеджменту в стратегію. Завдяки стратегічному плануванню управління ризиками стає пріоритетом не лише для керівництва, але й для всього персоналу. Це сприяє створенню культури, де кожен співробітник усвідомлює ризики, які можуть виникнути у його сфері діяльності, і бере участь у їхньому мінімізації. Такий підхід сприяє більш злагодженій роботі організації та підвищує ефективність управління ризиками. Наприклад, у компаніях, де ризик-менеджмент є частиною корпоративної

культури, співробітники активно повідомляють про потенційні проблеми, що дає змогу вчасно реагувати на загрози.

Стратегічне планування виконує роль містка між ризик-менеджментом і корпоративною стратегією, забезпечуючи їхню синергію. Це дає змогу організації ефективно ідентифікувати ризики, інтегрувати їх у стратегічні процеси та розробляти заходи для їхньої мінімізації. Завдяки цьому компанія отримує конкурентну перевагу, оскільки може швидко реагувати на зміни у зовнішньому середовищі та забезпечувати стійкий розвиток навіть у складних ринкових умовах. У підсумку, інтеграція ризик-менеджменту в корпоративну стратегію є не просто інструментом, а стратегічною необхідністю для забезпечення довгострокового успіху компанії.

Інтеграція ризик-менеджменту в корпоративну стратегію забезпечує комплексний підхід до прийняття рішень, що дозволяє враховувати всі можливі аспекти ризиків і знижувати їхній вплив на діяльність компанії. Завдяки стратегічному плануванню ризики оцінюються не ізольовано, а в контексті взаємозв'язків між різними підрозділами, процесами та цілями організації. Це дає змогу враховувати як внутрішні, так і зовнішні чинники, що впливають на стратегію, та уникати ситуацій, коли ігнорування одного з ризиків може поставити під загрозу весь проєкт або бізнес.

Комплексний підхід дозволяє приймати рішення на основі даних і прогнозів, що забезпечує їх більшу точність та ефективність. Завдяки інтегрованій системі ризик-менеджменту компанія може одночасно аналізувати фінансові, технічні, ринкові та операційні ризики. Це дозволяє визначати пріоритети, концентрувати ресурси на критичних зонах і уникати дублювання зусиль у різних підрозділах. Наприклад, у процесі розробки нового продукту комплексний аналіз може виявити ризики, пов’язані з розробкою технології, фінансуванням і ринковою конкуренцією, що дає змогу створити злагоджений план для їхньої мінімізації[31].

Інтеграція ризик-менеджменту також сприяє зниженню загальних ризиків шляхом узгодження стратегічних та операційних рішень. Це забезпечує цілісність усіх етапів діяльності компанії, від стратегічного планування до щоденних операцій. Такий підхід допомагає уникнути ситуацій, коли ризики в одній частині організації

нівелюють досягнення в іншій. Наприклад, якщо маркетинговий підрозділ запускає рекламну кампанію, не враховуючи технічних обмежень у виробництві, це може призвести до невиконання обіцянок перед клієнтами, що негативно вплине на репутацію компанії.

Комплексний підхід до управління ризиками дозволяє створювати стратегії, які адаптуються до змін у внутрішньому та зовнішньому середовищі. Замість того щоб реагувати на ризики постфактум, компанія може проактивно передбачати їх і розробляти відповідні заходи. Це значно підвищує ефективність управління та забезпечує стабільність навіть у нестабільних умовах ринку. Крім того, інтеграція ризик-менеджменту в стратегію дозволяє краще підготувати компанію до кризових ситуацій, оскільки всі процеси вже враховують можливість виникнення непередбачуваних подій.

Зниження ризиків у цілому досягається завдяки узгодженню дій між різними підрозділами компанії. Інтегрований підхід дозволяє кожному департаменту розуміти загальну картину ризиків і координувати свої дії з іншими відділами. Це мінімізує конфлікти інтересів, дублювання ресурсів і втрати часу. У підсумку, завдяки інтеграції ризик-менеджменту в корпоративну стратегію, компанія отримує ефективний механізм для управління ризиками, що забезпечує її довгострокову стійкість і конкурентоспроможність.

Розвиток культури управління ризиками: Під час стратегічного планування в IT-компаніях також важливо створювати культуру, орієнтовану на обізнаність і управління ризиками. Стратегічний підхід дозволяє інформувати співробітників компанії про важливість ризик-менеджменту та інтегрувати ці знання у щоденну практику бізнес-процесів.

Розвиток культури управління ризиками через стратегічне планування є ключовим фактором для формування стійкої корпоративної культури, орієнтованої на ефективне і систематичне управління ризиками. Стратегічне планування виступає платформою, на якій базується інтеграція ризик-менеджменту в усі аспекти діяльності компанії. Воно дозволяє не тільки структурувати підходи до управління ризиками, але й забезпечити їхнє органічне впровадження у повсякденні операції. Це

створює передумови для того, щоб всі рівні організації розуміли важливість управління ризиками і підтримували його на практиці[32].

Стратегічне планування сприяє формуванню корпоративної культури управління ризиками через впровадження чітких цілей, політик та процедур. Встановлення конкретних орієнтирів і стандартів забезпечує однакове розуміння ролі ризик-менеджменту серед керівництва та працівників. Політики, орієнтовані на управління ризиками, підкреслюють важливість проактивного підходу, коли потенційні загрози розглядаються не як проблеми, а як можливості для вдосконалення процесів і досягнення кращих результатів.

Важливим елементом створення культури управління ризиками є навчання та підвищення кваліфікації співробітників. Стратегічне планування передбачає впровадження освітніх програм, тренінгів та семінарів, які допомагають працівникам на всіх рівнях зрозуміти, як правильно ідентифікувати ризики, оцінювати їхній вплив і вживати заходів для їх мінімізації. Це формує спільну відповідальність за управління ризиками, стимулюючи кожного співробітника діяти на випередження. Завдяки цьому організація може оперативно реагувати на зміни та підтримувати стабільність у своїй діяльності.

Стратегічне планування також підтримує культуру відкритості та прозорості, що є основою для ефективного управління ризиками. Коли працівники мають змогу відкрито повідомляти про потенційні загрози або помилки без страху бути покараними, створюється атмосфера довіри та співпраці. Це підвищує оперативність у виявленні проблем і сприяє швидкому прийняттю рішень. Така культура прозорості сприяє зниженню негативних наслідків ризиків і підтримує сталий розвиток компанії.

Орієнтованість на управління ризиками як частину загальної стратегії дозволяє компанії бути гнучкою та стійкою до змін. Інтеграція ризик-менеджменту в корпоративну культуру допомагає формувати стратегії, які враховують як можливості, так і загрози. У результаті компанія стає не лише краще підготовленою до потенційних викликів, але й здатною використовувати ризики як каталізатор для нових можливостей зростання.

У довгостроковій перспективі стратегічне планування забезпечує гармонійне поєднання ризик-менеджменту з іншими аспектами управління, що сприяє створенню інноваційної та відповідальної корпоративної культури. Це дозволяє компанії бути конкурентоспроможною, адаптивною та успішною навіть у мінливих ринкових умовах, роблячи управління ризиками ключовим елементом її стратегії.

Інформування співробітників і залучення їх до процесів управління ризиками є важливим кроком для створення ефективної системи ризик-менеджменту в компанії. Відкрите спілкування та доступ до інформації про ризики забезпечують загальне розуміння ключових викликів і можливостей, які стоять перед організацією. Коли співробітники чітко усвідомлюють, з якими ризиками може зіткнутися компанія, і розуміють свою роль у їхньому вирішенні, це сприяє активнішій участі в управлінні ризиками.

Інформування сприяє формуванню культури відповідальності. Чітке донесення політик, процедур і стратегій управління ризиками допомагає кожному працівнику усвідомити свій внесок у цей процес. Наприклад, навчання тому, як розпізнавати ознаки потенційних загроз або оцінювати ризики в рамках власних завдань, робить працівників більш обізнаними та відповідальними.

Залучення співробітників до процесів управління ризиками сприяє створенню спільної відповідальності за результати. Коли працівники відчувають, що їхні знання, досвід та ідеї враховуються у процесі прийняття рішень, це підвищує їхню мотивацію і прихильність до компанії. Наприклад, спільне обговорення ризиків у робочих групах або під час регулярних нарад може сприяти виявленню прихованих загроз, які могли залишитися непоміченими керівництвом.

Інформаційні заходи, такі як тренінги, семінари та внутрішні комунікаційні кампанії, допомагають підвищити рівень обізнаності щодо ризиків. Ці заходи можуть бути спрямовані на розвиток навичок оцінки ризиків, пошуку рішень і управління складними ситуаціями. Також важливо створити платформи, на яких співробітники можуть ставити питання, ділитися досвідом і отримувати зворотний зв'язок щодо своїх ідей або дій.

Залучення співробітників також допомагає знизити опір змінам. Управління ризиками часто потребує впровадження нових підходів, інструментів або змін у процесах. Коли працівники беруть активну участь у цих змінах, вони краще розуміють їхню необхідність і відчувають свою залученість до досягнення спільних цілей. Це значно зменшує ризик саботажу або неефективного виконання нових політик.

У довгостроковій перспективі інформування і залучення співробітників забезпечують підвищення ефективності системи управління ризиками. Залучений колектив стає більш згуртованим, гнучким і здатним оперативно реагувати на потенційні загрози. Успіх управління ризиками залежить від того, наскільки кожен працівник розуміє важливість свого внеску, а отже, інформування та залучення є одними з найважливіших інструментів для досягнення цієї мети[33].

Таким чином, стратегічне планування є основою для ефективного управління ризиками в IT-компаніях. Воно дозволяє не лише зменшити негативні наслідки можливих загроз, але й використовувати їх як можливості для розвитку та підвищення конкурентоспроможності компанії.

РОЗДІЛ 2.
ДОСЛІДЖЕННЯ РИЗИКІВ У РОЗРОБЦІ ТА РОЗГОРТАННІ ІТ-ДОДАТКІВ

2.1. Моделі оцінки та аналізу ризиків

Аналіз і оцінка ризиків є надзвичайно важливими елементами в управлінні ІТ-проектами, оскільки дозволяють організаціям проактивно виявляти, оцінювати та контролювати потенційні загрози, які можуть суттєво вплинути на успіх розробки та впровадження ІТ-додатків. В умовах швидкого технологічного прогресу та високої конкуренції на ринку, своєчасна та якісна оцінка ризиків надає компаніям можливість адаптуватися до змін і уникати небезпечних ситуацій. Оскільки не всі ризики можуть бути виявлені на початкових етапах проекту, процес їх оцінки вимагає системного і регулярного підходу для забезпечення ефективного управління.

Ризики можуть проявлятися на різних етапах життєвого циклу проекту - від початкового планування до фінального впровадження та обслуговування. Кожен з цих етапів має свої специфічні ризики, які потребують окремого аналізу та управлінських рішень. Наприклад, у фазі планування можуть виникнути труднощі зі встановленням точних вимог або ресурсів, тоді як на етапі розгортання можуть з'явитися проблеми інтеграції з існуючими системами. Тому важливо мати систему, здатну комплексно оцінювати ризики вже на початковому етапі проекту та забезпечувати можливість регулярного перегляду та коригування ризик-менеджменту в процесі реалізації.

У такому контексті моделі оцінки ризиків виконують ключову роль, оскільки вони пропонують структурований підхід до аналізу, використовуючи як якісні, так і кількісні методи. Якісний підхід дозволяє виявляти й класифікувати ризики на основі думок експертів чи минулого досвіду, тоді як кількісний метод застосовує математичні та статистичні інструменти для визначення ймовірності виникнення ризиків та їх потенційного впливу. Обидва ці підходи мають свої переваги та недоліки, але разом вони забезпечують комплексний огляд ризиків та їх потенційного впливу на проект.

Одним із ключових елементів аналізу ризиків є розробка та впровадження моделей, які можуть допомогти не лише оцінити ймовірність ризиків, а й визначити їх можливий вплив на проект. Це дозволяє менеджерам проектів розробити ефективні стратегії для пом'якшення наслідків та зменшення ризиків. Такі моделі є особливо важливими в умовах нестабільності та швидких змін у сфері технологій, де навіть незначні помилки можуть привести до серйозних наслідків для компанії[34].

У цьому підрозділі ми розглянемо основні моделі оцінки ризиків, які використовуються в рамках управління IT-проектами.

Метод FMEA (Failure Modes and Effects Analysis) є одним із найпопулярніших і найбільш ефективних інструментів для оцінки ризиків у різних галузях, зокрема в IT-сфері. Основною метою FMEA є систематичне виявлення можливих збоїв або дефектів у системах і продуктах та визначення їхнього впливу на загальну функціональність, безпеку та якість кінцевого продукту чи послуги. Використання цього методу дозволяє суттєво знизити ймовірність виникнення критичних помилок, мінімізувати економічні збитки і, в кінцевому підсумку, підвищити якість IT-додатків.

Процес FMEA базується на детальному аналізі всіх можливих відмов на різних етапах життєвого циклу проекту. Він складається з наступних етапів, які забезпечують глибоке розуміння ризиків та їх потенційних наслідків.

Етап 1. Ідентифікація можливих моделей відмов. На початковому етапі команда проекту проводить генерацію ідей, збираючи всі можливі сценарії збоїв чи відмов. Цей етап є критично важливим для виявлення не лише очевидних ризиків, але й тих, що можуть здаватися малоймовірними, але здатні призвести до серйозних наслідків. Використання методу мозкового штурму або інтерв'ю з експертами може суттєво розширити перспективи аналізу.

Етап 2. Аналіз наслідків відмов: Кожна ідентифікована модель відмови підлягає детальному аналізу, щоб зрозуміти, як вона може вплинути на різні аспекти проекту. Це може включати технічні аспекти, такі як продуктивність і надійність системи, а також бізнес-наслідки, такі як втрата клієнтів, збільшення витрат або негативний вплив на репутацію компанії.

Етап 3. Оцінка ймовірності виникнення: Для кожної з ідентифікованих моделей збоїв команда на основі попереднього досвіду або статистичних даних визначає ймовірність її виникнення. Цей етап включає об'єктивну оцінку фактичних даних і відгуків з попередніх проектів або галузевих стандартів.

Етап 4. Оцінка можливості виявлення: Окрім оцінки ймовірності виникнення, важливо з'ясувати, наскільки легко чи складно буде виявити цю помилку на ранніх етапах розробки. Це дозволить зосередити зусилля на покращенні процесів контролю якості та раннього тестування.

Етап 5. Розрахунок пріоритетного числа ризику (Risk Priority Number, RPN): Цей показник обчислюється шляхом множення трьох факторів: серйозності наслідків, ймовірності виникнення та можливості виявлення проблеми. RPN дозволяє оцінити ризики у відносному порядку й визначити пріоритетність дій щодо усунення найбільш критичних ризиків.

Етап 6. Розробка плану заходів щодо зменшення ризиків: На підставі отриманого пріоритетного числа ризику команда проекту формулює стратегії зменшення ризиків. Ці стратегії можуть включати технічні заходи, спрямовані на усунення джерела проблеми, а також організаційні зміни в процесі розробки з метою поліпшення управлінських практик[35].

Отже розглянувши дану модель ми можемо навести наступні переваги FMEA:

- превентивний підхід. Метод FMEA дозволяє виявляти можливі проблеми ще на етапі планування, що допомагає уникнути серйозних наслідків у майбутньому.
- структурований аналіз. Процес FMEA передбачає систематичний підхід до ідентифікації й оцінки ризиків, що допомагає зменшити ймовірність пропуску важливих факторів.
- покращення якості продукту. Завдяки аналізу ймовірних відмов і розробці відповідних дій, FMEA допомагає підвищити загальну якість продукту або системи.
- командна робота. Метод залучає членів різних команд і підрозділів, що сприяє взаєморозумінню та кращій координації в процесі управління ризиками.
- універсальність. FMEA може бути застосований у різних галузях, включно з IT-сферою, виробництвом, охороною здоров’я тощо.

А також можемо виділити наступні недоліки:

- складність і тривалість процесу. Проведення FMEA може бути тривалим і вимагати великих ресурсів, особливо для складних систем або проектів.
- суб'єктивність оцінок. Ймовірність відмов і їхній вплив часто базуються на досвіді або суб'єктивних оцінках команди, що може призвести до неточностей у підсумковій оцінці ризиків.
- обмеження в передбаченні несподіваних ризиків. Хоча FMEA дозволяє виявляти очевидні та малоймовірні ризики, не всі можливі сценарії можуть бути передбачені, особливо якщо мова йде про нові або швидкозмінні технології.
- орієнтація на відомі проблеми. Метод здебільшого фокусується на тих відмовах, які вже відомі або передбачувані, тому може не врахувати нові, невідомі загрози.
- складність у визначенні пріоритетів. Підрахунок RPN (Risk Priority Number) може виявитися недостатньо точним, оскільки всі фактори мають однакову вагу, що не завжди відповідає реальності.

FMEA є надзвичайно ефективним інструментом для оцінки ризиків на етапах розробки, тестування та впровадження IT-додатків. Він не лише дозволяє командам виявляти потенційні збої, але також забезпечує можливість раннього втручання, що значно підвищує загальну якість проекту та знижує ймовірність серйозних помилок після запуску. Реалізація процесу FMEA в проектах допомагає створити культуру якості та відповідальності у команди, підвищуючи її здатність до управління ризиками та покращуючи показники успішності проектів.

Наступною розглянемо модель Монте-Карло (Monte Carlo Simulation) — це метод моделювання та оцінки ризиків, який використовує випадкові варіації та ймовірнісний підхід для прогнозування можливих результатів у складних системах. Ця модель особливо популярна в IT-секторі та в інших галузях для аналізу ризиків у проектах, де багато невизначеностей і факторів можуть впливати на кінцевий результат. Основною перевагою методу Монте-Карло є можливість моделювати широкий діапазон можливих результатів, враховуючи варіативність вхідних даних.

Основним принцип роботи моделі Монте-Карло заснований на генерації великої кількості випадкових сценаріїв або можливих варіантів розвитку подій для певної системи або проекту. Кожен сценарій розраховується окремо, і на основі отриманих результатів формується картина ймовірнісного розподілу можливих результатів. Такий підхід дозволяє зрозуміти, які ризики можуть бути найбільш критичними і як змінюватиметься проект при різних умовах.

Процес моделювання включає кілька ключових етапів:

1. Визначення проблеми та мети моделювання. Цей етап полягає у чіткому формулюванні проблеми або запитання, яке потрібно вирішити за допомогою методу Монте-Карло. Це може бути, наприклад, оцінка ризиків у процесі розробки ПЗ або аналіз ймовірності перевищення бюджету проекту. На цьому етапі команда повинна чітко визначити параметри, які підлягатимуть оцінці, а також ідентифікувати фактори, що можуть впливати на результат.

2. Визначення вхідних даних і розподілів ймовірностей. На цьому етапі потрібно визначити змінні, які можуть вплинути на результат проекту, і задати для них відповідні ймовірнісні розподіли. Це можуть бути тривалість етапів проекту - для кожного етапу розробки можна задати ймовірний час виконання із застосуванням нормального або трикутного розподілу; витрати на проект - оцінка вартості кожного етапу також може мати випадковий характер залежно від різних сценаріїв; ймовірність технічних збоїв - для систем можна задати ймовірності, з якими можуть виникнути технічні проблеми, і як вони вплинуть на загальний результат проекту.

3. Генерація випадкових варіантів розвитку подій. Метод Монте-Карло використовує генерацію великої кількості випадкових сценаріїв на основі заданих ймовірнісних розподілів. Для кожної варіації система генерує випадкові значення вхідних даних і проводить розрахунок результату. Таких ітерацій може бути тисячі або навіть сотні тисяч, залежно від складності проблеми та необхідної точності результату.

4. Обчислення результатів для кожної ітерації. Кожен із згенерованих сценаріїв моделює можливий варіант розвитку подій. Наприклад, для проекту з розробки ПЗ кожна ітерація може дати різні результати в плані тривалості, витрат або

технічних ризиків. Отримані дані аналізуються для формування ймовірнісного розподілу можливих результатів, що дає можливість побачити діапазон можливих наслідків.

5. Аналіз результатів та побудова ймовірнісного розподілу. Останній етап полягає в аналізі отриманих результатів та інтерпретації ймовірнісних розподілів. Результати можуть показувати ймовірність успішного завершення проекту в рамках бюджету або строків, розподіл можливих витрат на проект, оцінку найгірших та найкращих сценаріїв (відсоткові значення найбільш і найменш ймовірних результатів)[36].

На основі цих даних можна приймати більш обґрунтовані рішення щодо управління ризиками. Наприклад, якщо ймовірність перевищення бюджету є значною, то можна впровадити додаткові заходи для контролю витрат.

Дана модель має наступні переваги:

- Можливість оцінки широкого спектру сценаріїв. Модель дозволяє врахувати всі можливі варіанти розвитку подій, що робить її корисною для аналізу складних і невизначених проектів.
- Чіткіший аналіз ризиків. За допомогою Монте-Карло можна чітко визначити ймовірність виникнення певних ризиків, що дозволяє краще планувати та управляти ними.
- Гнучкість у використанні різних розподілів ймовірностей. Можна використовувати різні ймовірнісні розподіли для кожного параметра, що дозволяє врахувати специфіку проекту або системи.
- Підтримка прийняття обґрунтованих рішень. Оскільки результати моделювання надають детальну картину можливих результатів, це допомагає керівникам проектів приймати рішення на основі фактичних даних і ймовірностей.

