**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**Західноукраїнський національний університет**
**Факультет комп'ютерних інформаційних технологій**
Кафедра інформаційно-обчислювальних систем і управління

**ТОМИН Ірина Іванівна**

# Метод структурної декомпозиції ризиків у IT проєктах / Method of Structural Decomposition of Risks in IT Projects

спеціальність: 122 – Комп'ютерні науки
освітньо-професійна програма – Управління проєктами

Кваліфікаційна робота

Виконала студентка групи
КНУПм-21
І. І. Томин
_____

Науковий керівник:
к.е.н., доцент Г. М. Гладій
_____

Кваліфікаційну роботу
допущено до захисту:
«___» _____ 2023 р.
Завідувач кафедри
_____ М. П. Комар

ТЕРНОПІЛЬ – 2023

Факультет комп'ютерних інформаційних технологій
Кафедра інформаційно-обчислювальних систем і управління
Освітній ступінь «магістр»
Спеціальність 122 Комп'ютерні науки
Освітньо-професійна програма – Управління проєктами

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____М. П. Комар
«____» _____2022 р.

**ЗАВДАННЯ**
**НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ**
Томин Ірина Іванівна
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи:
Метод структурної декомпозиції ризиків у ІТ проєктах / Method of Structural Decomposition of Risks in IT Projects
керівник роботи: к.е.н., доцент Гладій Г. М.,
затверджені наказом по університету від 8 грудня 2022 року №491.

2. Строк подання студентом закінченої кваліфікаційної роботи: 1 грудня 2023 року.

3. Вихідні дані до кваліфікаційної роботи: завдання на кваліфікаційну роботу студента, наукові статті, технічна література.

4. Основні питання, які потрібно розробити:
- проаналізувати ризики ІТ-проєктів і виявити їхні особливості;
- розглянути існуючі підходи до класифікації ризиків ІТ-проєктів на предмет подальшої структуризації цих ризиків;
- запропонувати концепцію формування ієрархічної структури ризиків;
- розробити метод структурної декомпозиції ризиків;
- розробити програму для динамічного формування ризиків ІТ-проєктів.

5. Перелік графічного матеріалу у роботі:
- структура декомпозиції ризиків для проєктів у ІТ-галузі;
- розробка бази даних ризикових подій, категорій ризиків і мікродерев.

6. Консультанти розділів роботи

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| | | | |
| | | | |
| | | | |
| | | | |

7. Дата видачі завдання 8 грудня 2022 р.

## КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів кваліфікаційної роботи | Строк виконання етапів кваліфікаційної роботи | Примітка |
|---|---|---|---|
| 1 | Особливості ризиків в процесі реалізації IT-проєктів | 12.2022 р. – 03.2023 р. | |
| 2 | Методологія розробки структурної декомпозиції ризиків | 03.2023 р. – 05.2023 р. | |
| 3 | Програмна реалізація пропонованого підходу | 05.2023 р. – 11.2023 р. | |
| 4 | Повне завершення та представлення кваліфікаційної роботи на кафедру | 01.12.2023 р. | |

Студентка _____ І. І. Томин

Керівник роботи _____ к.е.н., доцент Г. М. Гладій

# РЕЗЮМЕ

Кваліфікаційна робота на тему «Метод структурної декомпозиції ризиків у ІТ проєктах» на здобуття освітнього ступеня «Магістр» зі спеціальності 122 «Комп'ютерні науки» освітньо-професійної програми «Управління проєктами» написана обсягом у 104 сторінки і містить 32 ілюстрації, 10 таблиць, 1 додаток і 50 використаних джерел.

Мета роботи – розробка методу структурної декомпозиції ризиків у сфері ІТ-проєктів.

Методи дослідження: системний підхід; загальнонаукові методи аналізу і синтезу, абстрагування, порівняння, індукції та дедукції; проєктування програмних систем.

Основні результати дослідження: проаналізовано ризики ІТ-проєктів і виявлено їхні особливості; розглянуто існуючі підходи до класифікації ризиків ІТ-проєктів на предмет подальшої структуризації цих ризиків; запропоновано концепцію формування ієрархічної структури ризиків; розроблено метод структурної декомпозиції ризиків і програма для динамічного формування ризиків ІТ-проєктів.

Ключові слова: РИЗИКИ ПРОЄКТУ, ІЄРАРХІЧНА СТРУКТУРА, ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, УПРАВЛІННЯ РИЗИКАМИ, СТРУКТУРНА ДЕКОМПОЗИЦІЯ.

# ABSTRACT

The qualification work on the topic "Method of Structural Decomposition of Risks in IT Projects" for Master's degree in the specialty 122 "Computer Science" educational and professional program "Project Management" is written on 104 pages and it contains 32 figures, 10 tables, 1 annex and 50 sources.

The purpose of this qualification work is to develop a method of structural decomposition of risks in the field of IT projects.

Research methods: systematic approach; general scientific methods of analysis and synthesis, abstraction, comparison, induction and deduction; design of software systems.

Research results: the risks of IT projects were analyzed and their features were identified; existing approaches to the classification of risks of IT projects were considered for the purpose of further structuring of these risks; the concept of forming a hierarchical structure of risks is proposed; a method of structural risk decomposition and a software for dynamic risk formation of IT projects were developed.

Keywords: PROJECT RISKS, HIERARCHICAL STRUCTURE, INFORMATION TECHNOLOGIES, RISK MANAGEMENT, STRUCTURAL DECOMPOSITION.

.

ЗМІСТ

# ВСТУП

Актуальність теми дослідження. Процес управління ризиками має першорядне значення в наш час. В епоху, коли технологічний прогрес стимулює інновації та розвиток, ІТ-проєкти стали ключовими для бізнесу в різних галузях. Однак, складність та динамічність цих проєктів призводять до багатогранних ризиків, які вимагають ретельного управління.

Упродовж останнього десятиліття мали місце інтенсивні дослідження та розробки в управлінні проєктними ризиками, зокрема в сфері інформаційних технологій. ІТ-проєкти передбачають численних учасників, чиї інтереси та вимоги необхідно враховувати в прийнятті управлінських рішень, щоб забезпечити успіх проєкту.

Дослідження на тему «Метод структурної декомпозиції ризиків в ІТ-проєктах» задовольняє цю критичну потребу, представляючи системний підхід до аналізу та управління ризиками, притаманними ІТ-проєктам. Насамперед, актуальність полягає у визнанні складного переплетення ризиків, пов’язаних з ІТ-проєктами. Ці проєкти охоплюють широкий спектр компонентів, таких як технологічні залежності, очікування зацікавлених сторін, дотримання нормативних вимог, проблеми кібербезпеки та мінливі ринкові ландшафти.

Структурна декомпозиція ризиків (СДР) є ієрархічно організованим описом виявлених ризиків проєкту, розташованих за категоріями та підкатегоріями, який ідентифікує різні області та причини можливих ризиків. Цей тип представлення має багато переваг і є зручним інструментом, оскільки пропонує синтетичний погляд на ризики за умов, що кожна із зацікавлених сторін може мати свій погляд на проєкт, а також він сумісний з еволюційною та динамічною природою проєктних ризиків. Однак, СДР страждає і недоліками, такими як: відсутність консенсусу про розроблення СДР для нового проєкту; невідповідності та відсутність ясності у визначенні категорій ризику; відсутність правил, що дають змогу передавати якісну та кількісну інформацію про ризики по всьому дереву.

Запропонований метод структурної декомпозиції пропонує комплексну основу для покращення процесу прийняття рішень в управлінні ІТ-проєктами. Розбиття численних ризиків на дрібні компоненти за допомогою структурної декомпозиції дає змогу тонше розуміти взаємозалежності та взаємозв'язки між різними чинниками ризику. Таке розуміння дає змогу керівникам і менеджерам проєктів ефективно управляти ризиками.

Метою роботи є розробка методу структурної декомпозиції ризиків у сфері ІТ-проєктів.

Об'єкт дослідження – набір ризиків у сфері інформаційних технологій.

Предмет дослідження – процеси управління ризиками ІТ-проєктів.

Для реалізації поставленої мети необхідно виконати такі завдання:

– проаналізувати ризики ІТ-проєктів і виявити їхні особливості;

– розглянути існуючі підходи до класифікації ризиків ІТ-проєктів на предмет подальшої структуризації цих ризиків;

– запропонувати концепцію формування ієрархічної структури ризиків;

– розробити метод структурної декомпозиції ризиків;

– розробити програму для динамічного формування ризиків ІТ-проєктів.

У дослідженні використано такі методи: системний підхід, при якому будь-яка система (об'єкт) розглядається як сукупність взаємозв'язаних елементів; загальнонаукові методи аналізу і синтезу, абстрагування, порівняння, індукції та дедукції; проєктування програмних систем.

Наукова новизна роботи – запропоновано підхід до формування структурної декомпозиції ризиків у ІТ-проєктах.

Практична значущість роботи полягає у використанні запропонованого підходу до управління ризиками проєктними менеджерами у сфері інформаційних технологій.

Апробація і публікації результатів. Результати дослідження доповідалися автором на ІІІ міжнародній науково-практичній конференції «Problems of creating scientific ideas about world development» (Оттава, Канада, 3-6 жовтня 2023 р.) і VII міжнародній науково-практичній конференції «Global problems of improving

scientific inventions», (Копенгаген, Данія), та опубліковані в матеріалах вказаних конференцій (див. додаток А).

# 1 ОСОБЛИВОСТІ РИЗИКІВ В ПРОЦЕСІ РЕАЛІЗАЦІЇ ІТ-ПРОЄКТІВ

## 1.1 Поняття проєктних ризиків і способи управління ними

Управління ризиками широко визнана як одна з найважливіших процедур і сфер можливості в галузі управління проєктами. Управління ризиками проєкту охоплює ширше поле ніж людина і структурна безпека. Проєкт – унікальний процес, утворений сукупністю скоординованої та керованої діяльності з датами початку та закінчення, розпочатий для досягнення мети, яка відповідає конкретним вимогам, включаючи обмеження щодо термінів, вартості та ресурсів. Таким чином, управління ризиками проєкту (УРП) спрямоване на зниження імовірності недосягнення цілей проекту. УРП призначене для максимізації позитивного результату завдяки певним можливостям і мінімізації (усунення) наслідків негативних ризикових подій.

Загальновідомо, що значна частка проєктів в області ІТ є невдалими в частині відповідності цілям, бюджету чи строкам – у середньому в світі цей показник перевищує 50%, а в державному секторі навіть 70%. Багато в чому такі проблеми пов’язані з недостатньо повним і якісним управлінням ризиками.

Оскільки УРП є масштабованою діяльністю, тому має порівнюватися з розміром і складністю розглянутого проєкту. Відповідно процес управління ризиками проєкту повинен адаптуватися для кожного конкретного випадку та проєкту.

Поновлення інтересу до УРП спричинене укладенням нових видів договорів, наприклад приватно-державного партнерства, де розробник може знадобитися для управління ризиками й після закінчення проєкту. Тоді УРП дійсно стає спільною метою для всіх партнерів проєкту, хоча вони можуть мати різні уявлення про належний розподіл ризиків. А тому можуть виникати суперечки між такими сторонами і це може створювати нові джерела ризиків для проєкту.

Дослідження показують [1, 2], що крім контрактів ризики переважно обробляються на основі досвіду, припущень і людських суджень. Оскільки ризики

є вельми ситуативні, експертне оцінювання надає достатні засоби управління ризиками. Проблеми виникають, коли ці знання експертів не документуються і не підлягають передачі. Відсутність прийнятої моделі аналізу ризиків змушує кожну компанію формувати і тестувати свої моделі управління ризиками. Інші ризики пов'язані з можливо упередженими ухваленнями рішень, коли особистий фон і припущення неминуче позначаються на людській оцінці.

Успіх проєкту варто розглядати з різних точок зору – власника, розробника, підрядника, користувача, широкої громадськості тощо. Ці різні точки зору поясняють причину, чому ж проєкт можна вважати успішним для однієї сторони і невдалим для інших. Зазвичай основними цілями проєкту є вартість, час і якість [3]. Хоча, в [4] вважають, що цей «трикутник» фокусується на короткострокових аспектах проєктної діяльності та успіху проєкту. Вони виокремили три додаткові аспекти для сталого успіху проєкту: вплив на навколишнє середовище, робоче середовище та інновації. Наприклад, «якість» може охоплювати як функціональні можливості продукту, так й інші виміри, такі як працівники, безпека чи довкілля [5].

Поліпшення практики переважно базується на розширенні (деталізації) принципів передової практики, яку всі учасники проєкту мають здійснити на кожному етапі проєкту для покращення УРП. Мета полягає в проведенні поглибленого аналізу ризиків на кожному етапі проєкту. Ця прогалина може бути заповнена шляхом розроблення інструментів моделювання, адаптованих до реального контексту проєкту та впливу важливих чинників.

