ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально–науковий інститут Інформаційних технологій

Кафедра Інженерії програмного забезпечення

Пояснювальна записка

до магістерської роботи
на ступень вищої освіти магістр

на тему «**РОЗРОБКА МОДЕЛІ ТА МЕТОДУ УПРАВЛІННЯ РИЗИКАМИ ІТ-ПРОЕКТУ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ»**

Виконав: студент 5 курсу, групи ПДМ - 62
спеціальності
121 Інженерія програмного забезпечення
(шифр і назва спеціальності)
Крута Юлія Валеріївна
(прізвище та ініціали)
Керівник Золотухіна О.А.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)

КИЇВ – 2022

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально–науковий інститут Інформаційних технологій

Кафедра Інженерії програмного забезпечення
Ступінь вищої освіти «Магістр»
Спеціальність підготовки 121 Інженерія програмного забезпечення

ЗАТВЕРДЖУЮ
Завідувач кафедри
Інженерії програмного забезпечення
_____О.В.Негоденко
“____” _____ 2022 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Крута Юлія Валеріївна
(прізвище, ім’я, по батькові)

1.Тема роботи: Розробка моделі та методу управління ризиками ІТ-проекту на основі нечіткої логіки

Керівник роботи Золотухіна Оксана Анатоліївна, к.т.н.,
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від « 12 » жовтня 2022 року № 122

2. Строк подання студентом роботи «31 » грудня 2022 року

3. Вихідні дані до роботи: Матеріали переддипломної практики, методи аналізу,
принципи побудови програмних і апаратних комп'ютерних засобів, метод математичного моделювання

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити).
4.1 Огляд предметної області
4.2 Розробка моделей та методів
4.3 Розробка програмного забезпечення моделей
4.4 Верифікація отриманих результатів

5. Перелік графічного матеріалу (презентація)
5.1 Мета, об’єкта та предмет дослідження
5.2 Етапи управління ризиками іт-проекту та причини невизначеності
5.3 Формалізація Вхідних змінних процесу управління ризиками іт-проекту на основі нечіткої логіки

5.4 Математична модель управління ризиками на основі нечіткої логіки

5.5 Метод нечіткого виведення

5.6 Структура інформаційної системи управління ризиками ІТ-проектів

5.7 Практичний результат

6. Дата видачі завдання «14» жовтня 2022року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1	Отримання завдання на магістерську роботу	14.10.2022	
2	Аналіз сутності та поняття ІТ-проект	17.10.2022	
3	Визначення характеристик ризиків та особливостей управління ними	20.11.2022	
4	Формалізація ризиків та розробка моделі їх представлення	22.11.2022	
5	Розробка методу управління ризиками ІТ-проекту на основі нечіткої логіки	23.11.2022	
6	Практична реалізація моделі управління ризиками ІТ-проекту на основі нечіткої логіки	01.12.2022	
7	Верифікація результатів	15.12.2022	
8	Написання та оформлення пояснювальної записки	21.12.2023	
9	Розробка графічних та презентаційних матеріалів	25.12.2023	
10	Захист магістерської роботи	17.01.2023	

Студент _____ Ю.В. Крута
(підпис) (прізвище та ініціали)

Керівник роботи _____ О.А. Золотухіна
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Текстова частина магістерської роботи: 70с., 24 рис., 1 дод., 30 джерел.

ІТ-ПРОЄКТ, РИЗИКИ, ВИТРАТИ, РЕСУРСИ, УПРАВЛІННЯ РИЗИКАМИ, НЕЧІТКА ЛОГІКА, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ.

Об`єкт дослідження – процес управління ризиками в ІТ-проектах.

Предмет дослідження – метод та модель управління ризиками в ІТ-проектах на основі нечіткої логіки.

Мета роботи – оптимізація управління ризиками ІТ-проекту на основі нечіткої логіки.

Методи дослідження – математичні: нечітка логіка, статистичні методи, методи представлення знань в системах підтримки прийняття рішень; емпірико-теоретичні: абстрагування, аналіз, синтез, методи математичного моделювання, візуалізація; методи проектування та розробки програмного забезпечення.

Проведено огляд та аналіз існуючих методів та моделей управління ризиками ІТ-проекту. Визначено принципи управління ризиками ІТ-проекту. Розроблено модель управління ІТ-ризиками на основі нечіткої логіки, яка відображає тристоронню схильність організацій до ризиків, пов'язаних з експлуатацією інформаційних систем: дії персоналу, збої систем, неліцензійність. Розроблено метод управління ризиками ІТ-проекту на основі нечіткої логіки, який забезпечує більш гнучку обробку факторів ризиків, дозволяють отримати лінгвістичний опис ступеня ризику, що дозволяє виявити пріоритети ризиків (дуже низький ризик; низький ризик; помірний ризик; високий ризик; дуже високий ризик) і вибрати план заходів щодо зниження рівня найбільш небезпечних загроз. Використання запропонованої моделі та методу управління ризиками ІТ проекту дасть можливість підвищити якість управління ризиками ІТ проекту, а також дозволить автоматизувати процес інтелектуального управління ризиками, що, зрештою, підвищить оперативність та об'єктивність прийнятих управлінських рішень.

ЗМІСТ

ЗМІСТ 7

ПЕРЕЛІК ВИКОРИСТАНИХ СКОРОЧЕНЬ, ТЕРМІНІВ, ОДИНИЦЬ, ПОЗНАЧЕНЬ 8

ВСТУП 9

1 ТЕОРЕТИЧНІ АСПЕКТИ УПРАВЛІННЯ РИЗИКАМИ ІТ-ПРОЕКТУ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ 11

1.1 ІТ-проект: сутність, поняття 11

1.2 Класифікація ризиків ІТ-проекту 15

1.3 Визначення принципів нечіткої логіки 21

1.4 Проблематика та постановка завдання 29

2 РОЗРОБКА МОДЕЛІ ТА МЕТОДУ УПРАВЛІННЯ РИЗИКАМИ ІТ-ПРОЕКТУ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ 31

2.1 Визначення характеристик ризиків та особливостей управління ними 31

2.2 Формалізація ризиків та розробка моделі їх представлення 37

2.3 Особливості формування стратегії управління ризиками ІТ-проекту 42

2.4 Метод управління ризиками ІТ-проекту на основі нечіткої логіки 47

2.4 Вимоги до структури та функціонування системи управління ризиками ІТ-проекту на основі нечіткої логіки 53

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА АПРОБАЦІЯ МЕТОДУ ТА МОДЕЛІ УПРАВЛІННЯ РИЗИКАМИ ІТ-ПРОЕКТУ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ . 59

3.1 Вимоги до вхідних та вихідних даних додатку для підтримки процесів управління ризиками ІТ-проектів на основі нечіткої логіки 59

3.2 Проектування та розробка додатку для підтримки процесів управління ризиками ІТ-проектів на основі нечіткої логіки 61

3.3 Верифікація результатів дослідження 65

ВИСНОВКИ 71

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 73

ПЕРЕЛІК ВИКОРИСТАНИХ СКОРОЧЕНЬ, ТЕРМІНІВ, ОДИНИЦЬ, ПОЗНАЧЕНЬ

ІБ	Інформаційна безпека
ІР	Інформаційні ризики
ПЗ	Програмне забезпечення
ALE	Annual Loss Expectancy
ARL	Aceptable risk level
ARO	Annualized Rate of Occurrence
HRL	High risk level
MRL	Middle risk level
RL	Risk level
ROI	Return on Investment
SDLC	Systems development lifecycle
TDD	Test Driven Development

ВСТУП

Актуальність теми дослідження. На сьогоднішній день розробка ІТ-проектів є одним із сегментів ринку, що найбільш активно розвиваються, що продиктовано постійно зростаючим попитом на продукти, які є результатом реалізації подібних проектів. Враховуючи динаміку зростання такого інтересу, що збільшується, до цієї сфери, можна припустити, що ця тенденція буде тільки збільшуватися. Ситуація, що склалася, не залишилася непоміченою інвесторами різних рівнів, які активно вкладають капітали в привабливі напрямки. Це зробило ІТ-сферу зоною високої конкуренції, а це, своєю чергою, диктує постійне нарощування темпу її розвитку.

Внаслідок такої рухливості якісні ІТ-проекти повинні відповідати великій кількості вимог, які можна назвати різноплановими за змістом. Основною з таких вимог є необхідність реалізації проектів у рамках мінімально можливих термінів при досягненні високого рівня ефективності, що є складним завданням. Це продиктовано тим, що практично неможливо точно визначити терміни, потрібні для реалізації таких проектів.

Враховуючи описані особливості, розробки у ІТ-сфері припускають проектну форму діяльності [1]. Також використання проектного підходу пояснюється орієнтацією на іноземний досвід та використання передових технологій.

В Україні ІТ-сфера активно розвивається, займаючи сьогодні далеко не останнє місце у рейтингу країн, які реалізують ІТ-проекти. При цьому процес є у більшості випадків копіюванням іноземних зразків, а не нарощуванням свого власного унікального досвіду, що знижує рівень конкурентоспроможності українських ІТ-фахівців. Як наслідок, найбільш прибуткові проекти реалізуються поза Україною.

Враховуючи рухливість сфери, її постійний розвиток та вихід на якісно нові рівні, наявні дослідження не можна назвати вичерпними [2], чим виправдана актуальність цієї роботи.

Мета та завдання дослідження. Метою дослідження є оптимізація управління ризиками ІТ-проекту на основі нечіткої логіки.

Для досягнення поставленої мети у роботі потрібно виконати такі завдання:

– розкрити методологію управління ризиками ІТ-проекту на основі нечіткої логіки;

– визначити принципи управління ризиками ІТ-проекту;

– сформувати алгоритм управління ризиками ІТ-проекту на основі нечіткої логіки;

– запропонувати метод управління ризиками ІТ-проекту на основі нечіткої логіки;

– виконати реалізацію розробленого методу;

– навести верифікацію результатів дослідження.

Об’єкт та предмет дослідження. Об’єктом роботи виступає процес управління ризиками в ІТ-проєктах.

Предметом є методи та моделі управління ризиками в ІТ-проєктах.

Методи дослідження – математичні: нечітка логіка, статистичні методи, методи представлення знань в системах підтримки прийняття рішень; емпірико-теоретичні: абстрагування, аналіз, синтез, методи математичного моделювання, візуалізація; методи проектування та розробки програмного забезпечення.

Практичне значення. Використання запропонованої моделі та методу управління ризиками ІТ проекту дозволить підвищити якість управління ризиками ІТ проекту, а також автоматизувати процес інтелектуального управління ризиками, що, зрештою, підвищить оперативність та об'єктивність прийнятих управлінських рішень.

Структура роботи. Структура роботи складається з вступу, трьох розділів, висновків, списку використаних джерел та додатку. Загальна кількість сторінок складає 83 сторінки.

1 ТЕОРЕТИЧНІ АСПЕКТИ УПРАВЛІННЯ РИЗИКАМИ ІТ-ПРОЕКТУ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ

1.1 ІТ-проект: сутність, поняття

Створення якісного ІТ-продукту – це, передусім, створення складних систем взаємодії між елементами продукту на всіх етапах життєвого циклу проекту. Завдання проектного підходу у такому разі – забезпечення такої взаємодії на якісно високому рівні з максимальним ефектом. Цей процес значно ускладнюється широким спектром напрямів ІТ-проектів за основною цільовою орієнтацією. Така особливість таких проектів наочно демонструє необхідність докладного аналізу та виділення класифікаційних особливостей.

ІТ-проект – це заплановані та задокументовані роботи, пов'язані зі створенням програмного продукту, модернізацією інфраструктури та впровадженням інформаційних систем.

Сутність ІТ-проектів характеризуються їх особливостями:

- високі ризики зриву термінів;
- перевищення планової трудомісткості;
- дорога реалізація;
- досягнення запланованих цілей які завжди відповідають результатам;
- висока інтенсивність, глибока деталізація календарно-мережевих графіків та ітераційність виконання робіт.

Як правило, організація зацікавлена в реалізації не одного, а кількох непов'язаних між собою ІТ-проектів. Саме тому керування кількома ІТ-проектами – важке завдання, для досягнення якого рекомендується використовувати спеціалізовані методи. Одним із широко застосовуваних формальних апаратів при оптимізації ведення кількох ІТ-проектів є методологія управління програмами ІТ-проектів. За статистичними даними, 70% ІТ-проектів не укладаються у відведені терміни, що призводить до перевищення бюджету проекту, і, як наслідок, невиконання основних заявлених вимог до проекту.

Для зручності аналізу та синтезу проектів, а також систем керування ними безліч різноманітних ІТ-проектів класифікується у відповідності до різних підстав.

У науковій літературі трапляються різні підходи до класифікації проектів [4]. Найчастіше застосовуваною класифікацією є класифікація наведена на рис. 1.1.

ІТ-проекти, як тимчасові підприємства, спрямовані на розробку унікальних продуктів з чітко визначеними рамками реалізації, обмеженнями ресурсів та конкретними показниками якості та концепціями успіху проекту, поділяються на три основні типи: розробка програмного забезпечення та комп'ютерних програм, продуктів для онлайн використання та розробка додатків. Крім характерних класифікаційних ознак виділено такі специфічні напрями класифікації: особливі ознаки класифікації масштабу ІТ-проектів, їхнього територіального поширення та рівня впливу процесу розробки інтерфейсу на проект загалом. Використовуючи цю класифікаційну систему, можна успішно визначити тип ІТ-проекту, що розробляється, що може стати вирішальним пунктом у визначенні методів планування та реалізації таких проектів.

Приклади світової практики проектної діяльності демонструють, що впровадження методологій управління програмами ІТ-проектів може допомогти компаніям збільшити прибуток, знизити витрати на внутрішнє планування, керувати змінами та ризиками, а також зменшити невизначеність при ухваленні інвестиційних рішень. Ці позитивні сторони найкращих практик дуже привабливі для українських організацій. Це особливо привабливо при веденні бізнесу в умовах ринкової невизначеності та необхідності підвищення якості надання послуг при внутрішніх фінансових та кадрових обмеженнях, пов'язаних із кризовими явищами в економіці. [3].

Як свідчить вітчизняна практика, у небагатьох організаціях керівники справді задоволені прибутковістю своєї проектної діяльності. [1]:

– лише 15-20% ІТ-проектів закінчуються вчасно;
– 25-35% ІТ-проектів зазнають невдачі;
– 50-60% ІТ-проектів на 90% перевищують бюджет;

– виконується лише 50-60% вимог до IT-проекту.

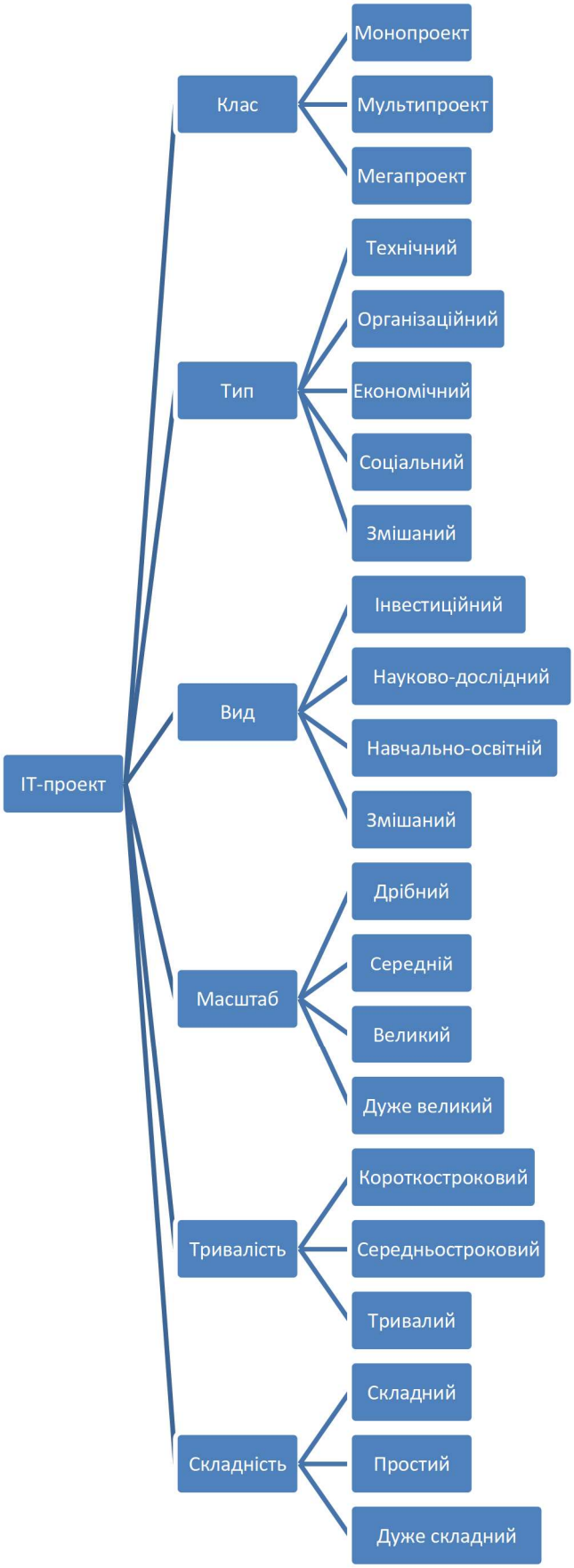


Рисунок 1.1 – Класифікація ІТ-проектів

Причина фіаско — недосвідченість та неправильний підхід до управління програмами ІТ-проектів:

– тотожний підхід до програмного управління ІТ-проектами;

– неякісна обробка вимог клієнтів;

– недостатнє забезпечення ІТ-проектів ресурсами;

– відсутність ітераційності проектів;

– відсутність досвіду попередньої розробки, його накопичення та навички застосування в умовах майбутнього використання;

– відсутність централізованої організаційної одиниці управління.

На прикладі організації, що займається веденням великомасштабних, витратних, довгострокових та міжнародних ІТ-проектів, проведено аналіз з метою розгляду існуючих процедур управління [5]. У результаті аналізу було отримано матеріал, яким визначено недоліки існуючого управління програмами ІТ-проектів:

1. Умови програмного управління проектами реалізовані невідповідним чином.

2. Пріоритети проектів у програмі не синхронізовані між собою та цілями організації.

3. Відсутність повного контролю над ресурсами менеджерів проектів.

4. Невідповідність поставлених цілей, помилки під час аналізу на етапах ініціації та завершення проектів.

5. Відмінності у меті стейкхолдерів.

6. Неточний аналіз ризиків та неправильне реагування на них.

7. Відсутність навичок розподілу ресурсів між проектами.

8. Невміння порівнювати та оцінити взаємовплив проектів.

9. Відсутність моніторингу процесів планування та виконання програми проектів.

10. Відсутність можливості узгодження вимог щодо проектів.

Наявні недоліки не дозволяють організації досягти 100% успішної реалізації IT-проектів. Це призводить до недоотриманого прибутку як мінімум у розмірі 30% від реалізованих проектів (за останні 3 роки).

1.2 Класифікація ризиків IT-проекту

Реалізація сучасних проектів включає збирання, обробку та аналіз великого обсягу інформації. У зв'язку з відстеженням коректного виконання кожного етапу робіт, а також з контролем над термінами виконання та бюджетом проекту при його управлінні та реалізації виникає безліч проблем. На сьогоднішній день використання інформаційних технологій розглядається як обов'язкова умова для ефективного управління підприємством та підвищення його конкурентоспроможності на ринку, а також спрощує кожен етап реалізації проекту [4].

Оскільки будь-який IT-проект є складним технічним та технологічним рішенням, він нерозривно пов'язаний із ризиками. Серед ризиків, зокрема, можна відзначити нерозуміння акціонерами ролі та місця інформаційних технологій, сумніви в окупності IT-проектів, низька ступінь готовності персоналу до використання нових технологій взагалі та інформаційних технологій, зокрема, слабку матеріально-технічну базу багатьох підприємств, яка перешкоджає створенню фундаменту для розвитку інформаційних технологій. Таким чином, вдосконалення методики управління ризиками IT-проектів актуальне з наступних причин:

1. Велика кількість факторів, що швидко змінюються, що впливають на успіх проекту;
2. Вимоги користувачів;
3. Відстеження та застосування нових технологій; ринкова конкуренція; еволюція стандартів;
4. Вимоги до безпеки.

Управління проектами у широкому сенсі– це професійна діяльність, заснована на використанні сучасних наукових знань, навичок, методів,

інструментів та прийомів з орієнтацією на досягнення ефективних результатів. Багато процесів управління проектами поділяється на п'ять груп, кожна з яких складається з декількох процесів. Принципова схема процесу управління проектом наведена на рис. 1.2.