Нажаль існують і недоліки:

- Залежність від якості вхідних даних. Якщо початкові дані або припущення щодо розподілів ймовірностей некоректні, результати моделювання можуть бути хибними.

- Висока вимогливість до обчислювальних ресурсів. Через велику кількість ітерацій модель може вимагати значних обчислювальних ресурсів для отримання точних результатів.
- Складність інтерпретації результатів. Для людей, які не знайомі з ймовірнісними методами, результати Монте-Карло можуть бути складними для розуміння та використання.

У розробці IT-додатків метод Монте-Карло часто використовують для прогнозування строків виконання проекту з урахуванням можливих затримок або ризиків. Наприклад, якщо команда оцінює, що певний етап може зайняти від 5 до 10 днів, метод Монте-Карло допоможе змоделювати сотні сценаріїв, щоб оцінити ймовірність завершення проекту в потрібний термін.

Таким чином, метод Монте-Карло є потужним інструментом для управління ризиками і прийняття рішень в умовах невизначеності, особливо в проектах з високою варіативністю вхідних даних, таких як IT-додатки.

Наступною моделлю, яку ми розглянемо, буде PERT (Program Evaluation and Review Technique) — це техніка оцінки та перегляду програм, яка широко використовується для управління проектами та особливо ефективна при роботі з невизначеністю в плануванні.

Техніка PERT була розроблена в 1950-х роках як інструмент управління великими, складними проектами, де точне передбачення часу виконання кожного етапу є складним завданням. Ця модель дозволяє використовувати три оцінки для визначення тривалості кожного завдання: оптимістичну (O), песимістичну (P) і найбільш ймовірну (M). Завдяки такому підходу техніка PERT дозволяє враховувати різноманітність можливих варіантів розвитку подій і оцінювати середню тривалість завдань з урахуванням невизначеності.

Основні етапи роботи з технікою PERT.

1. Визначення основних етапів і завдань проекту. Даний крок полягає в тому, щоб ідентифікувати всі ключові завдання, необхідні для завершення проекту. Це означає розбиття проекту на конкретні завдання, які повинні бути виконані для досягнення кінцевої мети. Завдання, які визначені на цьому етапі, можуть бути

простими або складними, залежно від масштабу проекту, але кожне повинно мати чіткий початок і кінець.

2. Оцінка тривалості кожного завдання. Для кожного завдання застосовуються три оцінки часу виконання:

- оптимістична оцінка (О): Найкращий сценарій, у якому завдання може бути виконано в мінімальні строки. Це час, коли все йде гладко без затримок.
- найбільш ймовірна оцінка (М): Це оцінка, яка є найбільш реалістичною, враховуючи нормальний перебіг подій. Найімовірніший час виконання враховує звичайні труднощі та можливі незначні затримки.
- песимістична оцінка (Р): Найгірший сценарій, коли завдання може бути виконане в максимальні строки. Ця оцінка враховує всі можливі ризики та затримки, які можуть виникнути під час виконання завдання.

3. Розрахунок очікуваної тривалості (ТЕ). Цей крок полягає у використанні формули PERT для розрахунку очікуваної тривалості кожного завдання.

Формула 1

$$TE = \frac{O + 4M + P}{6}$$

Ця формула дає змогу отримати середнє значення тривалості, яке найточніше відображає реалістичну тривалість завдання з урахуванням усіх можливих сценаріїв.

4. Створення мережевої діаграми проекту. На основі визначених завдань і оцінок тривалості будується мережева діаграма проекту. У цій діаграмі кожне завдання зображується як вузол, а залежності між завданнями — як стрілки, що з'єднують ці вузли. Важливо відзначити, що техніка PERT зосереджується на визначенні залежностей між завданнями, що дає змогу точно моделювати критичний шлях (Critical Path).

5. Визначення критичного шляху. Критичний шлях — це послідовність завдань, яка визначає найтриваліший час виконання проекту. Якщо одне із завдань на критичному шляху затримується, це автоматично призводить до затримки всього проекту. Модель PERT дозволяє легко ідентифікувати критичний шлях і звернути особливу увагу на його завдання, щоб запобігти затримкам.

6. Аналіз і коригування плану. На підставі отриманих результатів і аналізу критичного шляху команда проекту може розглянути можливості для оптимізації. Це може включати перерозподіл ресурсів для завдань на критичному шляху, впровадження заходів для зменшення ризиків затримок або коригування плану в разі значної невизначеності в оцінках[37].

Отже розглянувши методологію роботи даної моделі можемо стверджувати, що вона має свої недоліки та переваги.

До переваг моделі PERT ми можемо віднести:

- управління невизначеністю. PERT дозволяє враховувати невизначеність у строках виконання завдань, що робить її особливо корисною для складних і непередбачуваних проектів.
- оцінка критичного шляху. Модель допомагає виявити критичний шлях і сфокусувати увагу на найважливіших завданнях, від яких залежить завершення проекту.
- гнучкість у плануванні. PERT дозволяє коригувати план у процесі реалізації проекту на основі реальних даних, що сприяє більш точному прогнозуванню результатів.
- підвищення обґрунтованості рішень. Можливість використовувати три оцінки тривалості дозволяє ухвалювати рішення на основі більш повної інформації про ризики.

Натомість недоліки визначаємо наступні:

- трудомісткість і складність. Створення та підтримка мережевих діаграм PERT можуть бути досить складними й вимагати значних зусиль для великих проектів.
- залежність від точності оцінок. Якщо оцінки оптимістичних, ймовірних і песимістичних сценаріїв неточні, результати можуть бути спотвореними.
- не враховує інші види ресурсів. PERT фокусується на часових оцінках, але не враховує інші аспекти проекту, такі як витрати або людські ресурси.

Модель PERT широко використовується для планування розробки програмного забезпечення. Наприклад, у проекті зі створення нової платформи, де є

багато невідомих і потенційних затримок, PERT дозволяє оцінити час, необхідний для виконання завдань, таких як розробка окремих модулів, інтеграція, тестування тощо. Оцінки тривалості кожного етапу дозволяють більш точно спланувати строки завершення всього проекту та підготуватися до можливих затримок.

Завдяки використанню PERT проектні команди можуть краще керувати строками та ризиками, що особливо важливо в проектах з високим рівнем невизначеності та складності.

Ця модель надає інструменти для детального аналізу часових ризиків, що робить її важливим компонентом управління проектами, особливо в галузі інформаційних технологій.

Наступною пропонуємо розглянути COSO ERM (Enterprise Risk Management) — це модель управління ризиками на рівні підприємства, яка допомагає організаціям не тільки ідентифікувати та мінімізувати ризики, але й використовувати їх як можливості для досягнення стратегічних цілей.

Модель COSO ERM була розроблена Комітетом організацій-спонсорів Комісії Тредвея (Committee of Sponsoring Organizations of the Treadway Commission) і вперше представлена у 2004 році (хоча розроблена ще в 1992 році). COSO ERM пропонує системний підхід до управління ризиками, який інтегрується у всі процеси організації. Вона забезпечує компанії можливість розглядати ризики в контексті досягнення її цілей, таким чином впроваджуючи комплексний підхід до управління ризиками, що охоплює не лише реагування на загрози, а й використання їх як можливостей.

COSO ERM включає вісім взаємопов'язаних компонентів, які допомагають організаціям управляти ризиками на всіх рівнях — від стратегічного до операційного. Розглянемо всі з них.

1. Встановлення внутрішнього середовища. Це основний компонент, який формує основу для управління ризиками в організації. Внутрішнє середовище включає організаційну культуру, етичні стандарти та ставлення до управління ризиками, які задають тон у компанії. Важливими аспектами тут є політика управління ризиками, рівень відповідальності керівництва, а також готовність організації до прийняття ризиків. Цей компонент передбачає визначення того, як

ризики будуть розглядатися і керуватися в організації, включаючи рівень ризику, який організація готова прийняти для досягнення своїх цілей. Цей компонент також охоплює питання корпоративної культури, етичних стандартів і структури управління.

2. Встановлення цілей. Модель COSO ERM забезпечує, щоб організація встановлювала цілі, сумісні з її стратегією та апетитом до ризику. Це означає, що організація повинна узгоджувати свої стратегічні цілі з рівнем прийнятних ризиків, щоб уникнути невідповідності між намірами та можливостями. Організація має вирішити, чи готова вона прийняти ризики, пов'язані з конкретними стратегічними цілями. Ризики повинні розглядатися в контексті досягнення цих цілей, що дозволяє керівництву оцінити, чи виправдані певні ризики в контексті можливої вигоди. Таким чином, управління ризиками стає невід'ємною частиною процесу стратегічного планування.

3. Ідентифікація подій. На цьому етапі організація визначає як внутрішні, так і зовнішні події, які можуть вплинути на досягнення її цілей. Ці події можуть мати як позитивний, так і негативний характер. Позитивні події можна розглядати як можливості, а негативні події — як ризики. Ефективне управління подіями дозволяє організації не тільки реагувати на загрози, а й використовувати можливості для досягнення кращих результатів. Ідентифікація подій включає аналіз ринкових умов, нових технологій, змін законодавства, соціальних тенденцій тощо. Це допомагає організації бути готовою до змін та активно керувати невизначеністю.

4. Оцінка ризиків. Оцінка ризиків включає визначення ймовірності та впливу ідентифікованих подій на організацію. Ризики можуть оцінюватися як на кількісному, так і на якісному рівнях, що дозволяє приймати обґрунтовані рішення щодо того, як організація має реагувати на них. Модель COSO ERM передбачає оцінку ризиків у двох аспектах: на внутрішньому рівні (внутрішні процеси, ресурси) та на зовнішньому рівні (зміни на ринку, конкуренти, економічна ситуація). Цей процес допомагає визначити пріоритети в управлінні ризиками, зосереджуючи ресурси на найбільш серйозних загрозах або найбільших можливостях.

5. Реагування на ризики. Реагування на ризики може включати чотири основні стратегії: уникнення, зменшення, передача або прийняття ризику. Уникнення передбачає повне виключення діяльності, пов'язаної з певним ризиком. Зменшення — це вжиття заходів для мінімізації впливу ризику. Передача — це передача ризику на третю сторону (наприклад, через страхування або аутсорсинг). Прийняття ризику — це рішення організації взяти ризик на себе, оскільки очікувані вигоди можуть перевищувати потенційні втрати. Цей етап включає визначення того, як організація планує впоратися з кожним ризиком, і вибір стратегії управління ним.

6. Контроль і моніторинг. Ефективне управління ризиками передбачає постійний контроль за ризиками та їх впливом. Модель COSO ERM рекомендує використовувати систему постійного моніторингу та звітності, яка забезпечує організацію актуальною інформацією про стан ризиків. Це дозволяє керівництву своєчасно виявляти зміни в ризиках і відповідно коригувати свої дії. Моніторинг може бути регулярним (періодичні огляди) або спеціальним (реакція на раптові зміни). Важливо, щоб керівництво регулярно отримувало дані про стан управління ризиками, щоб приймати своєчасні рішення.

7. Інформація та комунікація. Управління ризиками неможливе без належної комунікації всередині організації. Модель COSO ERM підкреслює важливість передачі інформації про ризики на всіх рівнях управління. Інформація повинна бути доступною для тих, хто приймає рішення, щоб вони могли вживати відповідних заходів. Це включає як вертикальну (від керівництва до виконавців і назад), так і горизонтальну (між департаментами) комунікацію. Комунікація є важливою для побудови культури управління ризиками та забезпечення того, щоб усі співробітники розуміли свої ролі та відповідальність.

8. Відстеження ефективності. Цей етап включає оцінку того, наскільки ефективно організація управляє ризиками та досягає своїх цілей. Організація повинна постійно аналізувати свій підхід до управління ризиками, щоб покращувати процеси та реагувати на нові виклики. Відстеження ефективності також включає регулярні аудити та оцінки управлінських рішень, щоб переконатися, що вони адекватні і відповідають поточним умовам[38].

Переваги моделі COSO ERM:

- інтегрований підхід. COSO ERM об'єднує всі процеси організації в рамках єдиної стратегії управління ризиками, що дозволяє ефективніше реагувати на загрози і використовувати можливості.
- системність. Модель враховує всі рівні ризиків і процесів — від стратегічних до операційних, що допомагає приймати більш обґрунтовані рішення.
- гнучкість. COSO ERM дозволяє організації адаптувати свої процеси управління ризиками до змін в бізнес-середовищі та внутрішніх умовах.
- прозорість. Завдяки прозорій системі моніторингу й комунікації, всі учасники процесу можуть оперативно отримувати актуальну інформацію про ризики і їх вплив.

Недоліки моделі COSO ERM:

- трудомісткість впровадження. Впровадження COSO ERM вимагає значних зусиль, ресурсів і часу, особливо для великих організацій.
- високі витрати. Процеси моніторингу й аудиту можуть бути досить дорогими, особливо для компаній, які мають складні структури.
- залежність від культури управління. Ефективність моделі багато в чому залежить від того, наскільки глибоко вона вбудована в організаційну культуру.

У сфері IT COSO ERM використовується для управління різноманітними ризиками — від технологічних загроз (кібербезпека, неполадки в системах) до стратегічних (недосягнення бізнес-цілей, невідповідність ринку). Наприклад, при впровадженні нової IT-системи в організації COSO ERM дозволяє врахувати всі можливі ризики на кожному етапі — від аналізу ринкових умов до забезпечення безперебійної роботи системи після її запуску.

Ця модель є комплексним підходом до управління ризиками, що дає можливість як мінімізувати негативні впливи, так і використовувати ризики для отримання конкурентних переваг.

На останок розглянемо Аналітичну ієрархічну модель (AHP, англ. Analytic Hierarchy Process) — це потужний інструмент для прийняття рішень, розроблений Томасом Сааті в 1970-х роках. Вона дозволяє систематизувати й аналізувати складні

проблеми шляхом розподілу їх на ієрархічні рівні та оцінки альтернатив на основі багатокритерійного підходу. AHP широко використовується для оцінки та аналізу ризиків в IT-проектах, оскільки дозволяє приймати обґрунтовані рішення на основі чіткого порівняння різних факторів. Розглянемо етапи застосування AHP.

1. Чітке визначення основної мети або проблеми, яку потрібно вирішити. У контексті управління ризиками це може бути, наприклад, зниження ймовірності ризиків на етапі розробки ПЗ.

2. Побудова ієрархії. Вся система поділяється на кілька рівнів:

- На найвищому рівні знаходиться головна мета (наприклад, управління ризиками).
- Середній рівень складається з критеріїв або факторів ризику (наприклад, технічні ризики, фінансові ризики, ризики безпеки).
- На нижньому рівні розташовані альтернативи, які порівнюються між собою (наприклад, конкретні заходи або стратегії для зменшення ризиків).

3. Попарне порівняння критеріїв. Наступним етапом є порівняння критеріїв між собою в парах для оцінки їх відносної важливості. Кожен критерій оцінюється за шкалою від 1 до 9, де 1 означає рівну важливість, а 9 — надзвичайну перевагу одного критерію над іншим. Цей етап допомагає виявити, які критерії мають найбільший вплив на досягнення мети.

4. Обчислення вагових коефіцієнтів. Після порівняння кожного критерію розраховуються вагові коефіцієнти для кожного з них. Вони відображають, наскільки важливим є той чи інший фактор для загальної мети. Ці коефіцієнти допомагають у прийнятті більш обґрунтованих рішень.

5. Агрегування результатів. На заключному етапі оцінюються альтернативи з урахуванням вагових коефіцієнтів для кожного критерію. Підсумкові результати показують, яка альтернатива або стратегія є найкращою для досягнення головної мети[39].

Розглянувши дану модель можна вказати на наступні переваги AHP:

- структурованість і прозорість. AHP забезпечує чітку структуру для прийняття рішень, дозволяючи користувачам бачити, як різні критерії впливають на результат.
- можливість оцінки складних проблем. Метод підходить для багатокритерійних задач, коли важливо врахувати кілька факторів одночасно.
- гнучкість. AHP можна застосовувати в різних галузях, зокрема в управлінні IT-проектами, для оцінки ризиків, вибору стратегій або технологій.

Також можемо визначити і недоліки AHP:

- суб'єктивність. Процес попарного порівняння залежить від думки експертів, що може вплинути на точність результатів.
- велика кількість розрахунків. При великій кількості критеріїв та альтернатив процес може стати складним і вимагати багато часу.
- залежність від точності вхідних даних. Якщо на етапі порівняння критеріїв буде надано неправильну оцінку, це може суттєво вплинути на підсумковий результат.

Одним із дослідників, що розглядав застосування AHP у сфері управління ризиками, є Thomas L. Saaty, автор оригінальної методики AHP. Його праця "Decision Making for Leaders: The Analytic Hierarchy Process for Decisions in a Complex World" (1982) [40]стала однією з ключових робіт у галузі багатокритерійного аналізу рішень. Інші дослідники, як-от Winston W. Royce, активно використовують методику AHP для оцінки ризиків в IT-проектах.

Кожна з наведених моделей оцінки та аналізу ризиків відіграє важливу роль у процесі розробки IT-додатків, забезпечуючи різні підходи до ідентифікації та мінімізації ризиків. Використання цих моделей дозволяє не лише передбачати можливі проблеми, але й розробляти ефективні стратегії для їх уникнення, підвищуючи загальну ефективність та успішність проектів.

2.2. Методи зменшення ризиків при розробці та впровадженні IT-додатків

Процес розробки та впровадження IT-додатків є складним і багатоетапним, що створює численні ризики на кожному етапі. Від концептуалізації і проектування до тестування та інтеграції з іншими системами — кожен етап несе свої специфічні загрози, які можуть вплинути на успішність кінцевого продукту, його функціональність, безпеку та вартість. Ризики можуть бути технічними (пов’язаними з помилками в коді, недостатньою масштабованістю або несумісністю з іншими системами), організаційними (пов’язаними з управлінськими рішеннями, недостатньою комунікацією в команді або несвоєчасним виконанням завдань) і бізнесовими (пов’язаними з неправильним розумінням потреб клієнта чи ринку).

У зв'язку з таким різноманіттям можливих ризиків важливо використовувати ефективні методи зменшення й управління ними, щоб мінімізувати ймовірність їх виникнення та обмежити потенційні збитки. Правильний вибір та застосування таких методів дозволяє командам швидко реагувати на зміни в умовах проекту, оптимізувати процеси та забезпечити високу якість кінцевого продукту.

Існує багато різних методик, які можуть бути використані для управління ризиками в IT-проектах. Це гнучкі методології, що дають можливість швидко адаптуватися до змін, такі як Agile та DevOps, методи, орієнтовані на безпеку, як тестування безпеки, а також технічні підходи, як методика прототипування. Кожен з цих методів має свої специфічні переваги і вимагає окремого розгляду на різних етапах розробки.

Додатково, наявність стабільного плану управління змінами, резервного копіювання, тестування і моніторингу дає можливість знизити ризики при впровадженні програмного забезпечення в реальне середовище. Це важливо не лише для забезпечення безперебійної роботи додатка, а й для підтримки його актуальності, безпеки та ефективності у майбутньому.

У цьому підпункті ми розглянемо основні методи зменшення ризиків, які застосовуються на етапах розробки, тестування та впровадження IT-додатків, і детально проаналізуємо їх переваги.

Agile є однією з найбільш ефективних методологій для управління IT-проектами, оскільки дозволяє командам гнучко реагувати на зміни, що виникають у процесі розробки. Цей підхід полягає в розробці продукту через серії ітерацій, кожна з яких має чітко визначену мету та приносить конкретний результат. Це дозволяє коригувати напрямок розвитку продукту на кожному етапі, враховуючи нові обставини чи зміни в вимогах. У процесі роботи над проектом команда регулярно збирає зворотний зв'язок від замовника або кінцевих користувачів, що дозволяє реагувати на їхні потреби та вимоги своєчасно та ефективно.

Однією з головних особливостей Agile є гнучкість в управлінні вимогами та швидка адаптація до змінюваного середовища. Це робить методику надзвичайно корисною для проектів, де вимоги не є чітко визначеними з самого початку або часто змінюються в процесі розробки. Ітераційний підхід дозволяє команді постійно оцінювати та коригувати свою роботу, що значно знижує ризики, пов’язані з невизначеністю вимог та технічними помилками. Кожна ітерація приносить можливість для безперервного вдосконалення продукту, що дозволяє виявляти й усувати недоліки на ранніх етапах, не дозволяючи їм накопичуватися.

Крім того, Agile підтримує високу командну взаємодію та комунікацію, що позитивно впливає на ефективність роботи. Це дозволяє зберігати чіткий контакт з усіма учасниками процесу та вчасно реагувати на проблеми, що виникають. Переваги методики включають постійне тестування продукту, що дає можливість виявляти помилки на ранніх етапах і виправляти їх до того, як вони стануть значними. Постійний зворотний зв'язок з клієнтом дозволяє точніше виконувати вимоги та вдосконалювати кінцевий продукт[41].

Водночас методика Agile має й свої обмеження. Вона може бути менш підходящою для великих проектів, де вимоги до контролю за процесом, документацією та структурою розробки є більш строгими. Для таких проектів може бути потрібен більш традиційний підхід із детальнішим плануванням і документуванням. Тим не менше, Agile ідеально підходить для середніх і малих проектів, де важлива швидкість реакції на зміни і гнучкість у підходах.

Методика прототипування є одним із найбільш ефективних і практичних методів для зменшення ризиків при розробці IT-додатків, оскільки воно дозволяє на ранніх етапах створити неповну, але функціональну версію продукту, яка демонструє, як кінцевий продукт буде виглядати та функціонувати. Важливою особливістю цього підходу є можливість тестування окремих елементів системи, таких як інтерфейс користувача, ключові функціональні можливості або специфічні технологічні елементи. Прототипи можуть бути створені для різних частин додатку, що дає змогу перевірити не лише зовнішній вигляд, а й взаємодію користувачів з продуктом, що в свою чергу знижує ризики потенційних помилок або непорозумінь.