Насамперед важливо зрозуміти, що саме мається на увазі під ризиком, перш ніж приступити до управління ним. У літературі термін «ризик» використовується в різних значеннях з різними словами, такими як небезпеки або невизначеності. Виявлено, що не існує єдиного чіткого використання цього слова в літературі [6, 7]. Крім того, більшість визначень ризику були зосереджені лише на таких моментах як збитки або шкода, і знехтували потенціал зростання чи можливість отримати прибуток або доходи. Це слово має різний зміст для різних людей, тобто поняття ризику варіюється залежно від точки зору, поглядів і досвіду.

Огляд наукової літератури з управління ризиками проєкту виявив різноманітність тлумачення «ризику». Деякі з цих визначень мають спільну рису: вони визначають ризик з точки зору невизначених подій та їх впливу на цілі проєкту. Згідно з останнім PMBOK [8], ризик визначається як «невизначена подія чи умова, що у разі настання матиме позитивний чи негативний вплив на одну чи більше цілей проєкту». Схожі визначення дають відомі фахівці в сфері управління ризиками Девід Хіллсон [9], Ріта Мулкахі [10], Дуглас Хаббард [11], Стенлі Портні [12].

В [6] обговорюється концепція ризику детальніше і пропонується використовувати загальніше поняття невизначеності. Автори стверджують, що термін «ризик» часто асоціюється з неприємностями і зосереджується на загрозах, а не на можливостях. Часто члени проєктних команд сприймають ризик лише як негативну подію.

Багато суперечливих і неоднозначних значень «ризику» спричиняють поширення безладу, а також різні підходи до управління ризиками в різних областях. Прикладами деяких з виявлених ризиків є: дефектні роботи, графік затримки, перевитрата, соціальне середовище, коливання ринку тощо. Проблема в тому, що всі елементи неоднозначно називаються «ризик», тоді як затримка графіку та перевитрата коштів є «наслідком» для цілей проєкту та інші елементи є «джерелом» труднощів. Такий список є сумішшю різних визначень ризику і може спричинити низку труднощів у процесі управління ризиками проєкту.

Аналіз літератури вказує на використання двох взаємовиключних визначення «ризик». У табл.1.1 наведено деякі приклади з літератури. Ця плутанина спричинена, ймовірно, різними поглядами експертів з промислових ризиків і фахівців зі стихійних лих.

Таблиця 1.1 – Два різних визначення ризику

| Ризик: наслідки | Ризик: джерело події |
|---|---|
| Вплив невизначеності на цілі проекту. Ефект відхилення від очікуваних позитивних та/або негативних цілей. | Подія, яка має це спричинити, матиме позитивний або негативний вплив на досягнення цілей проєкту. |
| Поєднання ймовірності невизначеної події та її наслідків. Позитивний наслідок надає можливість; Негативний наслідок становить загрозу. | Ризик проєкту – це невизначена подія або умова, що, якщо вона відбувається, робить позитивний або негативний вплив на цілі проекту. |
| Ризик є функцією від наслідків/серйозності небезпеки та ймовірності виникнення небезпеки. | Це невизначена подія, що, якщо вона відбувається, має позитивний (можливості) або негативний (загрози) для цілей проекту. |
| Очікування небажаних результатів (але настання позитивних результатів може бути інтегроване). | Ймовірність того, що шкідливий випадок відбудеться з проектом. |
| Вихід на можливість економічного і фінансового збитку або прибутку, фізичного пошкодження або травми, або затримки, як наслідок невизначеності, пов’язаної з прийняттям конкретного курсу дій. | Вплив на шанс появи подій негативно чи позитивно впливають на цілі проекту як наслідок невизначеності. |

Важливо переконатися, що учасники процесу ідентифікації ризиків зосереджені на відмінності між ризиками та їх потенційного впливу чи результату. Говорячи простими словами, відмінність важлива, оскільки це перешкоджає списку ризиків стати заплутаною сумішшю ризиків і впливу, що робить процес реагування особливо складним, іноді неможливим.

Тому надалі згідно зі стандартом будемо розглядати «ризик» як ефект невизначеності на цілі проєкту.

Ризики проєкту завжди стосуються майбутнього. Як згадувалося вище, ризик – це невизначена подія або умова, яка, у випадку настання, впливає хоча б на одну ціль проєкту. Під цілями тут розуміються зміст, строки, вартість і якість. Ризик може бути спричинений одним або декількома чинниками і у разі виникнення може вплинути на один або декілька аспектів. Причиною може бути вимога, допущення,

обмеження або умова, яку створює ймовірність негативних або позитивних результатів.

Наприклад, причиною ризику може бути необхідність отримання дозволу від місцевого комітету з охорони навколишнього середовища або нестача персоналу, залученого для розробки проєкту. Настанням ризику в першому випадку буде затримка з видачею дозволу (несприятлива подія), а в другому – недостатній персонал, залучений для розробки проєкту, все ж зуміє своїми силами закінчити роботу вчасно, отже, на її виконання буде затрачено менше ресурсів. Виникнення будь-якої з цих невідомих заздалегідь подій може вплинути на вартість проєкту, його розклад або виконання. До умов виникнення ризиків можуть також належати аспекти середовища організації чи проєкту, що сприяють збільшенню ризику (наприклад, невдалий вибір методів при управлінні проєктом, відсутність загальних систем управління, одночасне виконання кількох проєктів або залежність від зовнішніх зацікавлених сторін проєкту, яких неможливо контролювати).

Причиною виникнення ризиків є невизначеність, присутня в усіх проєктах. Відомі ризики – це ті ризики, що вже були визначені та проаналізовані. Відносно них можливо спланувати відповідну реакцію. Проте таке планування неможливе для невідомих ризиків. Тоді розумним виходом для проєктної команди є виділення резервних ресурсів на можливі втрати. Ризик проєкту, який виник, також можна розглядати як проблему.

Організації сприймають ризик як вплив невизначеності на мету їхнього проєкту або корпоративні цілі. Для організацій та зацікавлених сторін проєкту прийнятними є різні ступені ризику. Це називається «готовністю приймати ризики». Ризики, які несуть загрозу для проєкту, можуть виявитися прийнятними, якщо вони знаходяться в межах готовності приймати ризики, або ризик менший за вигоду, яку можна отримати за умови прийняття цього ризику.

Ставлення до ризику окремих осіб і груп осіб обумовлено їхнім розумінням ризику та відповідною реакцією на його виникнення. В основі таких відносин лежать сприйняття, готовність приймати ризики та інші види необ’єктивності, які

необхідно старанно виявляти. Для кожного проєкту необхідно виробити послідовний підхід до ризиків, а інформація про ризики та управління ними має бути достовірною і відкритою. Реагування на ризики відображає розуміння організацією балансу між прийняттям ризиків і уникненням них.

Для досягнення успіху організація має заздалегідь і послідовно чинити запобіжні дії з управління ризиками упродовж усього проєкту. На всіх рівнях організації повинен бути зроблений усвідомлений вибір для активної ідентифікації та здійснення ефективного управління ризиками протягом всього життєвого циклу проєкту. Ризик існує з моменту зародження задуму проєкту. Просування проєкту вперед без виконання запобіжних дій з управління ризиками збільшує вплив певних ризиків на проєкт, що може призвести до невдачі.

Традиційний погляд на ризики є негативним, під яким розуміють небезпеку втрати, збитки та інші негативні наслідки. Але деякі нинішні настанови і стандарти для ризиків включають можливості вигоди або можливість, тобто невизначеності, які можуть мати позитивний вплив на досягнення цілей.

Проєктні ризики охоплюють невизначені події, які можуть мати як негативний вплив на цілі проєкту, так і позитивний ефект. Ці два типи ризику називаються, відповідно, загрози і можливості. Це важливо для вирішення як загроз так і можливостей у межах єдиного процесу управління ризиками проєкту.

Три основні обмеження для проєктів можуть бути класифіковані за графіком, цілями і ресурсами, і кожне з них може спричинити хвильовий ефект у проєкті, який потім перетікає у швидкий крах.

Для гарантування того, що ризик зведений до мінімуму, повинні бути чітко визначені заходи, завдання, статут проєкту, і, звичайно, цілі. Всі сфери застосування ризиків, кількісні чи ні, повинні бути визначені. Апаратні дефекти, дефекти програмного забезпечення, недостатньо визначені масштаби, несподівані зміни в правових і нормативних рамках та інтеграції дефектів можуть бути віднесені до широкої області ризиків областей видимості.

Є багато способів, які допомагають зацікавленим сторонам визначити цілі проєкту. Аналіз ризиків показує залежність проєкту від технології та ринку, а потім оцінює, як зміни в кожному з них будуть впливати на результат проєкту.

Структура робіт (WBS) також відповідає за ризики проєктів, які погано визначені й цілі неоднозначні.

Обсяг ризиків може бути мінімізований і керуватися через хороше планування. Чітке визначення проєкту, керування змінами обсягу впродовж усього проєкту, використання регістрів ризику для кращого управління ризиками, виявлення причинних чинників, відповідна реакція на ризиковані ситуації даватимуть великі дивіденди у довгостроковій перспективі.

Дотримання строків і узгодження критичного шляху є однією з найскладніших ситуацій, з якою в даний час стикаються керівники проєктів. Щоб звести до мінімуму ризики графіку, є кілька перевірених часом методів, які можуть бути поставлені на хороше застосування. Технологічна схема проєкту повинна бути розбита на невеликі, чітко визначені компоненти, де виділяються строки для кожного процесу відносно короткої тривалості (це дає змогу легко ідентифікувати речі, коли завдання відхиляється від графіка).

Люди і кошти є основною ресурсною базою будь-якого проєкту. Якщо люди некваліфіковані або нездатні виконати завдання, якщо проєкт перебуває в стадії комплектації з самого початку, або коли ключові учасники проєкту прийшли після його початку, існує очевидний ризик, що проєкт має погано заплановані людські ресурси.

Аналогічно з фінансової точки зору, якщо недостатньо коштів надається для виконання необхідних завдань, проєкт приречений на провал із самого початку. Чітко оцінюючи вартість проєкту, виділяючи відповідний бюджет для задоволення цих витрат, не маючи надмірних очікувань від співробітників, уникаючи неочікуваного виникнення несприятливих чинників допомагають звести до мінімуму ризики ресурсів проєкту.

Управління конфліктами, які, зазвичай, виникають упродовж виконання проєкту, також повинні бути розв’язані вміло, щоби проєкт мав плавний хід протягом всієї його тривалості.

У наступних підрозділах більше уваги приділено загрозам, ніж можливостям, але пропоновані методи і підходи можуть бути легко розширені, щоб покрити можливості також.

## 1.2 Класифікація ризиків у сфері інформаційних технологій

Галузь інформаційних технологій є одним з пріоритетних напрямків розвитку вітчизняної економіки. Автоматизація діяльності підприємств, впровадження програмних продуктів, розробка інноваційного програмного забезпечення є прикладами проєктів в ІТ-галузі. Оскільки діяльність у цій сфері тісно пов’язана з інноваційною діяльністю, ризики в ІТ-галузі характеризуються високою імовірністю та значним ступенем впливу на проєкти.

Управління ризиками проєкту можна визначити як «комплекс заходів, що охоплюють ідентифікацію, аналіз ризиків та прийняття рішень, спрямованих на зниження імовірності та ступеня їхнього впливу на хід, результати та продукти цих проєктів» [13].

Зазвичай, класифікацію ризиків проєкту здійснюють на етапі їхнього аналізу переважно за двома критеріями: ступенем впливу на проєкт та ймовірністю виникнення. Однак доцільно створити початкову класифікацію ризиків ІТ-проєктів як входом до їхньої ідентифікації. У цьому напрямку фахівці з ризик-менеджменту провели чималу аналітичну роботу [14]. Усі опубліковані варіанти класифікації ризиків мають багато спільного. Найчастіше за джерелом виникнення ризики прийнято розділяти на внутрішні та зовнішні (рис.1.1).