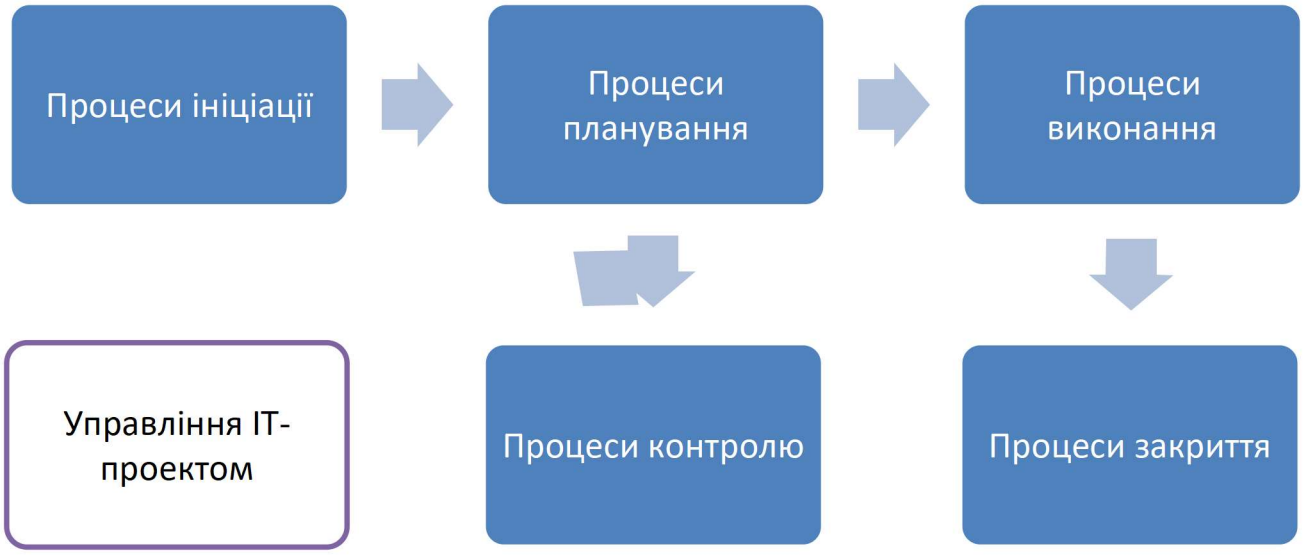


Рисунок 1.2 – Схема процесу управління IT-проектом

Виходячи з вищесказаного, можна зробити висновок про те, що IT-проекти є високо ризиковими [5, 6].

Наявність цих особливостей дає підстави говорити про необхідність застосування методології управління ризиками реалізації IT-проектів. Управління ризиками має на увазі дії для досягнення цілей. У разі реалізації IT-проекту метою є здавання якісно виконаного проекту, який не виходить за рамки бюджету, тимчасових термінів, а також не виходить за рамки обумовленого раніше проекту [3]. Основна класифікація ризиків для IT-проектів наведена на рисунку 1.3.

З описаної раніше класифікації ризиків можна зробити висновок: основні ризики, як правило, характерні для будь-яких IT-проектів, полягають у недотриманні термінів реалізації проекту, перевищенні вартості та недотриманні

параметрів якості [1]. Проте основною причиною виникнення цих ризиків, особливо у IT-проектах, є неготовність підприємства до реалізації таких проектів.

Рисунок 1.3 – Основна класифікація ризиків для IT-проектів [7]

Реалізація IT-проекту не є лінійним процесом. Всі його етапи взаємопов'язані і після майже кожного з них може виявитися необхідність повернення до попереднього. Відповідно до різноманітних джерел виділяється 6 основних процедур управління ризиками, які можна адаптувати до специфіки IT-проектів. На рис. 1.4 представлений життєвий цикл управління ризиками IT-проектів.

Розглянемо кожен із етапів циклу докладніше:

1. План управління ризиками – вибір підходів та інструментів планування для управління ризиками проекту.

2. Ідентифікація ризиків - ідентифікація ризиків, які мають вплив на функціонування проекту, документування їх характеристик.

3. Якісна оцінка ризиків – проведення аналізу ризиків та умов, за яких вони виникають, для визначення їх впливу на успішність проекту та його реалізацію .

4. Кількісна оцінка – аналіз ймовірності ризику та його впливу на проект.

5. План реагування на ризики – визначення процедур і методів пом'якшення несприятливих наслідків подій ризику та використання можливих переваг, які були виявлені.

6. Моніторинг та контроль ризиків – моніторинг ризиків, визначення залишкових ризиків, впровадження планів управління ризиками проекту та оцінка ефективності заходів щодо мінімізації ризиків.

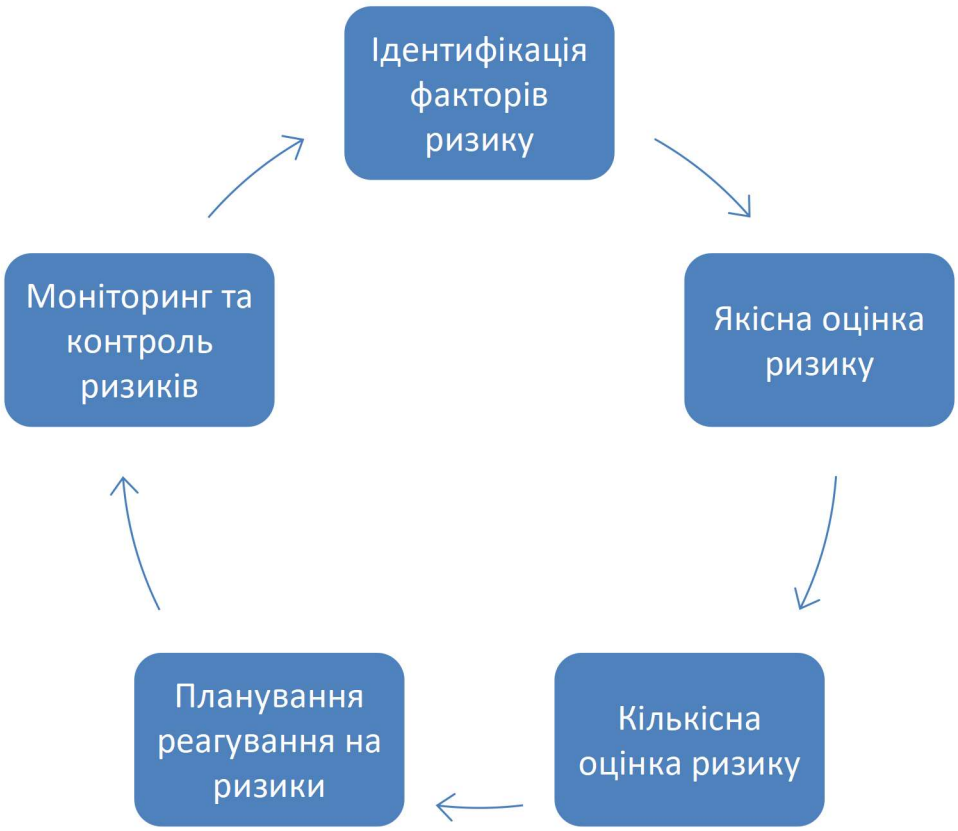


Рисунок 1.4 – Структура процесу управління ризиками IT-проекту [7]

Існуючі методології управління ризиками IT-проектів. Не існує очевидних правил, які стверджують, у якому конкретному випадку слід застосовувати ту чи

іншу методологію управління IT-ризиками. Щодо українських компаній ситуація ускладнюється обмеженнями вітчизняних програмних продуктів, призначеними для оцінки та управління IT-ризиками. Більшість їх базуються не так на методологіях управління IT-ризиками, але в стандартах інформаційної безпеки, тому дозволяють визначити рівень IT-ризиків, а ступінь відповідності тому чи іншому стандарту.

Розглянемо позитивні та негативні аспекти кожної із систем [2]. Коротка характеристика представлена у табл. 1.1.

Таблиця 1.1 – Переваги та недоліки існуючих систем управління IT-ризиками

Назва	Переваги	Недоліки
OCTAVE	власники інформації беруть активну участь у процесі визначення критично важливих інформаційних активів та пов'язаних з ними ризиків; гнучкість, адаптація під потреби конкретного підприємства	оцінка очікуваної шкоди, без оцінювання її ймовірності; відсутність кількісної оцінки;
CRAMM	універсальний інструмент; проведення обстеження інформаційної системи та видача супровідної документації на всіх етапах реалізації; проведення аудиту відповідно до стандарту Code of Practice for Information Security Management BS7799; розробка політик безпеки та планів забезпечення безперервності бізнесу	спеціальна підготовка та висока кваліфікація аудитора; процес займає багато часу і може зайняти місяці безперервної роботи аудитора; відсутність можливості створювати власні шаблони звітів або модифікувати наявні; можливості додавання доповнень до бази знань CRAMM недоступні для користувача, що створює особливі труднощі в адаптації до потреб конкретної організації; висока вартість ліцензії
CORAS	інформаційні системи представлені як складний комплекс з урахуванням людського фактору, а не тільки на основі використовуваних технологій; безкоштовне користування.	не передбачено періодичність проведення оцінки ризиків та оновлення їх величин; не дозволяє оцінити ефективність інвестицій, вкладених у

Назва	Переваги	Недоліки
RiskWatch	багатофазова перевірка; методика перевірки даних; критерії для оцінки та управління ризиками: «передбачення річних втрат» (Annual Loss Expectancy – ALE) та оцінка «повернення від інвестицій» (Return on Investment – ROI)	аналіз ризиків лише на рівні програмно-технічного захисту без урахування організаційно - адміністративних чинників; отримана оцінка ризику (математичне очікування збитку) не вичерпує розуміння ризику з системної точки зору. Цей метод не розглядає комплексного підходу до інформаційної безпеки; ПЗ RiskWatch доступне лише англійською мовою; висока вартість ліцензії
		впровадження заходів безпеки; не дозволяє знайти необхідний баланс між заходами, спрямованими на запобігання, виявлення, виправлення або відновлення інформаційних активів.

Продовження таблиці 1.1 – Переваги та недоліки існуючих систем управління ризиком

Для оцінки IT-ризиків, розробки заходів реагування на ризики, розрахунок прийнятного залишкового ризику корисно спиратися на відповідну методику управління IT-ризиками. Існує кілька методологій управління IT-ризиками, з яких до основних відносять OCTAVE, CRAMM, CORAS, RiskWatch. У кожній з методик можна виділити загальні кроки боротьби з IT-ризиками:

1. Ідентифікація загроз ресурсів та можливих вразливостей.
2. Угруповання щодо загроз або впливів з метою мінімізації обсягу роботи з аналізу ризиків.
3. Вимірювання ризиків.
4. Отримання звіту та обговорення результатів із замовниками.
5. Коригування за результатами обговорення.

1.3 Визначення принципів нечіткої логіки

Компанії стикаються з питаннями ефективного планування виробництва та потреб у ресурсах для забезпечення гарного результату функціонування. Сучасні IT-рішення дозволяють вирішувати ряд завдань, пов'язаних з управлінням виробництвом та логістикою.

Багато компаній задаються питанням «чи є загальне IT-рішення?», що підходить для всіх, оскільки практично кожна виробнича організація працює за своєю індивідуальною схемою. Звичайно, кожне підприємство, має свої особливості, проте вони об'єднані процесним типом виробництва. Це означає, що необхідно при плануванні ланцюжків поставок і автоматизації управління враховувати ряд особливостей: безперервний характер основних процесів, наявність технологічно складних бізнес-процесів, наявність паралельних виробничих ланцюжків і робота з ресурсами.

Також для будь-якої виробничої компанії є актуальним завдання планування. У зв'язку з цим власники або менеджери малих виробництв використовують недорогі та гнучкі IT рішення для управління та прийняття мобільних завдань на своїх підприємствах. Здебільшого використовують додаткові модулі вже встановлених ERP (Enterprise Resource Planning System – Система планування ресурсів підприємства) або беруть комп'ютерні програми для швидких розрахунків. Ця тенденція спостерігається з 2020 року. Впливає як все більша обізнаність, так і криза в SB-секторі (малий бізнес). Використання нечіткої логіки при бізнес-рішеннях в обмежений час стало доступним будь-якому менеджеру.

Нечітка логіка це узагальнення традиційної Аристотелевої логіки на випадок, коли істинність розглядається як лінгвістична змінна, що приймає значення типу: "дуже істинно", "менш істинно", "не дуже хибно" і так далі. Зазначені лінгвістичні значення видаються нечіткими множинами.

У 1965 р. у журналі «Information and Control» була опублікована відома робота Лотфі Заде під назвою «Fuzzy sets». Сприятливим мотивом уявлення Л.

Заде ідеї та теорії нечітких множин стала необхідність опису таких явищ та понять, які мають багатозначний та неточний характер. Відомі раніше математичні методи, що використовували класичну теорію множин і двозначну логіку, не дозволяли вирішувати проблеми цього типу. Практичний потенціал теорії нечітких множин і нечіткої логіки, здатність моделювати гнучкі та неточні обмеження, часткова явність властивостей і плавний перехід від однієї ситуації до іншої добре зарекомендували себе в цій галузі. до За останні два десятиліття було розроблено багато методів і моделей нечіткої математики в розпізнаванні образів, аналізі зображень, експертних системах, системах підтримки прийняття рішень і багатьох інших областях. Нечіткі моделі управління, які знайшли найширше промислове застосування, починаються з побутової техніки (пилососи, пральні машини з нечіткою логікою), керують складними технологічними процесами (контроль доменних печей, атомних електростанцій) і динамічними об'єктами (поїзди метро, а втомобілі, гелікоптери, роботи тощо).

Традиційні інтелектуальні системи, засновані на символічній обробці інформації та булевій логіці, не використовують чисельні методи для врахування невизначеності та неоднозначності, покладаючись на технології жорстких обчислень(hard computing). Тому відповідна комп’ютерна програма є прикладом закритої системи, яку важко модифікувати, де поовна відсутність потенціалу для самоорганізації, співпраці та еволюції складових. Професор Л.Заде у роботі «М'які обчислення, нечіткі множини та нейронні мережі» (1992 р.) одним із перших запропонував варіант побудови гібридних інтелектуальних систем на користь взаємної компенсації різнорідних моделей з компенсацією їх недоліків і поєднання переваг, при цьому в результаті можна отримати синергетичні (нелінійні) ефекти. У структурі м’яких обчислень три виміри інтелекту (управління невизначеністю, навчання та адаптація в еволюційних процесах) досліджуються шляхом подання нечітких моделей виробництва в оптимізованих нейронних мережах з використанням генетичних алгоритмів. На додаток до зазначених компонентів також можливі більш складні гібриди, включаючи хаотичні моделі, еволюційні обчислення, імовірнісний висновок, байєсовські

мережі та їх розширення, моделі навчання тощо. Послідовниками Заде запропоновані такі математичні конструкції як L-нечіткі множини зі значеннями приналежності в дистрибутивній решітці, R-нечіткі множини з інтервальними значеннями приналежності в кожній точці, імовірнісні множини, нечіткі множини, нечіткі множини. Водночас, успішно застосовуються й (у тому чи іншою мірою) альтернативні підходи – випадкові множини, безперервні логіки, теорія свідчень, наближені множини, недовизначені множини.

Розглянемо далі основні поняття, пов'язані з нечіткими множинами:

Лінгвістична змінна - це змінна задача, в якій використовуються лінгвістичні значення, що представляють якісні оцінки або нечіткі числа. Прикладами лінгвістичних змінних є швидкість чи температура, прикладами лінгвістичних значень є ознаки: великі, середні, малі, нечіткі числа Прикладами є: близько 5, близько 0.

Лінгвістична терм-множина — це набір усіх лінгвістичних значень, які використовуються визначення лінгвістичної змінної. Діапазон значень змінної - це безліч всіх числових значень, які може приймати той чи інший параметр досліджуваної системи, або безліч значень, значущих з точки зору задачі, що розв'язується.

Нечіткі множини. Нехай E – множина(універсальна), x – елемент, а R – властивість. Звичайна (чітка) підмножина A універсальної множини E, елементи якого задовольняють властивості R, визначаються як безліч упорядкованих пар $A = \{\mu_A(x)/x\}$ де $\mu_A(x)$ де - характеристична функція, що приймає значення 1, якщо властивість виконується, і 0 інакше..

Відмінність нечіткої підмножини від звичайної полягає у тому, що для елементів x з E немає однозначної відповіді ”так-ні” щодо властивості. Через це, нечітка підмножина універсальної множини E визначається як безліч упорядкованих пар $A = \{\mu_A(x)/x\}$ де $\mu_A(x)$ де – характеристична функція приналежності, що набуває значення упорядкованому множині (наприклад, $M = [0,1]$). Функція приналежності вказує ступінь приналежності елемента x безлічі M.

Безліч M називають безліччю приналежності. Якщо $M = \{0,1\}$, то нечітку множину можна розглядати як звичайну чітку множину.

Безліч елементів простору X, для яких $\mu_A(x) > 0$, називається носієм нечіткої множини A і має позначку $supp\ A$:

$$supp\ A = \{x \in X;\ \mu_A(x) > 0\} \tag{1.1}$$

Визначення висоти нечіткої множини A: $h(A) = \max\{\mu_A(x)\}$

Нечітку множину A називають нормальною тільки, якщо $h(A) = 1$. Якщо A не є нормальною, то її можна нормалізувати за допомогою формули:

$$\mu_{A_N}(x) = \frac{\mu_A(x)}{h(A)} \tag{1.2}$$

де $h(A)$ – висота множини.

Нечітка множина $A \subseteq R$, називається опуклою якщо, тільки для будь-яких $x_1, x_2 \in R$ і $\lambda \in [0,1]$ задовольняється умова:

$$\mu_A[\lambda x_1 + (1-\lambda)x_2] \geq \mu_A(x_1) \wedge \mu_A(x_2) = \min\{\mu_A(x_1), \mu_A(x_2)\}. \tag{1.3}$$

Операції з нечіткими множинами наведено далі.

Увімкнення. Нехай A і B являються нечіткими множинами на універсальній множині E. Кажуть що A втримається в B, якщо $\forall x \in E, \mu_A(x) \leq \mu_B(x)$.

Рівність. Якщо $\forall x \in E, \mu_A(x) = \mu_B(x)$., *то* A і B рівні.

Доповнення. Нехай $M = [0,1]$, A і B – нечіткі множини, задані на E. A і B, якщо $\forall x \in E, \mu_A(x) = 1 - \mu_B(x)$, то вони доповнюють один одного.

Перетин. $A \cap B$ – найбільша нечітка підмножина, що міститься в A і B одночасно:

$$\mu_{A \cap B} = \min(\mu_A(x), \mu_B(x)). \tag{1.4}$$

Об'єднання. $A \cup B$– найбільша нечітка підмножина, що містить всі елементи з A і B:

$$\mu_{A \cap B} = \max(\mu_A(x), \mu_B(x)) \tag{1.5}$$

Різниця. $A - B$– підмножина з функцією приналежності:

$$\mu_{A-B} = \min(\mu_A(x), 1 - \mu_B(x)). \tag{1.6}$$

Нечіткі відносини. Нехай $E = E_1 \times E_2 \times ... \times E_n$ – добуток множин(універсальних) і M – множина приналежностей. Нечітке n-арне відношення визначається як нечітка підмножина R на E, що набуває свої значення в M. Якщо $n = 2$ і $M = [0,1]$ нечітким відношенням R між множинами $X = E_1$ і $Y = E_2$ буде називатися функція $R: (X, Y) \to [0,1]$, що ставить у відповідність кожній парі елементів $(x, y) \in X \times Y$ величину $\mu_R(x, y) \in [0,1]$.

Нехай R_1 – нечітке відношення $R_1: (X \times Y) \to [0,1]$ між X і Y, і R_2 нечітке відношення $R_2: (X \times Y) \to [0,1]$ між Y і Z. Нечітке відношення між X і Z, що позначається як $R_1 \circ R_2$, визначене через R_1 і R_2 виразом $\mu_{R_1 \circ R_2}(x, z) = (\mu_{R_1}(x, y) \wedge \mu_{R_2}(y, z))$ називається композицією відносин R_1 і R_2.

Нечітка імплікація.

Нечітка імплікація є правилом виду: ЯКЩО$(x = A)$ ТО $(y = B)$ де $(x = A)$ - умова, а $(y = B)$ - висновок, причому A і B – нечіткі множини, задані своїми функціями приналежності $\mu_A(x)$, $\mu_B(y)$ та областями визначення X, Y відповідно. Позначається імплікація як $A \to B$.