Основною метою прототипування є надання замовнику чи користувачеві можливості «побачити» і «відчути» продукт ще до його завершення. Це дає змогу на ранньому етапі виявити можливі проблеми та недоліки, що можуть виникнути в процесі використання, і усунути їх до того, як буде розпочата основна розробка кінцевої версії. Завдяки прототипуванню можна досягти більш точного та реалістичного розуміння вимог і побажань замовника, що дозволяє значно зменшити ймовірність невідповідності результатів кінцевому продукту.

Прототипування є надзвичайно корисним для проектів, де існує значна невизначеність або неповне розуміння вимог з боку замовника, що часто виникає у випадках, коли проект тільки починається або коли замовник не може чітко сформулювати свої очікування. Створення прототипу дає можливість побудувати початкову модель продукту, яка може бути адаптована і змінена відповідно до відгуків користувачів і замовників на кожному етапі. Це дає змогу коригувати напрямок розвитку проекту на ранніх етапах і уникнути витрат на повну розробку і реалізацію помилкових або непотрібних функцій.

Процес прототипування не лише дозволяє знизити ризики, а й полегшує комунікацію між командою розробників і замовником. Прототипи надають наочне уявлення про те, як буде виглядати кінцевий продукт, що дозволяє замовникам чіткіше уявити результат, а також дає змогу команді точніше зрозуміти вимоги і побажання замовника. Таким чином, цей метод значно покращує ефективність

співпраці між усіма учасниками проекту і дозволяє досягти більш точного результату, який задовольняє обидві сторони.

Однією з основних переваг прототипування є те, що цей метод дозволяє виявити технічні або функціональні недоліки на ранніх етапах розробки, що дає можливість внести корективи до того, як буде завершена основна частина роботи над продуктом. Це значно знижує ймовірність великих витрат часу та ресурсів на виправлення помилок, що з’являться на більш пізніх етапах, коли внесення змін буде набагато складнішим та дорожчим. Окрім того, прототипування забезпечує швидкий зворотний зв'язок, що дозволяє оперативно реагувати на виявлені недоліки або зміни в вимогах замовника[42].

Проте метод прототипування має й деякі недоліки. Один із основних — це можливість необхідності переробки вже розроблених елементів продукту, що може призвести до значних витрат часу та ресурсів. Особливо це актуально для великих або складних проектів, де зміни на одному етапі можуть вимагати значної перебудови інших частин системи. Також важливо зазначити, що прототипування не завжди дозволяє досягти повної точності у відображенні всіх функцій кінцевого продукту, особливо на ранніх етапах, коли прототип лише демонструє основні ідеї.

Попри ці недоліки, прототипування є надзвичайно важливим методом для покращення розуміння вимог і зниження ризиків у проектуванні IT-додатків, зокрема для проектів, що мають складну чи змінну специфікацію.

Методика DevOps представляє собою набір практик, спрямованих на інтеграцію процесів розробки і експлуатації програмного забезпечення з метою забезпечення безперервного циклу постійного вдосконалення продукту. Вона фокусується на оптимізації та автоматизації всіх етапів життєвого циклу програмного забезпечення — від розробки до експлуатації. Основною метою DevOps є створення гнучкого та ефективного процесу, що дозволяє швидко доставляти програмні оновлення і виправлення, одночасно підвищуючи стабільність і безпеку продукту[43].

Ключовим аспектом DevOps є поєднання автоматизації в процесах розгортання, тестування та моніторингу з постійним зворотним зв'язком від кінцевих користувачів. Це дозволяє знизити ризики, пов'язані з помилками, оскільки зміни

можна швидко тестувати і виправляти ще до того, як вони потраплять до кінцевих користувачів. Водночас, постійна інтеграція і постійне тестування дозволяють виявляти навіть найменші помилки або уразливості на ранніх етапах, що мінімізує їхній вплив на кінцевий продукт.

DevOps також сприяє створенню тісної співпраці між командами розробників і операційними командами, що дозволяє значно зменшити ймовірність виникнення проблем під час розгортання або оновлення продукту. Оскільки обидві команди працюють спільно над одними й тими ж цілями — швидким випуском продукту, високою якістю та стабільністю — зменшується кількість конфліктів та помилок, пов'язаних з інтеграцією нових функцій[44].

Одна з найбільших переваг цього підходу полягає в безперервному тестуванні та моніторингу на всіх етапах розробки. Завдяки автоматизованим процесам тестування, розгортання і доставки програмного забезпечення, DevOps дозволяє значно зменшити час, необхідний для випуску оновлень, а також знижує ймовірність людських помилок. В автоматизованих процесах часто використовуються інструменти, які допомагають ефективно перевіряти функціональність, безпеку та продуктивність системи, що дозволяє розробникам фокусуватися на вдосконаленні функцій і виявленні можливих уразливостей у системі.

Крім того, завдяки регулярному моніторингу і зворотному зв'язку, DevOps дозволяє підтримувати високий рівень стабільності та безпеки продукту, оскільки будь-які зміни і потенційні проблеми можна швидко виявити і вирішити на ранніх етапах. Такий підхід знижує ймовірність серйозних інцидентів, які можуть виникнути під час розгортання нових версій продукту або його оновлення, що є особливо важливим для продуктів, які працюють в реальному часі або мають критичну для бізнесу інфраструктуру.

Однак, незважаючи на численні переваги, впровадження DevOps може бути викликом для компаній, які не мають розвиненої технічної інфраструктури або достатньо кваліфікованої команди. Для успішного впровадження цієї методики потрібно значно інвестувати в автоматизацію процесів і оновлення інструментів, що можуть бути складними для організацій з обмеженими ресурсами. Крім того, постійні

оновлення і зміни, характерні для цього підходу, можуть бути проблемою для великих проектів, що складаються з багатьох компонентів, які вимагають ретельного контролю і координації між різними командами та підрозділами.

Загалом, DevOps є потужним інструментом для тих компаній, які прагнуть підвищити ефективність і швидкість розробки, одночасно підтримуючи високі стандарти якості та безпеки продукту. Але для його успішного впровадження необхідно бути готовими до значних інвестицій в інфраструктуру та підготовку персоналу.

Методика тестування безпеки є однією з найважливіших складових для забезпечення надійного захисту даних і підтримки безпеки IT-додатків. Це набір процедур та інструментів, спрямованих на виявлення і усунення вразливостей, що можуть бути використані зловмисниками для атаки на систему. Зазвичай тестування безпеки включає кілька етапів, зокрема перевірку на вразливості, пенетраційне тестування та оцінку стійкості системи до зовнішніх загроз. Ці методи дозволяють виявити можливі слабкі місця в програмному забезпеченні та інфраструктурі ще до того, як продукт буде запущений у реальному середовищі.

Перевірка на вразливості є першим етапом у тестуванні безпеки, коли система сканується на наявність відомих уразливостей, таких як помилки в конфігурації, незахищені порти або старі версії бібліотек, які можуть бути використані для несанкціонованого доступу. Виявлення таких проблем дозволяє виправити їх до того, як система буде введена в експлуатацію, що значно знижує ймовірність атак на пізніших етапах.

Пенетраційне тестування, або тестування на проникнення, є більш глибоким і інтенсивним методом тестування безпеки, який моделює реальні атаки на систему. Воно включає спроби проникнути в систему або додаток, щоб виявити потенційні вразливості, через які зловмисники могли б отримати доступ до конфіденційної інформації або здійснити шкідливі дії. Це дозволяє виявити слабкі місця в захисті, на які не можна звернути увагу лише під час звичайної перевірки на вразливості. Пенетраційне тестування також дозволяє оцінити ефективність існуючих заходів безпеки та надає практичні рекомендації щодо їх посилення[45].

Крім того, тестування безпеки включає оцінку стійкості системи до атак, таких як відмови в обслуговуванні (DoS), SQL-ін'єкції, міжсайтові скриптові атаки (XSS) та інші види кіберзагроз. Застосування цих методів дозволяє зменшити ризики, пов’язані з кібератаками, що є критичними для багатьох сфер бізнесу, особливо у фінансових або медичних секторах, де безпека даних є пріоритетною.

Однією з основних переваг тестування безпеки є можливість мінімізації ризиків витоків конфіденційної інформації та запобігання зловмисним атакам. Це не лише покращує захист даних, але й підвищує довіру користувачів та партнерів до продукту. Продукти, що пройшли ретельне тестування безпеки, зазвичай користуються більшою популярністю серед споживачів, оскільки їхні користувачі впевнені, що їхні дані знаходяться в безпеці. Тому належний рівень безпеки є важливим чинником для забезпечення репутації компанії та її конкурентоспроможності на ринку.

Проте, застосування методів тестування безпеки може бути дорогим і ресурсномістким процесом, особливо для великих або складних систем, які потребують ретельної перевірки. Для великих організацій це може означати значні витрати на інструменти тестування, спеціалізовані кадри та час, необхідний для проведення тестувань. Зважаючи на це, для організацій важливо оцінювати співвідношення вартості тестування безпеки і потенційних ризиків, щоб прийняти зважене рішення про необхідність проведення таких тестів. У деяких випадках може бути доцільним виконання тестування на безпеку після основних етапів розробки, щоб збалансувати витрати і забезпечити належний рівень захисту.

Загалом, методика тестування безпеки є ключовим інструментом для забезпечення захисту від кібератак та інших загроз. Вона дозволяє виявити і усунути потенційні вразливості ще до того, як продукт потрапить до кінцевих користувачів, що в результаті знижує ризики витоку даних та репутаційні збитки для компанії.

Резервне копіювання та планування відновлення після катастрофи є одними з основних методів управління ризиками, які забезпечують безперервність бізнес-процесів і зменшують ймовірність втрати даних або критичних збоїв у системах. Основною метою резервного копіювання є створення регулярних копій усіх важливих

даних і системних налаштувань, що дозволяє швидко відновити інформацію в разі непередбачених ситуацій, таких як технічні збої, природні катастрофи, хакерські атаки або людські помилки. Цей процес передбачає використання різних типів зберігання даних, таких як локальні, віддалені сервери або хмарні сховища, щоб гарантувати доступність резервних копій в будь-який час[46].

Планування відновлення після катастрофи є невід'ємною частиною стратегії резервного копіювання. Він включає розробку детальних алгоритмів і процедур для відновлення роботи системи за мінімальний час після катастрофи, що дозволяє знизити час простою і обмежити збитки для компанії. Цей план зазвичай включає етапи відновлення даних, тестування працездатності відновлених систем і перехід до нормального функціонування. Забезпечення швидкого і ефективного відновлення є критично важливим, особливо для компаній, що працюють у сферах, де кожна хвилина простою може призвести до значних фінансових втрат або шкоди репутації.

Метод резервного копіювання дає можливість підтримувати цілісність і доступність даних, навіть якщо основна система зазнає збоїв. У разі серйозних аварій або втрати даних, компанія може швидко відновити критичну інформацію, що забезпечує безперервність її діяльності. Це особливо важливо для підприємств, які працюють з великими обсягами даних, таких як фінансові установи, медичні заклади чи онлайн-сервіси, де втрати інформації можуть мати серйозні наслідки. Такі заходи також знижують ризики, пов'язані з відмовами апаратного або програмного забезпечення, оскільки наявність резервних копій забезпечує додатковий рівень захисту.

Проте, метод резервного копіювання має і свої недоліки. Для великих компаній або систем з великими обсягами даних цей процес може бути ресурсно-затратним. Необхідно не лише зберігати резервні копії, а й регулярно їх оновлювати, що може вимагати значних інвестицій у відповідну інфраструктуру та персонал. Крім того, резервне копіювання не може запобігти самому виникненню атак чи технічних збоїв, тому воно має бути лише частиною комплексної стратегії безпеки, що включає також моніторинг, тестування безпеки та інші методи захисту.

У великих організаціях, де ризики та наслідки збоїв є ще більш значними, важливо поєднувати резервне копіювання з іншими заходами, такими як регулярні тренування з відновлення після катастроф, впровадження систем моніторингу та автоматичного реагування на інциденти. Це дозволяє знизити ймовірність виникнення непередбачуваних ситуацій і забезпечити швидке відновлення системи, що критично важливо для забезпечення безпеки та стабільності бізнесу[47].

Управління змінами є надзвичайно важливою методикою для зменшення ризиків під час розробки та впровадження IT-додатків. Воно включає систематичне й контрольоване внесення змін у проект або систему на всіх етапах її життєвого циклу — від початкового планування до тестування та запуску в реальному середовищі. Процес управління змінами гарантує, що всі модифікації будуть чітко документовані, оцінені з точки зору їхнього впливу на систему, і що зміни не призведуть до непередбачуваних чи небажаних наслідків для функціональності або безпеки додатку.

Ключовою метою управління змінами є забезпечення прозорості та контролю над усіма змінами, які вносяться в проект. Це дозволяє організаціям мати чітке уявлення про всі поточні та майбутні зміни, що вносяться в систему, а також оцінити їхній вплив на загальну архітектуру і продуктивність продукту. При цьому оцінка ризиків, пов'язаних із змінами, допомагає запобігти несподіваним помилкам або проблемам, що можуть виникнути через неправильно втілені зміни.

Завдяки належному управлінню змінами організація може мінімізувати потенційні негативні наслідки, такі як збої в роботі системи або порушення її цілісності. Кожен етап змін проходить через кілька рівнів перевірки, що дозволяє фахівцям чітко оцінити кожну зміну за її важливістю і впливом на кінцевий результат. Крім того, у разі виникнення проблем, система управління змінами дозволяє швидко повернутися до попередніх версій програмного забезпечення або проекту, що допомагає мінімізувати час і витрати на виправлення помилок.

Одним із важливих аспектів цієї методики є збереження стабільності IT-системи, що забезпечує безперервну роботу без втрат продуктивності. Вона також допомагає створити середовище для зворотного зв'язку, де розробники,

тестувальники та інші учасники процесу можуть обговорювати зміни та їх можливі наслідки, що підвищує загальний рівень контролю над проектом.

Управління змінами дозволяє знижувати ймовірність виникнення хаосу під час розробки проекту, оскільки всі зміни здійснюються за чітко визначеною процедурою, що включає затвердження, тестування та верифікацію. Це дозволяє зберігати повний контроль за проектом, уникати безладних змін і знижувати ймовірність негативних наслідків для кінцевого продукту.

Крім того, правильна система управління змінами сприяє оптимізації процесу впровадження змін, що дозволяє знижувати час на тестування та випуск оновлень. Це важливо для проектів з високою динамікою змін, де потрібно швидко адаптуватися до нових вимог або технологічних інновацій, зберігаючи при цьому стабільність і функціональність системи.

Загалом, управління змінами є важливим інструментом для забезпечення ефективного, контрольованого та стабільного розвитку IT-проектів, що допомагає знижувати ризики і забезпечує максимальну ефективність у розробці програмного забезпечення.

Управління ризиками в розробці та впровадженні IT-додатків є критичним елементом для забезпечення успішного виконання проектів і досягнення поставлених цілей. Вибір відповідних методик дозволяє не лише знижувати ймовірність виникнення негативних подій, але й забезпечувати стійкість та стабільність систем у процесі їхнього розвитку. Використання таких методів, як Agile, прототипування, DevOps, тестування безпеки, резервне копіювання, планування відновлення після катастроф, а також управління змінами, допомагає знижувати ризики, пов’язані з невизначеністю вимог, помилками в розробці, технічними збоїми або атаками на систему.

Кожна з описаних методик має свої особливості та переваги, що дозволяють вибрати найефективніший підхід у залежності від характеру та масштабу проекту. Наприклад, методика Agile забезпечує гнучкість і швидку адаптацію до змін, прототипування дозволяє на ранніх етапах отримати зворотний зв'язок від користувачів, а DevOps знижує ризики помилок через автоматизацію процесів.

Тестування безпеки допомагає виявити вразливості на етапі розробки, а резервне копіювання і планування відновлення після катастроф забезпечують безперервність роботи системи навіть у разі серйозних збоїв.

Управління змінами є основою для забезпечення контролю і стабільності протягом всього життєвого циклу проекту, зокрема шляхом ефективного керування внесенням змін в систему. Завдяки чіткому процесу управління змінами можна забезпечити належний рівень прозорості, мінімізувати ризики та своєчасно реагувати на проблеми, що виникають[48].

Загалом, комплексний підхід до управління ризиками та використання різноманітних методик дозволяє не лише мінімізувати можливі загрози, але й забезпечити стабільний і прогнозований розвиток IT-додатків, що в свою чергу сприяє досягненню бізнес-цілей та задоволенню потреб користувачів.

2.3. Аналіз ризиків на різних етапах життєвого циклу розробки

Розробка IT-додатків є складним та багатофакторним процесом, який складається з кількох етапів, кожен з яких має свої специфічні виклики та ризики. Ці етапи включають аналіз вимог, проектування, розробку, тестування, впровадження, супровід і підтримку, а також оцінку результатів. З огляду на технічну та організаційну складність кожного етапу, ризики, які можуть виникнути, мають значний вплив на кінцевий результат проекту, включаючи його ефективність, терміни та бюджет.

Управління ризиками є важливою частиною забезпечення успішної реалізації проекту, оскільки невчасно виявлені або погано управлінні ризики можуть призвести до серйозних проблем. Ризики на кожному етапі життєвого циклу IT-додатка можуть мати різні форми: від технічних недоліків, таких як помилки в коді або архітектурі, до організаційних проблем, таких як неповне розуміння вимог замовника або затримки в тестуванні. Усі ці ризики потребують чіткої стратегії управління, щоб мінімізувати їх вплив на кінцевий продукт.

У цьому підпункті буде здійснено детальний аналіз ризиків, що виникають на різних етапах розробки ІТ-додатків, а також розглянуто ефективні стратегії для їх мінімізації. Для кожного етапу життєвого циклу буде наведено типові ризики, способи їх виявлення та управління, а також приклади можливих інструментів та методів для зменшення ймовірності негативних наслідків.

Першим і дуже важливим етапом у процесі розробки ІТ-додатків є аналіз вимог. Цей етап визначає, які функціональні можливості та характеристики має включати майбутній додаток, а також з'ясовує реальні потреби замовника. Важливо заздалегідь правильно зрозуміти ці вимоги, оскільки від цього буде залежати вся подальша розробка, тестування та впровадження продукту. Проблеми на етапі збору вимог можуть призвести до неузгодженості між тим, що хоче отримати замовник, та тим, що в результаті розробляється.

Невизначеність вимог є одним із найбільших ризиків на етапі збору вимог. Це може трапитись, якщо замовник або кінцеві користувачі не можуть чітко сформулювати свої очікування або не мають досвіду у визначенні конкретних технічних або бізнес-потреб. В результаті цього можуть виникнути непорозуміння, а вимоги стануть неясними або занадто абстрактними, що значно ускладнить процес подальшої розробки та реалізації додатка. Щоб мінімізувати невизначеність вимог, необхідно створити чітку, зрозумілу і детальну документацію вимог. Це документ, в якому чітко описано, що саме потрібно замовнику, які функції має виконувати продукт, а також визначено технічні вимоги, необхідні для реалізації цих функцій. Така документація є основою для подальшої розробки і дозволяє уникнути непорозумінь в процесі реалізації.

Неповне розуміння потреб замовника є ще одним значним ризиком. Це трапляється, коли замовник не може чітко описати свої вимоги, або коли у нього є лише поверхневе розуміння того, як має виглядати продукт. Технічна команда може неправильно трактувати ці вимоги, що призведе до помилок при проектуванні та розробці продукту. Крім того, може виникнути проблема, коли замовник не враховує всі деталі, які можуть бути важливими для системи, і це виявляється лише на пізніших етапах. Для зменшення ризику неповного розуміння потреб замовника дуже важливо

активно залучати кінцевих користувачів і замовників до процесу збору вимог. Це можна досягти за допомогою різних методів, таких як інтерв'ю, опитування, фокус-групи або навіть спільні сесії для визначення вимог (workshops). Завдяки цьому можна не лише уточнити важливі деталі, а й визначити пріоритети для функціональності додатка, що дозволить побудувати точне уявлення про потреби замовника[49].

Зміни вимог під час розробки – це ще один поширений ризик, який може суттєво вплинути на весь життєвий цикл розробки. Вимоги можуть змінюватися з різних причин: через зміни в бізнес-цілях замовника, зміни у зовнішньому середовищі або нові технологічні вимоги. Це може призвести до затримок в розробці, адже команда повинна буде адаптувати код і функціональність під нові умови, що також збільшує витрати.

Щоб мінімізувати вплив змін вимог під час розробки, важливо організувати регулярні ревізії вимог і їх уточнення. Цей процес дає можливість вчасно виявити будь-які зміни та оцінити їх вплив на проект. Регулярні зустрічі з замовником, під час яких можна обговорити можливі зміни вимог, дозволяють зменшити ризик виникнення непорозумінь і зберегти точність проекту. Така взаємодія також допомагає своєчасно коригувати план і бюджет, якщо зміни вимог потребують додаткових ресурсів. Аналізуючи вище наведене, можемо виокремити проаналізовану інформацію у наступну схему.