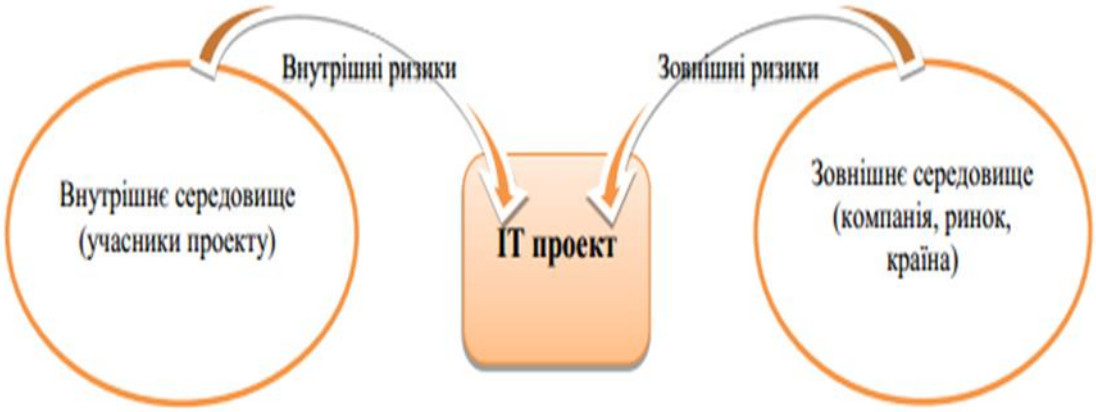



Рисунок 1.1 – Внутрішні та зовнішні ризики проєкту

На практиці часто класифікують ризики згідно з об’єктом, де вони виникають. Результат такої класифікації представлено у табл.1.2 [48].

Таблиця 1.2 – Класифікація ризиків проєкту за об’єктами їх виникнення

| № | Об’єкт | Визначення | Приклад |
|---|---|---|---|
| 1 | Внутрішні ризики | | |
| 1.1 | Час | Для проєктів створення програмних рішень, як виду інноваційної діяльності, характерне неточне визначення планових строків реалізації. | Розробка однієї з функцій створюваного програмного продукту по суб’єктивних причинах затребувала більше трудовитрат, ніж попередньо оцінив експерт |
| 1.2 | Бюджет | Ризики, пов’язані з фінансуванням проекту при створенні програмного рішення на замовлення і оптимістичними розрахунками окупності в проєктах створення тиражних рішень | Протягом реалізації проекту замовник неодноразово вносив поправки у вимоги до програмного продукту і, як наслідок перевитрат часу на внесення змін бюджет проєкту було вичерпано до моменту готовності продукту до здачі |
| 1.3 | Технологія | Ризики, пов’язані з вибором оптимальної технології виконання проекту | Концепція проекту розробки програмного продукту і всі проектні рішення передбачали реалізацію проекту на конкретній технологічній платформі, а в результаті частина функціоналу не змогла бути реалізована |

| | | | |
|---|---|---|---|
| 1.4 | Якість | Ризики, пов’язані з якісними характеристиками продуктів проєкту | У результаті проєкту автоматизації бізнес-процесів компанії пріоритетні для замовника процеси були не реалізовані, або реалізовані частково |
| 1.5 | Інфра-структура та матеріальні ресурси | Ризики, що пов’язані з матеріальними ресурсами та характеристиками програмно-апаратної інфраструктури проєкту | Неможливість проведення дослідного розвертання програмного комплексу через відсутність необхідного апаратного забезпечення |
| 1.6 | Трудові ресурси та їх кваліфікація | Ризики, пов’язані з наявністю трудових ресурсів, їх структурними змінами та кваліфікацією | Провідний спеціаліст звільняється в середині проєкту |
| 1.7 | Інтеграція | Ризики, пов’язані з процесами інтеграції на всіх рівнях програмної архітектури | Недостатня увага процесу інтеграції нової програмної системи в наявну |
| 2 | Зовнішні ризики | | |
| 2.1 | Держава | Ризики політичного, законодавчого та соціального характеру | Прийняття неочікуваного законопроекту, що матиме вплив на ефективність реалізації проєкту |
| 2.2 | Ринок | Ризики, що пов’язані з кон’юнктурою ринку, конкурентною боротьбою | Випуск конкурентами продукту з аналогічним функціональним наповненням |
| 2.3 | Зовнішня економіка | Ризики, пов’язані з валютними операціями, зовнішньо-економічними контрактами, організацією «віддалених робочих місць» | Введення змін на макроекономічному рівні, що матиме вплив на виконання дійсних міжнародних контактів |
| 2.4 | Контрагенти | Ризики, що можуть виникнути в процесі ведення взаєморозрахунків, виконання контрактних поставок та зобов’язань тощо | Порушення умов договорів поставки компонентів продукту проєкту |
| 2.5 | Природа та клімат | Ризики, що виникають внаслідок природних і кліматичних явищ | Удар блискавки в сервер баз даних |
| 2.6 | Науково-технічний прогрес | Ризики, що виникають у тривалих, негнучких проєктах, пов’язані з появою в галузі нової, кращої технології або інструментарію до завершення проєкту | Вихід на ринок нової версії технологічної платформи (базового компоненту для розробки) |

Ця класифікація може слугувати базою і потребує модифікації згідно з характеристиками, вимогами та обмеженнями конкретного проєкту.

Нами розроблена своя класифікація ризиків для ІТ-проєктів (табл.1.3).

Таблиця 1.3 – Розроблена класифікація ризиків для ІТ-проєкту

| № | Об’єкт | Приклад |
|---|---|---|
| 1 | Внутрішні ризики | |
| 1.1 | Створення графіку | Графік робіт, ресурси, визначення продукту диктуються замовником або вищим керівництвом і тому незбалансовані |
| 1.2 | Організація і управління | Проєкту не вистачає ефективного вищого керівництва |
| 1.3 | Середовище розробки | Засоби вчасно недоступні |
| 1.4 | Кінцеві користувачі | Кінцевий користувач наполягає на нових вимогах |
| 1.5 | Замовник | Замовник наполягає на нових вимогах |
| 1.6 | Контрагенти | Контрагент не доставляє компоненти вчасно |
| 1.7 | Вимоги | Вимоги були чітко визначені, але продовжують змінюватися |
| 1.8 | Продукт | Модулі, схильні до помилок, вимагають додаткового тестування, проєктування та реалізації |
| 1.9 | Зовнішнє середовище | Продукт залежить від державного регулювання, що змінюють несподівано |
| 1.10 | Проєктна команда | Процес найму займає більше часу, ніж очікувалося |
| 1.11 | Розробка та впровадження | Надмірно простий дизайн не вирішує основні проблеми і призводить до реконструкції і переробки |
| 1.12 | Процес | Велика кількість паперової роботи сповільнює прогрес |
| 2 | Зовнішні ризики | |
| 2.1 | Держава | Прийняття неочікуваного законопроєкту, що матиме вплив на ефективність реалізації проєкту |
| 2.2 | Ринок | Випуск конкурентами продукту з аналогічним функціональним наповненням |
| 2.3 | Науково-технічний прогрес | Вихід на ринок нової версії технологічної платформи (базового компоненту для розробки) |
| 2.4 | Форс-мажорні обставини | Землетрус, повінь, буря, ураган й інші стихійні лиха |

## 1.3 Управління ризиками проєкту як динамічний та ітераційний процес

Управління ризиками є систематичним процесом виявлення, оцінювання та реагування на ризики проєкту. Загальна мета процесу управління ризиками – максимальне використання можливостей і зведення до мінімуму негативних наслідків загроз ризику. Різноманітність моделей управління ризиками з різною градацією можна знайти в літературі.

Ще свого часу в роботах [15, 16] систематичний процес управління ризиками розділили на фази: класифікація ризиків, виявлення ризиків, аналіз ризиків і реагування на ризики, де остання розбивається на чотири дії – зберігання, відновлення, перенесення і уникнення. Потім Міжнародний стандарт «Управління ризиками проєкту – Настанови до застосування» [17] запропонував модель з чотирьох етапів: виявлення ризиків, оцінювання ризиків, обробка ризиків і огляду ризиків з моніторингом. За стандартом УПР включає процеси проведення планування управління ризиками, ідентифікацію, аналіз (кількісний, якісний), планування реагування, моніторинг і контроль над проектом (рисунок 1.2).

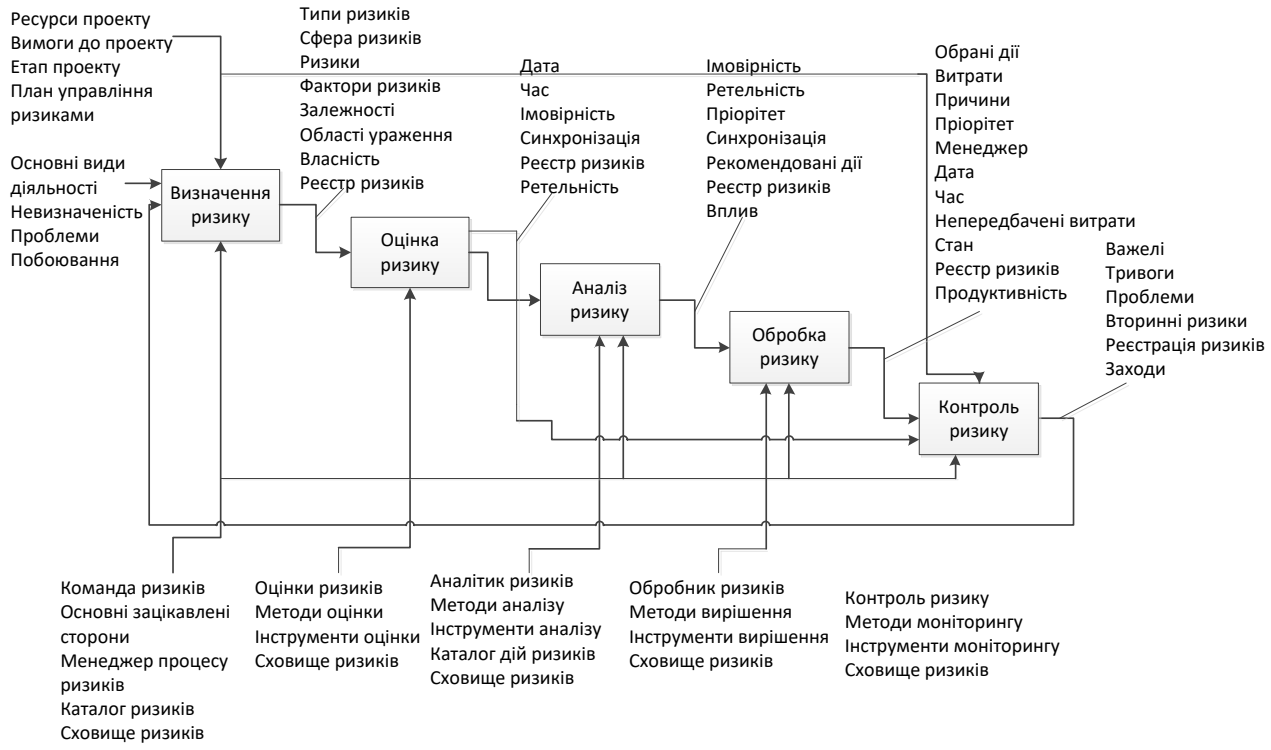



Рисунок 1.2 – Процес управління ризиками

У дослідженні [18] запропонували процес управління проєктними ризиками як логічну послідовність кроків, що складається з виявлення ризиків, виміру ризиків та переоцінювання. В [19] представлена комплексна методологія управління ризиками проєкту в крупних і складних проєктах. Модель складається з чотирьох фаз процесу: ініціація, балансування, технічного обслуговування і навчання. Кожен етап формується з декількох підетапів, які, відповідно, поділяються на різні види діяльності. У [20] рекомендують дев'ять кроків для успішного ризик-менеджменту: створення реєстру ризиків проєкту, ідентифікація ризиків проєкту, визначення можливостей, визначення ймовірності та впливу, планування реакції, оцінювання, призначення власників, регулярний перегляд, звіт про ризики проєкту. Перелік джерел можна продовжити, кожне з яких пропонує свій варіант з різною мірою деталізації.

Незважаючи на різноманітність існуючих моделей в літературі, всі вони мають спільну мету та подібні характеристики. Мета полягає в тому, щоб забезпечити системний підхід до управління ризиками за участю: ідентифікації джерел ризику; кількісного оцінювання їх наслідків (якісний і кількісний аналіз ризиків); розробки відповідей на ризики; контроль і моніторинг ризиків і реагування на ризики.

Ризиком неможливо управляти, якщо він неідентифікований. Тому після завершення планування управління ризиками наступний крок в ітераційному процесі управління ризиками проєкту спрямований на виявлення всіх можливих відомих ризиків розглядуваного проєкту.

Ідентифікація ризику – це процес систематичної та постійної ідентифікації, класифікації та оцінювання вихідної значущості ризиків, пов'язаних з IT-проєктом. Ідентифікація ризику визначає ризики, які можуть вплинути на проєкт і оформлення їх характеристик.