Відмінність між класичною і нечіткою імплікацією полягає в тому, що у разі класичного дотримання умови та висновки можуть бути як цілком істинними, так і абсолютно хибними, тоді як у нечіткому доступна х часткова істинність, яка належить до інтервалу від 0 до 1.

Насправді дуже мало ситуацій, у яких повністю виконуються умови правила, тому такий підхід має багато переваг. Через це висновки можуть бути не зовсім істинним.

У нечіткій логіці є різні оператори імплікації. Всі вони дають різні результати і ступінь ступінь їх впливу залежить саме від системи, що моделюється. Оператор Мамдані є одним з найпоширенішим. Ґрунтується на припущенні, що істинність заключення $\mu_B(y)$ не може перевищувати ступінь виконання умови$\mu_A(x)$:

$$\mu_{A\to B}(x,y) = \min(\mu_A(x), \mu_B(x)). \quad (1.7)$$

З моменту розвитку штучного інтелекту експертні системи отримали значне визнання як системи підтримки прийняття рішень. Вони здатні акумулювати знання, набуті людиною у різних сферах діяльності. Багато сучасних завдань, особливо адміністративних, можна вирішувати за допомогою експертних систем. Одним із основних методів представлення знань у експертних системах є продукційні правила, які можуть апроксимувати стилі людського мислення. Продукційні правила зазвичай записуються як:

«ЯКЩО (посилка) (зв'язка) (посилка)… (посилка) ТО (висновок)». (1.8)

Нечіткі системи (НС) також засновані на правилах продукційного типу, але використовують лінгвістичні змінні як передумови та висновки правил, що дозволяє уникнути обмежень, властивих традиційним продукційним правилам.

Таким чином, нечітка система - це система з такими описовими характеристиками:

– нечітка специфікація параметрів;
– нечіткий опис вхідних та вихідних змінних системи;
– нечіткий опис функціональності системи, що ґрунтується на продукційних правилах «ЯКЩО…ТО…».

Нечіткі системи управління (НСУ) є найважливішим класом нечітких систем. Одним із найважливіших компонентів НСУ є база знань. База знань є набором нечітких правил «ЯКЩО-ТО», що визначають взаємозв'язок між входами та виходами системи, яка досліджується. Існують різні типи нечітких правил, наприклад, лінгвістична модель, реляційна модель Такагі-Сугено та ін.

Багато застосунків, пов'язаних з керуванням процесами, потребують побудови моделей процесу, що аналізується. Інформація про моделі допоможе вибрати правильний регулятор (модуль управління). Однак побудова правильної моделі часто є складним завданням, яке може вимагати введення спрощень різного ступеня. Обізнаність щодо моделей цих процесів є необхідним для застосування теорії нечітких множин до управління процесами. Все, що потрібно - це формулювання правил дій у вигляді нечітких умовних суджень типу «ЯКЩО-ТО».

Процес, що управляє системою, безпосередньо пов'язаний з вихідними змінними нечіткою системи управління, але результат нечітких логічних висновків є нечітким, і фізичний виконавчий пристрій не може приймати такі команди. Структура нечіткої системи управління зображена на рисунку 1.5

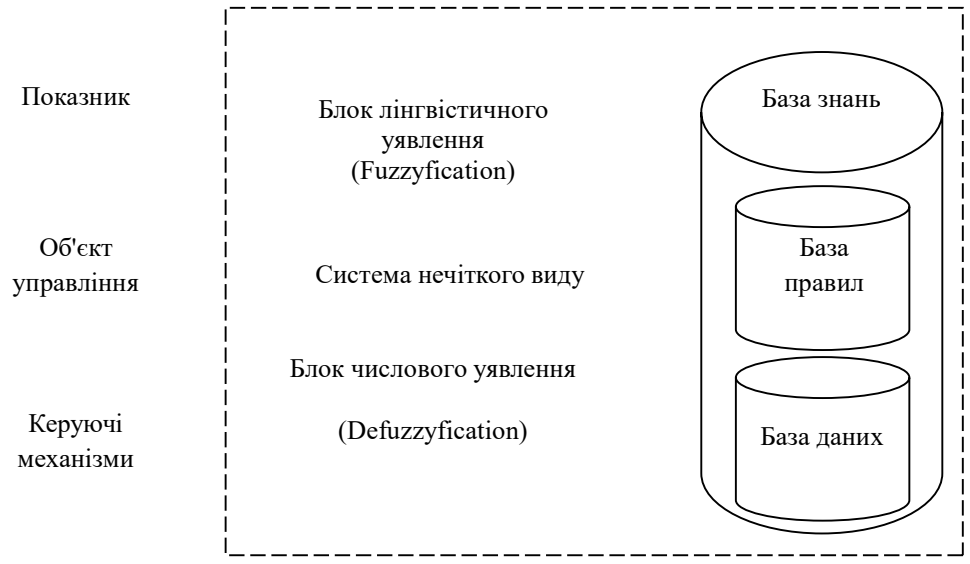


Рисунок 1.5 – Структура нечіткої системи управління

Потрібен спеціальний математичний метод, що дозволяє перейти від незрозумілого значення величини до конкретного значення. Загалом процес нечіткого управління ділиться на кілька етапів. Серед етапів виділяють такі: фаззифікація, розробка нечітких правил і дефаззифікація.

Фаззифікія являє собою перехід до нечіткості. За допомогою певних функцій приналежності, точні значення вхідних змінних перетворюються на значення лінгвістичних змінних.

Терми - значення будь-якої величини, які видаються не числами, а словами природної мови Тобто, значенням лінгвістичної змінної «Терміни» є терми «Довгі», «Короткі» і т. д. Щоб реалізувати лінгвістичну змінну, визначається точне фізичне значення її термів. Наприклад змінна «Терміни» може набувати будь-яке значення від 0 до 30 діб. Відповідно до положень теорії нечітких множин, кожному значенню відстані з діапазону в 30 діб може бути поставлене у відповідність деяке число, від нуля до одиниці, яке визначає ступінь належності даного фізичного значення термінів (наприклад, 5 діб) до того чи іншого терму лінгвістичної змінної. Тоді терміну 30 діб можна задати ступінь приналежності до терму «Довго», що дорівнює 0,85, а до терму «Коротко» – 0,15. Запитуючи, скільки всього термів у змінній необхідно для досить точного уявлення величини прийнято вважати, що достатньо 3-7 діб на кожну змінну для більшості процесів. Більшість застосувань цілком вичерпується використанням мінімальної кількості термів. Таке визначення містить два екстремальних значення (мінімальне та максимальне) та середнє. Що стосується максимальної кількості термів, воно не обмежене і залежить повністю від додатка і необхідної точності опису системи. Число 7 зумовлено ємністю короткочасної пам'яті людини, у якій, за сучасними уявленнями, може зберігатися до семи одиниць інформації.

Приналежність кожного точного значення одного з термів лінгвістичної змінної визначається за допомогою функції приналежності. Її тип абсолютно довільний, але формує концепцію так званих стандартних функцій, що зображені на рисунку 1.6.

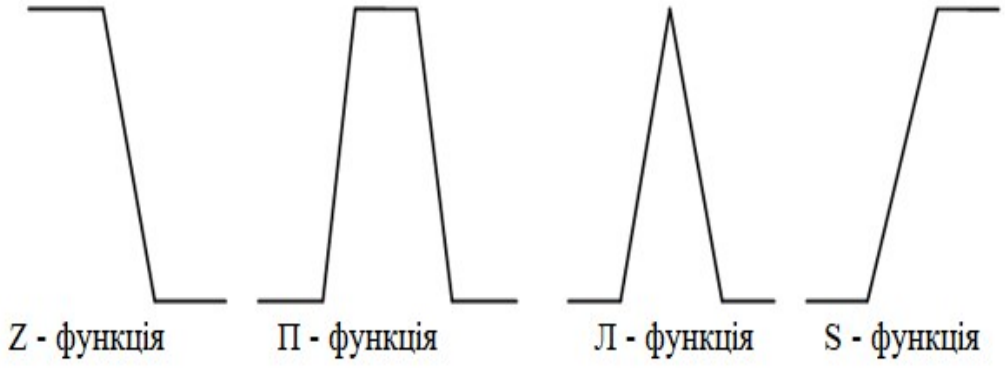


Рисунок 1.6 – Стандартні функції приналежності

Стандартні функції приналежності легко застосовувати до вирішення більшості завдань. Однак якщо потрібно вирішувати специфічне завдання, можна вибрати і більш відповідну форму функції приналежності, за рахунок чого одержати кращі результати роботи системи, ніж під час використання стандартних функцій.

1.4 Проблематика та постановка завдання

Нечітке управління виявляється особливо корисним, коли технологічні процеси надто складні для аналізу за допомогою загальноприйнятих кількісних методів, або коли доступні джерела інформації інтерпретуються неточно, невизначено. Експериментально показано, що нечітке управління дає кращі результати, порівняно з одержуваними при загальноприйнятих алгоритмах управління. Нечітка логіка, на якій засноване нечітке управління, ближче до людського мислення і природних мов, ніж традиційні логічні системи. Нечітка логіка переважно забезпечує ефективні засоби відображення невизначеностей і неточностей реального світу. Наявність математичних засобів відображення нечіткості вихідної інформації дозволяє побудувати модель адекватну реальності.

Деякі переваги fuzzy:

– Уміння працювати з неоднозначними вхідними даними: наприклад, значеннями, які безперервно змінюються в часі (динамічні завдання), значеннями, які неможливо чітко встановити (результати статистичних досліджень, рекламних компаній тощо).

– Можливість неоднозначної формалізації критеріїв оцінки та порівняння: працює з критеріями «більшість», «можливо», «переважно»;

– Можливість виконувати оцінку якості як вхідних даних, так і вихідних результатів: можливість маніпулювання як достовірністю, так і розподілом, а також значеннями даних.

– Можливість швидкого моделювання складних динамічних систем і порівняльного аналізу з певним ступенем точності: оперуючи принципами поведінки системи, описаними fuzzy-методами, по-перше, не витрачається багато часу на з'ясування точних значень змінних та складання описувальних рівнянь, по-друге, можна оцінити різні варіанти вихідних значень.

Метою дослідження є аналіз та виділення особливостей ІТ-проектів з метою розробки моделі та методу управління ризиками ІТ-проектів.

Для досягнення поставленої мети у роботі варто виконати низку завдань:

1. Розкрити методологію управління ризиками ІТ-проекту на основі нечіткої логіки.
2. Визначити принципи управління ризиками ІТ-проекту.
3. Сформувати алгоритм управління ризиками ІТ-проекту на основі нечіткої логіки.
4. Запропонувати метод управління ризиками ІТ-проекту на основі нечіткої логіки.
5. Виконати реалізацію розробленого методу.
6. Навести верифікацію результатів дослідження.

2 РОЗРОБКА МОДЕЛІ ТА МЕТОДУ УПРАВЛІННЯ РИЗИКАМИ ІТ-ПРОЕКТУ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ

2.1 Визначення характеристик ризиків та особливостей управління ними

Розглянемо особливості управління ризиками ІТ-проекту на прикладі підзадачі упраівління ризиками інформаційної безпеки. Цей клас ризиків є важливим елементом у загальному процесі управління ризиками безпеки, який є процесом забезпечення того, щоб позиція ризиків організації знаходилася в прийнятних межах, визначених вищим керівництвом, і складалася з чотирьох основних етапів: оцінка ризиків безпеки, тестування та спостереження, пом'якшення ризиків та операційна безпека [22].

Рисунок 2.1 – Напрямки оцінки ризику ІТ-проекту

Кількісні оцінки ризику інформаційної безпеки використовують математичні формули для визначення коефіцієнта експозиції та очікувану втрату однієї чи кожної загрози, а також ймовірності реалізації загрози, яка називається річною швидкістю виникнення (Annualized Rate of Occurrence, ARO) [22]. Перевагами використання цього підходу є можливість кількісно визначити наслідки виникнення інцидентів, проаналізувати витрати та вигоди при виборі засобів захисту та більш точного визначення ризику. До недоліків можна віднести залежність кількісних показників від їх обсягу та точності шкали вимірювання, неточності результатів, необхідність збагачення якісним описом, велику вартість проведення аналізу, що потребує більшого досвіду та сучасних інструментів.

Особливістю завдань оцінки ризиків інформаційної безпеки та підтримки рівня захищеності ІТ-проектів є те, що більшість даних про фактори ризику мають ознаки недосконалості та невизначеності: суперечливість, неточність, ненадійність чи неповноту, що є нелінійними та динамічно змінними. Останнім часом методи аналізу та оцінки ризиків, які ґрунтуються на елементах нечіткої логіки, розвиваються досить інтенсивно. Такі методи дозволяють змінити наближені табличні методи грубої оцінки ризиків на математичний метод, і навіть значно розширити можливості математичних методів аналізу ризиків [23]. Механізм оцінки ризиків за допомогою нечіткої логіки представляє собою експертну систему. Базу знань в такій системі становлять правила, які відбивають логіку взаємозв'язку вхідних величин факторів ризику та рівнів ризику. Механізм нечіткої логіки передбачає формування рівнів оцінок факторів та подання їх у вигляді нечітких змінних. Процес формування такого виду оцінок у загальному випадку має досить складний характер, оскільки потребує великої кількості джерел інформації, обліку їхньої якості та використання досвіду експертів. Таким чином, на сьогоднішній день сучасним та актуальним є завдання розробки нечітких моделей та методів для оцінки ризиків інформаційної безпеки та підтримки рівня захищеності ІТ-проектів при недосконалості та невизначеності вхідних даних.

Оскільки більшість IT-проектів обробляють та зберігають конфіденційну, особисту та комерційну інформацію стосовно співробітників, замовників, постачальників, перспектив та проектів, подальший розвиток за межами оригінальної схеми додає додатку підвищений ризик порушень безпеки даних та недотримання правил. Спеціальні розробки, як правило, становлять дуже малу частину всієї програми, але оскільки вони отримують доступ і обробляють ті ж дані, що і основна програма, вони становлять значний ризик для безпеки, який може потенційно завдати організації шкоди від порушення безпеки. Етапи управління ризиком IT-проекту наведено на рисунку 2.2.

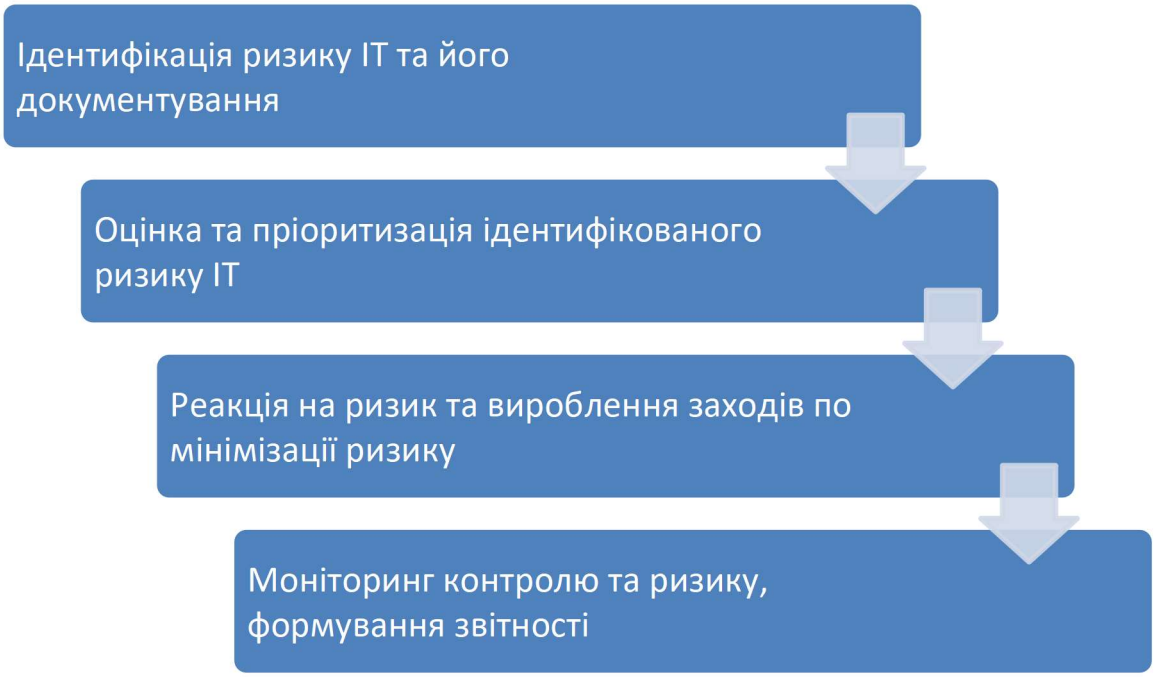


Рисунок 2.2 – Етапи управління ризиком IT-проекту

До основних загроз безпеки IT-систем відносяться навмисні дії порушників, наприклад, злочинців, шпигунів, диверсантів, або скривджених осіб із персоналу організації [24]. Загрози безпеки можуть бути класифіковані за різними ознаками:

– за результатами дій порушників (загроза витоку інформації, загроза модифікації інформації, загроза втрати інформації), за мотивами порушників (ненавмисні; навмисні) та ін., таких як повінь, ураган, землетрус, або пожежа;

- аварії чи техногенні катастрофи;
- збій чи відмови апаратного забезпечення;
- результат помилок при проектуванні та розробці компонентів IT-проекту, таких як апаратне забезпечення, бізнес-процеси, інформаційні технології, модулі та підпрограми, структури даних.;
- помилки в експлуатації системи адміністраторами, користувачами, операторами системи та інших видів персоналу.

Відповідно до нормативних документів у галузі технічного захисту інформації у моделі оцінки ризиків розглядають загрози наступних чотирьох типів відповідно до властивостей інформаційної безпеки:

1. Загрози, пов'язані з несанкціонованим доступом до інформації та загрози порушення конфіденційності інформації.
2. Загрози, пов'язані з несанкціонованою зміною інформації та загрозою цілісності інформації.
3. Загрози, що являють собою загрози, пов'язані з компрометацією можливості використання систем або інформації, що обробляється, а також загрози компрометації доступності інформації;
4. Загрози, що відносяться до порушення можливості спостереження, управління та контролю за діями користувачів, можливості легальністю доступу, можливості та здатності виконувати функції комплексом засобів захисту та становлять загрозу порушення спостережуваності інформації.

При проведенні аналізу негативних наслідків впливу на IT-проект різних видів інформаційних загроз, як правило, розглядаються такі категорії [24]:

- відмова та збої апаратного та/або мережного забезпечення системи, аварійні ситуації та інші події, що відбуваються без участі персоналу;
- ненавмисні чи помилкові дії адміністраторів, користувачів, операторів системи чи інших видів персоналу;
- несанкціонований доступ порушниками інформації, яка формується, обробляється та зберігається в IT-проекті, наприклад, інформація, що дозволяє виконувати управління та прийняття рішень, реалізовувати бізнес-процеси та

технології обробки інформації в ІТ-проекті; виконувати управління обладнанням ІТ-проекту, керування та роботу засобів захисту ІТ-проекту.

Серед найпоширеніших проблем безпеки ІТ-проекту можна зазначити такі загрози:

- затримка оновлень, які необхідні в основному для усунення слабких місць, виявлених у програмному забезпеченні, та встановлення яких є життєво важливим для запобігання можливості використання цих слабких місць;
- недостатній контроль прав доступу, які при неправильному налаштуванні стають потенційними внутрішніми ризиками для системи та загрожують порушенням цілісності та конфіденційності інформації;
- недостатня підготовка персоналу, що працює з системою, особливо це стосується нових працівників, які не мають глибоких знань про внутрішні процеси і помилки яких можуть порушити принципи бізнес-процесів;
- недостатня перевірка персоналу, що має безперешкодний доступ до системних процесів і можливість змінювати функціональність програмного забезпечення ІТ-проекту;
- використання неліцензійних програм, які можуть використовуватися разом з ІТ-проектом для досягнення єдиної мети (наприклад, підтримка даних про продаж в ІТ-проекті, але запуск звітів за допомогою Excel);
- помилки впровадження та конфігурації платформи (налаштування, неправильні облікові дані, відкриті порти і т. д.) ІТ-проекту, що має безліч файлів конфігурації, також можуть потенційно поставити під загрозу процес функціонування та дані;
- недотримання нормативних норм і постанов, призначених для захисту конфіденційної інформації, тягне за собою фінансові та репутаційні наслідки.