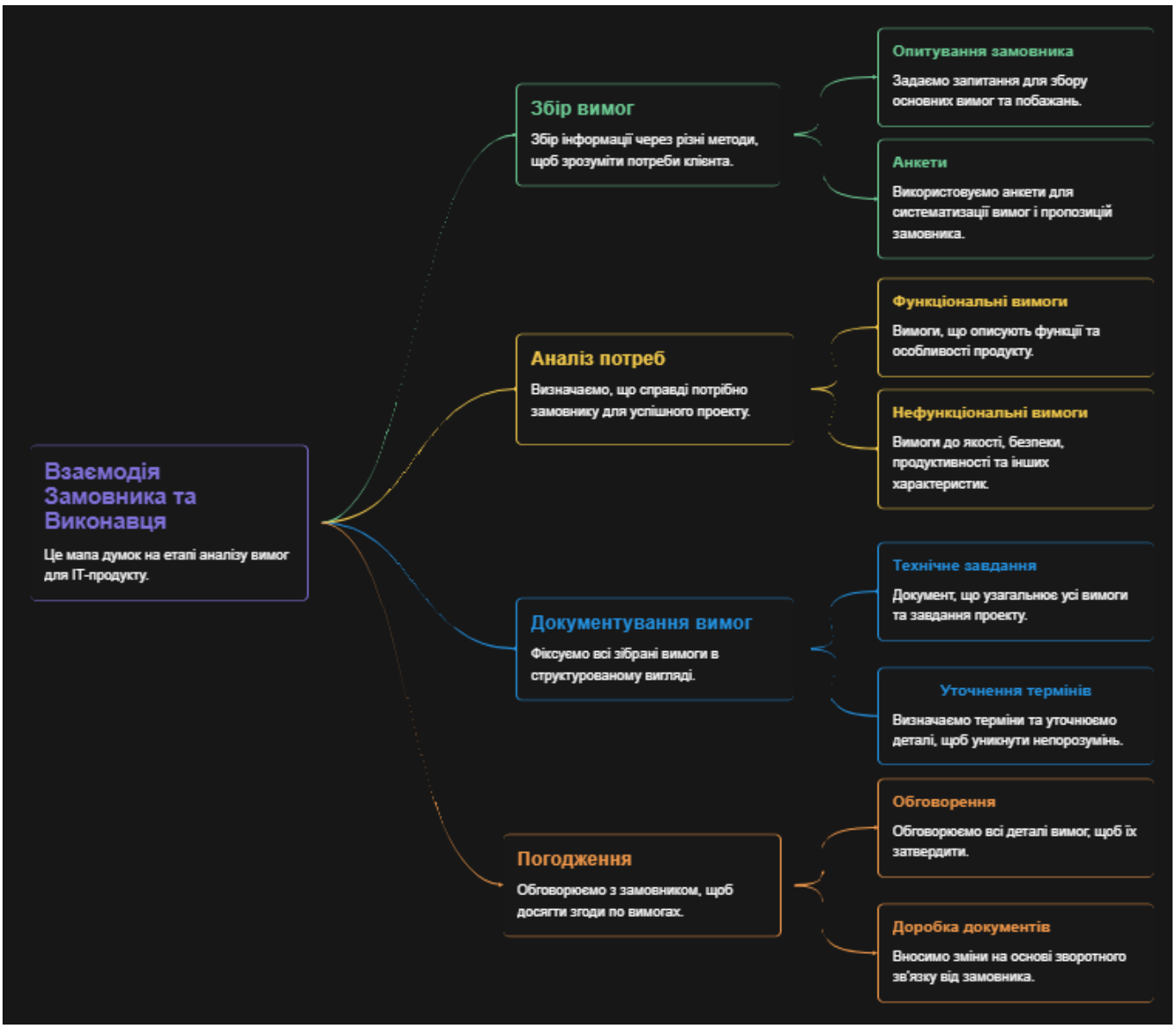

Рис. 2.1 Схема взаємодії замовника та виконавця IT-проекту.*

*Розроблена автором.

Загалом, успішне управління ризиками на етапі збору вимог дозволяє створити міцну основу для всього подальшого процесу розробки. Ключовими моментами є чітка документація вимог, активне залучення замовника та кінцевих користувачів до визначення вимог і регулярні зустрічі для уточнення змін. Такий підхід допомагає уникнути серйозних проблем, що можуть виникнути через непорозуміння чи зміну вимог під час подальших етапів проекту.

У результаті, правильно організований процес збору вимог не лише допомагає зменшити ризики, але й забезпечує наявність чіткої та стабільної бази для ефективного планування й реалізації всього життєвого циклу розробки IT-додатка.

Етап проектування є ключовим у процесі створення IT-додатка, оскільки саме тут закладаються основи його архітектури, визначаються основні компоненти, а також їхня взаємодія. На цьому етапі приймаються рішення, що впливають не лише на функціональність продукту, але й на його продуктивність, масштабованість, безпеку та довговічність. Успішне проектування забезпечує гладке проходження наступних етапів розробки та знижує ймовірність виникнення серйозних проблем у майбутньому.

Одним із ключових аспектів проектування є врахування вимог, отриманих від замовника, і адаптація цих вимог до технічних реалій. У процесі проектування команда розробки стикається з необхідністю вирішувати складні задачі, зокрема вибір технологій, що найкраще відповідають специфіці проекту, і визначення підходу до інтеграції з іншими системами. Крім того, цей етап вимагає системного підходу до оцінки ризиків, що можуть виникнути як через недоліки в архітектурі, так і через помилки в плануванні чи комунікації[49].

Зважаючи на важливість проектування, у цьому підрозділі будуть розглянуті типові ризики, що виникають на цьому етапі, а також стратегії управління ними. Ми зосередимо увагу на таких аспектах, як помилки в архітектурі, відповідність технічним вимогам і складність інтеграції з іншими системами. Кожен з ризиків буде проаналізовано окремо з точки зору його впливу на проект та ймовірності виникнення, а також буде запропоновано практичні стратегії для їх мінімізації.

Таким чином, етап проектування є не лише технічним процесом, але й стратегічним моментом, що визначає напрямок усього проекту. Ретельне управління ризиками та правильний підхід до проектування допоможуть уникнути значних втрат часу та ресурсів у подальшому, забезпечивши високу якість кінцевого продукту.

Помилки в архітектурі системи є однією з найпоширеніших проблем на етапі проектування, адже архітектура визначає основу всієї системи. Неправильний вибір архітектурного підходу або відсутність чіткого проектування може призвести до труднощів у масштабуванні, зниження продуктивності та нестабільності системи. Наприклад, монолітна архітектура, яка часто використовується в невеликих проектах, може стати перепоною для розширення функціональності у великих масштабованих

системах. Щоб уникнути таких проблем, важливо використовувати перевірені шаблони проектування, які забезпечують структурованість і передбачуваність архітектури. Наприклад, мікросервісна архітектура є оптимальним вибором для систем, що потребують високої гнучкості та легкої інтеграції. Такий підхід дозволяє розділяти функціональність на незалежні компоненти, спрощуючи управління, масштабування та оновлення. Окрім того, регулярні архітектурні рев'ю із залученням експертів допомагають ідентифікувати слабкі місця ще до початку розробки[50].

Іншим важливим ризиком є невідповідність технічним вимогам, що може виникнути через неправильну інтерпретацію вимог замовника, недостатню деталізацію технічної документації або неповне врахування нефункціональних характеристик. Наприклад, якщо вимоги до безпеки або продуктивності системи не були чітко визначені, це може призвести до недоліків у роботі продукту після впровадження. Для управління цим ризиком необхідно постійно перевіряти проектні рішення на відповідність початковим вимогам, що досягається шляхом проведення систематичних ревізій. Крім того, залучення незалежних експертів може забезпечити додаткову об'єктивність, а прозора комунікація між командою розробників і замовником дозволяє вчасно уточнювати технічні деталі. Використання таких інструментів, як моделювання сценаріїв або створення прототипів компонентів, дозволяє виявити можливі невідповідності до початку розробки.

Складність інтеграції з іншими системами є критичним ризиком, особливо для додатків, які повинні взаємодіяти з різноманітними платформами, програмами чи сервісами. Наприклад, недостатнє врахування особливостей вже існуючих систем може спричинити збої у взаємодії, що вплине на загальну ефективність продукту. Щоб знизити цей ризик, важливо використовувати стандартизовані протоколи обміну даними, такі як REST API або GraphQL, що забезпечують уніфікований спосіб взаємодії між системами. Додатково, тестування прототипів інтеграції ще на стадії проектування дозволяє виявити можливі технічні проблеми заздалегідь. Наприклад, перевірка сумісності даних або часу відгуку інтегрованих сервісів допомагає адаптувати проектні рішення до реальних умов. Залучення технічних консультантів із досвідом роботи з відповідними платформами також підвищує ймовірність

успішної інтеграції. Отже як підсумок вищенаведеної інформації можемо навести таблицю оцінки можливих ризиків на етапі проектування[51].

Таблиця 2.1*

Оцінка можливих ризиків проектування

Ризик	**Ймовірність**	**Вплив**	**Приклад наслідків**	**Стратегії управління**
Помилки в архітектурі	Висока	Критичний	Погана продуктивність, збої у роботі додатка	Використання шаблонів, залучення експертів
Невідповідність технічним вимогам	Середня	Високий	Неможливість реалізувати всі функції, зазначені в документації	Регулярні ревізії, перевірка відповідності вимогам
Складність інтеграції з іншими системами	Середня	Середній	Затримки у розробці, додаткові витрати на доопрацювання інтеграції	Стандартизація інтерфейсів, тестування інтеграції

*Розроблена автором.

Етап проектування є фундаментальним для успішної реалізації будь-якого IT-додатка, адже на цьому етапі визначаються рамки, у межах яких працюватиме вся команда. Неправильні рішення, прийняті на етапі проектування, можуть не лише уповільнити розробку, але й призвести до значного перевищення бюджету через потребу у виправленні помилок.

Ефективне управління ризиками на етапі проектування включає використання передових методик, таких як моделювання архітектури, впровадження шаблонів проектування та ретельний аналіз вимог. Успішне виконання цього етапу дозволяє не лише зменшити ймовірність проблем у майбутньому, але й підвищити якість кінцевого продукту, забезпечуючи задоволення потреб замовника та ефективність команди.

Етап розробки є центральним і критично важливим у життєвому циклі створення IT-додатків. На цьому етапі відбувається безпосередня реалізація всіх функцій, визначених на етапах аналізу вимог та проектування. Це ключовий момент,

коли концепція перетворюється на реальний продукт, що відповідає вимогам замовника та споживача. У процесі розробки необхідно створити програмний код, забезпечити інтеграцію різних компонентів системи, перевірити їхню сумісність, а також переконатися у відповідності визначеним технічним вимогам. Це включає не тільки розробку основної функціональності, а й розв'язання складних технічних завдань, таких як інтеграція з іншими системами, забезпечення високої продуктивності, безпеки даних та підтримка масштабованості системи.

Однак цей етап не є позбавленим ризиків, які можуть значно вплинути на якість кінцевого продукту, його строки реалізації та витрачені ресурси. Ризики на етапі розробки можуть виникати з різних причин, таких як помилки в програмному коді, невідповідність вимогам функціональності, технічні проблеми, а також організаційні та комунікаційні труднощі всередині команди. Вони можуть призвести до затримок у проекті, збільшення витрат, погіршення якості продукту, а інколи й до повної відмови від реалізації деяких функцій або навіть проекту в цілому.

Визначення та аналіз цих ризиків на ранніх етапах розробки дозволяє не лише зменшити ймовірність помилок, але й створити механізми для своєчасного реагування на непередбачені ситуації. Це включає розробку ефективних стратегій управління ризиками, що базуються на ретельному плануванні, прогнозуванні можливих проблем і впровадженні запобіжних заходів. Наприклад, використання методів автоматизації тестування дозволяє виявити дефекти на ранніх етапах, а стандарти кодування та регулярні ревізії коду допомагають мінімізувати помилки в програмному забезпеченні.

Крім того, комунікація в команді та з замовником є важливим аспектом управління ризиками. Налагоджена комунікація допомагає своєчасно виявити розбіжності між розробниками та замовниками, що може призвести до невідповідності функціональних вимог. Стандартизація процесів розробки, таких як використання єдиних фреймворків, мов програмування, інструментів тестування і документації, дає змогу значно знизити ймовірність помилок через людський фактор.

Інструменти автоматизації, такі як CI/CD (неперервна інтеграція та доставка), а також профілювальники продуктивності і статичний аналіз коду, допомагають

підтримувати високу якість коду, оптимізувати продуктивність системи та вчасно виявляти слабкі місця в архітектурі. Завдяки таким інструментам можна швидко виявляти помилки, коригувати їх на ранніх етапах розробки і уникати значних витрат часу на виправлення дефектів на пізніших етапах тестування або після впровадження.

Успішне управління ризиками на етапі розробки також передбачає адаптивність до змін. Врахування можливих змін вимог чи невизначеностей дозволяє гнучко коригувати процес розробки без значних втрат у часі або якості. Це також включає ефективну взаємодію з іншими етапами життєвого циклу, такими як тестування і впровадження, щоб забезпечити узгодженість і збереження високої якості на всіх етапах.

Програмні помилки є одними з найпоширеніших і найскладніших ризиків на етапі розробки. Вони можуть варіюватися від простих синтаксичних помилок до серйозних логічних чи архітектурних недоліків, які можуть призвести до збоїв у роботі програми або некоректного оброблення даних. Такі помилки можуть виникати з різних причин, зокрема через погане розуміння вимог, недостатню перевірку коду, відсутність належного тестування, а також через людські помилки, які можуть траплятися під час написання або внесення змін у код.

Для зменшення ймовірності програмних помилок важливо використовувати стандарти кодування, що чітко визначають правила написання коду та дозволяють знижувати ймовірність виникнення дефектів. Також дуже ефективним є проведення перегляду коду (code review), коли інші члени команди перевіряють код на наявність помилок і неточностей. Застосування автоматизованих тестувальних інструментів, які дозволяють швидко виявити помилки на ранніх етапах розробки, є ще одним важливим кроком. Крім того, використання статичних аналізаторів коду дозволяє виявити потенційні проблеми до етапу тестування, що дозволяє уникнути серйозних проблем у подальшій розробці[52].

Іноді, навіть після чіткого визначення вимог, розроблені функції можуть не відповідати очікуванням замовника або не виконувати необхідні бізнес-процеси. Це може статися через недостатню увагу до специфікацій, зміни вимог на пізніших етапах або через неефективну комунікацію між замовником і командою розробників.

У таких випадках важливо вчасно виявити невідповідності, оскільки їх усунення може потребувати значних змін в архітектурі програми або навіть переписування частин коду.

Для того, щоб знизити ризик невідповідності вимогам, корисним є поетапна розробка функціональності, що дозволяє поступово перевіряти кожен етап і порівнювати його з вимогами замовника. Створення прототипів і демонстрація мінімально функціонального продукту (MVP) також допомагають замовникам оперативно оцінити прогрес і вносити корективи, ще не завершивши весь цикл розробки. Це дозволяє отримати зворотний зв'язок раніше і вчасно виявити проблеми.

Технічні проблеми, такі як невраховані проблеми сумісності між різними компонентами системи, обмеження платформ або апаратного забезпечення, а також проблеми з продуктивністю чи безпекою, можуть серйозно вплинути на хід розробки і навіть призвести до критичних вразливостей у системі. Такі проблеми можуть значно затримати розробку або виявитися причиною великих витрат на виправлення дефектів після релізу продукту.

Одним із способів управління цими ризиками є регулярне тестування продуктивності за допомогою спеціальних інструментів, таких як профілювальники. Це дозволяє вчасно виявити проблеми з продуктивністю. Оптимізація коду з використанням ефективних алгоритмів та структур даних також є важливою стратегією для покращення продуктивності. Тестування сумісності коду з різними платформами і технологіями на ранніх етапах розробки дозволяє виявити сумісні проблеми ще до інтеграції системи в основну платформу. Крім того, запровадження стандартів безпеки для захисту системи від вразливостей і потенційних атак є необхідним для забезпечення надійності продукту.

Неефективна комунікація між членами команди може призвести до непорозумінь, дублювання роботи або навіть до зриву термінів виконання завдань. Це особливо стосується великих проектів, де в команді можуть працювати розробники, проектувальники, тестувальники та інші фахівці. Труднощі в координації зусиль можуть негативно вплинути на загальний прогрес розробки і якість кінцевого продукту.

Щоб уникнути таких проблем, важливо впроваджувати агільні методології, такі як Scrum чи Kanban, які передбачають регулярні зустрічі для обговорення прогресу та поточних проблем. Використання систем управління проектами, таких як Jira або Trello, допомагає централізовано відслідковувати завдання і забезпечує прозорість комунікацій в команді. Підтримка відкритої і регулярної комунікації серед усіх учасників проекту є важливою для своєчасного виявлення і вирішення проблем, що виникають.

Недооцінка складності завдань або технічних труднощів може призвести до затримок у виконанні роботи. Це часто трапляється, коли терміни розробки були визначені не зовсім реалістично або коли завдання не були правильно розподілені між членами команди. Такі помилки можуть призвести до затримок і, відповідно, до зростання витрат.

Для запобігання цьому корисно використовувати методи оцінки складності завдань, такі як story points або timeboxing, що дозволяє точніше прогнозувати необхідний час для виконання завдань. Оцінка складності завдань має постійно переглядатися протягом процесу розробки, з урахуванням поточного прогресу і труднощів. Гнучкість у плануванні дозволяє коригувати терміни і обсяг роботи у разі зміни вимог чи наявних проблем. Наступна таблиця є результаом дослідження даного етапу та вказує на співвідношення ризиків та стратегій на етапі розробки.

Таблиця 2.2*

Ризики та стратегії управління на етапі розробки

Ризик	**Ймовірні наслідки**	**Стратегії управління**
Програмні помилки	Затримки в розробці, збої в роботі, помилки в даних	Стандарти кодування, code review, автоматизоване тестування коду
Невідповідність вимогам функціональності	Некоректна робота програми, додаткові витрати	Поетапна розробка, прототипування, регулярні перевірки відповідності функціоналу
Технічні проблеми	Зниження продуктивності, проблеми з сумісністю чи безпекою	Регулярне проведення перформанс-тестів, інструменти оптимізації, стандарти безпеки

Комунікаційні проблеми в команді	Непорозуміння, дублювання роботи, затримки	Впровадження агільних методів, використання систем управління проектами, підтримка відкритої комунікації
Невиконання термінів через недооцінку складності завдань	Затримки в розробці, перевищення бюджету	Оцінка складності завдань, перегляд оцінок і планів, гнучкість у плануванні

*Розроблена автором.

Етап розробки є критично важливим і складним етапом у життєвому циклі створення ІТ-додатків, оскільки саме на цьому етапі реалізуються функціональні можливості, що визначають успішність проекту. Проте цей етап супроводжується різноманітними ризиками, які можуть негативно вплинути на якість кінцевого продукту, строки реалізації та витрачені ресурси. Важливою складовою успішного виконання проекту є своєчасне виявлення та управління цими ризиками.

Застосування ефективних стратегій, таких як стандарти кодування, перегляд коду, автоматизоване тестування, а також підтримка відкритої комунікації в команді і гнучкість у плануванні, дозволяє знизити ймовірність виникнення помилок, покращити продуктивність та забезпечити сумісність і безпеку системи. Розумне і стратегічне управління ризиками на етапі розробки є запорукою успішного завершення проекту, забезпечуючи стабільність і надійність кінцевого продукту, що в свою чергу дозволяє задовольнити вимоги замовника і досягти бізнес-цілей.

Тестування є критично важливим етапом у розробці ІТ-додатків, оскільки саме на цьому етапі виявляються дефекти та недоліки, які можуть серйозно вплинути на стабільність та ефективність роботи системи. Під час тестування перевіряється, чи відповідає продукт визначеним вимогам, чи працює він так, як очікується, та чи не має він вразливостей, які можуть загрожувати його безпеці або продуктивності. Це дозволяє не лише виявити очевидні помилки, а й розкрити потенційні проблеми, які можуть проявитися в майбутньому при зміні умов експлуатації чи зростанні навантаження[53].

Проте тестування, як і будь-який інший етап розробки, не є позбавленим ризиків. Існують численні фактори, які можуть негативно вплинути на його

ефективність, і це може призвести до затримок у проекті або навіть до серйозних проблем після випуску продукту. До таких ризиків належать, наприклад, невиявлені дефекти, які можуть залишитися непоміченими через неповне тестове покриття або недоліки у тестових сценаріях, а також затримки, що виникають через недостатнє або неякісне тестування. Крім того, сумісність продукту з різними платформами та середовищами може стати ще одним серйозним викликом на цьому етапі. Саме тому стратегічний підхід до тестування, що включає ретельне планування, використання різноманітних тестових технік і інструментів автоматизації, є ключовим для мінімізації цих ризиків.

Тестування є критично важливим етапом у розробці IT-додатків, оскільки на ньому виявляються дефекти та недоліки системи. Однак існує кілька ризиків, що можуть негативно вплинути на успішне виконання цього етапу.

Один із основних ризиків — невиявлені дефекти. Це може статися, якщо тестування не охоплює всі функціональні чи нефункціональні аспекти продукту, що, в свою чергу, може призвести до виявлення помилок уже після випуску продукту в експлуатацію. Проблеми можуть виникати внаслідок недостатнього тестового покриття, помилок в тестових сценаріях або людських помилок під час виконання тестів.

Інший ризик — затримки через недостатнє тестування. Якщо тестування проводиться без належного планування або не охоплює всі необхідні рівні перевірки, це може призвести до затримок у розробці продукту або до необхідності повторного тестування після виявлення помилок на пізніх етапах. Відсутність достатньої кількості часу або ресурсів для тестування може збільшити ймовірність виявлення помилок на етапі релізу.