Ідентифікація має виконуватися на регулярній основі впродовж усього проєкту. Мета полягає в тому, щоб визначити ризики максимального ступеня. Оскільки деякі ризики наперед невідомі, потрібно зробити процес управління ризиками ітеративним, повторювати процес визначення ризиків, щоб виявити нові

ризики, які стали відомі з попередньої ітерації процесу. Упродовж життєвого циклу проєкту можуть з’явитися нові ризики. Команда проєкту повинна бути залучена до цього процесу, щоб вони могли розвивати і підтримувати почуття відповідальності за ризики та пов’язані дії з реагування на них.

Учасниками діяльності з ідентифікації ризиків можуть бути: менеджер проєкту; члени проєктної команди; команда управління ризиками; експерти, які не є членами проєкту; замовники; кінцеві користувачі; зацікавлені сторони; експерти з управління ризиками. Оскільки процес управління ризиками значною мірою спирається на первинному етапі ідентифікації, успіх на подальших етапах управління ризиками є зіставним з якістю першої стадії ідентифікації [6].

Входи процесу ідентифікації ризиків включають мету проєкту, масштаби управління ризиками, план, а також історичні дані, пов’язані з проєктом. Цей документ, учасники та події, що існують в межах проєкту є джерелами інформації, які використовуються для ідентифікації ризиків. Ідентифікація ризику має бути використана ефективно для виявлення можливостей та загроз. Однак досвід більшості проєктних команд орієнтується на негативних моментах.

Існує велика кількість методів для виявлення ризиків, таких як мозковий штурм і семінари, контрольні списки та оперативні списки, анкети та інтерв’ю, різні підходи на основі діаграм (причинно-наслідкових діаграм, системної динаміки, діаграм впливу тощо). До них належать творчі методи та ті, що спираються на попередній досвід і групові підходи.

Вибір інструментів ідентифікації ризиків ІТ-проєктів має першочергове значення для успіху проєкту з кількох вагомих причин [21]. По-перше, ІТ-проєкти за своєю суттю є складними, часто містять численні технічні, операційні та стратегічні елементи. Правильні інструменти ідентифікації ризиків забезпечують комплексний і структурований підхід до виявлення широкого спектру потенційних ризиків. Це допомагає проєктним командам проактивно передбачати виклики, пом’якшувати потенційні проблеми та відповідно адаптувати свої стратегії. Крім того, ці інструменти сприяють ефективності та об’єктивності процесу ідентифікації

ризиків, зменшуючи ймовірність того, що критичні ризики будуть проігноровані через когнітивні упередження або відсутність структури.

По-друге, ці інструменти сприяють послідовності та повторюваності, полегшуючи для різних членів команди застосування стандартизованого підходу до управління ризиками. Вони пропонують механізми для визначення пріоритетності ризиків на основі їхнього впливу та ймовірності, допомагаючи розподіляти ресурси та приділяти увагу найзначущішим ризикам. Крім того, інструменти, засновані на даних, використовують кількісні та якісні дані для точної ідентифікації та оцінювання ризиків, що є особливо цінним в IT-проєктах, де переважають дані та технічні чинники. Чітка документація, яку надають ці інструменти, сприяє ефективній комунікації та управлінню ризиками протягом усього життєвого циклу проєкту, підвищуючи прозорість та підзвітність. По суті, правильні інструменти ідентифікації ризиків закладають основу для надійної системи управління ризиками.

Список доступних засобів і методів виявлення ризиків, запропонованої PMI [22], представлена в табл.1.4, виділяючи їхні сильні та слабкі сторони.

Процес мозкового штурму, запозичений з управління бізнесом, а не спеціально створений для управління ризиками, охоплює переосмислення проблеми, генерування ідеї, знаходження можливих рішень, розробку вибраних можливих рішень і проведення оцінювання. Запроваджений на початку 1950-х рр. мозковий штурм був запропонований як метод вирішення завдань, коли буде вироблятися набагато більша кількість ідей за менший час, ніж існуючі проблемні групи методів рішень.

Процес ідентифікації проходить легше, якщо проєкт розбивається на діяльності (чи піддіяльності). В [23] проєкт розкладають на чотири фази (ініціація, балансування, технічне обслуговування і навчання), кожна з яких розбита на підфази, діяльності та підвиди діяльності. Рекомендується мати від 30 до 50 заходів для великих проєктів. Такий тип розподілу є ідеєю від Work Breakdown Structure. Так у IT-проєктах відповідними фазами можуть бути: техніко-економічна, контракт, проєктування, розробка та експлуатаційна фаза.

Таблиця 1.4 – Інструменти і методи ідентифікації ризиків

| Технологія | Переваги | Недоліки |
|---|---|---|
| Аналіз припущень і обмежень | Простий структурований підхід. Може базуватися на припущеннях і обмеженнях, уже перерахованих в статуті проєкту. Фіксує конкретні проєктні ризики | Неявні / приховані припущення чи обмеження часто упускаються |
| Мозковий штурм | Дає змогу всім учасникам висловлювати свої думки і вносити свій вклад в обговорення. Можливе залучення всіх ключових учасників. Творча генерація ідей | Потрібне залучення стейкхолдерів, яких важко і дорого зібрати. Може дати помилкові результати через авторитаризм окремих учасників. Формуються неризики і дублікати, яких необхідно фільтрувати |
| Діаграми причин і наслідків | Візуальне представлення проєкту сприяє структурованому мисленню | Діаграма може швидко стати надто складною |
| Контрольний список | Використовує попередній досвід. Надає докладний перелік ризиків | Контрольний список може розростатися до громіздкого. Ризики поза списком будуть пропущені. Часто охоплює лише загрози, упускає можливості |
| Розгляд документів | Надає детальні ризики конкретних проєктів. Не вимагає спеціалізованих інструментів | Обмежується ризиками, котрі містяться у проєктній документації |
| Аналіз силового поля | Дає глибоке розуміння чинників, що впливають на цілі проєкту | Трудомісткий і складний метод. Зазвичай застосовується лише до однієї мети |
| Бази знань | Використовує попередній досвід. Допускає бенчмаркінг від зовнішніх організацій | Обмежується тим, що раніше відбулося. Втрачаються нові проєктні ризики |
| Схеми впливу | Надає ключові чинники ризику. Може генерувати нелогічні ідеї, недоступні за допомогою інших методів | Вимагає дисциплінованого мислення. Не завжди легко визначити відповідну структуру |
| Співбесіди | Адресує ризики детально. Генерування участі зацікавлених сторін | Часова тривалість. Формуються неризики, проблеми, турботи, яких необхідно фільтрувати |

Процес ідентифікації охоплює також класифікацію виявлених ризиків, визначення їхніх причин, особливостей, потенційних наслідків, їхній розподіл, а також первинну реакцію. Маючи таку інформацію про виявлені ризики, документація про ризики може бути переведена в стан «реєстрація ризику», тобто містить всі виявлені ризики та детальну інформацію для кожного з них і може допомогти команді проєкту в розгляді проєктних ризиків на регулярній основі протягом всього проєкту. В роботі [24] синтезовано тип інформації, котра може бути збережена в реєстрі ризиків. Для кожного ідентифікованого ризику зареєстрована інформація може охоплювати:

– тип, причини, опис;

– відповідна фаза, завдання;

– стан (прихований, очевидний, зниклий), наслідки (за вартістю, часом, продуктивністю);

– виявлення (наслідки або причини, в т.ч. попередніх подій);

– ймовірності виникнення (якісно-кількісного);

– вид (уникнення, трансфер, пом’якшення), необхідність ресурсів, взаємозалежність з іншими ризиками.

Використання каталогу ризиків є корисним довідковим матеріалом для ідентифікації. Однак це може бути проблематичним, коли проєкти різняться за типом, масштабом, цілями щодо бажаного рівня деталізації та перспективи зацікавлених сторін до ризиків. У [6] запропоновано створити декомпозицію структури – ієрархічну структуру ризиків для полегшення ідентифікації ризикових подій.

Процес аналізу ризиків є важливою ланкою між системною ідентифікацією ризиків і раціональним управлінням значущих ризиків. Процес аналізу ризиків спрямований на оцінювання наслідків, пов’язаних з ризиками і оцінювання впливу ризику за допомогою системи аналізу ризиків і методів вимірювання. Цей процес призводить до пріоритетної ідентифікації ризиків для подальших дій.

Головним входом для аналізу ризику є виявлені ризики в процесі ідентифікації ризиків. Ймовірність і наслідки виявлених ризиків є двома

ключовими змінними в оцінюванні ризику. Цей процес може бути в діапазоні від дуже простого якісного аналізу до складного кількісного аналізу:

– якісний аналіз заснований на описовій або номінальній шкалі, щоб описати події ризику та їхні наслідки. Цей аналіз використовується переважно для початкового оцінювання ризиків або для швидкого оцінювання. Його також можна використати, коли мало відомо про ймовірність виникнення. Цей метод дає змогу визначити індивідуальний ризик події з найзначущим впливом на цілі проєкту. Події ризику, які оцінюються як високопріоритетні можуть бути додатково проаналізовані з використанням кількісних методів аналізу ризику;

– напів-кількісний аналіз розширює процес якісного аналізу, призначаючи числові значення в описовій шкалі;

– кількісний аналіз використовує числові значення ймовірності настання ризикових подій (змінних і чинників ризику) та їхні наслідки.

Першим кроком процесу аналізу ризику є визначення рівня оцінювання проєкту. В цьому випадку вельми корисними є WBS-діаграми. Work Breakdown Structures (WBS) є ієрархічною структурою декомпозиції завдань проєкту і може бути встановлена на різних рівнях деталізації (проєкту/фаз/завдань/підзадач), кожна з яких прикріплена до відповідних акторів і ресурсів. Взаємозв’язок між WBS проєкту та його декомпозицією структури (СДР) є корисним методом для зв’язку ризиків. Подібно як WBS є основою для управління проєктом, так і СДР може бути використана як інструмент для структурування процесу управління ризиками. WBS може бути далі поділятися, щоб бачити докладнішу інформацію про кожне завдання. СДР робить те ж саме для виявлення ризиків, створення організованого переліку ризиків, який допомагає краще зрозуміти та інтерпретувати ризики. Метод поєднує в собі послідовно кількісні та якісні підходи, що дає змогу користувачеві вибрати найкращий для оцінювання ризику.

Процес якісного аналізу ризиків визначає і оцінює характеристики індивідуально ідентифікованих ризиків проєкту та пріоритети ризиків на основі узгоджених характеристик. Оцінювання індивідуальних ризиків, використовуючи якісний аналіз ризиків, визначає ймовірність того, що буде спричинювати кожен

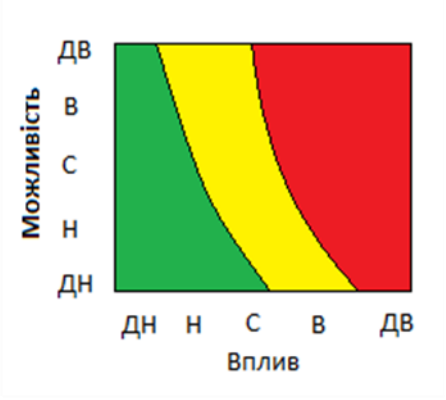
ризик і вплив кожного індивідуального ризику на цілі проєкту. Такий процес безпосередньо не стосується загального ризику цілям проекту, що є результатом комбінованого впливу всіх ризиків і їх потенційних взаємодій один з одним. Це, однак, може бути досягнуто за допомогою методів кількісного аналізу ризиків.

Типовий якісний аналіз ризиків, зазвичай, охоплює такі питання:

- короткий опис ризику;
- етапи проєкту, коли ризик може відбутися;
- елементи проєкту, які можуть бути пошкоджені;
- чинники, які впливають на ризик виникнення;
- зв’язки з іншими ризиками;
- ймовірність виникнення ризику;
- як ризик може вплинути на проєкт.

Прямі судження, ранжування варіантів, порівняльні варіанти та описовий аналіз також використовуються як якісний аналіз ризику.

Якісний аналіз може базуватися на ймовірностях матриці впливу, коли ймовірність і вплив кожного ризику оцінюються з використанням певних чинників нанесених на двовимірній решітці. Рис.1.3 ілюструє приклад матриці ризиків, запропонований WSDOT [25]. Наслідки оцінюються з точки зору потенційного впливу на критерії успіху проєкту. Коефіцієнти залежать від розміру проєкту, стратегії, рівня наявної інформації та необхідної точності. Ця матриця може бути використана для оцінювання загроз та можливостей за допомогою двох сіток негативних впливів (загроз) і позитивних впливів (можливостей). В обох випадках ризики з високою ймовірністю/високою віддачею є пріоритетними.




| Можливість (Ймовірність) | Синоніми | | Точність % |
|---|---|---|---|
| Дуже висока | Майже напевне | Дуже впевнено | ≥90% |
| Висока | Ймовірно | Досить впевнено | 80% |
| Середня | Можливо | Може бути | 50% |
| Низька | Навряд чи | Рідко | 20% |
| Дуже низька | Рідко | Неймовірно | ≤10 |
| **Наслідок (Вплив)** | **Синоніми** | | **Точність %** |
| Дуже високий | Дуже важливий | Дуже сильний | ≥10% |
| Високий | Критичний | Сильний | 8% |
| Середній | Помірний | Середній | 4% |
| Низький | Незначний | М'який | 2% |
| Дуже низький | Дуже малий | Дуже м'який | ≤1% |

Рисунок 1.3 – Приклад матриці ризиків

Аналіз ймовірності, аналіз чутливості, сценарний аналіз, аналіз моделювання, кореляційний аналіз, теорія портфеля, метод Дельфи, схеми впливу, дерева рішень, є дещо іншими доступними методами для якісного аналізу ризиків.