У загальному випадку розрахунок ризиків інформаційної безпеки ІТ-проектів повинен проводитися щодо кожного критичного бізнес-процесу і тільки за тими вразливостями, які актуальні для певного бізнес-процесу, причому слід мати на увазі, що ряд уразливостей може бути однаковим для всіх бізнес-процесів.

Кожній уразливості з актуального переліку уразливостей співвідноситься загроза, умовами реалізації якої може бути ця вразливість, а за кожною певною парою проводиться оцінка ймовірності її виникнення та оцінка впливу реалізації цієї пари на цілісність, конфіденційність, доступність та спостережуваність. Під ризиком мається на увазі поєднання ймовірності заподіяння шкоди шляхом подолання системи захисту з використанням уразливостей та тяжкості такої шкоди. Мінімізація ризиків здійснюється за допомогою розробки «політики безпеки» (схеми поведінки) та управління нею. Таким чином, поняття «ризик порушення інформаційної безпеки» має ґрунтуватися на аналізі «причин порушення інформаційної безпеки» та «наслідків порушення інформаційної безпеки». Оцінка ризику у найпростішому випадку виконується за допомогою двох факторів: ймовірність події та тяжкість можливих наслідків.

Як частина бізнес-ризиків підприємства, ризик інформаційної безпеки визначається як добуток втрат (фінансових) від порушення конфіденційності, цілісності, справжності або доступності інформаційних ресурсів (тяжкість наслідків) на ймовірність такого порушення (ймовірність події):

$$R = A * P_e \tag{2.1}$$

де: R – ризик реалізації загрози;

A – фінансові збитки від одноразової реалізації загрози;

P_e – ймовірність події.

Імовірність події (як ймовірність реалізації загрози) може бути об'єктивною або суб'єктивною величиною і повинна враховувати ймовірність загрози та рівень уразливості:

$$P_e = P_t * V \tag{2.2}$$

де: P_e – ймовірність події;

P_t – можливість загрози;

V – рівень уразливості.

Загальносистемний рівень ризику розраховується як сума ризиків за всіма активами та кожною загрозою з урахуванням уразливостей, а ефект від прийнятих контрзаходів – як різниця між сумою запланованих витрат на контрзаходи та сумарною оцінкою збитків за певного загальносистемного рівня ризику.

2.2 Формалізація ризиків та розробка моделі їх представлення

Для побудови моделі розрахунку оцінки ризику пропонується використовувати нечітку продукційну модель, представлену безліччю окремих нечітких продукційних правил виду «якщо А, то В», де А – передумова певного правила, а В – висновок правила у вигляді нечітких висловлювань. Модель призначена для визначення ступеня істинності висновків нечітких продукційних правил. Ступінь істинності визначається на основі передумов з певним ступенем істинності відповідних правил.

До опису факторів ризику застосуємо лінгвістичний підхід. Це забезпечить кількісний опис елементів моделі в умовах нечіткої інформації про значення рівня ризику, вартість ресурсу, вплив наслідків, ймовірність виникнення загрози, уразливість захисту ресурсу та способи уникнення негативного впливу реалізації ризиків. Для оцінки кожного з ризиків пропонується нечітка модель із чотирма вхідними параметрами (X1, X2, X3, X*) та одним виходом Y (структура MISO [24]). Кількість вхідних параметрів обрано до відповідної кількості факторів, що впливають на рівень ризику (5). Таким чином, оцінку ризику можна виразити як:

$$Y = f_Y(X_1, X_2, X_3, X_4), \tag{2.3}$$

де X_1 – цінність ресурсу,

X_2 – вплив наслідків,

X_3 – ймовірність виникнення загрози,

X_4 – виразність ресурсу.

Для підтримки рівня захищеності IT-проекту необхідно визначити, які ризики, відповідно до рівня їх оцінки – risk level (RL), потребують обробки з певними рекомендаціями. Для цього введемо 3 типи рівнів ризиків:

1. Прийнятний ризик – aceptable risk level (ARL) – вважатимемо незначним, обробка такого ризику не потрібна;
2. Середній ризик – middle risk level (MRL) – рекомендований для обробки з метою його мінімізації;
3. Високий ризик – high risk level (HRL) – вважатимемо суттєвим і його обробка обов'язкова.

Визначення типу ризику виконуватимемо наступним чином:

$$RL = \begin{cases} ARL, R_{ij} \in [min_R; Pr_1] \\ MRL, R_{ij} \in [Pr_1; Pr_2]; i \in IR, j \in Th \\ HRL, R_{ij} \in [Pr_2; max_R] \end{cases} \quad (2.4)$$

де: RL – тип рівня ризику;

R_{ij} – ризик і-го ресурсу при реалізації j-ї загрози;

min_R – мінімальне значення оцінки ризику;

max_R – максимальне значення оцінки ризику;

Pr_1 – параметр, максимальне значення оцінки ризику прийнятного типу;

Pr_2 – параметр, максимальне значення оцінки ризику середнього типу;

IR – безліч ресурсів системи;

Th – безліч загроз для системи.

Максимальне значення оцінки прийнятного та середнього ризику (Pr_1 та Pr_2 відповідно) встановлюються експертами.

Для опису лінгвістичної змінної Y будемо використовувати терм-множину T(Y) з п'яти якісних термів: T(Y) = («Дуже низький ризик» (VLR), «Низький ризик» (LR), «Середній ризик» (MR), Високий ризик (HR) Дуже високий ризик

(VHR). Область визначення EY лінгвістичної змінної Y встановимо на інтервалі [0; 100]. Діапазони інтервалів для спрощення розрахунку можна взяти з кроком 20. Враховуючи обрану область визначення оцінки ризику при визначенні типу ризику для надання рекомендацій щодо його зменшення, будемо використовувати наступні значення: $min_R = 0, max_R = 100$.

Цінність інформації будемо визначати як зв'язок між типом конфіденційності та критичністю – criticality (C) інформації. Оцінка цінності формується як сума балів, що відповідають типу та рівню критичності інформації (табл.2.1). Критичність інформації визначатимемо з огляду на оцінки наслідків порушення властивостей інформації. Для оцінки лінгвістичної змінної X_1 «Цінність ресурсу» використовуватимемо терм-множину T (X_1) з трьох якісних термів: T (X_1) = (Низька цінність (LW), Середня цінність (MW), Висока цінність (HW)). Область визначення EX_1 лінгвістичної змінної X_1 встановимо на інтервалі [4; 19]. Шкала оцінки рівня цінності для кожної лінгвістичної змінної визначається значеннями 4, 11 та 19 відповідно.

Таблиця – 2.1 Визначення оцінки цінності інформації

Тип інформації	Критичність інформації		(C)
	Незначна (1-3 бали)	Істотна (4-9 балів)	Критична (10-15 балів)
Відкрита (1 бал)	2-4	5-10	11-16
Для внутрішнього використання (2 бали)	3-5	6-11	12-17
Конфіденційна (3 бали)	4-6	7-12	13-18
Строго конфіденційна (4 бали)	5-7	8-13	14-19

Для оцінки лінгвістичної змінної X_3 «Рівень ймовірності загрози» використовуватимемо терм-множину T (X_3) з п'яти якісних термів: T (X_3) = (Дуже низька ймовірність загрози (VLT) Низька ймовірність загрози (LT) Середня ймовірність загрози (MT) Висока ймовірність загрози (HT) Дуже висока ймовірність (VHT)). Область визначення EX_3 лінгвістичної змінної X_3 встановимо на інтервалі [0,05; 365]. Терму VLT відповідає ситуація, коли загроза практично ніколи не реалізується або реалізується не більше ніж 2-3 рази на п'ять років (частота в діапазоні [0; 0,6]). Терму LT відповідає ситуація, коли загроза виникає 1-2 рази на рік (частота в діапазоні [1, 2]). Терму MT відповідає ситуація, коли загроза виникає 1 раз на 2-3 місяці (частота в діапазоні [4, 6]). Терму HT відповідає ситуація, коли загроза виникає 1-2 рази на місяць (частота в діапазоні [12, 24]). Терму VHT відповідає ситуація, коли загроза виникає від 1 разів на тиждень до 1 разу на день (частота в діапазоні [52; 365]).

Під час оцінки лінгвістичної змінної X_4 «Уразливість ресурсу» посилатимемося на загальну систему оцінки вразливостей Common Vulnerability Scoring System (CVSS), що дозволяють записувати ключові характеристики вразливості та створювати числову оцінку, що відображає її критичність [24]. Для отримання якісної метрики уразливостей будемо використовувати систему оцінки Національної бази даних уразливостей National Vulnerability Database (NVD) [12]. У базі даних NVD значення рівня безпеки вразливості обчислюються значеннями від 0 до 10 та описуються лінгвістично термами None, Low, Medium, High та Critical [13]. Відповідно до лінгвістичних терм бази NVD для оцінки лінгвістичної змінної X_4 «Вразливість ресурсу» будемо використовувати терм-множину T (X_4) з чотирьох якісних термів: T (X_4) = (Низька вразливість (LV) Середня вразливість (MV) Висока вразливість (HV) Критична вразливість (CV)). Область визначення EX_4 лінгвістичної змінної X_4 встановимо на інтервалі [0; 10].

У списку наведено оцінки рівня вразливості згідно NVD за балами та лінгвістично, опис наслідків експлуатації та відповідні рівні вразливості ресурсу за терм-множиною T (X_4):

– рівень вразливості LV: рівень за NVD None (уразливість не впливає на ресурс, бал за NVD 0.0) або Low (уразливість, що має незначний вплив на ресурс, не впливає на доступність, цілісність та конфіденційність інформації, бал за NVD 0.1–3.9)

– рівень вразливості MV: рівень за NVD Medium (уразливість, яка може мати певний вплив на ресурс, але має складність реалізації, або не тягне за собою серйозні наслідки; можливий доступ до конфіденційної інформації, зміна деякої інформації, але немає контролю над інформацією, чи масштаби втрат невеликі, відбуваються збої в доступності ресурсу, бал за NVD 4.0-6.9)

– рівень уразливості HV: рівень за NVD High (уразливість, що істотно впливає на ресурс, можливий доступ до конфіденційної інформації, зміна інформації та контроль над інформацією, суттєві збої в доступності ресурсу та зменшення продуктивності, бал за NVD 7.0–8.9)

– рівень вразливості CV: рівень за NVD Critical (вразливість, наслідок експлуатації якої має серйозний вплив на ресурс: повна втрата доступності та цілісності інформації, повне розкриття конфіденційної інформації, бал за NVD 9.0–10.0).

Таким чином, використання нечіткої моделі забезпечує більш гнучку обробку неточних/якісних факторів ризиків інформаційної безпеки та дозволяє перейти до числового уявлення будь-яких якісних характеристик. Запропонована нечітка модель може бути використана як для оцінки конкретних видів ризиків IT-проектів, так і загального ризику. В умовах реального підприємства використання нечіткої моделі передбачає виконання певного блоку підготовчих робіт, як:

- ідентифікувати конкретні об'єкти захисту IT-проекту; скласти перелік загроз та можливих уразливостей;
- скласти перелік актуальних пар загроза / вразливість (з урахуванням особливостей бізнес-процесів);
- виконати оцінку ймовірностей реалізації загрози з використанням зазначеної вразливості;

– виконати оцінку наслідків реалізації загрози, впливу реалізації загрози на цілісність, конфіденційність, доступність та спостережуваність інформації;

– здійснити оцінку ризику реалізації загрози;

– визначити ступінь ризику та дати рекомендації до необхідності його обробки;

– виконати оцінку ризику інформаційної безпеки за активом та бізнес-процесом.

2.3 Особливості формування стратегії управління ризиками IT-проекту

Рівню ризиків приділяється особливе значення, зокрема у класифікації проектів [14; 15; 16]. На ризикованість проекту впливають такі чинники, як рівень новизни в організації, складність проекту, його тривалість, доступність ресурсів, зокрема висококваліфікованих фахівців тощо [17]. Крім того, враховуючи необхідність налаштування ефективної комунікації під час виконання IT-проекту, але його ризикованість може суттєво впливати на використання спотвореної інформації.

Щодо поняття ризику, то загальноприйняті два основні підходи до визначення цього поняття ризику:

Класичний. Представники цього підходу розглядають ризик як можливість виникнення у реалізації інвестицій несприятливих обставин, які можуть викликати зниження його розрахункового ефекту;

Неокласичний підхід. Представники цього підходу розглядають ризик як можливість відхилення величини фактичного інвестиційного доходу (або конкретного умовно-грошового потоку) від очікуваного; чим мінливіша і ширша шкала коливань можливих доходів (потоків), тим вищий ризик, і навпаки.

Трактування такого складного і багатогранного поняття, як ризик, акцентує увагу на суті питання. Ризик – це абстрактна "невизначеність" чи "ймовірність

невдачі". Традиційно для оцінки інтервалів змін випадкових величин, вироблення гіпотез щодо законів їх розподілу, а також обліку та оцінки кореляційних зв'язків між цими змінними використовують статистична інформація, експертні оцінки, методи імітаційного моделювання, а також аналогові методи. При використанні статистичних та аналітичних методів фахівці стикаються з тим фактом, що ринкова невизначеність не має статистичної природи. Використання аналогових методів не дає потрібної чіткості отриманих даних, а при аналізі унікальних інноваційних проектів взагалі стає неможливим.

Присутність певних шаблонних елементів загалом не змінює фундаментальні та унікальні характеристики проектних робіт, що, у свою чергу, зумовлює певний ступінь невизначеності щодо кінцевого результату.

Відповідно до положень стандарту P2M, невизначеність є фундаментальною характеристикою проектів [18]. Відповідно до положень міжнародного стандарту ISO 31000: 2009, у найширшому сенсі невизначеність слід розглядати як «стан відсутності інформації щодо розуміння чи знання події, її наслідків чи ймовірності» [18].

За результатами аналізу публікацій [20; 21] були визначені такі основні причини невизначеності: випадковість, наявність взаємосуперечливих тенденцій, зіткнення інтересів, конфліктність ситуацій, неповнота, недостатність інформації про об'єкт, процес, явища, обмеженість, матеріальних, фінансових, трудових та ін. ресурсів при прийнятті та реалізації рішень, неможливість однозначного пізнання об'єкта при існуючому рівні та методах наукового пізнання, а також обмеженість свідомої діяльності людини, відмінності у соціально-психологічних установках, оцінках, поведінці.

Стандарт P2M вказує на можливість отримання успішних результатів за відсутності вжиття заходів щодо управління ризиками [24]. Крім того, ризик є основою для окремої предметної групи управління проектами у стандарті ISO/DIS 21500 [6]. Розуміння необхідності управління ризиками проекту також знаходить широке відображення у науковій літературі [5; 8; 10; 18].

У рамках предметної галузі управління проектами загальноприйнятим є думка про те, що управління проектними ризиками полягає в досягненні цілей проекту шляхом максимізації потенційно позитивних результатів (можливостей) та мінімізації потенційно негативних (загроз) за рахунок коректної ідентифікації, оцінки та контролю ризиків.

Враховуючи вищезазначене, пропонується розглядати ризик у контексті управління IT-проектами як загрозу або невикористання можливості, що може призвести до відхилення від цілей IT-проекту у вигляді отримання збитків, порушення термінів виконання та бюджету, недотримання вимог до заявленого функціоналу тощо. Відповідно, управління ризиками проекту у сфері інформаційних технологій доцільно розглядати як комплекс заходів щодо мінімізації впливу потенційних загроз та посилення впливу можливостей з метою досягнення цілей IT-проекту.

Такі заходи формалізовані як процесів з управління ризиками. Основні положення ризик-менеджменту загалом викладені у стандарті ISO 31000. Стандарт передбачає такі складові процесу управління ризиками, як встановлення контексту для ризиків, ідентифікація, аналіз, оцінка ступеня ризику, модифікація ризику, а також моніторинг та аналіз ризику.

У контексті IT-проектів моделювання може використовуватися для схематичного зображення процесів управління ризиками, відображення істотних параметрів проекту та визначення впливу зовнішніх і внутрішніх факторів на досягнення цілей IT-проекту. При цьому, як зазначалося вище, для IT-проектів характерне перевищення кінцевих термінів та бюджету, що свідчить про недостатньо ефективне управління ризиками. У зв'язку з цим актуальним науково-прикладним завданням є вдосконалення методів та моделей, які використовуються в управлінні ризиками проектів у сфері інформаційних технологій.

На застосування тих чи інших методів та моделей в управлінні ризиками IT-проекту істотно впливає методологія, яка використовується при розробці програмного забезпечення. Застосування методології до управління проектами

дозволяє фіксувати його цілі та результати, визначати час проекту, параметри вартості та якості, а також створювати реалістичний план реалізації.

За даними дослідження Pricewaterhouse Coopers, організації, які використовують ту чи іншу методологію, є ефективнішими порівняно з організаціями, які її не мають.

Внаслідок аналізу сучасних підходів до класифікації методологій управління проектом [28; 29; 30] було виділено дві групи методологій: методології, засновані на життєвих циклах системи (systems development lifecycle – SDLC) та методології стандарти.

Згідно з результатами вже згаданого дослідження Pricewaterhouse Coopers 41% організацій використовує PMBOK, 26% використовують методологію, а 9% виконують проекти з IT-методологіями, до яких були віднесені гнучкі та каскадні методології. Серед гнучких методологій найбільш популярними були Scrum – 43%, розробка через тестування (Lean & Test Driven Development (TDD) – 11% та екстремальне програмування (eXtreme Programming) – 10% [27]. управління ризиками IT-проектів важливим аспектом будь-якої методології критерії успішного виконання проекту, від яких залежать відповідні цільові показники. За результатами опитування [27] було встановлено, що успішність виконання проекту найчастіше визначається за такими критеріями, як задоволення потреб зацікавлених сторін (стейкхолдерів), виконання у межах відведеного часу та виконання в межах бюджету.

В результаті аналізу основних характеристик IT-проектів визначено такі принципи застосування методів та моделей в управлінні ризиками IT проектів у порівнянні з проектами в інших галузях:

– виконання IT-проектів є інноваційною діяльністю, спрямованою на створення унікального інтелектуалоємного продукту, та обумовлює високий рівень невизначеності до кінцевих результатів. У зв'язку з обмеженими можливостями щодо точного планування IT-проектів, доцільно використовувати методи, що передбачають формування резервів часу та коштів у разі несприятливих подій та враховувати їх при моделюванні;

– виконання ІТ-проекту спрямоване на створення нематеріального продукту, що у свою чергу ускладнює формулювання вимог і передбачає їх постійне уточнення. У зв'язку з цим використання методів та моделей в управлінні ризиками ІТ-проекту має враховувати можливість періодичного контролю ризиків та оперативного реагування на них шляхом постійної комунікації між заінтересованими сторонами проекту, а також аналізу інформації та накопичення знань про ризики;

– ІТ-проекти виконуються в умовах постійного розвитку технологій, швидко застарівають, та враховують мінливості очікувань користувачів. У зв'язку з цим важливим аспектом є вжиття заходів для забезпечення своєчасного виконання ІТ-проекту та врахування таких заходів під час використання методів та моделей в управлінні ризиками;

– процес виконання ІТ-проекту залежить від життєвого циклу розробки систем (методології, що використовується під час розробки програмного забезпечення). У зв'язку з цим при виборі методів та моделей в управлінні ризиками ІТ-проектів необхідно враховувати особливості методологій, що використовуються при розробці програмного забезпечення.

Слід зазначити, що процес управління ризиками сам собою багатоваріантний, що зумовлює пошук комплексних рішень щодо підвищення ефективності управління ризиками в проектах. Щодо ІТ-проектів, то для них зазначена проблема є особливо актуальною у зв'язку з відставанням накопичених знань від розвитку технологій та нематеріальними результатами, що обмежують можливості початкового планування та контролю ризиків.

З урахуванням нечіткості вхідних та вихідних даних процесу управління ризиками ІТ-проекту стратегію управління ризиками можна описати схемою на рис. 2.3.

Першим етапом є планування заходів щодо управління ризиками. Далі йдуть виявлення(ідентифікація) ризиків, якісна оцінка ризиків та кількісне оцінювання ризиків. Самец на цих трьох етапах частіше виникають невизначеності, такі як:

– випадковість,

– наявність взаємосуперечливих тенденцій,

– зіткнення інтересів, конфліктність ситуацій,

– неповнота, недостатність інформації про об'єкт, процес, явища,

– обмеженість, матеріальних, фінансових, трудових та інших ресурсів при прийнятті та реалізації рішень,

– неможливість однозначного пізнання об'єкта при існуючому рівні та методах наукового пізнання

– обмеженість свідомої діяльності людини, відмінності у соціально-психологічних установках, оцінках, поведінці

Саме тому для цих етапів доцільно застосовувати нечітку логіку. І останнім етап управління ризиками – моніторинг та контроль ризиків.