Третій важливий ризик — проблеми із сумісністю. Це стосується ситуацій, коли система не працює коректно на різних платформах або в різних середовищах. Проблеми можуть виникати через непередбачувану взаємодію між різними компонентами системи або через неврахування всіх варіантів середовища.

Щоб мінімізувати ці ризики, застосовуються різні стратегії управління.

По-перше, важливо використовувати різні рівні тестування, щоб забезпечити всебічну перевірку продукту. Це включає модульне тестування, яке дозволяє перевіряти окремі компоненти системи на наявність помилок, інтеграційне тестування для перевірки взаємодії між компонентами, а також системне тестування, яке дозволяє виявити проблеми в загальній роботі системи.

Автоматизація тестування є ще однією стратегією для зменшення ризиків. Автоматизовані тести дозволяють швидше перевіряти повторювані сценарії, що забезпечує більш стабільну та швидку верифікацію функціональності та допомагає знайти помилки на ранніх етапах розробки. Використання таких інструментів дозволяє знижувати навантаження на тестувальників і зменшити ймовірність пропуску дефектів.

Складання детального плану тестування, що включає визначення пріоритетів тестів, є важливим кроком у зниженні ризиків. План тестування дозволяє чітко визначити, які функції та аспекти додатку необхідно перевірити першочергово, а також визначити, які типи тестування є найважливішими для виявлення потенційних проблем.

Таблиця2.3*

Типи тестів та їх роль у зменшенні ризиків

Тип тесту	**Роль у зменшенні ризиків**
Модульне тестування	Виявляє помилки на рівні окремих компонентів, що дозволяє виправити їх на ранніх етапах.
Інтеграційне тестування	Перевіряє взаємодію між компонентами, що допомагає виявити проблеми сумісності та інтеграції.
Системне тестування	Перевіряє продукт в цілому, забезпечуючи виявлення проблем на рівні всієї системи.
Тестування продуктивності	Виявляє проблеми з навантаженням та ефективністю, що дозволяє уникнути збоїв при високому навантаженні.
Тестування безпеки	Виявляє вразливості та потенційні загрози для системи, забезпечуючи її захищеність.

*Розроблена автором.

Етап тестування є критично важливим для забезпечення якості ІТ-додатків і мінімізації ризиків, пов’язаних з невиявленими дефектами, затримками або проблемами із сумісністю. Використання різних рівнів тестування, автоматизація тестів та складання чіткого плану тестування є важливими стратегіями для успішного

управління цими ризиками. Крім того, різноманітні типи тестування, включаючи модульне, інтеграційне та системне тестування, відіграють ключову роль у виявленні помилок на різних етапах розробки, що дозволяє забезпечити стабільність і надійність кінцевого продукту.

Етап впровадження є критичним, оскільки він забезпечує перехід розробленого IT-додатку до реального використання в продуктивному середовищі. Успішне впровадження вимагає належної інтеграції та підготовки кінцевих користувачів до роботи з системою. Однак цей етап супроводжується кількома ризиками, які можуть серйозно вплинути на ефективність та безперебійність роботи додатку після його запуску. Спираючись на підрозділ 2.2 даної роботи можемо виокремити ряд ризиків, характерних для етапу впровадження.

Серед технічних ризиків можна виділити несумісність із існуючими системами, що виникає через відсутність підтримки необхідних протоколів або стандартів API. Відсутність достатнього тестування під час інтеграції може призводити до збоїв. Щоб уникнути таких проблем, доцільно створювати тестові середовища, ретельно документувати технічні вимоги та залежності, використовувати стандарти обміну даними (наприклад, REST або GraphQL) та впроваджувати систему поетапно, наприклад, на обмеженій групі користувачів.

Організаційні ризики часто стосуються недостатнього навчання користувачів, через що вони можуть не розуміти, як ефективно використовувати нову систему. Це підвищує навантаження на технічну підтримку. Відсутність якісної документації або навчальних матеріалів також ускладнює адаптацію. Для вирішення цієї проблеми рекомендується розробляти інтерактивні мануали, відеоінструкції чи онлайн-курси, організовувати тестові періоди для ознайомлення користувачів із системою та забезпечувати підтримку впродовж перших місяців після запуску.

Бізнесові ризики, такі як втрата довіри користувачів через технічні збої, можуть негативно вплинути на репутацію продукту. Збої у роботі системи, зниження продуктивності чи ризик втрати даних спричиняють незадоволення користувачів. Запобігти таким ситуаціям допоможуть системи моніторингу в реальному часі, як-от Azure Monitor або Grafana, резервне копіювання з планами відновлення даних і

попереднє стрес-тестування для оцінки здатності системи витримувати високі навантаження.

Безпекові ризики, наприклад неправильна конфігурація системи, можуть створювати уразливості для кібератак. Невірно налаштовані права доступу або застарілі методи аутентифікації значно підвищують ризик витоку даних. Для забезпечення безпеки необхідно проводити аудит системи перед запуском, використовувати багаторівневу аутентифікацію (наприклад, MFA), сучасні протоколи шифрування даних та регулярно оновлювати безпекові механізми, усуваючи вразливості.

Проблеми у комунікації між командами розробки, тестування, впровадження та технічної підтримки також становлять ризики, що можуть спричинити затримки або помилки. Відсутність належної координації чи труднощі у передачі інформації про зміни у вимогах погіршують результати. Ефективним рішенням є організація регулярних зустрічей і статус-апдейтів, використання платформ для управління завданнями (таких як Jira чи Slack) і призначення відповідальних за ключові етапи впровадження.

Ще одним важливим аспектом є користувацький досвід, адже неінтуїтивний або складний інтерфейс може викликати опір і знижувати продуктивність. Щоб уникнути цього, варто проводити опитування користувачів і тестування інтерфейсу ще до запуску, впроваджувати зміни поступово та залучати кінцевих користувачів до тестування прототипів на ранніх етапах розробки.

Аналіз ризиків етапу розробки можемо навести в наступній таблиці.

Таблиця 2.4*

Результати аналізу ризиків на етапі впровадження.

Тип ризику	Ризик	Ймовірність	Вплив	Стратегія вирішення
Технічний	Несумісність з існуючими системами	Висока	Високий	Тестування у тестовому середовищі, використання стандартів обміну даними (REST, GraphQL)
	Невірна конфігурація серверного оточення	Середня	Високий	Детальне налаштування серверного оточення, перевірка налаштувань перед запуском

	Проблеми з масштабуванням при високих навантаженнях	Середня	Високий	Стрес-тестування, використання балансування навантаження
Організаційний	Недостатнє навчання користувачів	Середня	Середній	Розробка навчальних матеріалів, тестовий період для користувачів
	Відсутність чіткої документації про нову систему	Висока	Середній	Створення детальної документації, відео-інструкцій
	Низька залученість співробітників до процесу впровадження	Середня	Середній	Проведення мотиваційних заходів, організація зустрічей з користувачами
Бізнесовий	Втрата довіри користувачів через технічні збої	Висока	Високий	Впровадження моніторингу в реальному часі, резервне копіювання та стрес-тестування
	Відставання від конкурентів через затримки впровадження	Середня	Середній	Планування поетапного запуску, ретельний моніторинг конкурентів
	Недостатнє фінансування для масштабування системи	Середня	Високий	Оцінка потреб в ресурсах на ранніх етапах, пошук додаткових інвестицій
Безпековий	Неправильна конфігурація системи	Низька	Високий	Аудит безпеки, багаторівнева аутентифікація, регулярні оновлення безпеки
	Витік даних через ненадійні канали зв'язку	Середня	Високий	Використання шифрування, захищені протоколи передавання даних
	Атаки через вразливості в сторонніх бібліотеках чи компонентах	Низька	Високий	Регулярне оновлення сторонніх компонентів, використання тільки перевірених бібліотек
Комунікаційний	Недостатня взаємодія між командами	Середня	Середній	Регулярні зустрічі та використання платформ для комунікації (Jira, Slack)
	Невизначеність у комунікаціях щодо змін вимог і часу впровадження	Середня	Середній	Постійні зустрічі зі всіма зацікавленими сторонами, чітке документування змін
	Відсутність чіткої координації між розробниками та відділом технічної підтримки	Висока	Середній	Спільна робота на всіх етапах проєкту, регулярні оновлення статусу

Користувацький	Низька прийнятність системи серед користувачів	Середня	Високий	Тестування інтерфейсу, збір відгуків, залучення користувачів до тестування прототипів
	Висока складність у використанні нової системи	Середня	Середній	Спрощення інтерфейсу, організація тренінгів та навчальних сесій
	Відсутність належної адаптації інтерфейсу до потреб користувачів	Середня	Середній	Опитування користувачів, регулярні оновлення та адаптація інтерфейсу

*Розроблена автором.

Ця таблиця дає більш детальний огляд ризиків, що можуть виникнути під час впровадження IT-додатку з огляду на різні аспекти. Для кожного ризику визначено ймовірність, вплив на проект і можливі стратегії вирішення. Натомість, якщо розглядати кожен етап впровадження окремо можемо визначити ряд ризиків, які відображаються в наступній таблиці.

Таблиця 2.5

Основних ризиків відповідно до різних етапів впровадження.

Етап впровадження	Основні ризики	Заходи мінімізації ризиків
Планування	Неправильне визначення вимог, недоліки в ресурсному плануванні	Докладний аналіз вимог, залучення ключових зацікавлених осіб, створення резерву ресурсів
Тестування	Невиявлені баги або вразливості, неповне тестування	Проведення різних типів тестування: функціонального, навантажувального, безпеки
Навчання	Недостатня підготовка користувачів, опір змінам	Організація навчальних сесій, підтримка користувачів, залучення тренерів
Пілотний запуск	Проблеми під час запуску, невідповідність очікуванням	Обмежене впровадження на обраних користувачах, зворотний зв'язок для корекції
Масштабування	Складнощі з масштабуванням системи, проблеми з продуктивністю	Поетапне масштабування, забезпечення гнучкості архітектури, резервне планування
Підтримка	Збої в роботі системи, відсутність швидкого реагування	Постійний моніторинг, створення команди підтримки, планування резервних заходів

*Розроблена автором.

Цією таблицею ми відображаєм основні ризики для кожного етапу процесу впровадження та кроки для мінімізації цих ризиків.

Отже, у даному підрозділі ми розглянули різні етапи життєвого циклу IT-додатку включно до впровадження та відповідні ризики, що можуть виникнути на кожному етапі, разом з можливими стратегіями для їх мінімізації. На етапі аналізу вимог визначено такі ризики, як невизначеність вимог та неповне розуміння потреб замовника, для усунення яких запропоновано створення чіткої документації та регулярні ревізії вимог. Проектування і розробка можуть супроводжуватись помилками в архітектурі системи та програмними помилками, що вирішуються за допомогою шаблонів проектування та паралельного тестування. На етапі тестування, для мінімізації дефектів, важливо застосовувати різні рівні тестування та автоматизацію процесу. Впровадження передбачає ризики, пов'язані з інтеграцією на продуктивному середовищі та недостатнім навчанням користувачів, для чого рекомендується поетапне впровадження та створення плану відновлення. Візуалізації, такі як схеми та таблиці, допомагають краще зрозуміти та контролювати процеси управління ризиками на кожному етапі.

РОЗДІЛ 3.
ПРАКТИЧНЕ ЗАСТОСУВАННЯ СТРАТЕГІЙ ЗМЕНШЕННЯ РИЗИКІВ В ІТ-ПРОЕКТАХ

3.1. Оцінка ризиків у реальному ІТ-проєкті

У сучасних ІТ-проєктах управління ризиками є критично важливим елементом, оскільки кожен етап розробки і впровадження може бути підданий різноманітним загрозам, які впливають на кінцевий результат. Одним із таких проєктів є UMSystem — система керування навчальними закладами, яка спрямована на підвищення конкурентоспроможності освітніх установ через інтеграцію з сучасними технологіями, такими як C#, React, Azure, MongoDB.

UMSystem включає в себе різноманітні інструменти для управління навчальним процесом, аналізу результатів, планування розкладу та контролю якості знань, що робить його комплексним і багатофункціональним продуктом. Оскільки система охоплює широкий спектр завдань та інтеграцій, то на кожному етапі її розробки та впровадження можуть виникати різноманітні ризики, що потребують ретельної оцінки та управління.

У цьому підрозділі ми дослідимо основні ризики, з якими може стикнутися команда під час розробки UMSystem, а також методи їх оцінки та класифікації. Це дозволить глибше зрозуміти потенційні загрози, які можуть вплинути на успішність реалізації проєкту, а також сформувати підґрунтя для розробки стратегії управління ризиками, яка буде розглянута у наступних розділах.

Ураховуючи складну ситуацію в Україні, воєнний контекст суттєво впливає на всі аспекти ІТ-проєктів. У цьому підрозділі ми розглянемо всі можливі ризики для UMSystem з урахуванням сіми категорій: технічні, організаційні, бізнесові, безпекові, комунікаційні та користувацькі та ризики, пов'язані з законодавством та регулюванням.

1. Технічні ризики. Технічні ризики є важливою частиною управління ІТ-проєктами, оскільки вони стосуються безпосередньо технологічної реалізації та

стабільності роботи системи. У випадку з UMSystem, технічні ризики мають ще більшу значущість через специфіку освітнього процесу, що включає в себе зберігання важливих даних, інтеграцію з іншими системами та забезпечення безперервної роботи платформи для студентів та викладачів. Враховуючи ситуацію війни в Україні, технічні ризики набувають додаткової складності. Війна створює додаткові загрози для інфраструктури, комунікацій та доступу до сервісів, що можуть призвести до серйозних наслідків для стабільної роботи системи.

До технічних ризиків UMSystem належать:

- збої в інфраструктурі та доступі до сервісів: війна та наслідки бойових дій можуть призвести до пошкодження або знищення інфраструктури, що підтримує роботу системи. Зокрема, у випадку використання хмарних технологій (Azure) або серверів, що знаходяться в зонах, де є ризик обстрілів чи пошкоджень, може статися відключення від сервісів, зниження продуктивності або втрати даних. Проблеми з електропостачанням або доступом до інтернет-з'єднання можуть вплинути на доступність системи UMSystem для кінцевих користувачів.
- вразливість до зовнішніх атак: у часи війни збільшується ймовірність хакерських атак на IT-системи, зокрема на освітні платформи. Система UMSystem, що містить персональні дані студентів і викладачів, може стати ціллю для кібератак, таких як DDoS-атаки, зломи акаунтів або спроби викрадення даних. Кіберзлочинці можуть скористатися нестабільною ситуацією в країні для проникнення в систему з метою виведення конфіденційних даних або порушення її роботи.
- невідповідність вимогам безпеки та стандартам: зі змінами у законодавстві та посиленням вимог до захисту даних, зокрема в умовах війни, система UMSystem може не встигнути адаптуватися до нових стандартів безпеки або змін у політиках захисту персональних даних. Це може включати необхідність оновлення програмного забезпечення або застосування нових протоколів для забезпечення відповідності вимогам захисту даних, що в свою чергу потребуватиме додаткових ресурсів та часу для адаптації.
- проблеми з масштабованістю та оптимізацією: війна та економічна нестабільність можуть негативно вплинути на можливості масштабування та

розвитку системи. Зміни в інфраструктурі, обмеження в ресурсах або обмежений доступ до нових технологій можуть ускладнити реалізацію оновлень, покращень та розширення функціональності платформи. Технічні проблеми з масштабуванням системи можуть призвести до зниження її ефективності під час пікових навантажень, коли кількість користувачів або запитів зростає.

- проблеми з інтеграцією та оновленнями: у часи війни може бути ускладнений доступ до оновлень програмного забезпечення, нових бібліотек чи технологій, які використовуються в UMSystem. Це може спричинити затримки в інтеграції нових можливостей або виправленні помилок, що можуть вплинути на стабільність системи та користувацький досвід.
- недостатній моніторинг та відновлення після збоїв: через відсутність належного моніторингу інфраструктури або недостатню кількість ресурсів на відновлення роботи системи після збоїв, можуть виникнути проблеми з швидким відновленням працездатності UMSystem після технічних проблем або атак.

Урахування цих технічних ризиків є критичним для забезпечення безперервної роботи UMSystem, особливо в умовах війни, коли технологічні загрози можуть змінюватися надзвичайно швидко. Для зниження впливу цих ризиків важливо мати на увазі не лише технічні аспекти, але й організаційні та стратегічні заходи, спрямовані на забезпечення стійкості платформи до зовнішніх та внутрішніх загроз.

2. Організаційні ризики.

Організаційні ризики пов’язані з процесами управління проєктом, координацією роботи команди, ефективністю комунікацій та забезпеченням необхідних ресурсів для виконання завдань. Для проєкту UMSystem, де команда складається з чотирьох фахівців, а робота організована через виконання окремих завдань без застосування спринтів, організаційні ризики є особливо актуальними.

У контексті війни в Україні організаційні проблеми можуть бути посилені через складнощі координації, перебої у доступі до ресурсів або неспроможність оперативно реагувати на зміни у вимогах користувачів чи законодавства. Крім того, зважаючи на специфіку проєкту, що обслуговує освітню сферу, важливо забезпечити

синхронність роботи між різними учасниками навчального процесу та стейкхолдерами.

До основних організаційних ризиків належать:

- недостатня комунікація в команді: через невеликий розмір команди може виникнути ризик неузгодженості дій між розробниками, а також недостатньої обізнаності про зміни в задачах або пріоритетах. Відсутність формалізованого процесу планування (наприклад, через спринти) може посилити цей ризик.
- залежність від ключових фахівців: у маленькій команді відхід чи недоступність навіть одного учасника може значно вплинути на прогрес проєкту. Особливо це стосується фахівців із критичними знаннями, такими як робота з хмарними сервісами (Azure) або основна архітектура системи.
- недостатність ресурсів для забезпечення роботи: у складних умовах війни можуть виникати перебої з доступом до необхідного обладнання, хостингових сервісів чи навіть базових офісних інструментів. Це може уповільнити виконання завдань або ускладнити їх реалізацію.
- проблеми з адаптацією до змін: в умовах війни та економічної нестабільності часті зміни вимог (зокрема, від законодавчих органів чи користувачів) можуть ускладнити координацію завдань, оскільки неформалізовані процеси планування можуть не дозволити команді швидко адаптуватися.
- віддалена робота та мобільність: війна змусила багато команд перейти на віддалений формат роботи, що може створювати труднощі в комунікації, синхронізації процесів та контролю за виконанням завдань. Відсутність стабільного зв’язку чи доступу до інструментів для віддаленої роботи може ускладнити виконання навіть базових задач.

Організаційні ризики для UMSystem потребують уважного аналізу та чітких стратегій зниження. В умовах нестабільності, викликаної війною, важливо забезпечити не лише гнучкість у виконанні завдань, але й стабільність процесів управління проєктом. Це дозволить уникнути збоїв у роботі системи та забезпечити її відповідність потребам користувачів.

3. Бізнесові ризики.

Бізнесові ризики стосуються впливу зовнішніх факторів та умов ринку на успішність і життєздатність проєкту. У випадку UMSystem, який розробляється як сучасна система для управління навчальними закладами, ці ризики можуть суттєво вплинути на конкурентоспроможність продукту, його прийняття на ринку та фінансову стабільність. В умовах війни в Україні бізнесові ризики стають особливо критичними, оскільки економічна нестабільність, обмежені фінансові ресурси та зміни в освітніх пріоритетах можуть створювати додаткові виклики.

До основних бізнесових ризиків належать такі:

- зниження платоспроможності клієнтів: через економічну нестабільність багато освітніх закладів можуть стикатися з обмеженим фінансуванням. Це може ускладнити залучення нових клієнтів для UMSystem або призвести до скорочення бюджетів існуючих користувачів на підтримку системи.
- зміна пріоритетів у галузі освіти: у воєнний час заклади освіти можуть змінювати свої пріоритети, наприклад, спрямовувати ресурси на гуманітарні потреби чи забезпечення базових умов навчання, замість інвестування у цифрові системи управління. Це може зменшити попит на UMSystem у коротко- та середньостроковій перспективі.
- конкуренція з іншими продуктами: попри унікальні функції UMSystem, на ринку можуть бути присутні інші системи управління освітнім процесом. Умови війни та обмежені ресурси клієнтів можуть спонукати їх обирати більш доступні або локальні рішення, навіть якщо вони мають обмежену функціональність.
- залежність від фінансування та інвесторів: в умовах економічної кризи пошук інвесторів або стабільного фінансування для розвитку UMSystem може стати складнішим. Це обмежує можливість реалізації довгострокових планів, таких як масштабування проєкту чи впровадження нових функцій.
- ризик втрати репутації: через технічні або організаційні проблеми, що виникають в умовах війни, UMSystem може зіткнутися з репутаційними втратами, якщо не зможе своєчасно відповідати очікуванням клієнтів. Негативні відгуки чи скарги на нестабільну роботу системи можуть вплинути на залучення нових користувачів.

- труднощі в масштабуванні проєкту: через економічні виклики та нестабільність ринку команда UMSystem може зіткнутися з проблемами під час розширення своєї клієнтської бази або входження на нові ринки. Це може включати недостатню кількість ресурсів для підтримки більшої кількості клієнтів чи адаптації системи під нові вимоги.

Бізнесові ризики для UMSystem є одним із ключових викликів, які потребують системного аналізу та ефективної стратегії управління. Успішне подолання цих ризиків дозволить зберегти стабільність проєкту навіть в умовах війни, забезпечити його конкурентоспроможність та відповідність потребам освітнього ринку.