Напівкількісний аналіз ризиків дуже зручний у випадку швидкого чи порівняльного оцінювання. Він заснований на результатах якісного аналізу та ідентифікації числових значень за допомогою показників, а також заходів можливості, наслідків і пріоритетів.

Ризики можуть бути прораховані за допомогою стандартизованих показників. Наприклад, в [26] використано два показники частоти та тяжкості, і для кожного ризику визначався індекс значення як добуток частоти і тяжкості індексів (за 0-100% шкалою).

Кількісний аналіз спрямований на розрахунок сукупного ефекту ризику на цілі проєкту, використовуючи такі інструменти як аналіз чутливості, дерева рішень, метод Монте-Карло. Вони включають побудову моделі всього проєкту чи ключових елементів, що відображають невизначеності в моделі, і аналіз сукупного впливу на результат проєкту. Процес розрахунку зазвичай охоплює такі етапи:

1) моделювання проєкту і поділ на задачі;

2) оцінювання ступеня невизначеності в кожній плановій операції чи елементі витрат;

3) налаштування списку завдань проєкту, обмежень і прийнятних невизначеностей;

4) визначення взаємозв’язку між невизначеністю і ступенем ризику;

5) оцінювання проєкту в цілому, невизначеності/ризику та відповідного актора(ів).

Хоча перший крок не є необхідним для всіх методів кількісного аналізу ризиків, проте він забезпечує зручну базу для кращого розуміння проєктних ризиків.

Для опису невизначеності та їх наслідків для проєкту можуть бути використані багато методів. Опис ймовірностей є одним з найпоширеніших методів. Результатом є розподіл ймовірностей проєктної вартості й дати завершення на основі виявлених ризиків у проєкті. Інструменти кількісного аналізу дають змогу змоделювати загальний план проєкту. Використовуючи метод Монте-Карло, можуть бути змодельовані графік і розподіл витрат за проєктом. Від використання цих методів моделювання для визначення поширення в часі та вартості змінних, може бути встановлена ризикованість проєкту. Але на практиці, зазвичай, більшість рішень на основі якісного аналізу, легші та швидші в реалізації, ніж за допомогою кількісних оцінок.

Кількісні та якісні процеси аналізу ризиків порівнюються у табл.1.5. Ефективне виявлення ризиків, якісний аналіз ризиків і відповідних типових проєктних моделей, розгляд взаємодій ризиків, збір якісних і об’єктивних даних ризиків є важливими чинниками успіху для ефективного кількісного аналізу ризику.

Таблиця 1.5 – Порівняння процесів якісного і кількісного підходів

| Якісний аналіз ризику | Кількісний аналіз ризику |
|---|---|
| Опис індивідуальних ризиків | Прогнозування можливих результатів проєкту, заснованих на поєднанні впливу ризиків |
| Оцінка дискретної ймовірності виникнення та впливу на цілі | Використання ймовірнісних розподілів для характеристики ймовірності та впливу ризиків |
| Розподіл пріоритету індивідуальних ризиків для подальшої обробки | Використання моделі проєкту |
| Додавання до реєстру ризиків | Використання кількісного методу вимагає спеціальних інструментів |
| Приводить до кількісного аналізу ризиків | Оцінювання ймовірності досягнення цілей і невизначеностей, необхідних для досягнення бажаного рівня комфорту |
| | Визначає ризики з найбільшим впливом на загальні ризики проєкту |

Наступним кроком після виявлення й аналізу ризиків проєкту є розробка варіантів і визначення зручних дій, орієнтуючись на найзначущі ризики для збільшення шансів на користь успіху проєкту та мінімізації негативних наслідків загроз цілям проєкту. Цей процес спрямований на визначення ефективних дій реагування, які підходять за пріоритетом індивідуальних ризиків і загального ризику проєкту. Він враховує ризики відносин зацікавлених сторін проєкту і угод, зазначених у плані управління ризиками. Коли дії реагування застосовуються, вони впливають на цілі проєкту і можуть генерувати додаткові ризики. Вони відомі як вторинні ризики, яких потрібно проаналізувати і спланувати таким же чином, як і первинні ризики. Рис.1.4 надає ключові чинники успіху планування реагування на ризики.

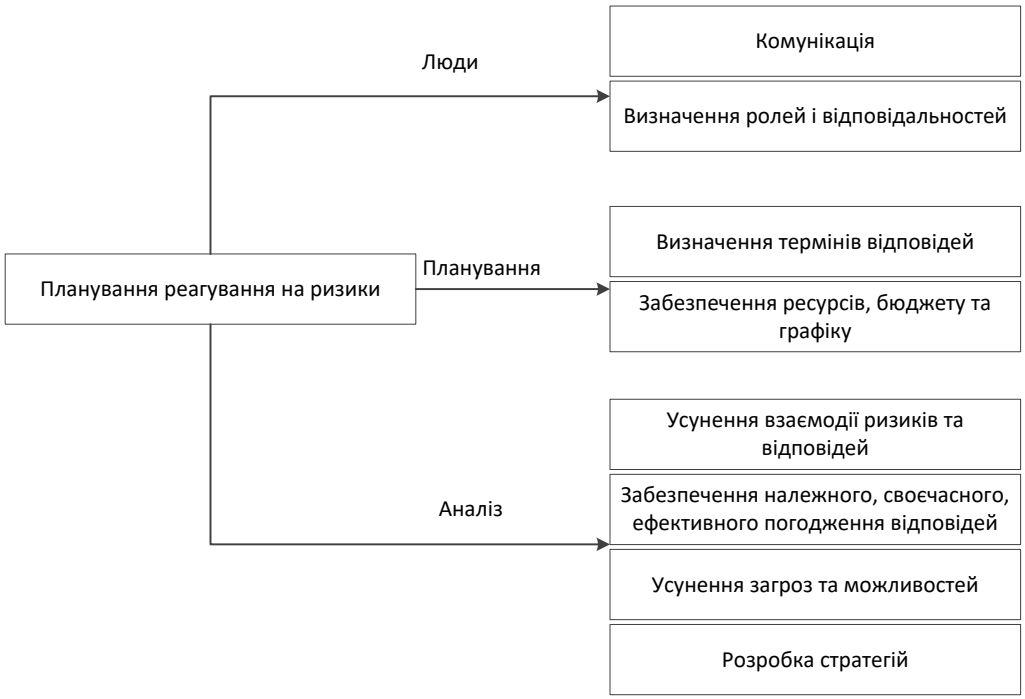



Рисунок 1.4 – Критичні чинники успіху для процесу реагування на ризики

Дія реагування на ризики (загрози) може бути одиничною або комбінацією таких варіантів:

– запобігання: полягає в зниженні ймовірності та наслідків загрози до прийнятного порогу. Воно може зайняти ресурси або час, а тому може бути компромісом однієї мети з іншою. Цей метод найширше використовується;

– уникнення: передбачає зміну плану проєкту для усунення ризику чи захисту цілей проєкту (строки, вартість, обсяг, якість) від його впливу. Коли організація чи замовник відмовляються ризикувати, то ризик уникається. Це означає, що експозиції ризику не дозволено існувати. Існує низка способів, за допомогою яких ризиків можна уникнути, наприклад, проведення торгів за дуже високими цінами, ставлячи умови на торгах, попередньо обговорюючи за контрактом, яка зі сторін приймає певні ризики, і яка не претендує на велику долю ризику контракту;

– перенесення: це стратегія перенесення ризику іншому партнеру чи третій стороні, яка краще може зреагувати на вирішення тієї чи іншої загрози. Цей метод зазвичай не усуває ризиків, а лише робить так, що хтось інший повинен турбуватися про це. Прикладом може бути передача фінансових наслідків ризику

страхової компанії. Інструменти переносу можуть бути досить різноманітні та охоплювати страхування, гарантії, санкції тощо;

– прийняття: ця стратегія застосовується, коли інші стратегії не можуть бути застосовані. У цьому методі вигоди, які можуть бути отримані від прийняття ризику, мають бути збалансовані з втратами. Тут не чиниться ніяких дій, якщо ризик фактично не відбувається. У цьому випадку надзвичайні чи резервні плани дій можуть бути розроблені заздалегідь, щоб бути реалізованими, якщо ризик проявить себе.

Планування реагування на ризики має поєднувати дії боротьби із загрозами, а також ті, які забезпечують відповідні можливості. Рис.1.5 зображує просту матрицю відповідальності, коли обрана дія залежить від ступеня ризику.

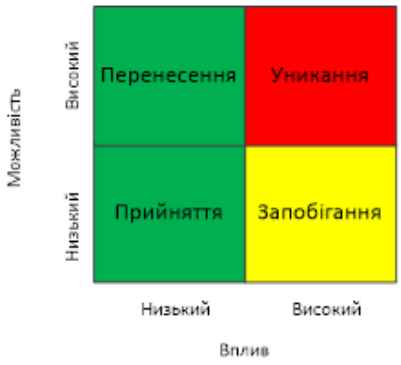



Рисунок 1.5 – Проста матриця відповідальності

Висновки до розділу 1

1. У розділі були детально розглянуті основні поняття управління ризиками проєкту, а також представлені деякі з найважливіших практик у сфері управління ризиками IT-проєктів.

2. Задля запобіганню будь-яких непорозумінь чи плутанини в наступних розділах уточнено основні терміни управління ризиками проєкту (наприклад, «проєкт», «ризик», «управління ризиками» тощо).

3. Розглянуто основні етапи процесу управління ризиками, представлено і порівняно різні доступні інструменти й методи ідентифікації та аналізу ризиків.

# 2 МЕТОДОЛОГІЯ РОЗРОБКИ СТРУКТУРНОЇ ДЕКОМПОЗИЦІЇ РИЗИКІВ

## 2.1 Концепція формування ієрархічної структури ризиків

Насамперед зазначимо, що концепція структурної декомпозиції ризиків (СДР) не пов’язана з однією особою чи конкретною датою запровадження, і немає загальновизнаного засновника цієї концепції, як і для деяких інших інструментів та методологій управління проєктами. Натомість, розвиток і використання СДР розвивалися з часом як частина ширшої сфери управління ризиками та управління проєктами. Вона була колективно розроблена і вдосконалена практиками, експертами та організаціями в цій галузі.

Багато науковців, практиків та організацій зробили свій внесок у розробку та застосування структур розбиття ризиків та пов’язаних з ними інструментів і методів управління ризиками. Ці внески походять з різних галузей, включаючи управління проєктами, системну інженерію та аналіз ризиків. Такі відомі організації, як Інститут управління проєктами (PMI) і Міжнародна організація зі стандартизації (ISO), опублікували настанови і стандарти, пов’язані з управлінням ризиками, в яких обговорюються питання СДР [27-31].

Ідентифікацію ризиків часто зводять до довгого переліку ризиків, якими важко керувати. Список може бути пріоритетним для визначення, які ризики мають бути першими за рейтингом, але це не дає ніякого уявлення про структуру ризиків за проєктом. Найкращий спосіб справитися з великою кількістю даних – структурувати інформацію для досягнення розуміння. Це може забезпечити структурна декомпозиція ризиків, яка групує виявлення ризикових подій на різних рівнях, розподіл проводиться знизу вгору [32].

Коротке визначення СДР стосовно проєктів наведено в стандарті ISO: «декомпозиція загроз і можливостей для проєкту чи програми» [33]. Більш ширше трактування можна знайти в 5-му виданні PMBOK: «ієрархічне представлення ризиків відповідно до їхніх категорій ризику» [22] та Інституту проєктного менеджменту: «Структурна декомпозиція ризиків (Risk Breakdown Structure) – це

ієрархічно організоване представлення ідентифікованих проєктних ризиків за категоріями та підкатегоріями ризиків, яке визначає різні сфери та причини потенційних ризиків» [27].