Рисунок 2.3 – Етапи управління ризиками ІТ-проекту

2.4 Метод управління ризиками ІТ-проекту на основі нечіткої логіки

Ризик розглядатимемо як можливість виникнення втрат, що випливає зі специфіки тих чи інших видів людської діяльності; можливість прийняття невірних чи неприйняття необхідних управлінських рішень; ймовірність

отримання незапланованих результатів під час здійснення тієї чи іншої діяльності [11].

Для кожного ризику, здатного надати негативний вплив на досягнення мети програмного проекту, необхідно вибрати стратегію або комбінацію стратегій реагування, яка є найбільш ефективною:

- ухилення від ризику,
- передачу ризику,
- зниження ризику,
- прийняття ризику.

Джерелами інформації при виявленні ризиків вважатимемо різні доступні контрольні списки ризиків програмних проектів, які слід проаналізувати на застосування до даного конкретного проекту. Ризики у нових проектах – це, як правило, проблеми завершених та виконуваних проектів. Головними ризиками, які торкаються більшості проектів, є нереалістичні терміни та бюджет, плинність кадрів, роздування вимог, низька продуктивність [12]. Крім основних ризиків, необхідно враховувати і другорядні, властиві проектам з певною специфікою завдань.

Найважливішим етапом управління ризиками є ідентифікація і оцінка, тобто виявлення ризиків, здатних вплинути на проект, та визначення їх характеристик (імовірність настання, можливі несприятливі наслідки, ступінь небезпеки, причина виникнення).

Вхідні дані для завдання управління ризиками програмних проектів, як правило, характеризуються тим чи іншим ступенем невизначеності, обумовлені неповнотою, внутрішньою суперечливістю, неоднозначністю, і є наближені кількісні або якісні оцінки параметрів процесів проектування та управління проектуванням [13].

Отже, оскільки вихідні дані завдання важко формалізуються, доцільно застосувати один із інтелектуальних методів, заснований на нечіткій логіці. Нечіткі алгоритми, що оперують лінгвістичними змінними, значення яких задаються нечіткими множинами, зручні для опису процесів, що слабо

формалізуються. Такі алгоритми інтуїтивно зрозуміліші. Основну увагу при застосуванні методів нечіткої логіки слід звернути на адекватну побудову функцій власності за знаннями експерта.

Система нечіткого висновку перетворює значення вхідних змінних процесу управління вихідні змінні на основі використання нечітких правил.

Процес нечіткого висновку виконуємо за такими етапами.

1. Формування основи правил систем нечіткого виводу.

2. Фаззифікація вхідних змінних (введення в нечіткість). Передбачає окремий етап виконання нечіткого виведення та процедуру знаходження значень функцій належності нечітких множин (термів) на основі звичайних вихідних даних.

За основу взято шматково-лінійну функцію приналежності у формі трапеції:

$$f_T(x,a,b,c,d) = \begin{Bmatrix} 0, & x \le a \\ \frac{x-a}{b-a}, & a \le x \le b \\ 1, & b \le x \le c \\ \frac{d-x}{d-c}, & c \le x \le d \\ 0, & d \le x \end{Bmatrix} \quad (2.5)$$

де a, b, c, d – параметри трапеції, що визначаються в ході опитування експертів;

x – значення лінгвістичної змінної.

В таблиці 2.1 представлено список лінгвістичних змінних,універсуми, одиниці виміру та безліч їх термів.

Таблиця 2.1 – Список лінгвістичних змінних та безліч їх термів

Лінгвістична змінна	Універсум	Одиниця виміру	Безліч термів
Вхідні змінні			

«зміна вимог»	0–30	разів	{дуже низька, низька, середня, висока, дуже висока}
«участь у подібних проектах»	0–100	проект	{дуже мала, мала, середня, велика, дуже велика}

Продовження таблиці 2.1 – Список лінгвістичних змінних та безліч їх термів

Лінгвістична змінна	Універсум	Одиниця виміру	Безліч термів
«недотримання термінів»	0–30	тиждень	{занадто незначне, незначне, помірне, значуще, надто значуще}
«часовий інтервал»	0–180	доба	{незначний, невеликий, помірний, великий, значний}
«число сутностей бази даних»	0 –60	штук	{низька, середня, висока}
«число рядків коду»	0–1000	тисяч рядків	{низька, середня, висока}
«кількість фахівців»	0–60	осіб	{низька, середня, висока}
«число модулів»	0–500	штук	{низька, середня, висока}
«кількість помилок тестування»	0-10000	штук	{дуже низька, низька, середня, висока, дуже висока}
«період командної роботи»	0-120	місяць	{дуже мала, мала, середня, велика, дуже велика }
«кількість несуттєвих завдань»	0–500	штук	{мале, середнє, велике}
«остання комунікація із замовником»	0–365	діб	{недавно, не так давно, давно, надто давно}
Вихідні змінні			
«ризик зриву	0–100	бал	{ні, ігнорований,

проекту»			помірний, критичний, катастрофічний}
«ризик масштабу»	0–100	бал	{ні, ігнорований, помірний, критичний, катастрофічний}
«ризик зриву термінів»	0-100	бал	{ні, ігнорований, помірний, критичний, катастрофічний}
«ризик порушення специфікацій»	0-100	бал	{ні, ігнорований, помірний, критичний, катастрофічний }

3. Агрегування умов у нечітких правилах продукцій. Визначаємо ступінь істинності умов щодо кожного з правил системи нечіткого висновку. Для цього використовуємо одну з можливих операцій – логічну диз'юнкцію або кон'юнкцію нечітких висловлювань А та В:

$$T(A \vee B) = max\{T(A), T(B)\} \quad (2.6)$$

$$T(A \wedge B) = min\{T(A), T(B)\} \quad (2.7)$$

де A, B – нечіткі висловлювання про фактори ризику програмного проекту;

$T(A), T(B)$, $T(A \vee B)$ – значення істинності відповідного нечіткого висловлювання про фактори ризику програмного проекту.

4. Активізація чи композиція підукладень у нечітких правилах продукції.

За ваговими коефіцієнтами для усіх правил нечітких продукцій знаходимо ступінь істинності кожного з підвиходів. З цією метою використовуємо модифікацію методу нечіткої композиції – Min-активизацию:

$$\mu'(y) = min\{c_i, \mu(y)\} \quad (2.8)$$

де $\mu(y)$ – функція приналежності терму, який є значенням деякої вихідної змінної $\omega(y)$, заданої на універсумі Y;

c_i – ступінь істинності підукладень для кожного з правил, що входять до бази правил системи нечіткого висновку;

$\mu'(y)$ – активізована функція приналежності заключення.

За замовчуванням вагові коефіцієнти всіх правил прийняті за одиницю, кожне правило у цій методиці має один висновок.

5. Акумулювання висновків нечітких правил.

Знаходимо функції належності для кожної з вихідних лінгвістичних змінних множини $W = \{w_1, w_2, w_3, w_4\}$. Мета даного етапу - об'єднання або акумулювання всіх ступенів істинності висновків для отримання функції належності кожної з вихідних змінних за формулою

$$\mu_V(x) = max\{\mu_A(x), \mu_B(x)\} \tag{2.9}$$

де V – акумульована безліч нечітких висловлювань А та В про фактори ризику програмного проекту;

$\mu_A(x), \mu_B(x)$ – значення функції належності фактора ризику x універсуму X відповідної нечіткої множини А, В.

6. Дефаззифікація для отримання конкретного числового значення результату.

Для кожної з вихідних лінгвістичних змінних множини $W = \{w_1, w_2, w_3, w_4\}$ знаходимо звичайне значення. Застосовуємо метод центру тяжіння (алгоритм Мамдані) для дефазифікації [14]:

$$y = \frac{\int_{min}^{max} x \cdot \mu(x) dx}{\int_{min}^{max} \mu(x) dx} \tag{2.10}$$

де y – ступінь ризику в діапазоні від 0 до 10 (результат дефазифікації);

x – змінна, що відповідає вихідній лінгвістичній змінній ω;

$\mu(x)$ – функція приналежності нечіткої множини, що відповідає вихідній змінній ω після етапу акумуляції;

min, max – ліва і права точки інтервалу носія нечіткої множини вихідної змінної ω, що розглядається (універсум ризику в інтервалі від 0 до 10).

2.4 Вимоги до структури та функціонування системи управління ризиками ІТ-проекту на основі нечіткої логіки

У ході дослідження ділимо ІТ-ризики на три категорії.

Перша – це ризики, спричинені діями персоналу. Сюди належить управління доступом до ресурсів, забезпечення його у суворій відповідності до виконуваних співробітником функцій та контроль використання ресурсів.

Другий тип – ризики технологічні, куди ставляться збої чи відмови устаткування. У рамках управління цим видом ризиків забезпечується безперервність надання користувачам ІТ-сервісів належної якості.

Третій тип – ризики, пов'язані із використанням нелегального програмного забезпечення. У рамках управління цим видом ризиків забезпечується оптимізація використання програмного забезпечення, запобігання юридичним, технологічним, діловим ризикам.

З позиції системного аналізу рішення завдання управління ІТ-ризиками включає перелік основних етапів, які можна представити у вигляді [20]:

$$CP = \langle DO, CT, CC, CO, A \rangle \tag{2.11}$$

де DO – збирання та передача інформації про систему, а також аналіз системи (ідентифікація).

CT – вибір мети управління. На даному етапі формуються цілі управління та критерії оптимізації керуючого впливу, відповідно до поточного стану об’єкта управління. Зазначимо, що ціль управління може змінюватися відповідно до функціонального стану об’єкта управління.

СС – формування управлінь. Відповідно до цілей управління формуються безлічі допустимих альтернативних управлінь. На даному етапі перевіряється керованість системи при заданих значеннях параметрів та цілях. Якщо процес некерований, то постановнику завдання слід переглянути процедури DO та СТ.

СО – формування оптимальних управлінь. Як правило, процес управління протікає за умов, що обмежують значення керованих змінних та різних критеріїв оптимізації управління. Оптимальне управлінське рішення приймається в умовах багатокритеріальності та за умови керованості системи.

А – видача керуючих впливів на об'єкт керування.

Аналіз представленої моделі функціонування управління ризиками призводить до висновку, що з підвищення ефективності процесу формування управлінь, слід автоматизувати процедури DO, СТ, у вигляді реалізації автоматизованої системи управління ризиками АСУР. Структура системи управління ризиками представлена на рисунку 2.3.

Вихідним об'єктом управління є IT-ризики, які описується у вигляді [31]:

$$x = \langle It, B, I, V, R, P \rangle, \tag{2.12}$$

де It – безліч IT-ресурсів,

B – безліч бізнес-процесів,

I – безліч інцидентів,

V – безліч уразливостей,

R – безліч ризиків,

P – збитки/прибуток.

It описує безліч IT-ресурсів організації:

$$It = (It^1, \dots, It^n) \tag{2.13}$$

$$P(t) = \left(P^1(t), \dots, P^n(t)\right) \tag{2.14}$$

$P^n(t)$ описує прибуток або збитки від IT-ризиків. Фазовий вектор об'єкта $x = \langle It, B, I, V, R, P \rangle$.

$$B = (B^1, ..., B^n), V = (V^1, ..., V^n), R = (R^1, ..., R^n), I = (I^1, ..., I^n) \quad (2.15)$$

B^n описує бізнес-процеси, що спираються на ITресурси.

I^n визначає інциденти, що відбуваються з IT-ресурсами.

V^n описує уразливості, які є у IT-ресурсах.

R^n визначає ризики, виявлені під час аналізу статистики.

$u(t)$ – керуючий чинник, ним є заходи щодо зниження ризиків.

Метою управління є виконання наступної дії:

$$min(Q_t) \quad (2.16)$$

де $Q_t = \sum_{n=1}^{m} P_n(t) \cdot \mu$ – загальні прибутки/збитки, m – кількість IT-ресурсів, μ – рівень значущості кожного ресурсу.

При цьому Qt показує економічну обґрунтованість та доцільність заходів захисту від IT-ризиків. Після оцінки можливої шкоди та ймовірності настання того чи іншого ризику необхідно вибрати найбільш серйозні ризики та працювати з ними. Витрати на запобігання ризику не повинні перевищувати можливу шкоду від нього.

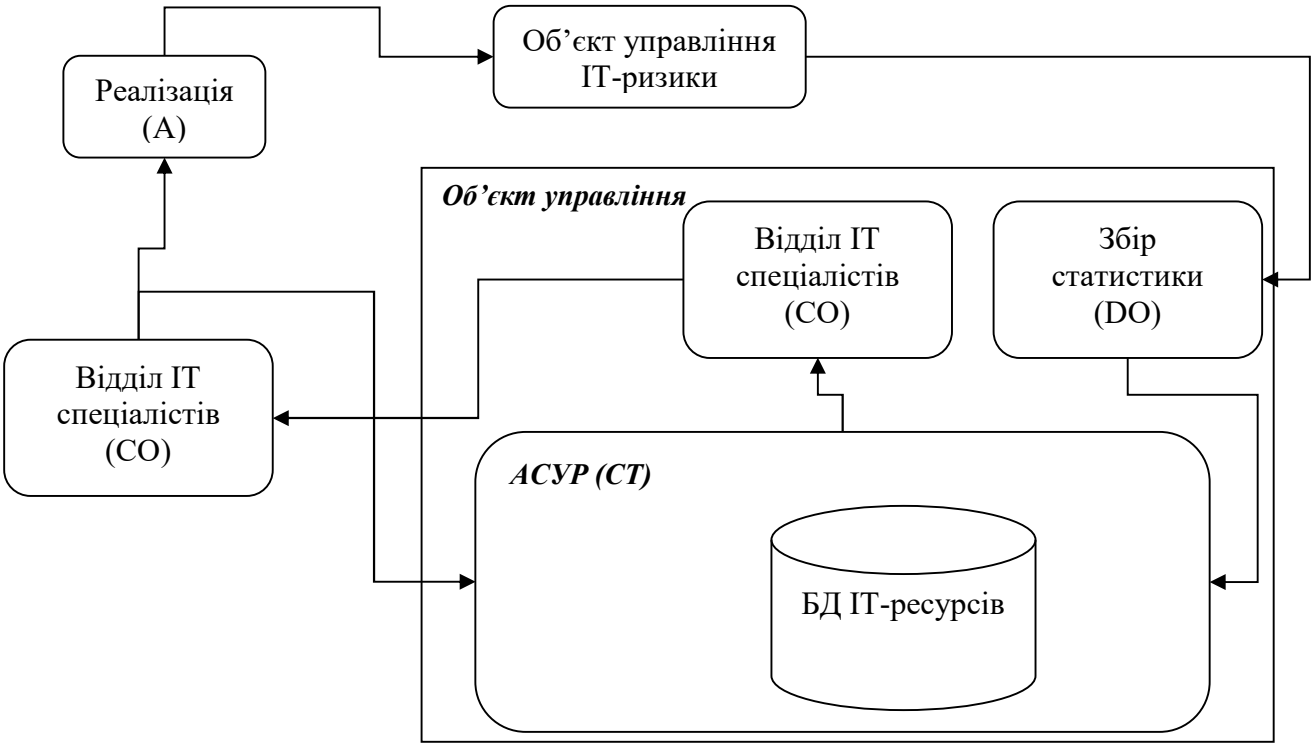


Рисунок 2.3 – Структурна схема системи управління IT-ризиками

АСУ IT-ризиками є системою, що складається з наступних елементів:

- підсистема опису бізнес-процесів;
- підсистема збору статистики;
- інтегруюча підсистема управління ризиками;
- база даних конфігураційних одиниць;
- підсистема перевірки уразливостей;
- АРМ операційного менеджера;
- підсистема аналітики та звітності.

Функціональний склад даних підсистем представлений у таблиці 2.2.

Таблиця 2.2 – Функціональний склад АСУ IT-ризиками

Підсистема	Функції

Підсистема опису бізнес-процесів	побудова дерева бізнес-процесів; опис IT-сервісів, що використовуються для реалізації цих бізнес-процесів; опис вхідних та вихідних даних для бізнес-процесів
Підсистема збору статистики	завантаження інформації з файлу статистики, отриманого при використанні сторонніх програм; зберігання статистичної інформації про зареєстровані інциденти; передача статистичної інформації в підсистему оцінки ризиків та підсистему візуалізації
Інтегруюча підсистема управління ризиками	формування оцінки завантаження анкет із файлу; формування експертних оцінок ризиків у вигляді анкетування; збереження та редагування анкет; планування заходів щодо впливу на ризик
База даних одиниць конфігурації	опис складу конфігураційних елементів IT-інфраструктури організації
Підсистема перевірки уразливостей	завантаження файлу потенційних уразливостей пошук у файлі потенційних уразливостей для елементів бази даних
АРМ операційного менеджера	надання користувачеві можливості координування роботи, відстеження ризикових подій
Підсистема аналітики та звітності	надання IT-спеціалістам статистичної інформації у зручному вигляді

Спроектована модель управління IT-ризиками, відображає тристоронню схильність організацій до ризиків, пов'язаних з експлуатацією інформаційних систем:

– дії персоналу,

– збої систем,

– неліцензійність.

Автоматизована система управління IT-ризиками відповідно до виділених категорій ризиків передбачає:

Для першого виду ризику у системі передбачається можливість проведення анкетування працівників виявлення загрози ризиків.

У рамках управління другим видом ризиків забезпечується завантаження файлу статистичних даних про інциденти в інформаційній структурі підприємства,

завантаження файлу потенційних уразливостей та перевірка конфігураційних одиниць інфраструктури на їх наявність.

Управління останнім видом забезпечується за допомогою зіставлення встановленого програмного забезпечення та наявних ліцензій нею.

Інформація щодо всіх ризиків надходить в інтегруючу підсистему управління ризиками, яка забезпечує оцінку ризиків та планування заходів щодо їх зниження та усунення. Таким чином, автоматизована система управління IT-ризиками дозволить менеджерам на операційному рівні здійснювати процес управління ризиками, відстежувати статистику щодо ризикових подій, що є практично значущим та теоретичним цінним виходом роботи.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА АПРОБАЦІЯ МЕТОДУ ТА МОДЕЛІ УПРАВЛІННЯ РИЗИКАМИ ІТ-ПРОЕКТУ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ

3.1 Вимоги до вхідних та вихідних даних додатку для підтримки процесів управління ризиками ІТ-проектів на основі нечіткої логіки

Процес управління ризиками, враховуючи його трудомісткість доцільно автоматизувати. Нині на українському ринку є понад десяток систем даного класу.

Основними обмеженнями даних систем щодо їх застосування для управління ризиками програмних проектів є [15]:

– орієнтація на ризики інформаційної безпеки;

– необхідність постійного доступу до Інтернету для повсякденного управління ризиками;

– компіляція різних методик оцінки ризиків, що дає специфічно-експериментальний результат.

У зв'язку з цим було прийнято рішення щодо розробки власної програмної системи. Програмна система включає Windows-додаток, що реалізує основний алгоритм роботи. Програмна система представляє сукупність методичних та програмних засобів вирішення наступних завдань:

– формування бази знань, виходячи з думок експертів (анкетування експертів);

– ідентифікація та оцінка ризиків програмних проектів за алгоритмом Мамдані;

– підтримка прийняття рішень щодо реагування на ризики на основі експертних рекомендацій;

– формування звітів щодо виявлених ризиків.

Вхідними даними програмної системи є: ризик-передумови (вимоги замовника програмного забезпечення, інформація про етапи проекту та ін.),

експертні правила та рекомендації, технічне завдання та перелік ризиків програмного проекту.

У якості керуючого впливу виступають розпорядження керівника в ході проекту, стандарт підприємства. Ресурсами та учасниками, що підтримують виконання функцій, є керівник проекту, замовник програмного забезпечення, програмісти, апаратне та програмне забезпечення підприємства.

На виході програмної системи формуються: звіт про поточний стан виконання проекту, оцінка виявлених ризиків та стратегія управління ризиками.

Для побудови моделі знань у вікні редактора структури можна встановити всі лінгвістичні змінні. Під час опитування експерти оцінили нижні та верхні межі кожного терму в діапазоні значень від 0 до 30. Далі розраховані параметри трапецієподібної функції за формулами:

$$a = min(a_j) \tag{3.1}$$

$$b = min\{max(a_j), min(b_j)\} \tag{3.2}$$

$$c = max\{max(a_j), min(b_j)\} \tag{3.3}$$

$$d = max(b_j) \tag{3.4}$$

де a_j, b_j – оцінка нижньої та верхньої межі терму j-го експерта.