4. Безпекові ризики.

Безпекові ризики охоплюють загрози, що можуть поставити під загрозу конфіденційність, цілісність та доступність даних в UMSystem, а також загальний рівень інформаційної безпеки платформи. В умовах війни ці ризики стають особливо критичними, оскільки кіберзагрози зростають, а навчальні заклади можуть стати мішенню для атак через їхню соціальну значущість. Забезпечення належного рівня захисту даних користувачів та стійкості системи до зовнішніх атак є пріоритетним завданням для UMSystem. До безпекових ризиків ми відносимо:

- фізична загроза інфраструктурі: війна може призвести до пошкодження або знищення важливої інфраструктури, яка підтримує роботу системи UMSystem (сервера, дата-центри, мережі зв'язку). Зокрема, це може торкнутися обладнання, розміщеного в зонах бойових дій чи на територіях, які потрапили під обстріли.
- кіберзагрози в умовах війни: у часи війни спостерігається посилення кібернападів, у тому числі з боку державних або неурядових акторів, які можуть здійснювати атаки на інформаційні системи. Хакерські атаки, націлені на освітні платформи, можуть викрасти або знищити важливі дані користувачів, а також порушити роботу системи UMSystem.
- мобільність і безпека персоналу: фізична безпека співробітників може бути під загрозою через війну. Втрата доступу до працівників або їх евакуація може призвести до серйозних затримок у роботі над проєктом.

- технічна безпека в умовах бойових дій: в умовах війни можуть бути знижені або порушені заходи безпеки на рівні мережі та комунікацій. Наприклад, якщо зруйновані мережі зв'язку або інтернет-канали, це може призвести до тимчасового зупинення роботи системи UMSystem або її вразливості до зовнішніх атак.

- шахрайство та кіберзлочинність: в умовах війни може зрости кількість випадків шахрайства з боку недоброчесних користувачів або третіх осіб, що використовують ситуацію для власної вигоди. Можливі випадки використання зламаних акаунтів або фальшивих запитів для доступу до даних.

Таким чином, війна є одним із серйозних безпекових ризиків, і ці загрози повинні бути враховані при плануванні стратегії управління ризиками для UMSystem. Враховуючи високий рівень нестабільності та загрози, яка виникає через війну, особливо важливо забезпечити надійний захист даних, інфраструктури та фізичної безпеки співробітників.

5. Комунікаційні ризики охоплюють виклики, пов’язані з передачею інформації між членами команди, зацікавленими сторонами та кінцевими користувачами. Для UMSystem, де команда невелика, ефективна комунікація є критичною для успішного виконання проєкту. Умови війни створюють додаткові труднощі, такі як перебої з інтернетом, відсутність стабільного зв’язку та зростання рівня стресу, що може вплинути на якість комунікації.

Основні ризики у цій категорії:

- перебої в комунікаціях: через віддалену роботу, викликану війною, можуть виникати технічні труднощі зі зв’язком між членами команди чи клієнтами. Це може призвести до втрати важливої інформації, уповільнення прийняття рішень або розбіжностей у розумінні завдань.

- непорозуміння між командою та клієнтами: недостатня або неякісна комунікація з освітніми закладами може спричинити ситуації, коли система не відповідає їхнім потребам або очікуванням. Це може знизити задоволеність клієнтів та вплинути на репутацію UMSystem.

- відсутність єдиної комунікаційної платформи: якщо команда та клієнти використовують різні інструменти для зв’язку, це може ускладнити координацію завдань і взаємодію між учасниками проєкту.
- високий рівень стресу та емоційного навантаження: через війну комунікація може стати менш ефективною, оскільки учасники проєкту можуть відчувати стрес або бути обмеженими у своїй доступності. Це впливає на швидкість та якість ухвалення рішень.
- невідповідність очікувань через неправильну комунікацію: якщо комунікація з клієнтами є недостатньо прозорою або незрозумілою, це може призводити до різниці у сприйнятті можливостей системи та її фактичної функціональності.

Комунікаційні ризики є серйозним викликом для команди UMSystem. Щоб їх мінімізувати, необхідно впровадити єдину комунікаційну платформу, оптимізувати процеси обміну інформацією та забезпечити гнучкість у вирішенні проблем зі зв’язком. Прозора взаємодія з клієнтами та своєчасна передача інформації допоможуть уникнути непорозумінь та зберегти довіру користувачів до системи.

6. Користувацькі ризики.

Користувацькі ризики стосуються проблем, які можуть виникнути через очікування, поведінку або рівень залученості користувачів системи UMSystem. У випадку освітньої платформи, успіх її впровадження та використання залежить від задоволеності та активності її кінцевих користувачів – студентів, викладачів та адміністрації навчальних закладів.

В умовах війни ці ризики стають більш значущими, адже освітні заклади стикаються з постійними змінами умов роботи, обмеженими ресурсами та високим рівнем стресу у викладачів і студентів.

Основні ризики у цій категорії:

- низька залученість користувачів: через нестачу часу, ресурсів або технічних навичок користувачі (особливо викладачі) можуть недостатньо активно використовувати систему. Це знижує її ефективність та вартість для клієнтів.

- недостатній рівень технічної грамотності: окремі користувачі, особливо у невеликих або сільських навчальних закладах, можуть не мати достатнього досвіду роботи з сучасними платформами. Це може призводити до помилок під час використання UMSystem, негативного користувацького досвіду та зниження задоволеності.
- опір змінам: впровадження нових технологій може зустрічати опір, особливо серед викладачів, які звикли до традиційних методів роботи. Умови війни можуть посилити цей ризик, оскільки ресурси та увага освітніх закладів часто спрямовані на більш нагальні потреби.
- складності у налаштуванні системи під потреби користувачів: якщо система UMSystem недостатньо гнучка або складна в освоєнні, це може ускладнити її адаптацію під конкретні потреби навчальних закладів, зокрема тих, що працюють у нестандартних умовах через війну.
- проблеми зі стабільністю роботи для кінцевих користувачів: перебої у роботі системи (зокрема, через технічні чи організаційні проблеми) можуть викликати незадоволення користувачів, особливо у критичних періодах, таких як сесії або вступна кампанія.

Для зниження користувацьких ризиків UMSystem має запропонувати інтуїтивно зрозумілий інтерфейс, забезпечити навчання та підтримку користувачів на всіх етапах роботи з платформою. Гнучкість у налаштуванні системи під специфічні потреби закладів та ефективна комунікація з користувачами допоможуть підвищити їхню задоволеність і забезпечити успішне впровадження навіть у складних умовах.

7. Ризики, пов'язані з законодавством та регулюванням.

Законодавчі зміни та регуляторні вимоги можуть суттєво вплинути на роботу будь-якої ІТ-системи, особливо коли йдеться про освітні платформи, що працюють з персональними даними. У контексті UMSystem, де зберігаються дані студентів та викладачів, а також інші чутливі відомості, ці ризики можуть стати критичними:

- зміни в законодавстві про захист персональних даних: в умовах війни можуть бути прийняті нові закони, які регулюють обробку та захист персональних

даних. Це може вимагати швидкого оновлення політик конфіденційності та змін в архітектурі системи для забезпечення відповідності новим вимогам.

- нові регулювання щодо цифрових підписів та автентифікації: можливі зміни в законодавстві, що стосуються використання електронних підписів або методів автентифікації в освітніх установах. Це може вимагати інтеграції нових технологій або змін у процесах взаємодії з користувачами.
- зміни в податковому законодавстві: під час війни можуть відбутися зміни в податковому законодавстві, які стосуються фінансування та підтримки освітніх проєктів. UMSystem може потребувати адаптації до нових податкових вимог або змін у механізмах бюджетування.
- правові наслідки в разі порушення прав користувачів: у разі несанкціонованого доступу до даних студентів чи викладачів, або порушення інших правових норм, проєкт може зіткнутися з серйозними правовими наслідками, включаючи штрафи чи судові позови.
- зміни в нормативних вимогах для освітніх установ: зміни в регуляціях для освітніх закладів щодо використання технологій для навчання можуть вимагати адаптації функціоналу UMSystem для відповідності новим стандартам. Це може включати, наприклад, вимоги до обліку навчальних досягнень або нового формату звітності.

Ці ризики вимагають постійного моніторингу змін у законодавстві, а також гнучкості в адаптації системи до нових нормативних вимог.

Шляхом експертного опитування користувачів та розробників UMSystem було визначено ступінь ймовірності та впливу кожного ризику.

Таблиця 3.1*

Оцінка ймовірності та впливу ризиків на UMSystem

Тип ризику	Ризик	Ймовірність (1-5)	Вплив (1-5)	Загальний бал
Технічні ризики	Збої в інфраструктурі та доступі до сервісів	4	5	20
	Вразливість до зовнішніх атак	5	5	25
	Невідповідність вимогам безпеки та стандартам	4	4	16

	Проблеми з масштабованістю та оптимізацією	3	4	12
	Проблеми з інтеграцією та оновленнями	3	4	12
	Недостатній моніторинг та відновлення після збоїв	4	4	16
Організаційні ризики	Недостатня комунікація в команді	3	4	12
	Залежність від ключових фахівців	4	5	20
	Недостатність ресурсів для забезпечення роботи	4	4	16
	Проблеми з адаптацією до змін	3	4	12
	Віддалена робота та мобільність	4	3	12
Бізнесові ризики	Зниження платоспроможності клієнтів	3	4	12
	Зміна пріоритетів у галузі освіти	3	4	12
	Конкуренція з іншими продуктами	3	4	12
	Залежність від фінансування та інвесторів	4	5	20
	Ризик втрати репутації	3	5	15
	Труднощі в масштабуванні проєкту	3	4	12
Безпекові ризики	Фізична загроза інфраструктурі	5	5	25
	Кіберзагрози в умовах війни	5	5	25
	Мобільність і безпека персоналу	4	4	16
	Технічна безпека в умовах бойових дій	5	5	25
	Шахрайство та кіберзлочинність	4	5	20
Комунікаційні ризики	Перебої в комунікаціях	4	4	16
	Непорозуміння між командою та клієнтами	3	4	12
	Відсутність єдиної комунікаційної платформи	3	3	9
	Високий рівень стресу та емоційного навантаження	4	4	16
	Невідповідність очікувань через неправильну комунікацію	3	4	12
Користувацькі ризики	Низька залученість користувачів	3	4	12
	Недостатній рівень технічної грамотності	3	4	12
	Опір змінам	4	3	12
	Складності у налаштуванні системи під потреби користувачів	3	4	12

	Проблеми зі стабільністю роботи для кінцевих користувачів	4	4	16
Ризики, пов'язані з законодавством	Зміни в законодавстві про захист персональних даних	4	5	20
	Нові регулювання щодо цифрових підписів та автентифікації	3	4	12
	Зміни в податковому законодавстві	3	4	12
	Правові наслідки в разі порушення прав користувачів	4	5	20
	Зміни в нормативних вимогах для освітніх установ	3	4	12

*Розрахована автором.

В цій таблиці ми оцінювали ймовірність і вплив кожного ризику за шкалою від 1 до 5. Ймовірність: 1 — дуже низька ймовірність, 5 — дуже висока ймовірність. Вплив: 1 — мінімальний вплив, 5 — критичний вплив.

Отримані результати ми розбили за категоріями небезпеки наступним чином.

Низький ризик: 6–9 балів

Середній ризик: 10–12 балів

Високий ризик: 13–16 балів

Катастрофічний ризик: 17 і більше балів.

Дана табличка дає нам можливість визначити критичність ризику на який необхідно звернути увагу першочергово. Так ми вибрали катастрофічні ризики та надали рекомендації по них у наступній табличці.

Таблиця 3.2*

Відбір та реагування на катастрофічні виклики

Катастрофічний ризик	**Загальний бал**	**Рекомендації**
Вразливість до зовнішніх атак	25	Впровадити систему багаторівневої безпеки, зокрема фаєрволи, IDS/IPS, антивірусні системи.
		Постійно оновлювати програмне забезпечення та патчі для систем.
		Регулярно проводити пентести та аудит безпеки.
Кіберзагрози в умовах війни	25	Посилити заходи безпеки, враховуючи можливі кібернапади з боку державних і приватних акторів.
		Використовувати шифрування даних та багатофакторну автентифікацію.

		Створити план дій для боротьби з кіберзагрозами в умовах війни.
Технічна безпека в умовах бойових дій	25	Розробити план забезпечення безпеки інфраструктури під час бойових дій, включаючи відновлення після катастроф.
		Перевіряти та посилювати фізичну безпеку серверів і важливих мереж.
		Впроваджувати резервні рішення для критичних систем.
Фізична загроза інфраструктурі	25	Визначити і посилити фізичну безпеку серверів і мереж (охоронні системи, доступ за картками тощо).
		Забезпечити місце для розміщення резервних серверів у безпечному місці (підземні бункери, віддалені дата-центри).
		Мати наявність планів евакуації для персоналу.
Залежність від фінансування та інвесторів	20	Диверсифікувати джерела фінансування для зменшення залежності від одного інвестора.
		Створити фінансовий резерв для подолання фінансових криз.
		Вести активну комунікацію з інвесторами для залучення додаткових коштів у кризові моменти.
Ризик втрати репутації	20	Реагувати на інциденти та негативні відгуки користувачів у найкоротші терміни.
		Проводити регулярні тренінги з комунікаційної стратегії для менеджменту.
		Впроваджувати програми захисту репутації в соціальних мережах та на платформах відгуків.
Зміни в законодавстві про захист персональних даних	20	Постійно відстежувати зміни в законодавстві та вчасно адаптувати політики безпеки та захисту персональних даних.
		Впровадити додаткові заходи для забезпечення відповідності GDPR та місцевим стандартам.
		Створити внутрішні механізми моніторингу для забезпечення безпеки персональних даних.
Правові наслідки в разі порушення прав користувачів	20	Розробити внутрішню політику відповідальності за порушення прав користувачів.
		Впровадити регулярні перевірки на відповідність правовим вимогам.
		Мати юридичну команду для оперативного реагування на будь-які правові питання.

*Розроблена автором.

Оцінка ризиків є важливим етапом у процесі управління ризиками, оскільки дозволяє визначити, які з них можуть мати найбільший вплив на успіх проєкту, а

також прийняти відповідні заходи для їхнього зниження або усунення. Для ефективної оцінки ризиків використовуються різноманітні інструменти та методи, які допомагають визначити ймовірність виникнення кожного ризику та його потенційні наслідки.

3.2. Розробка та впровадження стратегії управління ризиками

Ефективне управління ризиками є ключовим елементом успішного функціонування IT-проектів, зокрема таких складних систем, як UMSystem. Завдяки впровадженню стратегій управління ризиками можливо зменшити ймовірність виникнення проблем, мінімізувати негативні наслідки та підвищити стійкість системи до зовнішніх і внутрішніх викликів.

Цей підрозділ детально розглядає цілі та завдання стратегії управління ризиками, різновиди стратегій (уникнення, зменшення, передача, прийняття), а також методи їх реалізації. Особливу увагу приділено адаптації стратегій до специфіки UMSystem, враховуючи використання сучасних технологій, таких як Azure, MongoDB, та унікальні особливості функціонування системи в умовах реальних ризиків.

Розробка стратегії управління ризиками для UMSystem має на **меті** забезпечення стабільного функціонування системи та її успішного розвитку в умовах змінного середовища. Для досягнення цієї мети пропонуються такі основні **завдання:**

- зниження ймовірності та впливу негативних ризиків (досягається шляхом систематичної ідентифікації ризиків, впровадження превентивних заходів та ефективного реагування на виявлені проблеми);
- максимізація позитивних можливостей (використання можливостей для покращення роботи системи, таких як інтеграція нових технологій чи адаптація до потреб користувачів, дозволяє підвищити її конкурентоспроможність);
- оптимізація процесів управління проектом (забезпечення прозорості та прогнозованості ризиків сприяє ефективному управлінню ресурсами, часу та фінансами, що знижує невизначеність);

- підвищення стійкості до зовнішніх та внутрішніх факторів (враховуючи виклики, зокрема ті, що пов’язані з війною в Україні та загальною економічною нестабільністю, стратегія має забезпечити гнучкість та адаптивність системи);
- покращення залученості команди до процесів управління ризиками (формування культури відповідального ставлення до ризиків серед команди проєкту є важливою складовою для довгострокового успіху).

Для ефективного управління ризиками UMSystem пропонується застосувати чотири основні типи **стратегій**: уникнення, зменшення, передача та прийняття ризиків. Кожна з них має свої переваги та підходить для різних типів загроз.

Уникнення ризику. Ця стратегія спрямована на виключення ризику шляхом зміни плану, підходів або умов роботи. Приклад для UMSystem: уникнення ризиків, пов’язаних із невідповідністю законодавству, через регулярний аудит нормативних змін і своєчасну адаптацію функціоналу.

Зменшення ризику. Полягає у зниженні ймовірності виникнення ризику або його впливу шляхом вжиття превентивних заходів. Приклад для UMSystem: впровадження автоматизованого моніторингу стабільності системи для виявлення помилок на ранніх етапах та регулярне резервне копіювання даних.

Передача ризику. Передбачає передачу відповідальності за ризик іншим сторонам. Приклад для UMSystem: укладення договорів із хостинг-провайдерами (Azure) щодо забезпечення безперервності роботи системи та гарантійного обслуговування.

Прийняття ризику. Використовується тоді, коли ризик є маловпливовим або неможливо усунути чи мінімізувати. Приклад для UMSystem: прийняття ризику короткочасного зниження продуктивності при виконанні критичних оновлень, якщо це необхідно для довгострокової стабільності.

Ці стратегії дозволяють гнучко реагувати на різні типи ризиків, балансуючи між витратами на їхнє управління та досягненням цілей проекту.

Для успішного впровадження стратегій управління ризиками в UMSystem доцільно використовувати комплексний підхід, що охоплює як технічні, так і організаційні **методи**.

Розробка плану дій для кожного виду ризику (визначення конкретних заходів, відповідальних осіб та строків реалізації для управління кожним ризиком). Наприклад для UMSystem це створення алгоритму дій у разі технічного збою, включаючи швидкий перехід на резервні сервери Azure.

Використання інструментів моніторингу та управління ризиками (впровадження програмного забезпечення для відстеження ризиків, їхньої ймовірності, впливу та стану реалізації заходів). Прикладом може бути використання платформ, як-от Jira, для управління тасками, пов'язаними із зменшенням ризиків, а також для моніторингу стану системи.

Регулярний аналіз ризиків та оновлення стратегії (проведення регулярних нарад команди для аналізу нових ризиків, перегляду актуальності заходів і корекції стратегії). Наприклад щоквартальні зустрічі для обговорення нових загроз (наприклад, змін у законодавстві) та їхнього впливу на систему.

Навчання та залучення команди до стратегії управління ризиками (організація тренінгів та семінарів для команди з метою підвищення їхньої обізнаності про ризики та методи їхнього уникнення). Прикладом може слугувати навчання співробітників щодо реагування на кібератаки та дій під час порушень у роботі бази даних MongoDB.

Використання бенчмаркінгу та обміну досвідом (аналіз рішень інших компаній з аналогічними проблемами та їх адаптація до власних потреб). Тут прикладом для UMSystem є вивчення практик інших освітніх платформ для вдосконалення безпеки даних та роботи з великим навантаженням.

Ці методи сприяють ефективному впровадженню стратегій, забезпечуючи систематичність і послідовність в управлінні ризиками.

Впровадження стратегій управління ризиками для системи UMSystem є важливим етапом забезпечення її стабільності, надійності та відповідності вимогам користувачів і ринку. З огляду на технологічну специфіку проєкту, особливості його використання в освітній сфері та зовнішні чинники, розробка чітких заходів для кожної категорії ризиків дозволяє проєкту не лише запобігти потенційним проблемам, а й ефективно використати свої сильні сторони для подальшого розвитку.

Для технічних ризиків, таких як можливі збої в роботі інфраструктури або непередбачувані баги, важливо впровадити автоматизоване тестування та моніторинг роботи серверів у режимі реального часу. Це дозволить оперативно виявляти та усувати помилки. Окрім того, підписання договорів SLA з провайдерами послуг, зокрема Azure, забезпечить додатковий захист від значних технічних збоїв. Для мінімізації можливих проблем, що виникають під час оновлень, оновлення системи слід планувати в години мінімальної активності користувачів.

Організаційні ризики, такі як затримки у виконанні завдань через недостатнє планування або відсутність узгодженості між членами команди, можуть бути мінімізовані через використання інструментів управління проєктами, таких як Jira або Trello. Регулярні спринти та ретельна перевірка кожного завдання перед його виконанням дозволять уникнути затримок, а застосування гнучких методологій розробки, наприклад Scrum, дасть змогу швидко адаптуватися до змін у проєкті.

Для бізнесових ризиків важливо проводити регулярний аналіз ринку, щоб виявляти нові потреби клієнтів і адаптувати функціонал системи. Окрім цього, слід забезпечити постійний моніторинг законодавчих змін, які можуть вплинути на функціонування системи, а також розробити стратегію фінансової стійкості, щоб компенсувати можливі втрати.

У сфері безпеки необхідно забезпечити багаторівневий доступ до даних студентів і викладачів, що дозволить уникнути витоків конфіденційної інформації. Регулярні перевірки на наявність вразливостей та залучення експертів із кіберзахисту забезпечать додатковий рівень захисту системи.

Комунікаційні ризики можуть бути знижені завдяки впровадженню централізованих каналів обміну інформацією. Регулярний зворотний зв’язок із користувачами дозволить виявляти слабкі місця системи та оперативно реагувати на них. Розробка зрозумілої документації для команди сприятиме покращенню внутрішньої взаємодії.