СДР є структурою, яка системно класифікує та організовує ризики в межах проєкту, програми чи організації. Вона є цінним інструментом в управлінні ризиками, який допомагає ідентифікувати, аналізувати та інформувати про потенційні ризики у структурований та зрозумілий спосіб. Суть концепції СДР полягає в її здатності розбивати складні ризикові сценарії на менші, більш керовані компоненти, що полегшує зацікавленим сторонам оцінювання та ефективне зниження ризиків.

Ієрархічна структура ризиків упорядковує ризики в деревоподібній структурі з кількома рівнями, починаючи з категорій високого рівня та поступово розбиваючи на більш детальні та конкретні чинники ризику. Такий структурований підхід має вирішальне значення для всебічного розуміння та управління ризиками.

СДР базується на таких поняттях (компонентах):

1. Ієрархія – система управління ризиками організована за ієрархічним принципом, де найвищий рівень представляє широкі категорії ризиків, а кожен наступний рівень розбиває ці категорії на детальніші підкатегорії чи окремі ризики. Ієрархія може розширюватися до декількох рівнів залежно від складності проєкту.

2. Категоризація – ризики класифікуються на основі різних критеріїв, таких як джерело ризику (внутрішнє чи зовнішнє), характер ризику (технічний, фінансовий, операційний тощо) або фаза проєкту, на якій ризик може виникнути (наприклад, планування, виконання, моніторинг або закриття).

3. Декомпозиція – ризики на вищих рівнях СДР розкладаються на менші, дрібніші ризики на нижчих рівнях, що допомагає провести детальний аналіз кожного ризику і полегшує розподіл обов’язків щодо зниження ризиків.

4. Зрозумілість і комунікація – СДР забезпечує чіткий і стандартизований спосіб інформування про ризики в проєктній групі. Це сприяє кращому розумінню та співпраці між зацікавленими сторонами й гарантує, що всі знаходяться на одній позиції стосовно потенційних ризиків.

5. Оцінювання ризиків – після ідентифікації та класифікації ризиків у межах СДР, їх можна оцінити з точки зору їхньої ймовірності та впливу на цілі проєкту. Це допомагає визначити пріоритетність ризиків і зосередити ресурси на найважливіших з них.

Ризики варто групувати в деревоподібну ієрархічну структуру, враховуючи такі моменти:

1. Групування ризиків в ієрархічному дереві забезпечує ясність і організацію. Це дає змогу зацікавленим сторонам побачити загальну картину, а також заглибитися в конкретні зони ризику. Ця структура спрощує складний ландшафт ризиків, розбиваючи їх на керовані частини.

2. Вона полегшує ідентифікацію ризиків, класифікуючи їх за природою, походженням або впливом. Також полегшує розпізнавання ризиків, які можна не помітити, розглядаючи їх ізольовано.

3. Ієрархічні структури допомагають визначити пріоритетність ризиків. Категорії високого рівня можуть представляти значніші ризики, і в міру просування вниз по дереву ризики стають детальнішими та керованішими. Пріоритизація ризиків на різних рівнях забезпечує розподіл ресурсів у найкритичніших сферах.

4. Вона покращує комунікацію між зацікавленими сторонами, ефективно передаючи інформацію про ризики, оскільки забезпечує загальну структуру для обговорення ризиків на різних рівнях організації.

5. Групуючи ризики, керівники проєктів можуть більш ефективно розподіляти ресурси. Вони можуть розподіляти спеціалізовані ресурси для конкретних категорій ризику на основі свого досвіду та фокусу.

6. Вказана структура допомагає в розробці цілеспрямованих стратегій зменшення ризиків. Після класифікації ризиків стає легше розробляти та впроваджувати стратегії, адаптовані до унікальних характеристик кожної категорії.

Кількість рівнів в ієрархії ризиків може змінюватися залежно від складності та конкретних потреб проєкту. Однак зазвичай використовують від трьох до п’яти рівнів ієрархічної структури ризиків.

Рівень 1 (верхній рівень) – найвищий рівень, де представлено широкі категорії ризику чи основні параметри ризику. Він містить огляд основних проблемних питань. На рівні 2 категорії першого рівня розбиваються на більш конкретні підкатегорії, котрі можуть представляти різні аспекти або чинники, що сприяють ширшим ризикам. Рівень 3 заглиблюється ще глибше, забезпечуючи додаткову деталізацію. Він може містити конкретні події ризику, причини або компоненти, пов’язані з підкатегоріями рівня 2. У деяких випадках рівень 4 може знадобитися для надзвичайно складних проєктів, пропонуючи додаткові рівні деталізації та конкретності. Рівень 5 (нижній рівень) відображає найконкретніші та найдетальніші ризики, часто зосереджені на окремих подіях або компонентах ризику. Він може містити детальні описи, потенційні впливи та стратегії пом’якшення.

За аналогією можна побудувати ієрархічну структуру ризиків, як у випадку WBS (Work Breakdown Structure) [33, 34]. Risk Breakdown Structure (RBS)[33] і WBS справді схожі за своєю структурою та підходом до організації та розгортання інформації, але вони використовуються для різних цілей в проєктному управлінні. У них є спільні моменти, а саме:

– якщо розглядати їхню загальну структуру, обидва підходи використовують ієрархічну деревовидну структуру. У випадку WBS ця структура розкладає проєкт на робочі пакети (робочі елементи), починаючи з високорівневих фаз та завдань і розгортаючи їх на дрібніші підзадачі;

– RBS також використовує принцип декомпозиції, де загальні ризики чи категорії ризиків розкладаються на конкретніші та докладніші ризики;

– обидва підходи допомагають в керуванні процесом – WBS допомагає визначити всі робочі елементи проєкту, тоді як RBS допомагає ідентифікувати та категоризувати ризики, що можуть впливати на проєкт.

Однак важливо розуміти, що їхні цілі та спрямування різняться:

– WBS є інструментом, що використовується для розкладання проєкту на окремі завдання та робочі пакети для забезпечення ефективного управління

проєктом. Це допомагає визначити, як будуть виконуватися завдання та контролюватися їхні строки та бюджет;

– RBS є інструментом для ідентифікації, класифікації та категоризації ризиків, які можуть вплинути на проєкт або організацію. Він допомагає розглядати ризики на різних рівнях і дає змогу зосередитися на стратегіях управління ризиками.

Отже, обидва підходи є корисними в ініціюванні та управлінні проектами, але вони використовуються для різних аспектів проєктного менеджменту: WBS – для роботи з завданнями та ресурсами, а RBS – для розгляду ризиків та управління ними.

Таким чином, обидва підходи корисні для ініціювання та управління проєктами, але вони використовуються для різних аспектів управління проєктами: WBS – для роботи із завданнями та ресурсами, а RBS – для розгляду та управління ризиками.

Хоча фундаментальна концепція СДР залишається незмінною в усіх галузях, конкретні категорії та елементи в ній можуть значно відрізнятися залежно від характеру проєкту чи галузі. Ось кілька основних особливостей, якими СДР для IT-проєктів може відрізнятися від проєктів в інших галузях.

Кожна галузь має власний унікальний набір ризиків, які є специфічними для її діяльності та процесів. Наприклад, IT-сфера може зіткнутися з ризиками кібербезпеки, проблемами розробки програмного забезпечення та застарілістю технологій, тоді як будівельні проєкти можуть зіткнутися з ризиками, пов’язаними з правилами безпеки, погодними умовами та дефіцитом матеріалів.

IT-проєкти часто передбачають високий рівень технічної складності, що може призвести до певного набору ризиків, пов’язаних із помилками програмного забезпечення, апаратними збоями, проблемами системної інтеграції та витоком даних. Ці технічні ризики не настільки поширені в інших галузях.

Різні галузі підпорядковуються різним нормативним вимогам і стандартам відповідності. Наприклад, проєкти в галузі охорони здоров’я можуть вимагати дотримання суворих правил захисту даних пацієнтів (наприклад, HIPAA у США

[35]), тоді як фінансові проєкти мають відповідати стандартам фінансової звітності та аудиту (наприклад, SOX [36]). IT-проєкти в цих галузях матимуть певні ризики, пов’язані з дотриманням нормативних вимог.

Наявність і розподіл ресурсів може значно відрізнятися між галузями. Наприклад, будівельні проєкти можуть бути більше заклопотані нестачею робочої сили, обладнання та матеріалів, тоді як IT-проєкти можуть зіткнутися з проблемами, пов’язаними з наявністю кваліфікованого персоналу та витратами на ліцензування програмного забезпечення.

Стадія та життєвий цикл проєкту також можуть впливати на склад СДР. Наприклад, ризики, пов’язані з ініціацією проєкту, можуть відрізнятися від ризиків на етапах виконання або закриття.

Масштаб і складність IT-проєктів можуть бути різними. СДР для великого багаторічного проєкту трансформації IT може містити більш детальні та численні ризики порівняно з меншим рутинним проєктом обслуговування IT.

Такі галузі, як фінанси, торгівля та готельний бізнес, сильно залежать від ринкової динаміки та конкуренції. Однак ризики, пов’язані зі зміною ринкових умов, уподобаннями клієнтів і конкурентним тиском, не такі значимі для IT-проєктів. Аналогічно, деякі галузі, такі як енергетика та виробництво, стикаються з підвищеною увагою до проблем навколишнього середовища та сталого розвитку. Ризики, пов’язані з екологічними нормами, виснаженням ресурсів і викидами вуглецю, можуть займати важливе місце в їхніх СДР.

Формування RBS для IT-проєктів зазвичай охоплює кілька етапів для систематичної ідентифікації, категоризації та організації ризиків (рис.2.1):


Рисунок 2.1 – Етапи формування RBS

Оскільки різні стандарти або настанови можуть пропонувати інше визначення концепції управління ризиками, надалі, щоб запобігти будь-якому непорозумінню або плутанині, будуть розглядатися поняття:

– чинник ризику: низка чинників, які в сукупності є потенціалом для шкоди, травми, пошкодження або втрат. Чинники ризику не впливають на проєкти чи діяльність безпосередньо, але можуть зробити це за допомогою ризикових подій;

– ризикова подія: будь-який факт або подія, чия поява може мати деякий вплив/наслідки, принаймні, на одну з цілей проєкту, і постраждалих від чинників ризику. Подія також може не відбутися. Часто відмінність між чинником ризику і ризиковою подією є дещо штучною, оскільки це залежить від того, наскільки ми повернемося до аналізу причин. Як приклад, «дизайн-проєкт не відповідає нормам стандартів і критеріїв» є ризиковою подією, яка сама по собі залежить від зазначених чинників ризику;

– категорія ризику: спосіб об’єднати декілька ризикових подій. Всі категорії можуть бути розділені на підкатегорії, коли потрібне детальніше представлення, або навпаки, можуть бути згруповані разом з іншими категоріями, коли потрібен загальніший вигляд.

СДР – загальний і дуже практичний інструмент, широко використовуваний на різних етапах життя проєкту в галузі управління ризиками. Він може бути використаний на етапі ідентифікації ризиків, і це може забезпечити підтримку на пізніших стадіях (оцінювання ризиків і реагування на ризики), так як він пропонує огляд ризиків, які впливають на проєкт.

Рис.2.2 ілюструє приклад СДР, запропонований в [32].