При підстановці даних параметрів у формулу отримані графіки функцій приналежності.

Далі задаються конкретні значення вхідних змінних.

Після агрегування умов, активізації підзаключень та акумулювання висновків нечітких правил за формулами отримуємо фігуру на графіку «Ризик зриву проектів».

Для опису значення ризику зриву проекту використовуємо терм-множину T(Y) з п'яти якісних термів: T(Y) = («Дуже низький ризик» (VLR), «Низький ризик» (LR), «Середній ризик» (MR), Високий ризик (HR) Дуже високий ризик (VHR). Область визначення EY лінгвістичної змінної Y встановимо на інтервалі [0; 100]. Діапазони інтервалів для спрощення розрахунку беремо з кроком 20. Враховуючи обрану область визначення оцінки ризику при визначенні типу ризику для надання рекомендацій щодо його зменшення, будемо використовувати наступні значення: $min_R = 0$, $max_R = 100$. Обчислюючи центр тяжкості фігури, визначаємо чисельне значення ризику зриву проекту (перпендикуляр позиції 2 – червона лінія). Приклад візуалізації функції, що описує нечітке значення ризику зриву проекту представлено на рис 3.1.

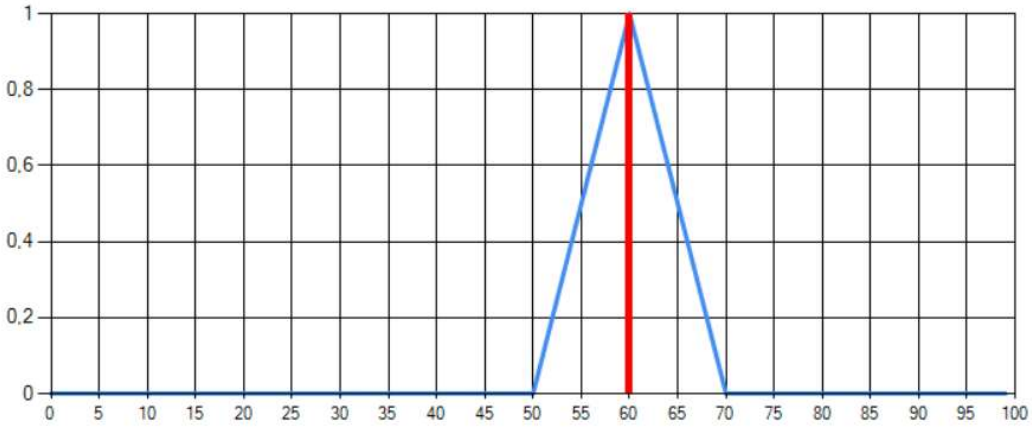


Рисунок 3.1 – Приклад візуалізації нечіткого значення ризику зриву IT проекту

3.2 Проектування та розробка додатку для підтримки процесів управління ризиками IT-проектів на основі нечіткої логіки

Інтерфейс прогрмаи складається з наступних вікон:

– Головне вікно програми;
– Вікно виведення правил;
– Вікно виведення графіків.

Структура інтерфейсу зображена на рисунку 3.2.

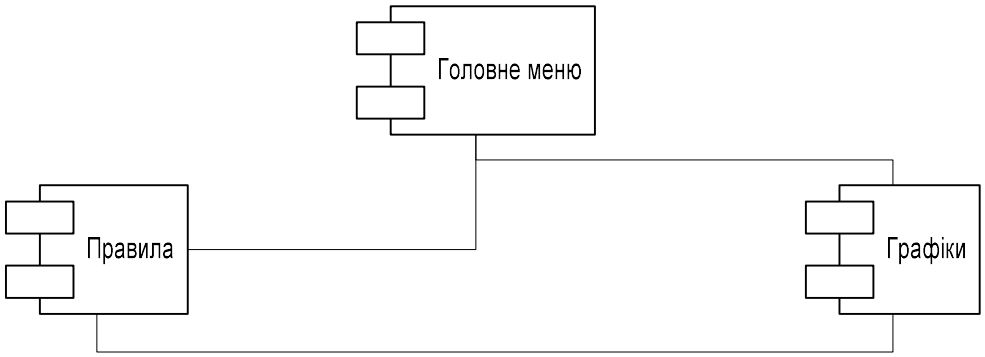


Рисунок 3.2 – Схема інтерфейсу ПЗ для управління ризиками IT проекту

Для реалізації інформаційної моделі проектованої системи програмного комплексу для управління ризиками IT проекту, використовується уніфікована мова моделювання UML. Далі формуються вимоги до системи а також функції та завдання, які необхідно реалізувати та вирішити [15].

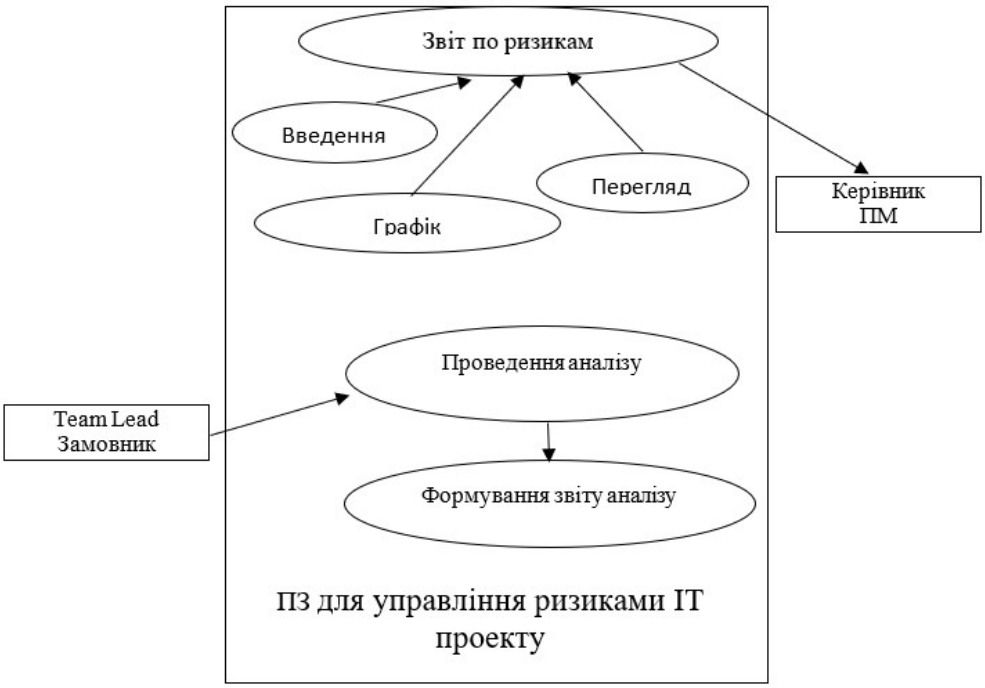


Рисунок 3.3 – Схема варіантів використання ПЗ для управління ризиками IT-проектів

Методи структурного аналізу дуже корисні для аналізу систем та організацій. Однак, методи об'єктно-орієнтованого аналізу дозволяють зручніше передавати інформацію між моделлю аналізованої системи та моделлю ПЗ. Ці методи використовують діаграми варіантів використання як графічної моделі замість діаграм потоків даних. Однак діаграми варіантів використання трохи менш інформативні ніж відповідні діаграми потоків даних. Процеси та сховища об'єднані у прецеденти відповідно до принципів об'єднання даних та тим, як з ними працювати, показуючи лише зв'язки між варіантами використання та дійовими особами. Для надання іншої інформації кожен варіант використання може бути доповнений різним набором діаграм UML (діаграми дій, діаграми сценаріїв тощо).

На основі отриманих даних створюємо систему варіантів використання (рис.3.3).

У процесі роботи із системою працюють два активні об'єкти, один із яких працює з даними (Team lead, замовник), другий — із реальними окремими користувачами (керівник, ПМ).

Рисунок 3.4 – Загальна діаграма діяльності ПЗ для управління ризиками IT проекту

Передбачаються такі варіанти використання системи:

– встановлення початкових значень,

– формування звіту щодо ризиків,

Завданнями програмних модулів програмного комплексу управління ризиками ІТ-проектів є: забезпечення зручного процесу виконання управління ризиками ІТ-проектів. Для вирішення цієї проблеми було розроблено інтерфейс користувача, який забезпечує прозору та інтуїтивно зрозумілу реалізацію управління ризиками ІТ-проектів.

Для розуміння поведінки програмного комплексу управління ризиками ІТ-проектів складемо діаграму діяльності (рис. 3.4).

Модулі, які керують системою, являють собою набір асоціацій між службами та відповідними потребами в ресурсах кожного фізичного досліду управління ризиками ІТ проекту. Загальна структура системи управління ризиками ІТ-проекту на основі нечіткої логіки зображена на рис. 3.5.

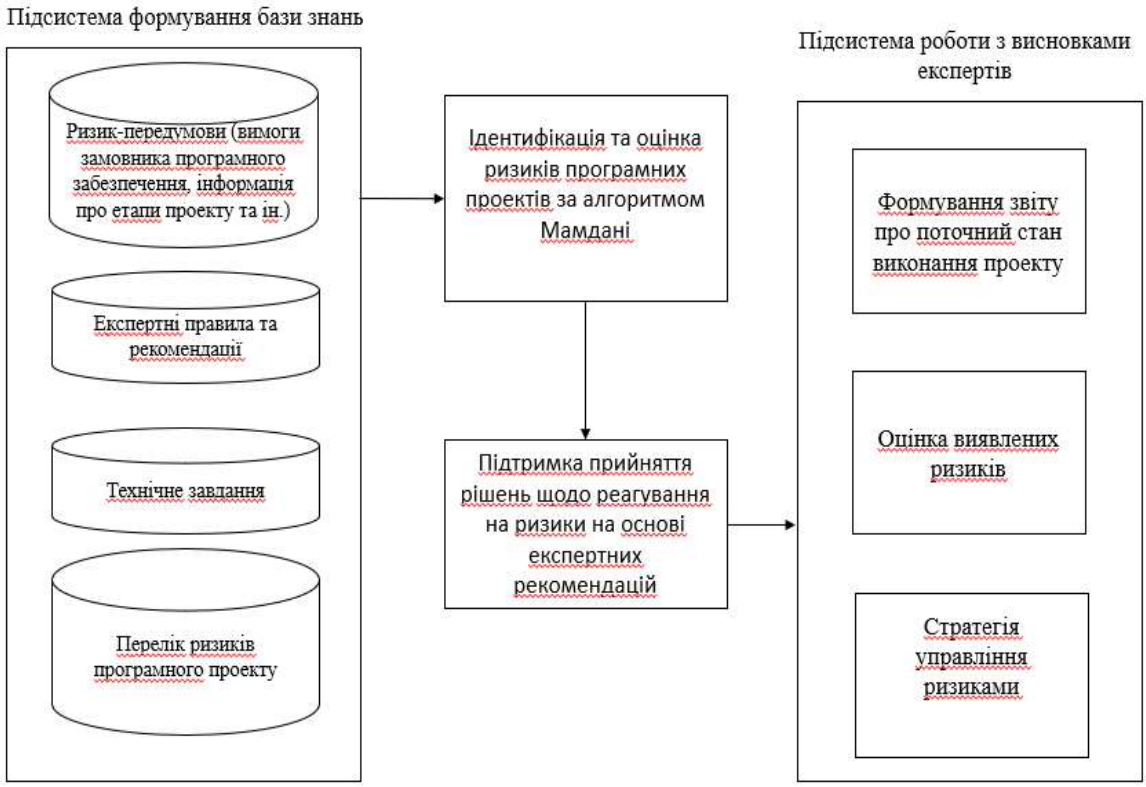


Рисунок 3.5 – Загальна структура системи управління ризиками ІТ-проекту на основі нечіткої логіки

Система управління ризиками ІТ-проекту на основі нечіткої логіки складається з наступних блоків:

1. Підсистеми формування бази знань яка містить: базу ризиків-передумов (вимоги замовника програмного забезпечення, інформація про етапи проекту та ін.), базу експертних правил та рекомендацій, технічне завдання та перелік ризиків програмного проекту.

2. Ідентифікація та оцінка ризиків програмних проектів за алгоритмом Мамдані;

3. Підтримка прийняття рішень щодо реагування на ризики на основі експертних рекомендацій;

4. Підсистема роботи з висновками експертів містить блоки формування звіту про поточний стан виконання проекту, оцінки виявлених ризиків та визначення стратегії управління ризиками.

Дана система має помітну відмінність від інших аналогічних систем, за рахунок того, що розрахована на велике коло користувачів та має можливість виведення графіків на екран та здійснення моделювання експерименту. Тобто кожен бажаючий має можливість скористатися послугами системи та отримати модель експерименту з виведенням на екран графіків.

У запропонованій моделі акцент робиться на запобігання ризику, оскільки зниження ризиків на пізніх стадіях життєвого циклу розробки програмного забезпечення призводить до дорогих і неефективних впливів, що управляють. Цей підхід відрізняється тим, що використовує модель, що базується на профілактичному управлінні ризиками на ранніх стадіях програмних проєктів на основі нечіткого логічного висновку.

3.3 Верифікація результатів дослідження

Проаналізувавши різні методики, програмні продукти та послуги аудиторів доцільно використовувати такі принципи управління ризиками ІТ-проекту:

– провести оцінювання ризиків;

– встановити централізоване управління ризиками;

– запровадити необхідні політики та відповідні засоби контролю для моніторингу стану ризиків;

– сприяти обізнаності співробітників у галузі ризиків проекту;

– контролювати та оцінювати ефективність політики та механізмів контролю та управління ризиками.

Отримані результати забезпечують підхід до подальшої оцінки ризиків та визначають необхідні зміни політики та заходів контролю. Усі ці дії централізовано координуються представниками бізнес-підрозділів та адміністраторами організації. На рисунку 3.6 показано цикл управління ризиками.

Зменшення ризиків передбачає визначення пріоритетів, проведення оцінок та реалізацію відповідних засобів управління скороченням ризиків.

Оскільки повне усунення ризику, як правило, неможливе, вище керівництво організації, менеджери функціональних та бізнес-підрозділів несуть відповідальність за те, щоб реалізувати засоби управління та контролю, що дозволяють знизити ризики до прийнятного рівня, з мінімальним несприятливим впливом на ресурси організації.

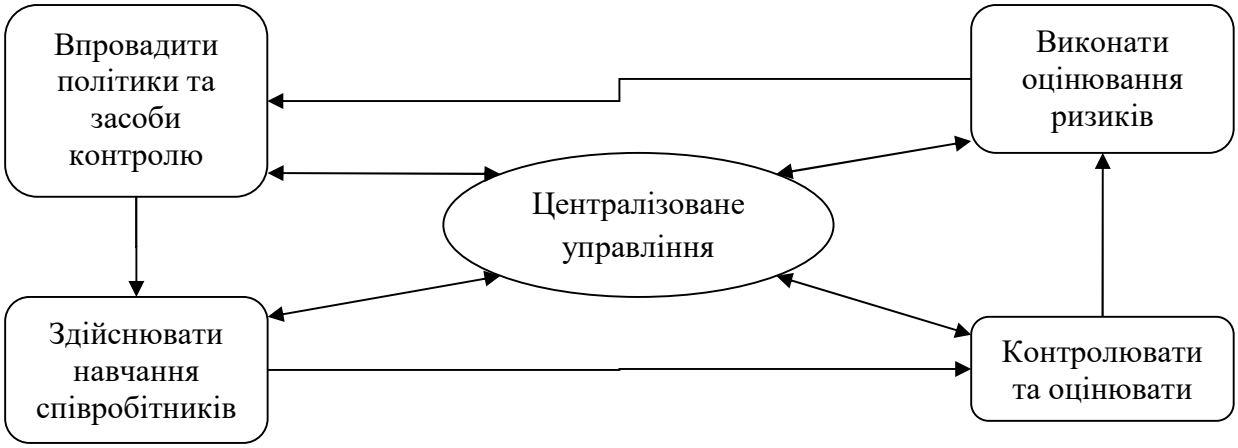


Рисунок 3.6 – Цикл управління ризиками

Зменшення ризиків є послідовною та систематизованою методологією, яка має використовуватися вищим керівництвом для зменшення ризиків.

Зменшення ризиків може бути досягнуто застосуванням будь-якої з наведених нижче опцій щодо зменшення ризику.

1. Прийняття ризику. Приймати потенційний ризик і використовувати інформаційно – телекомунікаційні системи, чи реалізувати засоби управління, дозволяють знизити ризик до прийнятного рівня.

2. Запобігання ризику. Уникати ризиків, усуваючи причину ризику та/або його наслідки (наприклад, утриматися від використання деяких функцій системи або закрити систему, коли ризики повністю ідентифіковані).

3. Обмеження ризику. Обмежувати наявний ризик на основі застосування засобів управління, які мінімізують несприятливий вплив здійснення загрози для вразливості (наприклад, використання підтримуючого, профілактичного чи детективного контролю).

4. Планування ризику. Керувати ризиком шляхом розробки плану дій щодо зменшення ризику, який може передбачати запровадження певних пріоритетів, реалізацію та проведення контролю.

5. Дослідження та повідомлення. Зменшити ризик можливих втрат шляхом повідомлення про наявність вразливості або недоліків системи та дослідження засобів контролю для виправлення вразливості.

6. Перенесення ризику. Переміщення ризику за допомогою інших опцій, щоб отримати компенсації за можливі втрати, наприклад, шляхом страхування інформаційних ресурсів та інформаційних ризиків.

Вибір підходів до оцінки ризиків, який визначається характером діяльності організації, рівнем її інформатизації, а також рівнем зрілості організації.

При реалізації підходів до оцінки та управління ризиками в організації необхідно спиратися, перш за все, на здоровий глузд, існуючі стандарти і методології, що добре зарекомендували себе. Ефективність процесу управління ризиками визначається точністю та повнотою аналізу та оцінки факторів ризику, а

також ефективністю використовуваних в організації механізмів прийняття управлінських рішень та контролю їх виконання.

На рисунку 3.7 зображена реалізація головного вікна додатку управління ризиками IT-проекту. Інтерфейс складається з таких вікон: головне вікно програми; вікно виведення правил; вікно виведення графіків.