Для зменшення користувацьких ризиків, пов’язаних із можливими труднощами в роботі з системою, варто проводити навчання студентів та викладачів, а також оптимізувати інтерфейс для покращення зручності користування. Попереднє

тестування нових функцій на обмеженій групі користувачів допоможе уникнути масових скарг на нововведення.

Законодавчі ризики можна ефективно зменшити шляхом моніторингу змін у нормативній базі, залучення юристів для перевірки відповідності функціоналу системи та створення спеціальної команди, яка буде відповідати за адаптацію до нових вимог.

У результаті реалізації цих заходів UMSystem зможе забезпечити стабільну роботу, знизити ймовірність критичних збоїв і ризиків, а також підвищити рівень задоволеності користувачів. Використання стратегій уникнення, зменшення, передачі та прийняття ризиків дозволяє не лише ефективно реагувати на поточні виклики, але й планувати подальший розвиток системи з урахуванням її сильних сторін і можливостей.

3.3. SWOT-аналіз UMSystem: стратегії вдосконалення

У рамках проєкту UMSystem важливо застосовувати інструменти для виявлення можливих проблем, зокрема пов’язаних з технічними, організаційними та безпековими аспектами. Вибір конкретних методів оцінки дозволяє більш точно прогнозувати вплив ризиків і розробити стратегії для їх управління. Визначивши основні ризики ми проведемо SWOT-аналіз UMSystem, визначимо SO - заходи, які необхідно провести з метою покращення використання сильних сторін системи для збільшення її можливостей; ST - заходи, які необхідно провести з метою покращення використання сильних сторін для запобігання загроз; WO - заходи, які необхідно провести з метою мінімізації впливу слабких сторін для збільшення його можливостей та WT - заходи, які необхідно провести з метою мінімізації впливу слабких сторін для запобігання загроз. Ці заходи носитимуть рекомендаційний характер та будуть надані для команди розробників для ознайомлення.

SWOT-аналіз UMSystem.

1. Сильні сторони (Strengths) - це внутрішні переваги, які можуть допомогти в успішному подоланні ризиків або зменшенні їхнього впливу.

- гнучкість і адаптивність: оскільки UMSystem вже функціонує, команда може зосередитися на виконанні необхідних задач і швидко реагувати на змінні вимоги або проблеми, що виникають у процесі.
- модульність та гнучкість системи: UMSystem є потужною та адаптивною платформою, яка може швидко реагувати на зміни потреб і умов, що дає змогу оперативно змінювати налаштування та функціонал за необхідності.
- використання сучасних технологій: система базується на надійних технологіях, таких як Azure, MongoDB, React/Remix, що підвищує її надійність та масштабованість і мінімізує технічні ризики.

2. Слабкі сторони (Weaknesses) - це внутрішні проблеми, які можуть погіршити здатність системи впоратися з ризиками.

- відсутність структурованих спринтів на етапі експлуатації: оскільки система функціонує без регулярних спринтів, можуть виникати труднощі з плануванням масштабних оновлень або покращень. Це також може спричиняти відсутність чіткої організації процесів на майбутнє, коли виникне потреба в інтеграціях чи додаткових функціях.
- залежність від технологічних постачальників: якщо постачальники інфраструктури або технологічних компонентів, таких як Azure або MongoDB, зазнають проблем, це може викликати збої в роботі системи.
- складність адаптації до змін законодавства: постійні зміни в законодавстві можуть вимагати оперативних змін у системі, і без чіткої організаційної структури та процесів адаптація може бути не такою швидкою.

3. Можливості (Opportunities) - це зовнішні фактори, які можуть створити нові можливості для системи або допомогти знизити ризики.

- інтеграція з новими технологіями: використання новітніх інструментів для розробки та моніторингу дозволяє знизити технічні ризики та підвищити надійність системи.
- розширення ринку через законодавчі ініціативи: зміни в законодавстві, спрямовані на підтримку онлайн-освіти, можуть відкрити нові можливості для UMSystem на ринку.

- гнучкість роботи в умовах війни: UMSystem має достатню гнучкість для адаптації до умов, що змінюються, і може знизити негативні впливи від зовнішніх факторів, таких як війна чи економічні труднощі.

4. Загрози (Threats) - це зовнішні фактори, які можуть негативно вплинути на систему і збільшити ризики.

- війна та економічна нестабільність: війна та економічна нестабільність можуть серйозно вплинути на роботу системи, зокрема через перебої в постачанні технологій і інфраструктури, а також ризики для безпеки даних.
- зростання кіберзагроз: кіберзагрози, зокрема в умовах війни, можуть поставити під загрозу безпеку даних користувачів та функціонування системи.
- зміни в законодавстві: часті зміни в законодавстві, особливо в контексті цифровізації освіти, можуть вимагати додаткових витрат на адаптацію системи до нових вимог і стандартів.

На основі даного дослідження визначимо SO- ST- WO- та WT-заходи.

SO - заходи, які необхідно провести з метою покращення використання сильних сторін UMSystem для збільшення її можливостей.

1. Інтеграція нових технологій та інновацій.

Застосування можливості інтеграції з новими технологіями: Завдяки гнучкості та адаптивності системи, UMSystem може швидко впроваджувати новітні інструменти для розробки та моніторингу. Це дозволяє знижувати технічні ризики та покращувати функціональність, що дає можливість вийти на нові ринки, забезпечуючи високу конкурентоспроможність. Для цього можна використати наступні заходи: використання сучасних методів автоматизації тестування та CI/CD (безперервна інтеграція та розгортання) для підвищення стабільності системи; оновлення технологічного стеку для забезпечення масштабованості та підвищення продуктивності, зокрема для підтримки нових стандартів безпеки та законодавчих вимог.

2. Розширення ринку через нові можливості законодавства.

Застосування можливості розширення ринку через зміни в законодавстві: Оскільки законодавчі ініціативи можуть підтримувати розвиток онлайн-освіти, це

створює нові можливості для UMSystem на ринку. Пропонуємо наступні дії: створення спеціалізованих модулів в UMSystem для підтримки нових законодавчих вимог у сфері освіти; розробка функціоналу, що забезпечує автоматизовану відповідність новим вимогам законодавства для онлайн-освітніх платформ, що може збільшити привабливість продукту для організацій, що працюють у цій сфері.

3. Використання гнучкості для адаптації до умов війни.

Застосування можливості гнучкості роботи в умовах війни: оскільки система вже адаптована до змінних умов, вона може бути використана для швидкої зміни функціоналу в умовах зовнішніх загроз. Для цього можна використати розробку та впровадження стратегій для забезпечення безперебійної роботи системи в умовах військової нестабільності (наприклад, резервні дата-центри або використання хмарних рішень для збереження даних); підвищення безпеки даних та резервне копіювання для захисту від кіберзагроз та зловмисних атак, пов'язаних з військовими конфліктами.

4. Активне використання надійних технологій для масштабування.

Застосування надійних технологій, таких як Azure та MongoDB, для масштабування системи дозволяє швидко реагувати на змінювані потреби ринку.
Тут можуть допомогти використання додаткових функцій масштабування в Azure для швидкого адаптування до зростання навантаження на систему та/або поглиблене використання MongoDB для зберігання великих обсягів даних, що дозволить системі бути більш стійкою до збоїв і забезпечить високу доступність.

5. Продовження розвитку технологічної та організаційної гнучкості.

Застосування гнучкості в процесах для подолання будь-яких внутрішніх або зовнішніх викликів, таких як зміни на ринку чи потреби клієнтів, дозволить ефективно реагувати на нові можливості та мінімізувати вплив можливих загроз.
Можна використати розробку гнучкої системи керування проектами, що дозволяє команді ефективно адаптуватися до вимог і швидко виконувати задачі; поглиблення співпраці з ключовими партнерами та постачальниками для підвищення надійності системи та забезпечення гнучкості в управлінні проектами.

Для збільшення можливостей UMSystem варто активно використовувати наявні сильні сторони, такі як гнучкість, технологічна надійність та масштабованість, а також наявність сучасних інструментів для адаптації до змін. Це дозволить ефективно використовувати нові можливості ринку, в тому числі в умовах змінного законодавства та нестабільних зовнішніх обставин, таких як війна.

ST - заходи, які необхідно провести з метою покращення використання сильних сторін UMSystem для запобігання загроз:

1. Покращення надійності та безпеки системи в умовах війни

Застосування гнучкості та надійності для запобігання загрозам, пов'язаним з війною: оскільки в Україні триває війна, існує підвищений ризик втрати даних, перебоїв у роботі та атак на інфраструктуру. Система повинна бути стійкою до цих загроз завдяки використанню надійних технологій та гнучкості в роботі. Цьому можуть сприяти наступні заходи: впровадження стратегій відновлення після катастроф (disaster recovery) з використанням резервних хмарних рішень, таких як Azure, для забезпечення безперервної роботи; створення додаткових серверних інфраструктур або розподілених дата-центрів для зниження ризику від збоїв у зв'язку з фізичними атаками чи природними катастрофами; шифрування даних і впровадження надійних механізмів аутентифікації та доступу для захисту інформації.

2. Використання технологій для мінімізації технічних збоїв і забезпечення стабільності. Застосування надійних інструментів та гнучкості для запобігання технічним загрозам: оскільки системи можуть бути вразливі до технічних збоїв і багів, важливо активно використовувати сильні технології та засоби моніторингу для попередження та швидкого реагування на такі загрози. Тут можна запропонувати наступні шляхи вирішення: постійне оновлення і вдосконалення програмного забезпечення (наприклад, використання регулярного тестування та оновлень для запобігання багам і вразливостям); впровадження систем моніторингу для оперативного виявлення технічних збоїв (наприклад, через Azure Monitor, Datadog або інші інструменти); використання автоматизованих тестувань для підвищення надійності системи та зменшення ризику виникнення технічних помилок.

3. Застосування сучасних технологій для підвищення безпеки даних.

Застосування сильних сторін для запобігання загрозам, пов'язаним з кібербезпекою: системи, пов'язані з онлайн-освітою, можуть бути вразливими до атак, таких як DDoS, фішинг або зловмисні доступи до персональних даних. Зважаючи на високий рівень кіберзагроз в умовах сучасних конфліктів, важливо посилити захист даних. Надійними варіантами цього є: інтеграція з передовими засобами кібербезпеки (наприклад, використання багатофакторної автентифікації, системи запобігання вторгненням); розробка спеціалізованих протоколів для захисту особистої та фінансової інформації студентів і викладачів; постійне тестування на вразливості та регулярний аудит безпеки для виявлення та усунення потенційних загроз.

4. Адаптація до змін в законодавстві через використання гнучких технологій. Застосування технологічної гнучкості для запобігання загрозам, пов'язаним із змінами в законодавстві: зміни в законодавстві можуть створити нові загрози для діяльності UMSystem, такі як вимоги щодо зберігання даних або специфічні правила обробки персональної інформації. Оскільки система вже має технічну гнучкість, можна використовувати цю перевагу для швидкої адаптації.

Найкращими заходами для цього є: модернізація системи для забезпечення відповідності новим стандартам безпеки та зберігання даних, встановленим законодавством; розробка внутрішніх політик та механізмів моніторингу для дотримання змін у законодавстві, особливо в контексті захисту персональних даних.

5. Зниження людських ризиків через автоматизацію процесів. Застосування технологічних можливостей для зниження людських загроз: людський фактор може бути значним джерелом ризиків, таких як помилки у коді чи неправильне використання системи. Завдяки наявності сильних технічних можливостей, можна зменшити вплив цих загроз. До таких можливостей відносяться: використання автоматизованих процесів тестування та контролю якості, щоб зменшити вплив людських помилок на кінцевий результат; розробка механізмів контролю доступу та прав, щоб уникнути небажаних змін у системі з боку неавторизованих користувачів; навчання персоналу для підвищення обізнаності щодо важливості правильного використання технологій безпеки.

ST-стратегії для UMSystem повинні фокусуватись на використанні сильних технологічних сторін системи для зменшення ризиків, які виникають внаслідок зовнішніх загроз, таких як війна, зміни в законодавстві чи кіберзагрози. Це дозволить зберегти стабільність та безпеку системи навіть в умовах постійних змін і зовнішніх викликів.

WO - заходи, які необхідно провести з метою мінімізації впливу слабких сторін для збільшення можливостей UMSystem:

1. Посилення комунікації та координації в команді

Мінімізація впливу слабкої комунікації для збільшення ефективності: однією зі слабких сторін UMSystem може бути недостатня комунікація між учасниками проекту, особливо в умовах розподіленої роботи. Для збільшення можливостей системи потрібно вдосконалити процеси комунікації та координації. Для цього необхідні запровадження ефективних інструментів для внутрішнього спілкування та колаборації (наприклад, Microsoft Teams, Slack, Asana або інші інструменти для управління проєктами); регулярні зустрічі команди для обговорення поточного стану задач, вирішення проблем та визначення пріоритетів; навчання команди щодо ефективних методів комунікації та використання доступних технологій для забезпечення прозорості та взаємодії в проєкті.

2. Оптимізація планування та управління ризиками. Мінімізація впливу недостатнього планування для зниження непередбачуваних ситуацій: якщо планування в UMSystem не завжди було на належному рівні, потрібно зосередитись на створенні більш точних і детальних планів для управління проектом і ризиками, а саме впровадження покращеного процесу планування, зокрема у вигляді чітких дорожніх карт розвитку системи, де всі етапи, терміни та ресурси будуть чітко визначені; використання спеціалізованих інструментів для управління ризиками (наприклад, Microsoft Project або інші програмні засоби для створення детальних планів ризиків); розробка резервних планів для кожного значущого етапу, щоб швидко адаптуватися до непередбачених змін.

3. Поліпшення адаптації до нових технологій та змін.

Мінімізація впливу обмеженої гнучкості до змін у технологіях для збільшення конкурентоспроможності, якщо система має проблеми з адаптацією до нових технологій чи змін, це може стати слабкою ланкою. Рішенням є посилення гнучкості та здатності до швидкої адаптації. Можемо застосувати такі заходи, як постійне навчання та перекваліфікація команди з новітніх технологій, таких як нові інструменти для баз даних, хмарні сервіси чи мови програмування; впровадження механізмів для швидкого тестування і впровадження нових технологій у розробку, що дозволить швидко адаптуватися до змін на ринку; співпраця з постачальниками програмного забезпечення для отримання оновлень і підтримки нових технологій, які можуть підвищити ефективність UMSystem.

4. Забезпечення відповідності до нових вимог законодавства.

Мінімізація впливу недосконалості адаптації до нових законодавчих вимог, якщо в UMSystem існують слабкі місця в адаптації до законодавчих змін, це може спричиняти юридичні ризики. Важливо покращити ці аспекти, щоб забезпечити відповідність вимогам. Це можуть бути визначення ключових змін у законодавстві та правових нормах, що стосуються обробки та зберігання даних, та постійне оновлення системи відповідно до нових вимог; створення спеціалізованих робочих груп для моніторингу змін у законодавстві та розробки планів дій для адаптації системи до цих змін; впровадження системи звітності для відстеження відповідності всіх процесів та діяльності UMSystem чинному законодавству.

5. Покращення управління змінами в умовах непередбачуваних ситуацій.

Мінімізація впливу недостатнього управління змінами на розвиток системи, в умовах війни та постійних змін на ринку можуть виникати непередбачувані ситуації, що вимагатимуть швидких рішень і адаптації. Для цього потрібно удосконалити управління змінами. Підійдуть наступні заходи: розробка чіткої стратегії управління змінами, що включає визначення критеріїв для швидкого прийняття рішень у разі виникнення кризових ситуацій; використання технологій для відстеження змін і впливу цих змін на проект, що дозволить оперативно реагувати на будь-які зовнішні фактори, що можуть зашкодити роботі системи; створення резервних ресурсів для

підтримки непередбачуваних змін у проекті, зокрема в кадровому, фінансовому та технологічному аспектах.

WO-стратегії для UMSystem зосереджуються на мінімізації слабких сторін системи шляхом покращення планування, комунікації, адаптації до нових технологій і законодавства. Вони дозволять покращити внутрішні процеси і забезпечити більшу гнучкість у розвитку системи, що в свою чергу збільшить її можливості і конкурентоспроможність на ринку.

WT - заходи, які необхідно провести з метою мінімізації впливу слабких сторін UMSystem для запобігання загроз.

1. Посилення безпеки та захисту даних

Мінімізація ризику витоку даних через слабкий рівень безпеки, якщо є слабкі місця у захисті інформації, це може створювати серйозні загрози, зокрема в умовах війни та змін у законодавстві щодо захисту даних. Для подолання цих загроз можемо використати підвищення рівня безпеки за допомогою багаторівневого шифрування та регулярного оновлення програмного забезпечення безпеки; впровадження протоколів безпеки для захисту конфіденційних даних від несанкціонованого доступу та витоків, зокрема для персональних даних студентів та працівників; проведення регулярних аудиторських перевірок та тестування на вразливості для виявлення та виправлення недоліків у системі безпеки.

2. Покращення управління проектами та моніторинг виконання задач.

Мінімізація впливу поганого управління проектами, яке може призвести до зриву строків і перевитрати ресурсів: Якщо управління проектами в UMSystem має слабкі місця, це може призвести до затримок у виконанні завдань та високих витрат. Щоб цього уникнути необхідно застосувати впровадження більш суворого контролю за термінами виконання задач, створення чітких графіків та регулярних звітів про стан проекту, використання інструментів для моніторингу та управління проектами, таких як Jira або Asana, для відстеження виконання завдань та своєчасного реагування на відставання, підвищення рівня відповідальності членів команди за виконання конкретних завдань, що дозволить зменшити ймовірність пропусків та затримок.

3. Забезпечення відповідності до законодавства та змін в регулюванні.

Мінімізація впливу правових загроз через недостатнє знання законодавчих змін якщо UMSystem не встигає адаптуватися до нових законодавчих вимог або не реагує на зміни в правовому полі, це може призвести до юридичних санкцій або втрати довіри. Цьому зарадить створення окремої групи для моніторингу змін у законодавстві та регулюванні, що стосуються даних, захисту персональних даних та інших аспектів, регулярні консультації з юридичними фахівцями для визначення актуальних вимог та розробки плану адаптації системи до нових нормативних вимог, впровадження механізмів для швидкого внесення змін до системи в разі необхідності, зокрема у частині обробки даних та звітності.

4. Покращення гнучкості та адаптації до змін.

Мінімізація впливу недостатньої гнучкості в умовах змін зовнішнього середовища, в умовах війни та швидких змін на ринку системі необхідно бути більш адаптивною. Слабка здатність до адаптації може призвести до неефективності та зриву проектів. Тому необхідна розробка планів гнучкості для швидкого реагування на зміни: наприклад, можливість швидко адаптуватися до нових технологій, ринкових умов або змін у запитах клієнтів; створення системи резервування ресурсів для непередбачених ситуацій, таких як збої в інфраструктурі або нестабільність постачальників; впровадження agile-методології, що дозволяє команді швидко адаптуватися до змінних вимог і забезпечує більш швидку реакцію на потреби клієнтів.

5. Посилення управління змінами та кризовими ситуаціями.

Мінімізація впливу кризових ситуацій, пов’язаних з невизначеністю через війни або ринкові коливання, в умовах війни можуть виникати значні кризові ситуації, що потребують ефективного управління змінами та кризами. Для цього необхідні розробка чіткої стратегії управління кризами, яка включатиме план дій у разі виникнення непередбачених обставин, таких як технічні проблеми або зовнішні загрози; визначення відповідальних осіб для управління змінами та кризовими ситуаціями, зокрема для взаємодії з постачальниками, клієнтами та іншими зацікавленими сторонами; підготовка команди до можливих кризових ситуацій через регулярні тренінги та симуляції кризових ситуацій.

WT-стратегії для UMSystem орієнтовані на мінімізацію негативного впливу слабких сторін для запобігання потенційним загрозам. Заходи, спрямовані на підвищення рівня безпеки, покращення управління проектами, адаптацію до змін у законодавстві та забезпечення гнучкості, допоможуть значно знизити ймовірність виникнення загроз для системи, підвищивши її стійкість та ефективність.

Проведений SWOT-аналіз дозволив визначити сильні та слабкі сторони, а також можливості та загрози для UMSystem. На основі отриманих результатів розроблено чотири типи стратегій: SO, ST, WO та WT.

Сильні сторони системи, такі як сучасна технологічна платформа, інтуїтивний інтерфейс та адаптація до освітніх потреб, сприяють її розвитку. Однак слабкі сторони, зокрема обмежені ресурси команди та недостатня інтеграція користувачів, потребують вирішення.

Запропоновані стратегії допомагають:

SO — посилити переваги та використати можливості для підвищення конкурентоспроможності.

ST — ефективно протидіяти загрозам, зокрема зовнішнім ризикам, використовуючи внутрішні сильні сторони.

WO — мінімізувати слабкі сторони через оптимізацію процесів і використання можливостей.

WT — зменшити негативний вплив слабких сторін і загроз за допомогою превентивних заходів.

Отримані рекомендації слугують базисом для покращення управління проектом, зниження ризиків і підвищення ефективності роботи UMSystem в умовах постійних викликів та змін.