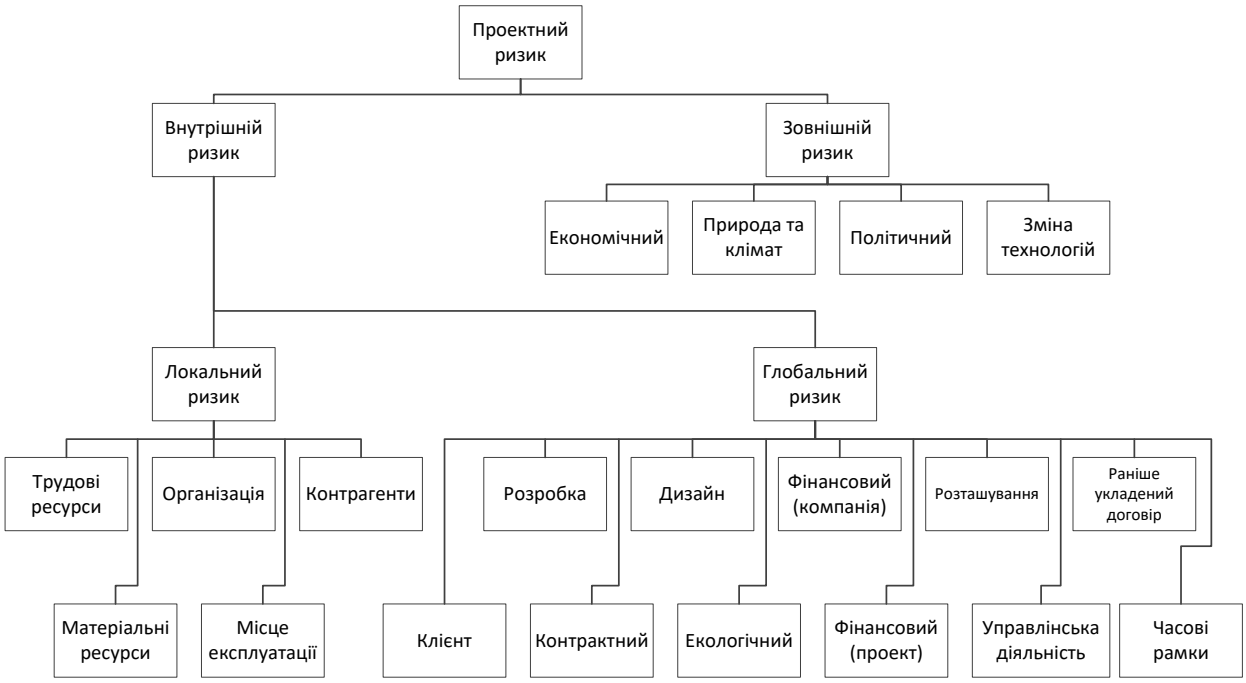



Рисунок 2.2 – Приклад СДР

Відомий ризик-менеджер Хіллсон [37] вважає, що СДР є потужним засобом виявлення, оцінювання та звітності щодо ризиків, а також можливість розподіляти знизу-вверх або згори-вниз, щоб відповідний рівень забезпечував нові ідеї в загальній схильності ризику проєкту. Спільну мову і термінологію полегшує крос-проєктна звітність та уроки навчання. СДР має потенціал, щоб стати найціннішим інструментом надання допомоги менеджеру проєкту для розуміння і управління ризиками проєкту. Тим не менш, СДР страждає деякими недоліками, такими як відсутність консенсусу як розробити СДР нового проєкту, відсутність ясності та непослідовність у визначенні категорій ризику, відсутність правил, які дають змогу передавати якісну/кількісну інформацію про ризики по структурі. Стосовно останнього випадку, загальних методів агрегації для оцінювання впливу всіх пов’язаних ризикових подій до кожної категорії ризику (вихідне максимальне значення, середнє значення, модифіковане середнє значення і т.д.) недостатньо, щоб розглянути обидва значення і кількість ризикових подій, котрі вплинули. Зазвичай, вони призводять до нереальних результатів.

Упродовж десятиліть були розроблені різні класифікації ризиків, проте більшість з них вважають, що джерело критеріїв є найважливішим. Також зазвичай

класифікують ризики як динамічний/статичний, корпоративний/індивідуальний, внутрішній/зовнішній, позитивний/негативний, прийнятний/неприйнятний, страховий/нестраховий і т.д. На сьогодні не існує будь-якого стандарту чи погодженості про те, як класифікувати ризики.

Рис.2.3 ілюструє СДР, запропоновану в [38], яка заснована на інтеграції всіх задіяних в проєкті сторін, і також відрізняє «внутрішні» і «зовнішні» ризики.

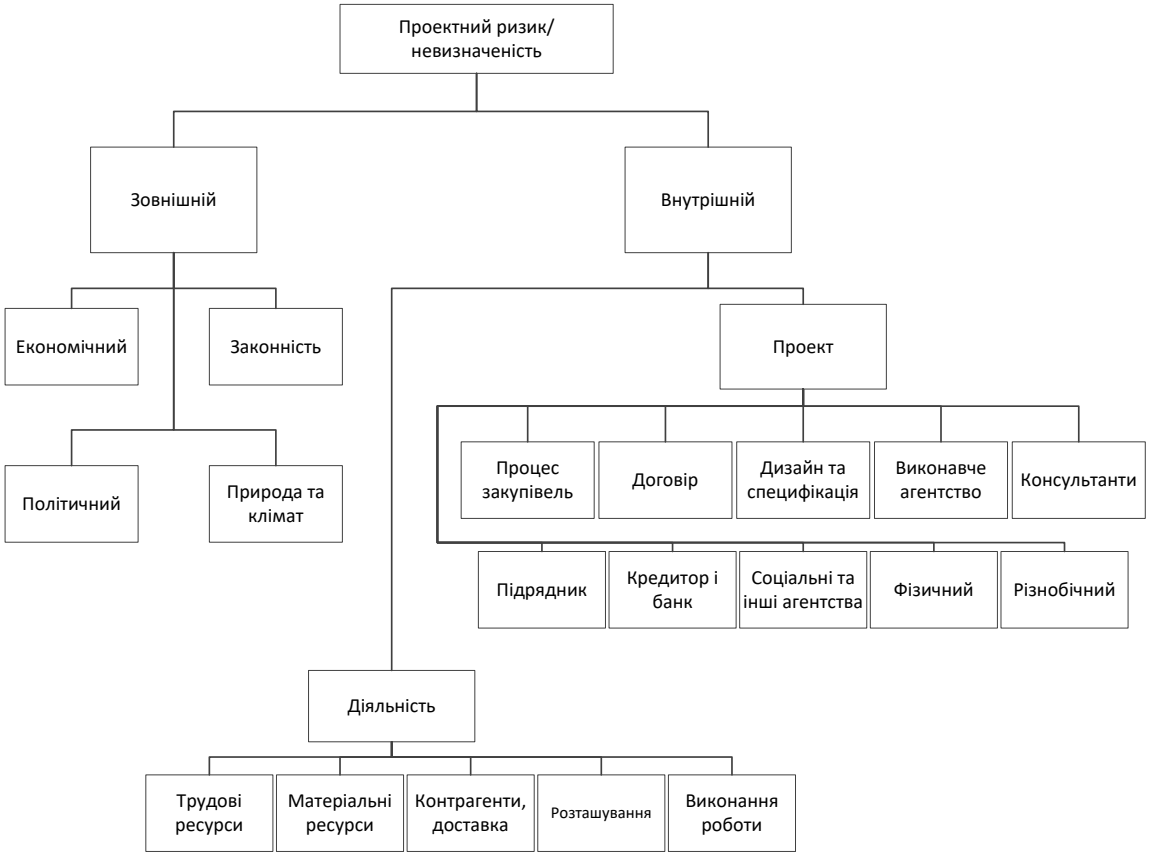



Рисунок 2.3 – Приклад СДР

Наведемо ще один приклад СДР (див. рис.2.4), де глобальні ризики проєкту розбиваються на три основні категорії – внутрішні, зовнішні та конкретні для певного проєкту.

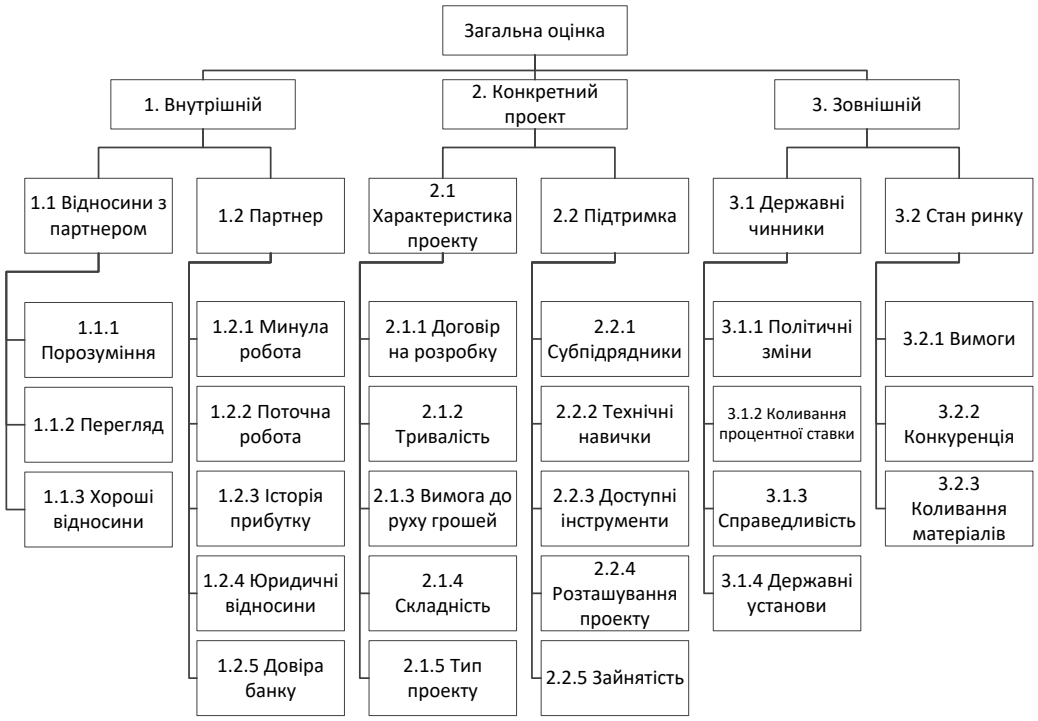



Рисунок 2.4 – Ієрархічна структура проєктних ризиків

Створення СДР (RBS) для IT-галузі передбачає організацію ризиків, характерних для проєктів або операцій у сфері інформаційних технологій, у ієрархічній структурі. Нижче наведено спрощений приклад RBS для IT-галузі (рис.2.5)

У цьому прикладі ієрархічна структура починається з категорій Рівня 1, наприклад «Ризики IT-проєкту», а потім переходить до підкатегорій Рівня 2 і Рівня 3, забезпечуючи дедалі більшу деталізацію. Це дає змогу IT-фахівцям і зацікавленим сторонам виявляти й усувати ризики на різних рівнях деталізації. Кожну підкатегорію можна додатково розширити, щоб включити конкретні події ризику, їхній потенційний вплив, стратегії пом’якшення та відповідальні сторони.

Проєктні системи, по суті, ризиковані, оскільки вони є унікальними, обмеженими, за умов невизначеності і складності. Вони складаються з багатьох взаємозалежних об’єктів різної природи і повинні досягти багатьох цілей, які можуть бути взаємопов’язані або навіть суперечливими.

| Рівень 1 | Рівень 2 | Рівень 3 | Рівень 4 |
|---|---|---|---|
| Ризики IT проєкту | Технічні ризики | Апаратні ризики | Несправність обладнання |
| | | | Недостатні апаратні можливості |
| | | | Проблеми сумісності |
| | | Ризики програмного забезпечення | Програмні помилки та збої |
| | | | Проблеми інтеграції ПЗ |
| | | | Питання ліцензування та комплаєнсу |
| | | Мережеві ризики | Простої мережі |
| | | | Порушення безпеки мережі |
| | | | Обмеження пропускної здатності |
| | Ресурсні ризики | Ризики людських ресурсів | Дефіцит кваліфікованих кадрів |
| | | | Плинність ключових кадрів |
| | | | Конфлікти розподілу ресурсів |
| | | Фінансові ризики | Перевитрати бюджету |
| | | | Непередбачувані витрати |
| | | | Коливання валютних курсів |
| | Ризики, пов'язані з розкладом | Ризики планування проєкту | Неточний розрахунок часу |
| | | | Повзучість обсягу |
| | | | Нереалістичні графіки проєктів |
| | | Зовнішні залежності | Затримки у виконанні робіт третіми сторонами |
| | | | Регуляторні погодження |
| | | | Ризики, пов'язані з постачальниками |
| | Безпекові ризики | Ризики безпеки даних | Порушення даних |
| | | | Несанкціонований доступ |
| | | | Втрата даних |
| | | Ризики кібербезпеки | Атаки шкідливих програм та програм-вимагачів |
| | | | Спроби фішингових атак |
| | | | Уразливості в IT-системах |
| | Комплаєнс-ризики | Дотримання нормативів | Недотримання галузевих норм і правил |
| | | | Юридичні та комплаєнс-питання |
| | | Конфіденційність даних | Порушення вимог GDPR |
| | | | Порушення захисту персональних даних |
| | | | Недотримання політики конфіденційності |

Рисунок 2.5 – RBS для проєктів у IT-галузі

Події ризику проєкту взаємопов’язані, тобто не є незалежними подіями. Більшість сучасних методик нехтують існуючими взаємодіями і розглядають їх як незалежні. Однак, в деяких роботах моделюються складні взаємозв’язки між подіями ризику. У дослідженні [39] була запропонована методологія кластеризації на основі взаємодій, спрямована на сприяння координації комплексних проєктів за рахунок зниження інтерфейсу при роботі з ризиками. Метод заснований на

кластеризації ризикової події таким чином, що швидкість взаємодії максимальна всередині кластерів і мінімальна зовні.

Для представлення цих взаємодій між різними РП в [40] запропоновано використовувати орієнтований граф. У цьому випадку кожній стрілці присвоюється мітка, в т.ч. трьом параметрам (тип, і, р). «Тип» вказує на форму взаємодії, які можуть бути одним із зазначених випадків, а «і» і «р» вказують на кількість змін за ймовірністю та впливу цілі події ризику (рис.2.6).