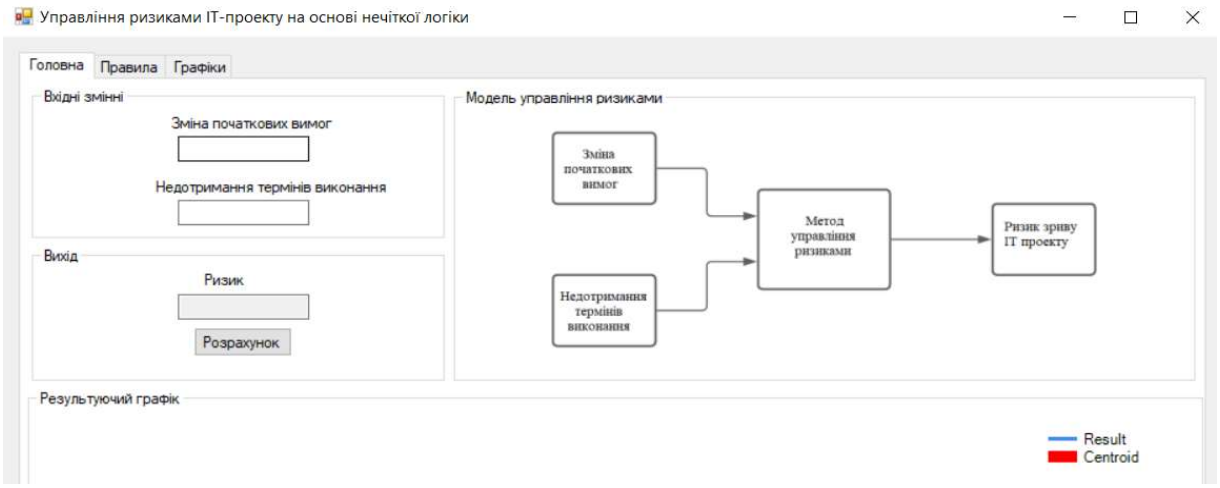
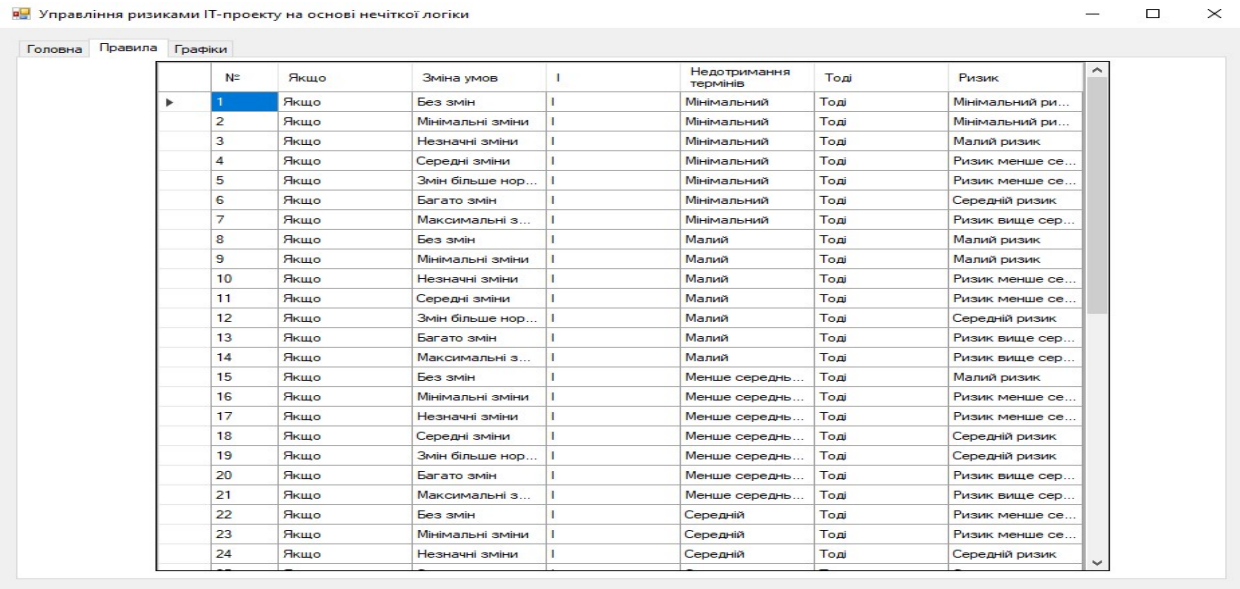


Рисунок 3.7 – Головне вікно додатку

Головне вікно програми містить поля введення початкової інформації, тобто встановлення значень проекту, модель управління ризиками та поле виведення результуючого графіку. Правила та їх значення для визначення рівня ризику зображено на рис. 3.8.

На рис. 3.9-3.10 зображені результати тестування ПЗ для управління ризиками IT проекту. На даних графіках представлено результат роботи. Зображено графіки такі, як різниця початкових та кінцевих умов виконання проекту (VC - Без змін; CD - Мінімальні зміни; CL - Незначні зміни; NR - Середні зміни; LH - Змін більше норми; HT - Багато змін; VH - Максимальні зміни), різниця у термінах виконання(PL – Максимальний; PM – Великий; PS - Більше середнього; NU – Середній; NS - Менше середнього; NM – Малий; NL – Мінімальний), а також ризик зриву проекту за кожним показником (VS - Мінімальний ризик; SL - Малий ризик; LS - Ризик менше середнього; NO -

Середній ризик; LF - Ризик вище середнього; FT - Високий ризик; VF - Максимальний ризик).



№	Якщо	Зміна умов	І	Недотримання термінів	Тоді	Ризик
1	Якщо	Без змін	І	Мінімальний	Тоді	Мінімальний ри...
2	Якщо	Мінімальні зміни	І	Мінімальний	Тоді	Мінімальний ри...
3	Якщо	Незначні зміни	І	Мінімальний	Тоді	Малий ризик
4	Якщо	Середні зміни	І	Мінімальний	Тоді	Ризик менше се...
5	Якщо	Змін більше нор...	І	Мінімальний	Тоді	Ризик менше се...
6	Якщо	Багато змін	І	Мінімальний	Тоді	Середній ризик
7	Якщо	Максимальні з...	І	Мінімальний	Тоді	Ризик вище сер...
8	Якщо	Без змін	І	Малий	Тоді	Малий ризик
9	Якщо	Мінімальні зміни	І	Малий	Тоді	Малий ризик
10	Якщо	Незначні зміни	І	Малий	Тоді	Ризик менше се...
11	Якщо	Середні зміни	І	Малий	Тоді	Ризик менше се...
12	Якщо	Змін більше нор...	І	Малий	Тоді	Середній ризик
13	Якщо	Багато змін	І	Малий	Тоді	Ризик вище сер...
14	Якщо	Максимальні з...	І	Малий	Тоді	Ризик вище сер...
15	Якщо	Без змін	І	Менше середнь...	Тоді	Малий ризик
16	Якщо	Мінімальні зміни	І	Менше середнь...	Тоді	Ризик менше се...
17	Якщо	Незначні зміни	І	Менше середнь...	Тоді	Ризик менше се...
18	Якщо	Середні зміни	І	Менше середнь...	Тоді	Середній ризик
19	Якщо	Змін більше нор...	І	Менше середнь...	Тоді	Середній ризик
20	Якщо	Багато змін	І	Менше середнь...	Тоді	Ризик вище сер...
21	Якщо	Максимальні з...	І	Менше середнь...	Тоді	Ризик вище сер...
22	Якщо	Без змін	І	Середній	Тоді	Ризик менше се...
23	Якщо	Мінімальні зміни	І	Середній	Тоді	Ризик менше се...
24	Якщо	Незначні зміни	І	Середній	Тоді	Середній ризик

Рисунок 3.8 – Правила та їх значення для визначення рівня ризику.

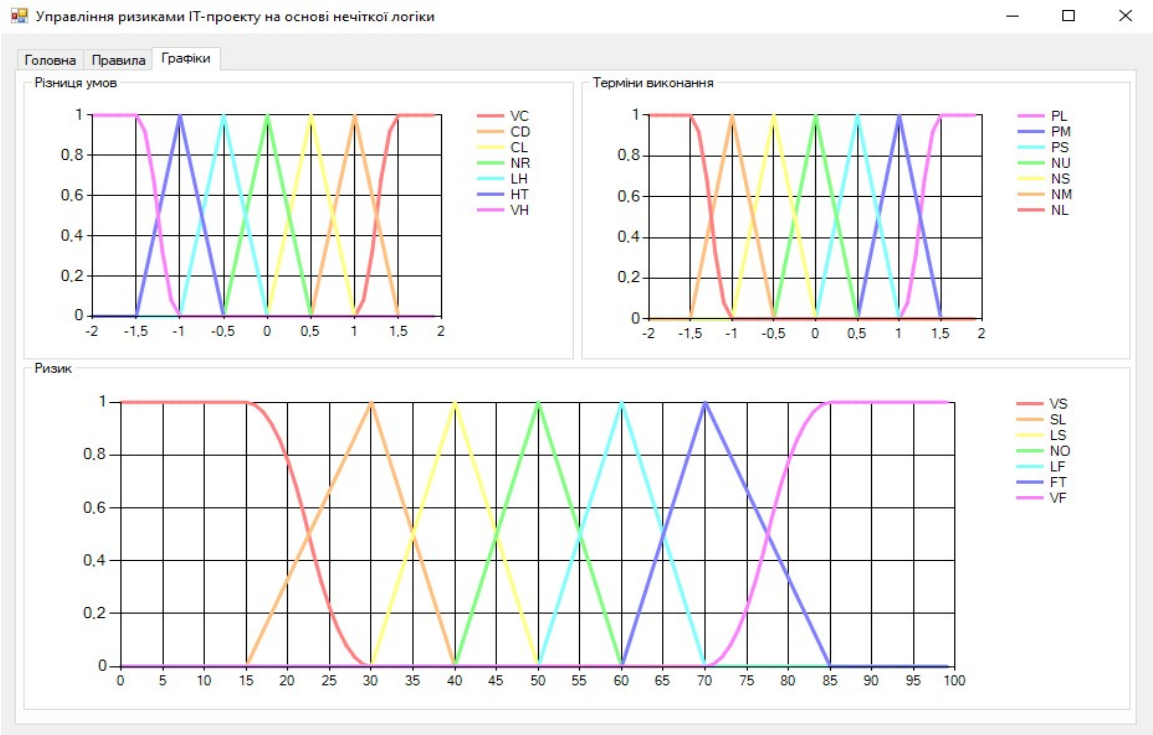


Рисунок 3.9 – Результати тестування ПЗ для управління ризиками IT проекту

Для побудови моделі знань у вікні редактора структури можна встановити всі лінгвістичні змінні. Під час опитування експерти оцінили нижні та верхні межі кожного терму в діапазоні значень від 0 до 30. Далі розраховані параметри трапецієподібної функції.

Далі отримано графіки функцій приналежності та задаються конкретні значення вхідних змінних. Після агрегування умов, активізації підзаключень та акумулювання висновків нечітких правил за формулами отримуємо фігуру на графіку «Ризик зриву проєктів», зображену на рис.3.10.

Обчислюючи центр тяжкості фігури, визначаємо чисельне значення ризику зриву проєкту (перпендикуляр позиції 2 – червона лінія).

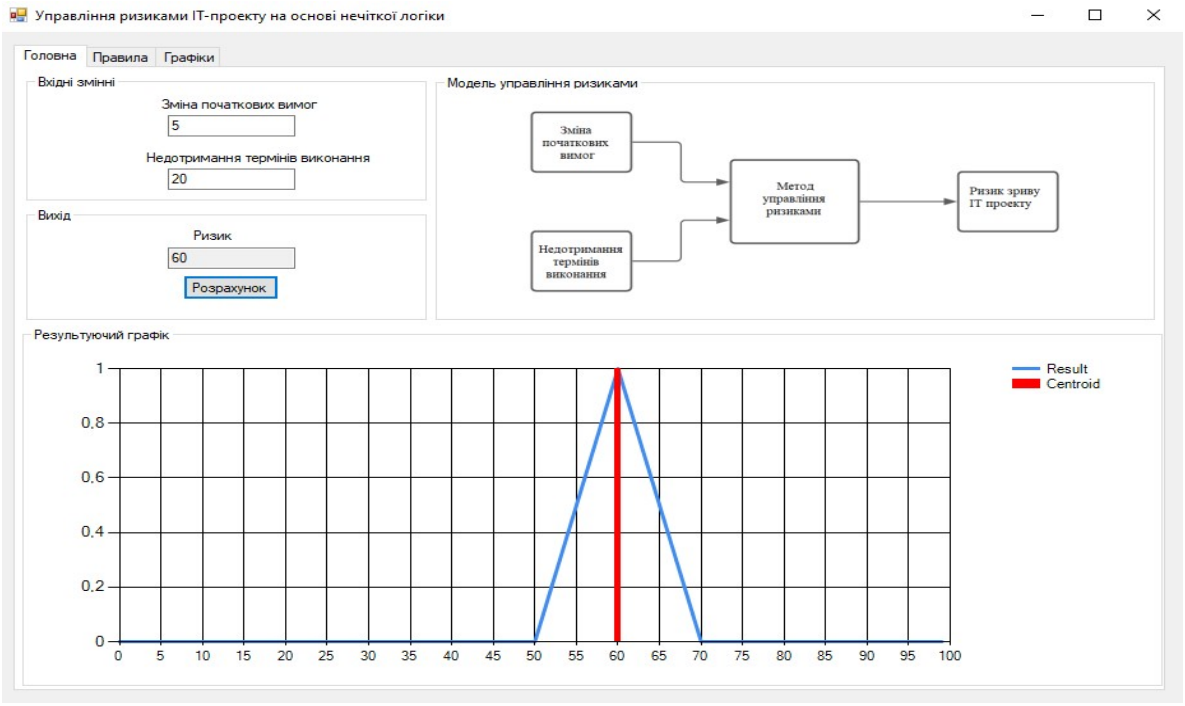


Рисунок 3.10 – Результати тестування ПЗ для управління ризиками IT проекту

Використання програми, що реалізує розроблену модель на основі нечіткої логіки, дозволяє користувачу здійснювати візуальне представлення ризиків у зручній формі з виведенням графіків та моделі управління на екран.

ВИСНОВКИ

Під час виконання даного дослідження здійснено розробку моделі та методу управління ризиками IT-проекту на основі нечіткої логіки та розроблено програмне забезпечення для управління ризиками IT-проектів. На підставі вищевикладеного можна зробити такі висновки:

1. Проведено огляд та аналіз існуючих методів та моделей управління ризиками іт-проекту. Ключовими недоліками використання традиційних підходів є: неможливість оперувати нечіткими вхідними даними: наприклад, значення, які постійно змінюються в часі (динамічні завдання), значення, які неможливо чітко задати (результати статистичних досліджень, рекламні компанії тощо); необхідність великої кількості спостережень для отримання достовірної оцінки ризику; складність залучення незалежних експертів з широким досвідом у домені, що аналізується, та суб'єктивність їх оцінки; орієнтованість на зміни лише одного чинника проекту, що призводить до недообліку кореляції зі всіма іншими чинникам;

2. Визначено принципи управління ризиками іт-проекту.

3. Розроблено модель управління IT-ризиками на основі нечіткої логіки, яка складається з: підсистеми формування бази знань, де формуються експертні правила на основі технічного завдання, формується перелік ризиків програмного продукту; ідентифікації та оцінки ризиків програмних проектів за алгоритмом Мамдані; підтримки прийняття рішень щодо реагування на ризики на основі експертних рекомендацій; підсистема роботи з висновками експертів - інформація щодо всіх ризиків надходить в інтегруючу підсистему управління ризиками, яка забезпечує оцінку ризиків та планування заходів щодо їх зниження та усунення.

4. Розроблено метод управління ризиками іт-проекту на основі нечіткої логіки, який забезпечує більш гнучку обробку факторів ризиків, що дозволяє виявити пріоритети ризиків (дуже низький ризик; низький ризик; помірний ризик; високий ризик; дуже високий ризик) та забезпечити підтримку прийняття рішення

в процесі визначення плану заходів щодо зниження рівня найбільш небезпечних загроз.

5. Використання запропонованої моделі та методу управління ризиками IT проекту дасть можливість підвищити якість управління ризиками іт проекту, а також дозволить автоматизувати процес інтелектуального управління ризиками, що, зрештою, підвищить оперативність та об'єктивність прийнятих управлінських рішень.

6. У моделі акцент робиться на запобігання ризику, оскільки зниження ризиків на пізніх стадіях життєвого циклу розробки програмного забезпечення призводить до дорогих і неефективних впливів, що управляють. Цей підхід відрізняється тим, що використовує модель, яка базується на профілактичному управлінні ризиками на ранніх стадіях програмних проектів на основі нечіткого логічного висновку.

7. Розроблена методика дозволяє автоматизувати процес інтелектуального управління ризиками, що, зрештою, позитивно впливає на оперативність та об'єктивність прийнятих управлінських рішень.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Rahman, Rasha. (2022). Why IT Project Fail. – https://www.researchgate.net/publication/242184301_Why_IT_Project_Fail

2. Проектний менеджмент: управління ризиками та змінами в процесах прийняття управлінських рішень : монографія / О. Б. Данченко, В. О. Занора. – Черкаси : ПП Чабаненко Ю.А., 2019. – 278 с.

3. Sytnyk, V.A., Bulashov, V.V. Methodology for managing the development of it projects with open source/ 5th International conference on Eurasian scientific development in 2018: new methods and solutions». Proceedings of the Conference (September 02, 2018). Premier Publishing s.r.o. Vienna. 2018.46 p. ISBN-13 978-3-903197-73-2

4. Шматковська, Тетяна & Дзямулич, Микола & Стащук, Олена. (2021). Особливості моделювання бізнес-процесів в умовах формування цифрової економіки. Економіка та суспільство. 10.32782/2524-0072/2021-26-66.

5. Aljabali, Rami. (2021). The Importance of Business -Process Optimization for Modern Companies. Economics. 104. 146-152. 10.36962/104/3-5/202101146.

6. Ситник, В.А., Булашов, В.В. Аналогова модель управління IT проектами з відкритим кодом//5-th International Conference on Information technology and interactions (IT&I-2018). Taras Shevchenko National University of Kyiv, November 20-21, 2018.

7. Schindler, E. OSS/Linux Development Survey [Electronic Resource] // Evans Data Corporation Strategic Reports http://evaiisdata.coin/reports/viewRelease.php?reportID=7.

8. Bollier, David. (2022). Why Open Source Software Is Fundamental to a Robust Democratic Culture. – https://www.researchgate.net/publication/42765735_Why_Open_Source_Software_Is_Fundamental_to_a_Robust_Democratic_Culture

9. Teslia, Iurii & Khlevna, Iulia & Yehorchenkov, Oleksii. (2018). Технологічні аспекти реалізації конкретизованої методології управління

проектами. Technical Sciences And Technologies. 128-135. 10.25140/2411-5363-2018-4(14)-128-135.

10. Sazonets, O. & Nykonchuk, V.. (2020). Методологія дослідження процесів інтелектуалізації в сучасній економіці. Bulletin National University of Water and Environmental Engineering. 2. 198. 10.31713/ve2202019.

11. D.Taghiyeva, Khadija & Dadasheva, Aygul. (2021). A multi-criteria decision-making process for project risk management method selection. – https://www.researchgate.net/publication/360626239_A_multi-criteria_decision-making_process_for_project_risk_management_method_selection

12. Nikolopoulos, Kanellos-Panagiotis & Dana, Léo-Paul. (2017). Social Capital Formation in EU ICT SMEs: The Role Played by the Mobility of Knowledge Workers: Social Capital Formation in EU ICT SMEs. European Management Review. 14. 10.1111/emre.12113.

13. Bergman, Annette. (2022). An algorithm for distributing LISP processes / https://www.researchgate.net/publication/35582168_An_algorithm_for_distributing_LISP_processes

14. Muller, Gerrit. (2022). Systems Thinking and Agility; Think Big, Act Small. – https://www.researchgate.net/publication/242517816_Systems_Thinking_and_Agility_Think_Big_Act_Small

15. Zanora V. Integrated management of project-oriented organizations: methodological basis / V. Zanora, V. Lepskyy // European Journal of Economics and Management Sciences, «East West» Association for Advanced Studies and Higher Education. – 2017. – №2. – P. 24–26.

16. Teslenko, P. Increasing probability of successful projects complete / P. Teslenko, S. Antoshchuk V.Krylov // Proceedings of the International Research Conference at the Dortmund University of Applied Sciences and Arts took place on June 30th -July 1st 2017 for the seventh time. 2017. Dortmund : the Dortmund University. P. 28-30

17. Управління проєктами розвитку міжнародного бізнесу: Навчально-методичний комплекс дисципліни [Електронний ресурс]: навч. посіб. для здобувачів другого (магістерського) рівня вищої освіти, спеціальності 073 «Менеджмент», освітньо-професійної програми «Менеджмент міжнародного бізнесу» / КПІ ім. Ігоря Сікорського ; уклад.: А. Р. Дунська, М.О. Кравченко, КПІ ім. Ігоря Сікорського. Київ : КПІ ім. Ігоря Сікорського, 2022. 105 с.

18. Teslenko, P. 3-Level Approach to the Projects Planning / P. Teslenko, S. Antoshchuk, D. Bedrii, H. Lytvynchenko // XIII th International Scientific and Technical Conference «Computer science and information technologies» 11-14 September, 2018. Lviv, 2018. pp. 195-198.

19. Chernova, Lub.S. & Titov, S.D. & Chernova, Lud.S.. (2022). Модельний підхід у методології управління проектами. Transport development. 40-51. 10.33082/td.2021.4-11.04.

20. Сальник В.В., Гуж О.А., Закусіло В.С., Сальник С.В., Бєляєв П.В. Методика оцінки порушень захищеності інформаційних ресурсів в інформаційно-телекомунікаційних системах. Збірник наукових праць Харківського національного університету Повітряних Сил. 2021. № 4(70). С. 77-82.

21. Данчук, К. (2022). Синергетична модель квазіінтелектуальних освітніх інформаційних систем (Віртуальний університет) нового покоління. – https://www.researchgate.net/publication/268361733_SINERGETICNA_MODEL_KVAZIINTELEKTUALNIH_OSVITNIH_INFORMACIJNIH_SISTEM_VIRTUALNIJ_UNIVERSITET_NOVOGO_POKOLINNA

22. Лоскоріх, Габріелла & Грабчук, Ірина & Рогаль, Вікторія. (2021). Облікове забезпечення управління ризиками діяльності ІТ-підприємств. Економіка, управління та адміністрування. 75-80. 10.26642/ema-2021-4(98)-75-80.