ВИСНОВКИ

У ході даної роботи було досліджено різні підходи до управління ризиками в IT-компаніях. Зокрема була розглянуті стратегії реагування на невизначеність, загрози та можливості. Було визначено, що для покращення ефективності управління ризиками в IT-проєктах слід удосконалювати чинні процеси з урахуванням як можливостей, так і загроз, а також впроваджувати нові, ще не реалізовані. Досягти цього можна шляхом створення та впровадження інформаційної технології управління ризиками, яка враховуватиме всі аспекти ризиків і можливостей. Також було досліджено підхід, де рекомендується здійснювати управління ризиками проєктів за чотирма етапами: ідентифікації, аналізу, планування та моніторингу і контролю. Звичайно були розглянуті стратегії, які світова практика виділяє як основні: стратегії уникнення, передачі, прийняття ризику, стратегія реагування на ризик та стратегія гнучкості та адаптації. В ході розгляду цих підходів ми визначили, що управління ризиками в IT-проєктах є ключовим фактором їх успішної реалізації, адже на кожному етапі виникають численні загрози та можливості, які можуть вплинути на результат. Важливість вибору стратегії управління ризиками, що відповідає особливостям проєкту, його масштабам, складності та унікальним умовам, є надзвичайно високою. У контексті швидких технологічних змін та динамічного зовнішнього середовища, проактивний підхід до виявлення, оцінки та мінімізації ризиків стає запорукою успіху. Грамотне впровадження стратегій управління ризиками сприяє стабільності проєкту в умовах невизначеності, підвищенню якості виконання та досягненню поставлених цілей. Аналіз і врахування не лише загроз, а й можливостей дає змогу проєктним командам не лише уникати негативних наслідків, але й максимально використовувати потенційні переваги для забезпечення конкурентоспроможності та успіху в довгостроковій перспективі.

Також в даній роботі ми проаналізували та оцінили вплив ризиків на ефективність на різних етапах роботи IT-додатків. Нами були розглянуті метод FMEA, модель Монте-Карло, техніка PERT, модель COSO ERM та аналітичну ієрархічну модель. Кожна з представлених моделей оцінки та аналізу ризиків є ключовим інструментом у процесі розробки IT-додатків, адже вони пропонують

різноманітні підходи до ідентифікації, оцінки та мінімізації потенційних загроз. Завдяки їхньому застосуванню проєктні команди можуть не лише завчасно виявляти можливі проблеми, але й розробляти обґрунтовані та дієві стратегії для їх уникнення або зменшення впливу. Це сприяє не тільки забезпеченню стабільності та передбачуваності процесу розробки, а й підвищує загальну ефективність і результативність реалізації проєктів. Використання таких моделей дозволяє системно підходити до управління ризиками, враховуючи всі етапи життєвого циклу проєкту. Це сприяє створенню умов для безперервного вдосконалення процесів, зміцнює позиції команди в умовах високої конкуренції та забезпечує досягнення стратегічних цілей у межах встановлених ресурсів і часу. У сучасних умовах динамічності ринку й технологічного прогресу такі моделі стають важливим елементом управління проєктами, формуючи надійний фундамент для їхнього довгострокового успіху.

Крім цього під час даного дослідження було проведено всебічний аналіз ключових ризиків, що супроводжують процеси розробки та впровадження системи UMSystem. Ця система, орієнтована на забезпечення конкурентоспроможності освітніх установ та оптимізації їхніх робочих процесів, стикається з численними викликами в сучасних умовах, особливо в умовах військових дій та економічної нестабільності. Проведене дослідження дозволило ідентифікувати ці ризики та визначити їх рівень небезпеки, що стало основою для подальшої розробки ефективних рекомендацій щодо їх мінімізації. Виявлені ризики були розділені на технічні, організаційні, бізнесові, безпекові, комунікаційні, користувацькі та законодавчі.

Технічні ризики виявились одними з найбільш загрозливих для успішного впровадження UMSystem. Збої в інфраструктурі, вразливість до зовнішніх атак та проблеми з масштабованістю становлять серйозну небезпеку для стабільної роботи системи, особливо в умовах інтенсивних кіберзагроз. Зокрема, вразливість до кіберзагроз в умовах війни була оцінена як катастрофічний ризик. Для зменшення ймовірності реалізації цих загроз було запропоновано впровадження багаторівневої системи кібербезпеки, що включає використання фаєрволів, систем виявлення

вторгнень (IDS/IPS), шифрування даних та багатофакторної автентифікації. Регулярні аудити та пентести допоможуть виявляти потенційні вразливості на ранніх етапах.

Особливу увагу було приділено масштабованості та оптимізації системи. Недоліки в цій області можуть призвести до значних проблем у майбутньому, коли система розширюватиметься та збільшуватиметься кількість користувачів. Для уникнення цього ризику важливо розробити стратегію з розширення можливостей системи, включаючи попереднє тестування під навантаженням і планування масштабування на основі реальних даних щодо продуктивності.

Організаційні ризики також відіграють важливу роль у загальній картині ризиків для UMSystem. Однією з ключових проблем, виявлених у цьому контексті, є залежність від ключових фахівців. В умовах війни та нестабільності ця залежність стає ще більш загрозливою, адже працівники можуть бути мобілізовані або вимушені залишити свої робочі місця. Для мінімізації цього ризику важливо впровадити програми передачі знань та системи дублювання функцій, щоб зменшити залежність від конкретних спеціалістів. Крім того, залучення зовнішніх експертів та тимчасових працівників може допомогти зменшити навантаження на основні кадри.

Іншим організаційним ризиком є недостатність ресурсів для забезпечення роботи проєкту. Це може включати як людські, так і фінансові ресурси, що часто стає перепоною для реалізації великих IT-проектів. Для вирішення цієї проблеми рекомендовано застосовувати гнучкі методології управління проектами (наприклад, Agile), які дозволяють оптимально розподіляти ресурси та коригувати їхнє використання на основі актуальних потреб проекту.

Бізнесові ризики, такі як залежність від фінансування та інвесторів, є ще однією важливою проблемою для UMSystem. Враховуючи нестабільну економічну ситуацію та можливі зміни в пріоритетах галузі, існує ризик зменшення фінансування або втрати інвесторської підтримки. Для мінімізації цього ризику важливо диверсифікувати джерела доходу та створювати резерви для кризових ситуацій. Крім того, необхідно підтримувати постійний контакт з інвесторами та доносити до них важливість проекту, забезпечуючи прозорість фінансової діяльності.

Ризик втрати репутації є ще одним критичним бізнесовим фактором. В умовах сучасного ринку негативні відгуки користувачів або невиконання зобов'язань можуть призвести до швидкої втрати довіри клієнтів. Впровадження систем управління відгуками та програми швидкого реагування на негативні ситуації дозволять зменшити цей ризик.

Безпекові ризики є найважливішими для будь-якої IT-системи, особливо в умовах сучасної війни та кіберзагроз. Фізична загроза інфраструктурі, зокрема серверним приміщенням та дата-центрам, становить значну небезпеку для роботи системи. Для захисту фізичної інфраструктури рекомендовано використовувати віддалені дата-центри, резервне копіювання даних та планування аварійного відновлення.

Кіберзагрози в умовах війни також набувають критичного значення. Постійні спроби хакерських атак, а також шахрайство та кіберзлочинність потребують впровадження додаткових заходів безпеки. Регулярні оновлення програмного забезпечення, впровадження сучасних засобів захисту та навчання співробітників щодо безпеки є основними заходами для мінімізації цих загроз.

Управління комунікаційними ризиками є важливим аспектом для підтримки ефективної взаємодії між членами команди та із зовнішніми стейкхолдерами. Перебої в комунікаціях можуть призвести до неправильного виконання завдань або невідповідності очікуванням клієнтів. Для уникнення цих ризиків рекомендовано впроваджувати єдині платформи для комунікації, такі як Jira або Slack, а також проводити регулярні синхронізаційні зустрічі між командами та замовниками.

Окрім зазначених вище категорій ризиків, важливо звернути увагу на користувацькі ризики та законодавчі ризики. Зміни у вимогах користувачів можуть призвести до невідповідності функціоналу системи їхнім очікуванням, що знижує лояльність. Для вирішення цієї проблеми необхідно активно залучати користувачів до процесу розробки та враховувати їхні потреби на всіх етапах створення продукту.

Законодавчі зміни стосуються як захисту персональних даних, так і інших аспектів діяльності освітніх установ, що використовують UMSystem. Постійне

відстеження нових регуляцій та відповідність нормативним вимогам дозволять уникнути можливих санкцій або юридичних проблем.

SWOT-аналіз UMSystem показав, що система має низку сильних сторін, таких як гнучкість, адаптивність та використання сучасних технологій, що дозволяють оперативно реагувати на зміни та забезпечувати стабільну роботу. Сильні сторони включають потужну модульну архітектуру та інтеграцію новітніх технологій (Azure, MongoDB, React/Remix), що робить систему масштабованою та надійною. Водночас, слабкі сторони полягають у недостатній структурованості процесів управління, таких як відсутність регулярних спринтів на етапі експлуатації, що може призвести до затримок в оновленнях та інтеграціях. Додатково, залежність від технологічних постачальників, таких як Azure, є важливим викликом для забезпечення постійної безперебійної роботи системи.

SWOT-аналіз також виявив низку можливостей, що дозволяють UMSystem розширити свою присутність на ринку. Зокрема, законодавчі ініціативи, спрямовані на розвиток онлайн-освіти, відкривають нові можливості для розширення функціоналу та залучення нових клієнтів. Інтеграція з новими технологіями може значно підвищити надійність системи, забезпечуючи можливість масштабування та адаптації до змін.

Найбільшими загрозами для системи залишаються кіберзагрози, війна та економічна нестабільність. В умовах війни існує підвищений ризик фізичних атак на інфраструктуру, що може негативно вплинути на функціонування системи. Кіберзагрози, такі як атаки на дані користувачів, потребують посилених заходів безпеки, включаючи багаторівневий захист і регулярні пентести.

Таким чином, проведений аналіз продемонстрував, що ефективне управління ризиками є ключовим фактором для забезпечення успіху UMSystem. Впровадження сучасних методів аналізу та управління ризиками дозволить не тільки уникнути критичних проблем у роботі системи, але й забезпечити її сталий розвиток у майбутньому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Frank H. Knight. Risk, Uncertainty, and Profit. URL:https://www.econlib.org/library/Knight/knRUP.html

2. Hubbard D. W. Failure of Risk Management: Why It's Broken and How to Fix It. Wiley & Sons, Incorporated, John, 2020. 384 с.

3. Schmidt W. H., Tannenbaum R. Management of Differences. Harvard Business Review. 1960. Vol. 11. URL: https://hbr.org/1960/11/management-of- differences

4. Богдан Н., Оболенцева Л., Войт В., Махортов М. Ризик-менеджмент як чинник стратегії адаптації підприємств туристичного та готельного бізнесу до кризових умов. Економічний аналіз. 2023. Т. 33. № 3. С. 42-54. DOI: https://doi.org/10.35774/econa2023.03.042

5. ДСТУ ISO Guide 73:2013. Керування ризиком. СЛОВНИК ТЕРМІНІВ. [Чинний від 2014-01-07]. Київ, 2014. 17 с. (Національний стандарт України). URL: https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_iso_guide_73_2013.pdf

6. Москаленко В. О. Теоретичні аспекти аналізу проектних ризиків. Наукові праці Національного університету харчових технологій. 2013. № 52. С. 129-136.

7. Гавриш О. А., Мельникова В. А. Роль проектного ризику в загальній системі ризик-менеджменту. Бізнес, інновації, менеджмент: проблеми та перспективи : зб. тез доп. II Міжнар. наук.-практ. конференції, 22 квітня 2021 р. Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. С. 50-51.

8. Скопенко Н. С., Євсєєва І. В., Москаленко В. О. Управління ризиками в проектному менеджменті. Інвестиції: практика та досвід. 2013. № 24. С. 41-44.

9. Федулова І. В. Ідентифікація ризиків як складова ризик-менеджменту.Інтелект XXI. 2016. №4. С. 29-45.

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

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

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

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

14. Макарчук, І. В. Управління ризиками ІТ-проєктів на підприємстві Дис. канд. екон. Наук. https://knute.edu.ua/file/Mg==/adcd9a7a02ff2aff4977bfaab4ba86ba.pdf.

15. Грабіна К. В., Шендрик В. В. Метод управління ризиками ІТ-проєктів з врахуванням загроз та можливостей. Управління розвитком складних систем. Київ, 2023. No 55. С. 18 – 28, dx.doi.org\10.32347/2412-9933.2023.55.18-28.

16. A Guide to the Project Management Body of Knowledge. (7 Ed.). Chicago: Project Management Institute, 2019. 250 p

17. Bedrii D. Integrated anti-risk management of conflicts of a scientific project in a behavioral economics. Scientific Journal of Astana IT University. Astana, September 2020. Vol. 3. P. 4–14. DOI: 10.37943/AITU.2020.15.62.001.

18. Danchenko E., Bakulich O., Teslenko P., Bedrii D., Bielova O., Semko I. Information technology of integrated risk management of scientific projects under uncertainty and behavioral economy. Scientific Journal of Astana IT University. Vol. 5, March 2021. Astana, 2021. P. 63-76. DOI: 10.37943/AITU.2021.69.52.006.

19. Журан О.А., Глава М.Г., Управління ризиками в іт-проектах URL:http://dspace.opu.ua/jspui/bitstream/123456789/6314/1/%D0%A3%D0%9F%D0%A0%D0%90%D0%92%D0%9B%D0%86%D0%9D%D0%9D%D0%AF%20%D0%A0%D0%98%D0%97%D0%98%D0%9A%D0%90%D0%9C%D0%98%20%D0%92%20%D0%86%D0%A2-9F%D0%A0%D0%9E%D0%95%D0%9A%D0%A2%D0%90%D0%A5.pdf

20. Беляков М. А. Управління ризиками в ІТ-проектах автоматизації. Актуальні задачі сучасних технологій. Матеріали V Міжнародної науково-технічної конференції молодих учених та студентів (м. Тернопіль, 17-18 листопада 2016 р.). Тернопіль, 2016. С. 291–292.

21. A Guide to the Project Management Body of Knowledge (PMBOK® Guide). (2021). Seventh Edition. USA: PMI, 250.

22. Онищенко І. І. Аналіз ризиків в процесі управління ІТ-проектами. Вісник НТУ «ХПІ». Серія: Стратегічне управління, управління портфелями, програмами та проектами. Харків: НТУ «ХПІ», 2014. № 3 (1046). С. 95–100.

23. Данченко О. Б., Бедрій Д. І., Семко О. В., Заяц О. В. Метод управління інформаційними ризиками в проєктах діджиталізації бізнес-процесів. Вісник Національного технічного університету «ХПІ». Серія: Стратегічне управління, управління портфелями, програмами та проектами. Харків : НТУ «ХПІ», 2022. № 2(6). С. 25–29. DOI: 10.20998/2413-3000.2022.6.5.

24. Danchenko O. B., Shendryk V. V., Hrabina K. V. Target models of integrated risk management for IT projects. The scientific heritage. Budapest, 2021. № 71(71). С. 55–61. DOI: 10.24412/9215-0365-2021-71-1-55-61.

25. Шендрик В. В., Данченко О. Б., Грабіна К. В. Синергетичний ефект від управління загрозами та можливостями в ІТ-проєктах Project, Program, Portfolio Management. V міжнародна науково-практична конференція (м. Одеса, 04-05 грудня 2020 року). Одеса: ОНПУ, 2020. С. 26–30.

26. Шендрик В. В., Данченко О. Б., Грабіна К. В. Складові управління ризиками ІТ-проєктів. Інформатика. Культура. Технології. VIII Міжнародна науково-практична конференція (м. Одеса, травень 2021). Одеса: ОНПУ, 2021. С. 124–126.

27. Грабіна К. І., Шендрик В. В., Данченко О. Б., Мазуркевич А. Г. Застосування SWOT-аналізу для ідентифікації ризиків проекту. Управління проектами у розвитку суспільства. XVIII Міжнародна науково-практична конференція (м. Київ, травень 2021). Київ: КНУБА, 2021. С. 133–137.

28. Данченко О.Б. Методологія інтегрованого управління відхиленнями в проєктах : автореф. дис. д-ра техн. наук: 05.13.22. Київ. нац. ун-т буд-ва і архітектури. Київ, 2015. 45 с.

29.Бедрій Д. І. Інтегроване протиризикове управління науковими проєктами в умовах невизначеності та переходу до циркулярної економіки: дис. ... д-ра техн. наук : 05.13.22. Одеса: Держ. ун-т «Одеська політехніка», 2021. 431 с.

30. Лебедовський В. Як ІТ-компанії в Україні страхують свої проекти [Електронний ресурс] / В. Лебедовський // Режим доступу: http://brit-mark.com/ua/press-centre/brit-mark-media/2013/kak-it-kompanii-v-ukraine-strahuyut-svoi-proektyi

31. Бащінська І. О., Полещук А. А., Мотова А. В. Удосконалення системи управління ризиками на підприємстві. Причорноморські студії. 2017. Вип. 17. С. 91-94.

32. Мороз В. М, Мороз С. А. Ризик-менеджмент : підручник. Харків : НТУ«ХПІ», 2018. 139 с.

33. Скопенко Н. С., Захарченко І. С. Методичні підходи до формування системи ризик-менеджменту. Ефективна економіка. 2023. № 2. URL: https://www.nayka.com.ua/index.php/ee/article/view/1141/1150

34. Марченко В. М. Поведінковий підхід до управління ризиками проєкту. Формування ринкових відносин в Україні. 2019. № 12. С. 38-45.

35. Федулова І. В., П'ятницька Г. Т. Сигніфікація ризик-менеджменту, антикризового управління та комплаєнсу в управлінні фінансовою безпекою підприємства. Економіка та держава. 2020. № 8. С. 26-34.

36. П’ятницька Г., Григоренко О. Електронна комерція B2C: розвиток у східній Європі, ризики та ефект інституціонального витіснення. Менеджмент та підприємництво в Україні: етапи становлення та проблеми розвитку. Вид- во Львівська політехніка. 2019. Т. 1. № 1. С. 121-130.

37. Скопенко Н. С., Федулова І. В. Ризик-апетит і методи його оцінювання. Теоретичні та прикладні питання економіки. 2020. Вип. 1 (40). С. 16-25.

38. Friedman, Milton, and Leonard J. Savage. "The utility analysis of choices involving risk." Journal of political Economy 56.4 (1948): 279-304.

39.Theory of Risk Aversion. URL: https://www.hetwebsite.net/het/essays/uncert/aversion.htm

40. Saaty, T. L. (1982). Decision Making for Leaders: The Analytic Hierarchy Process for Decisions in a Complex World. New York: McGraw-Hill

41. Pratt J. W. Risk Aversion in the Small and in the Large. Econometrica. 1964. Vol. 32. №1/2. P. 122-136. URL: https://doi.org/10.2307/1913738

42. Іванова, Н. Ю., Беднарчик В. Б., Карпенко О. О. Схильність до ризику як фактор ефективності діяльності фірми. НАУКОВІ ЗАПИСКИ. Економічні науки. 2003. Т.21. С. 38-41. URL: https://ekmair.ukma.edu.ua/server/api/core/ bitstreams/0db5242d-f10d-4453-872d-0e51053ee67d/content

43. Посохов І. М., Падалка П. А. Аналіз сучасного стану превентивного управління ризиками в Україні. Менеджмент і маркетинг на транспорті. 2022. URL: https://repository.kpi.kharkov.ua/server/api/core/bitstreams/a537b775-0464-4778-ad27-4277b39f9550/content

44. Щегельська А. О., Фоменко В. К. Сучасні підходи до ризик- менеджменту банку. Економіко-правові та управлінсько-технологічні виміри сьогодення: молодіжний погляд: матеріали Міжн. наук.-практ. конф. Дніпро: Університет митної справи та фінансів, 2021. Т. 1. 432 с., 2021. Т. 2. 73 с.

45. Вітлінський В. В. Кількісне оцінювання ступеня економічного ризику. Вісник ЖДТУ. Економіка, управління та адміністрування. 2010. №1 (51). С. 159-162.

46. Bai, S., Fedulova, I., Drozdova, Y. Management decision-making: multi- criterion assessment of uncertainty Financial and Credit Activity: Problems of Theory and Prac-tice, 2023, 4(51), pp. 190–201. URL: https://doi.org/10.55643/fcaptp.4.51.2023.4066

47. Kondratiuk O., Stoianenko I. Digitalization of business under global challenges. Вісник Київського національного торговельно-економічного університету. 2020. № 6. С. 26-36. URL: http://doi.org/10.31617/visnik.knute.2020(134)03

48. Кондратюк О., Стояненко І. Економічні ризики підприємства: постковідна трансформація. Вісник Київського національного торговельно- економічного університету. 2021. № 4. С. 4-18. URL:https://doi.org/10.31617/visnik.knute.2021(138)01

49. Stoianenko, I., Kondratiuk, O., Mostova, A., Pikus, R., Kachan, H., & Ilchenko, V. (2022). Digitization of the Econo-my Under the Influence of the COVID-19 Pandemic. Post-modern Openings, 13(4), 127-141. URL:https://doi.org/10.18662/po/13.4/510

50. Ганечко І.Г. Ринок проєктного фінансування: тенденції розвитку та галузева структура. Зовнішня торгівля: економіка, фінанси, право. 2021. № 6. С. 119 – 130. URL: https://doi.org/10.31617/zt.knute.2021(119)10

51. Вітлінський В. В., Наконечний С. Е. Ризик у менеджменті. Київ: ТОВ «Борисфен-М», 1996. 245 с.

52. Ястремський О. І. Основи теорії економічного ризику: Навч. посіб. Київ : АртЕк, 1997. 248 с.

53. Arrow, Kenneth J. "The theory of risk-bearing: small and great risks." Journal of risk and uncertainty 12 (1996): 103-111.