23. Leighton, J. Security Controls Evaluation, Testing, and Assessment Handbook / J. Leighton, Syngress, 2018. 678 p

24. Abhishek kumar srivastav, Irman Ali, Shani Fatema. A Quantitative Measurement Methodology for calculating Risk related to Information Security. IOSR

Journal of Computer Engineering (IOSR-JCE). Volume 16 Issue 1, Ver. IX (Feb. 2017), PP 17–20.

25. The Top Project Management Methodologies [Electronic resource]. – Access mode: https:// www.wrike.com/project-management-guide/ methodologies/

26. Moira Alexander. How to pick a project management methodology [Electronic resource]. – Access mode: http://www.cio.com/article/2950579/ p r o j e c t m a n a g e r / h o w - t o - p i c k - a - p r o j e c t - management-methodology.html

27. Victorian Government CIO Council. Selecting a project management methodology [Electronic resource]. – Access mode: https://ofti.org/wpcontent/uploads/2013/08/PM-GUIDE-01-Project-management-methodologyselection-guideline.pdf

28. Department for business innovation and skills. Guidelines for managing projects [Electronic resource]. – Access mode: https://www.gov.uk/ government/uploads/system/uploads/attachment_ data/file/31979/ 10-1257-guidelines-for-managingprojects.pdf

29. . J. Smyrk. What does the term "ITx project" actually mean?: a challenge to the IT profession [Electronic resource]. http://philica.com/display_observation.php? observation_id=36

30. Software Education Group. Project Classification Software [Electronic resource]. – Access mode: http:/ /www.softed.com/assets/Uploads/Resources/ Business-Analysis/Projectclassification. Pdf

ДОДАТОК А ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра інженерії програмного забезпечення

МАГІСТЕРСЬКА РОБОТА

«РОЗРОБКА МОДЕЛІ ТА МЕТОДУ УПРАВЛІННЯ РИЗИКАМИ ІТ-ПРОЕКТУ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ»

Виконала: студентка групи ПДМ-62 Крута Юлія Валеріївна

Керівник: к.т.н., доц., доцент кафедри ІПЗ Золотухіна О.А.

Київ - 2022

МЕТА, ОБ'ЄКТ, ПРЕДМЕТ ДОСЛІДЖЕННЯ

Мета роботи - оптимізація управління ризиками ІТ-проекту на основі нечіткої логіки.

Об'єкт дослідження: процес управління ризиками ІТ-проекту.

Предмет дослідження: метод та модель управління ризиками ІТ-проекту на основі нечіткої логіки.

ЕТАПИ УПРАВЛІННЯ РИЗИКАМИ ІТ-ПРОЕКТУ ТА ПРИЧИНИ НЕВИЗНАЧЕНОСТІ

Основні причини невизначеності в ІТ-проектах, що викликають ризики:

- випадковість,
- наявність взаємосуперечливих тенденцій,
- зіткнення інтересів, конфліктність ситуацій,
- неповнота, недостатність інформації про об'єкт, процес, явища,
- обмеженість, матеріальних, фінансових, трудових та інших ресурсів при прийнятті та реалізації рішень,
- неможливість однозначного пізнання об'єкта при існуючому рівні та методах наукового пізнання
- обмеженість свідомої діяльності людини, відмінності у соціально-психологічних установках, оцінках, поведінці

3

ФОРМАЛІЗАЦІЯ ВХІДНИХ ЗМІННИХ ПРОЦЕСУ УПРАВЛІННЯ РИЗИКАМИ ІТ-ПРОЕКТУ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ

Лінгвістична змінна	Універсум	Од. виміру	Множина термів
«зміна вимог»	0–30	разів	{дуже низька, низька, середня, висока, дуже висока}
«участь у подібних проектах»	0–100	проект	{дуже мала, мала, середня, велика, дуже велика}
«недотримання термінів»	0–30	тиждень	{занадто незначне, незначне, помірне, значуще, надто значуще}
«часовий інтервал»	0–180	доба	{незначний, невеликий, помірний, великий, значний}
«число сутностей бази даних»	0 –60	штук	{низька, середня, висока}
«число рядків коду»	0–1000	тисяч рядків	{низька, середня, висока}
«кількість фахівців»	0–60	осіб	{низька, середня, висока}
«число модулів»	0–500	штук	{низька, середня, висока}
«кількість помилок тестування»	0-10000	штук	{дуже низька, низька, середня, висока, дуже висока}
«тривалість командної роботи»	0-120	місяць	{дуже мала, мала, середня, велика, дуже велика }
«кількість несуттєвих завдань»	0–500	штук	{мале, середнє, велике}
«остання комунікація із замовником»	0–365	діб	{недавно, не так давно, давно, надто давно}

4

ФОРМАЛІЗАЦІЯ ВИХІДНИХ ЗМІННИХ ПРОЦЕСУ УПРАВЛІННЯ РИЗИКАМИ ІТ-ПРОЕКТУ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ

Лінгвістична змінна	Універсум	Од. виміру	Множина термів
«ризик зриву проекту»	0–10	бал	{ні, ігнорований, помірний, критичний, катастрофічний}
«ризик масштабу»	0–10	бал	{ні, ігнорований, помірний, критичний, катастрофічний}
«ризик зриву термінів»	0-10	бал	{ні, ігнорований, помірний, критичний, катастрофічний}
«ризик порушення специфікацій»	0-10	бал	{ні, ігнорований, помірний, критичний, катастрофічний }

5

МАТЕМАТИЧНА МОДЕЛЬ УПРАВЛІННЯ РИЗИКАМИ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ

Функція приналежності нечітких множин (термів) на основі звичайних вихідних даних:

$$f_T(x,a,b,c,d) = \begin{Bmatrix} 0, & x \le a \\ \frac{x-a}{b-a}, & a \le x \le b \\ 1, & b \le x \le c \\ \frac{d-x}{d-c}, & c \le x \le d \\ 0, & d \le x \end{Bmatrix}$$

де a, b, c, d – параметри трапеції, що визначаються в ході опитування експертів; x – значення лінгвістичної змінної.

Способи агрегування умов у нечітких правилах продукцій:

$$T(A \vee B) = max\{T(A), T(B)\}$$
$$T(A \wedge B) = min\{T(A), T(B)\}$$

де A, B – нечіткі висловлювання про фактори ризику програмного проекту;

$T(A), T(B), T(A \vee B)$ – значення істинності відповідного нечіткого висловлювання про фактори ризику програмного проекту.

Спосіб активізації чи композиції підкладень у нечітких правилах продукції:

$$\mu'(y) = min\{c_i, \mu(y)\}$$

де $\mu(y)$ – функція приналежності терму, який є значенням деякої вихідної змінної $\omega(y)$, заданої на універсумі Y; c_i – ступінь істинності підкладень для кожного з правил, що входять до бази правил системи нечіткого висновку; $\mu'(y)$ – активізована функція приналежності заключення.

6

МАТЕМАТИЧНА МОДЕЛЬ УПРАВЛІННЯ РИЗИКАМИ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ (ПРОДОВЖЕННЯ)

Спосіб акумулювання висновків нечітких правил:

$$\mu_V(x) = max\{\mu_A(x), \mu_B(x)\}$$

де V – акумульована безліч нечітких висловлювань A та B про фактори ризику програмного проекту;
$\mu_A(x), \mu_B(x)$ – значення функції належності фактора ризику x універсуму X відповідної нечіткої множини A, B.

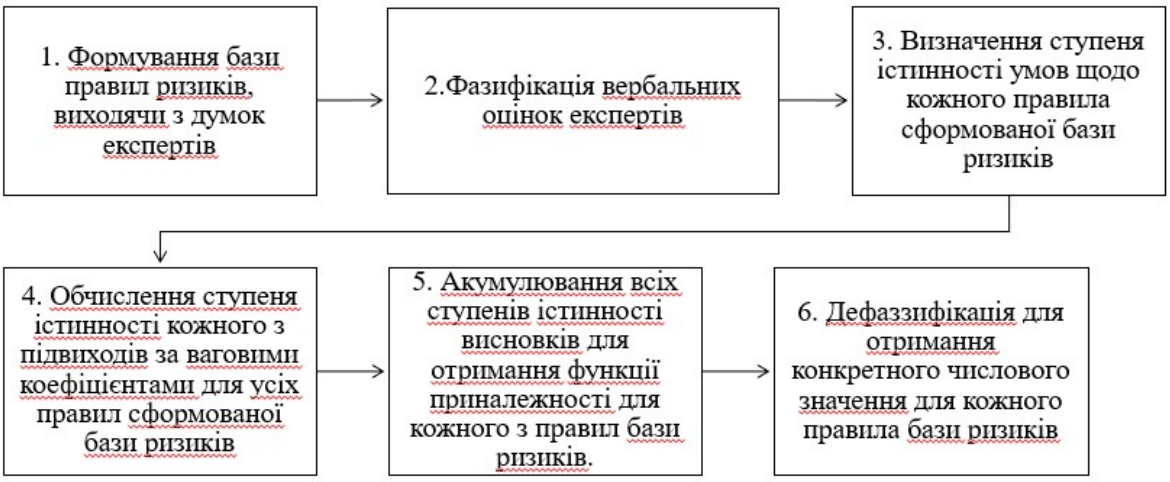
Спосіб дефазифікації:

$$y = \frac{\int_{min}^{max} x \cdot \mu(x)dx}{\int_{min}^{max} \mu(x)dx}$$

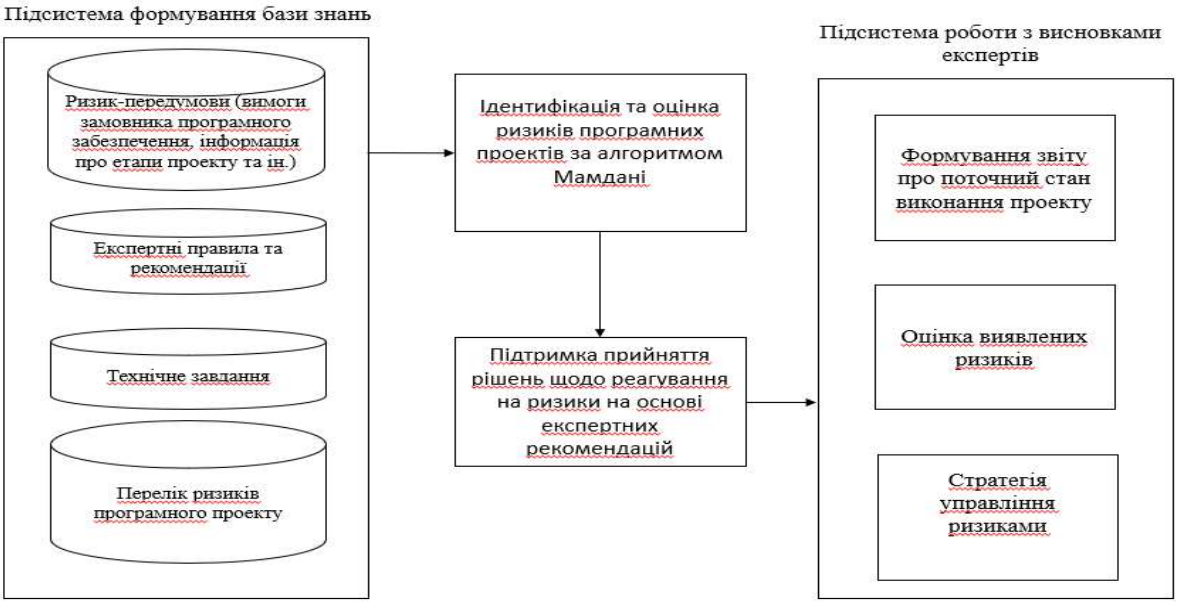
де y – ступінь ризику в діапазоні від 0 до 10 (результат дефазифікації);
x – змінна, що відповідає вихідній лінгвістичній змінній ω;
$\mu(x)$ – функція приналежності нечіткої множини, що відповідає вихідній змінній ω після етапу акумуляції;
min, max – ліва і права точки інтервалу носія нечіткої множини вихідної змінної ω, що розглядається (універсум ризику в інтервалі від 0 до 10).

7

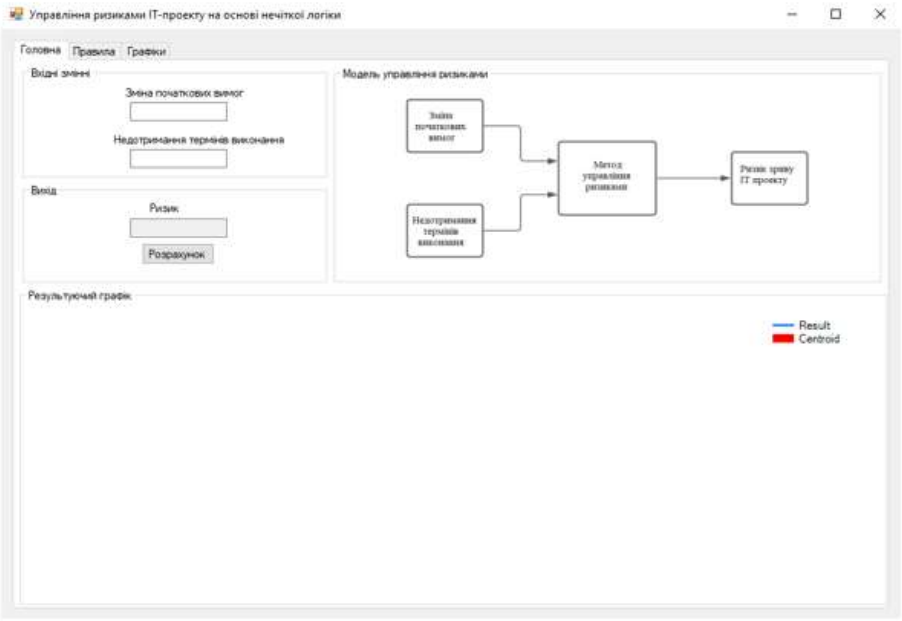
МЕТОД НЕЧІТКОГО ВИВЕДЕННЯ ДЛЯ ФОРМУВАННЯ УПРАВЛЯЮЧОГО РІШЕННЯ



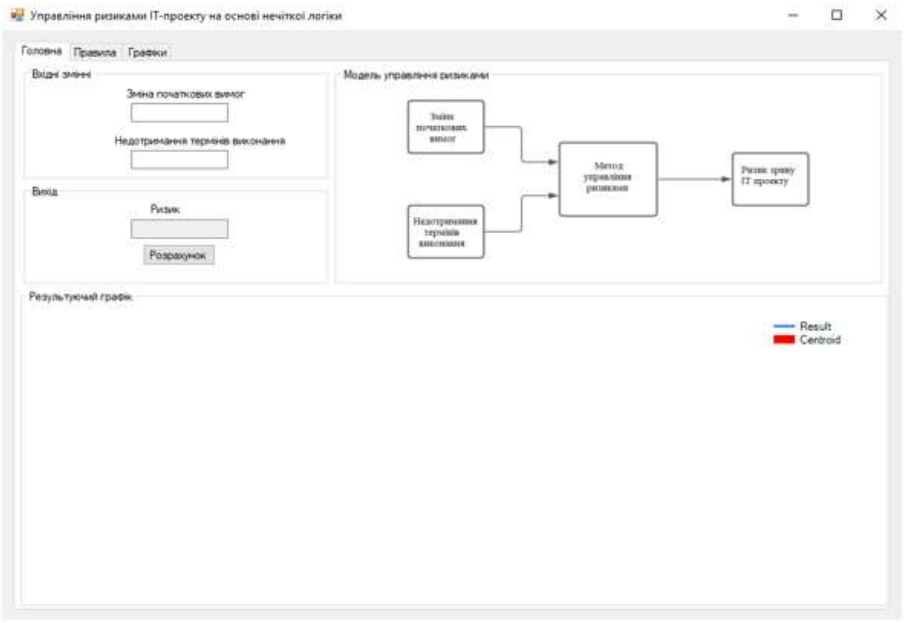
СТРУКТУРА СИСТЕМИ УПРАВЛІННЯ РИЗИКАМИ IT-ПРОЕКТУ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ



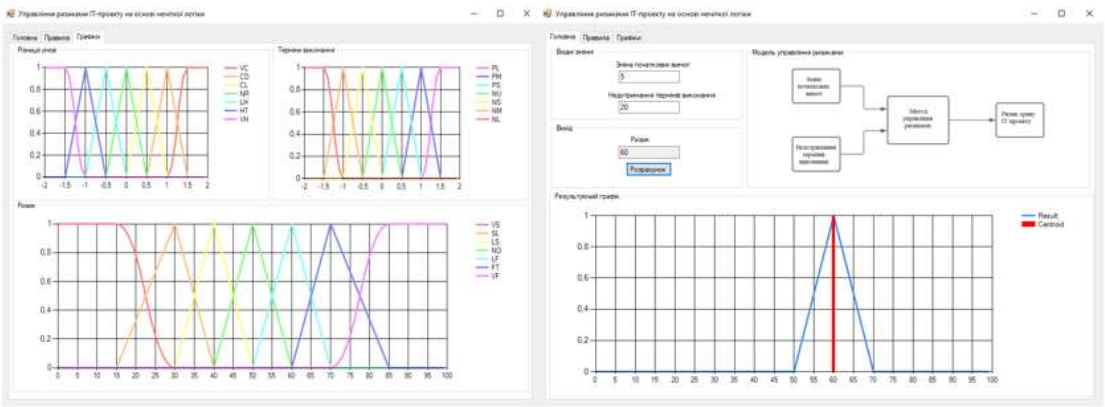
ПРАКТИЧНИЙ РЕЗУЛЬТАТ



ПРАКТИЧНИЙ РЕЗУЛЬТАТ



РЕЗУЛЬТАТИ МОДЕЛЮВАННЯ



ВИСНОВКИ

1. Проведено огляд та аналіз існуючих методів та моделей управління ризиками ІТ-проекту. Ключовими недоліками використання традиційних підходів є: неможливість оперувати нечіткими вхідними даними: наприклад, значення (динамічні завдання), що безперервно змінюються в часі, значення, які неможливо задати однозначно (результати статистичних опитувань, рекламні компанії і т.д.); необхідність великої кількості спостережень для отримання достовірної оцінки ризику; складність залучення незалежних експертів з широким досвідом у домені, що аналізується, та суб'єктивність їх оцінки; орієнтованість на зміни лише одного чинника проекту, що призводить до недообліку кореляції зі всіма іншими чинникам;
2. Визначено принципи управління ризиками ІТ-проекту.
3. Розроблено модель управління ІТ-ризиками на основі нечіткої логіки, яка відображає тристоронню схильність організацій до ризиків, пов'язаних з експлуатацією інформаційних систем: дії персоналу, збої систем, неліцензійність. Для першого виду ризику у системі передбачається можливість проведення анкетування працівників виявлення загрози ризиків. У рамках управління другим видом ризиків забезпечується завантаження файлу статистичних даних про інциденти в інформаційній структурі підприємства, завантаження файлу потенційних уразливостей та перевірка конфігураційних одиниць інфраструктури на їх наявність. Управління останнім видом забезпечується за допомогою зіставлення встановленого програмного забезпечення та наявних ліцензій нею.
4. Розроблено метод управління ризиками ІТ-проекту на основі нечіткої логіки, який забезпечує більш гнучку обробку факторів ризиків, дозволяють отримати лінгвістичний опис ступеня ризику, що дозволяє виявити пріоритети ризиків (дуже низький ризик; низький ризик; помірний ризик; високий ризик; дуже високий ризик) і вибрати план заходів щодо зниження рівня найбільш небезпечних загроз.
5. Використання запропонованої моделі та методу управління ризиками ІТ проекту дає можливість підвищити якість управління ризиками ІТ проекту, а також дозволяє автоматизувати процес інтелектуального управління ризиками, що, зрештою, підвищує оперативність та об'єктивність прийнятих управлінських рішень.

ПУБЛІКАЦІЇ ТА АПРОБАЦІЯ РОБОТИ

Стаття: Золотухіна О.А., Крута Ю.В. Інформаційна система управління ризиками ІТ-проєкту на основі нечіткої логіки// Телекомунікаційні та інформаційні технології. №3, 2022. Прийнято до друку

Тези доповідей: Золотухіна О.А., Крута Ю.В. Щодо алгоритмічного забезпечення процесу управління ризиками ІТ-проєкту на основі нечіткої логіки// Математика та математичне моделювання у сучасному технічному університеті: Збірник тез доповідей І Міжнародної науково-практичної конференції студентів та молодих вчених, 30 листопада 2022 р. Луцьк: ДонНТУ. С.121-122.

ДЯКУЮ ЗА УВАГУ!