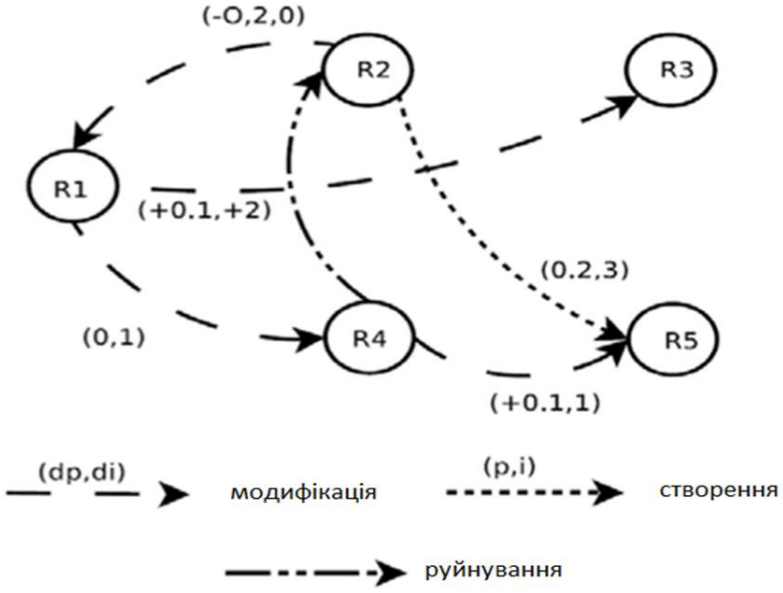



Рисунок 2.6 – Застосування орієнтованого графа
представлення взаємозалежності ризиків

Взаємозалежності ризику можна застосовувати в аналізі ризиків за допомогою ієрархічної структури ризиків. Взаємозалежність ризику може бути розташована навіть на рівні категорії ризиків. Таким чином, ймовірність кожної категорії ризику в СДР можуть бути порушені значеннями іншої категорії. Рис.2.7 надає приклад цього методу. У цьому СДР RC#3 залежить від двох подій, а також RC#4 ризику, яка сама залежить від трьох ризикових подій.

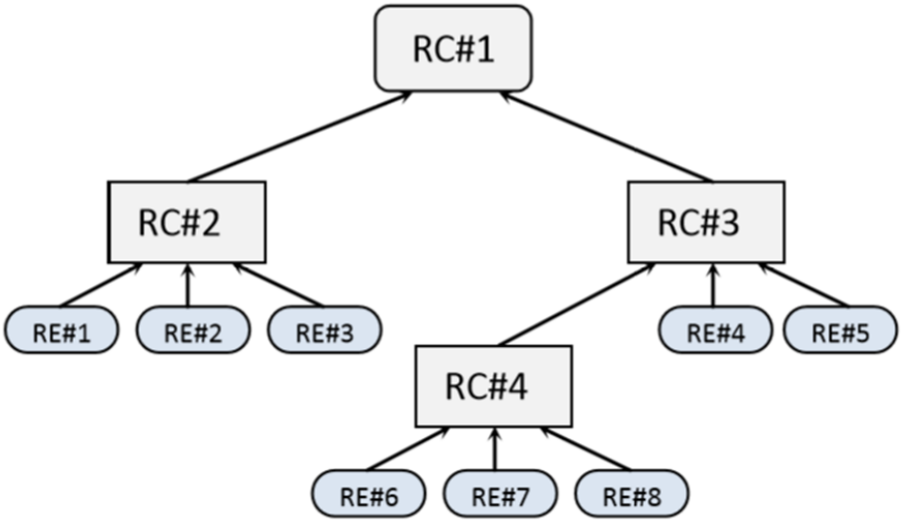



Рисунок 2.7 – Взаємодія ризиків у аналізі ризиків за допомогою СДР

Уже згадувалося, що ідентифікація взаємозалежностей ризику допомагає не лише точному процесові аналізу ризиків, а й ідентифікації нових ризикових подій. У пропонованому способі найважливіші виявлення ризикових подій представлені по колу і взаємодії між ними зображені векторами (рис.2.8). Ризикові події, як початкова точка багатьох стрілок взаємодій, є ключовими ризиковими подіями, котрі за умови виникнення можуть мати значний вплив на проєкт. З іншого боку, ризикова подія може бути спричинена багатьма іншими РП, а тому ймовірність виникнення може істотно зрости. Маючи таку інформацію, управління ризиками проекту стає проактивним і дає змогу менеджерові проєкту краще контролювати взаємодії між ризиковими подіями.

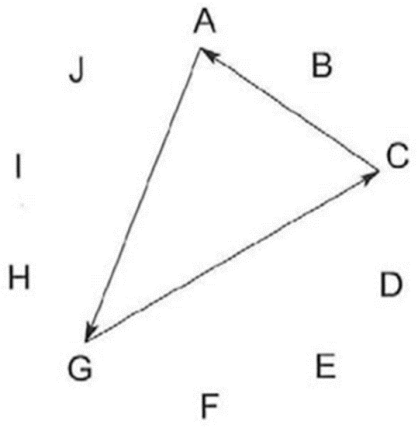



Рисунок 2.8 – Представлення взаємозалежностей ризиків

Виявлення взаємодій ризиків в аналізі ризиків проєкту не є головною ціллю. Однак пропонована методологія використовується для генерації індивідуальних СДР і процесу аналізу ризиків.

## 2.2 Процес побудови структурної декомпозиції ризиків

Управління проєктними ризиками є динамічним процесом упродовж життєвого циклу проєкту і містить звичайні етапи виявлення ризиків, аналізу ризиків (якісний або кількісний), реагування і управління ризиком, щоб гарантувати, що цілі проєкту будуть виконані. Цей процес є ітеративним, оскільки на кожному етапі проєкту з'являється нова інформація і можуть відбутися нові події, які потребують оновлення стратегії. Існує безліч інструментів, які можуть бути використані для зв'язку виявлених ризиків для зацікавлених сторін, таких як регістри ризику, матриці ризиків та карти ризиків проєкту. Ієрархічний опис ризиків вельми практичний інструмент, який полегшує управління ризиками. Він може базуватися на структурній декомпозиції ризиків, яка пропонує глобальний погляд на ризики.

В літературі було запропоновано багато підходів до класифікації ризиків [41-44]. Переважно класифікують ризики залежно від їх походження в двох основних групах – внутрішніх і зовнішніх ризиків. Також їх поділяють за природою і величиною, вказуючи різницю між первинними і вторинними ризиками. Ділять ризики залежно від їх величини і важливості на три основні групи: верхні, середні та нижні ризиків. Існує й спеціальна класифікація ризиків щодо різних етапів проєкту та розподілу ризиків між різними партнерами проєкту. Проте сьогодні не існує стандарту про те, як класифікувати ризики.

Розглядуваний нами підхід має низку переваг:

– пропонується штучний погляд на ризики, які можуть бути згруповані в кілька категорій ризиків, що охоплюють ряд ризикових подій. Такий погляд корисний, коли учасники проєкту повинні обговорювати ризики. Він забезпечує

перспективу знань, звідки ризики беруться і де вони зосереджені. Маючи групи подібних ієрархічно організованих ризиків, легше знайти дублюючі ризики і визначити залежності між ризиками. Крім того, можна встановити, як різні ризики корелюють між собою. Це може бути важливим для відстеження походження ризиків;

– кожна із зацікавлених сторін може мати свою власну точку зору на проєкт, тоді СДР може бути корисною на будь-якій стадії проєкту, пропонуючи різні представлення одних і тих самих знань, будучи впевненим, що різні представлення залишаються незмінними;

– СДР сумісна в часі з еволюційним і динамічним характером ризиків проєкту. Вона може «жити» з проєктом, його гілки можуть бути більше чи менше розвинені (або замінені іншими), коли деякі категорії ризику змінюють свою важливість і адаптуються до рівня наявної інформації і бажаної уваги користувача;

– метод дає змогу збирати інформацію з гілок, від основи до вершини, якщо були визначені правила для цієї агрегації (наприклад, як наслідки ризикових подій варіюються на різних рівнях дерева);

– СДР може бути доповнена другим представленням, які можуть бути об’єднані таким чином, щоб утворити «ієрархічну матрицю».

Однак СДР страждає низкою недоліків, головним з яких є відсутність єдиної точки зору на те, як розробляти СДР. Наприклад, на першому рівні можлива структуризація полягає в розділенні «проєктних ризиків» на «внутрішні ризики» і «зовнішні ризики». Проте інші можливості полягають у розділенні за фазами проєкту (ініціація, планування, реалізація, тестування, ...) або відповідно з різними зацікавленими сторонами (клієнт, консультант, ...). Насправді, кожен користувач розробляє власну СДР без дотримання будь-яких керівних настанов. Результатом є те, що неможливо визначити «хороші напрацювання» для розвитку СДР, причому відсутність ясності та непослідовність не є рідкістю.

У загальному випадку не існує чіткого визначення розуміння категорій ризиків, оскільки одні й ті ж можуть охоплювати різні елементи. Інша складність випливає з визначення правил, що дає змогу передавати якісну/кількісну

інформацію про ризики вздовж усього дерева. Чутливість результатів до правил заслуговує уважного вивчення. Однією з основних критик СДР є те, що вони мають труднощі виявлення взаємодій між ризиками через їхню ієрархічну структуру, коли основні процеси реального проєкту є більш складними. Тому наша мета полягає в розробці методології, яка враховує вигоду всіх переваг СДР, нівелюючи її недоліки.

Дане дослідження спрямоване на розробку алгоритму для проєктування СДР, щоби більш ефективним способом визначати і організовувати ризики в IT-проєктах. Цей метод може забезпечити суттєву інформацію для прийняття обґрунтованого рішення, щоб вибрати ефективні відповідні дії (уникнення, перенесення, прийняття і т.д.). Однією з цілей є те, що в кожному новому проєкті різні сторони, підпорядковуючись загальному керівництву, матимуть можливість будувати свої власні СДР відповідно до їх цілей і їхнього окремого погляду на проєктні ризики, тоді як загальна думка про ризики також залишиться. Це зробить можливим «багатомасштабний підхід», в якому кожен партнер може зосередитися на деяких особливих ризиках і розвивати СДР за допомогою ще кількох підкатегорій в конкретних областях. Звичайно, методика повинна бути, з одного боку, достатньо загальною, щоб охопити всі IT-проєкти загалом і, другого боку, досить конкретною, щоб бути адаптованою до даного конкретного проєкту.

Ця методика заснована на:

– створенні системи ризикових подій і категорій ризику, на основі огляду існуючої літератури;

– ідентифікації бази даних елементарних дерев, або мікродерев, які показують, як кожну категорію ризику (КР) можна поділити на підкатегорії. Кожне мікродерево визначається «батьківським вузлом» КР, можливими підкатегоріями в безпосередньо нищому рівні, зв’язками з іншими мікродеревами, щоб забезпечити сумісність і уникнути дублювання чи змішування, коли СДР буде побудована. Ця база даних може містити як конкретні дерева, які є унікальними, так і загальні дерева, які можуть бути продубльовані в СДР, бо така ж структура може з’явитися в декількох місцях (наприклад, кілька фаз проєкту або декілька зацікавлених сторін);

– узагальненні бази знань, яка містить ризикові події, категорії ризиків і мікродерева, будуючи набір зв’язків, що формалізує всі можливі ієрархічні зв’язки;

– визначенні низки критеріїв, які дають змогу кількісно оцінити «якість» в СДР. Питання якості є центральним, оскільки немає «оптимальної СДР», а є СДР, які більш-менш пристосовані до даної ситуації та конкретної мети;

– розробці стратегії для побудови СДР, яка задовольняє основним вимогам для даної ситуації. Ця стратегія заснована на ієрархічній природі СДР і на тому факті, що вона є масштабована і тому повинна бути адаптована «в реальному часі»;

Останній пункт визначатиме правила, що дають можливість передавати інформацію від нижньої до верхньої частини СДР.

Дане дослідження засноване на аналізі та огляді літератури з управління ризиками, щоб:

– ідентифікувати, для кожної СДР її загальну типологію і яким цілям відповідає структуризація;

– визначити логічні зв’язки між КР в кожній СДР (Як категорії структуруються? Які ризикові події вони охоплюють? Які ризикові події вони виключають?);

– визначити набір простіших ризикових подій при заданому рівні деталізації, і як вони можуть бути згруповані за категоріями.

Рис.2.9 ілюструє процес розробки відповідної бази даних, де аналіз проводиться у поєднанні методами знизу-вгору і зверху-вниз.

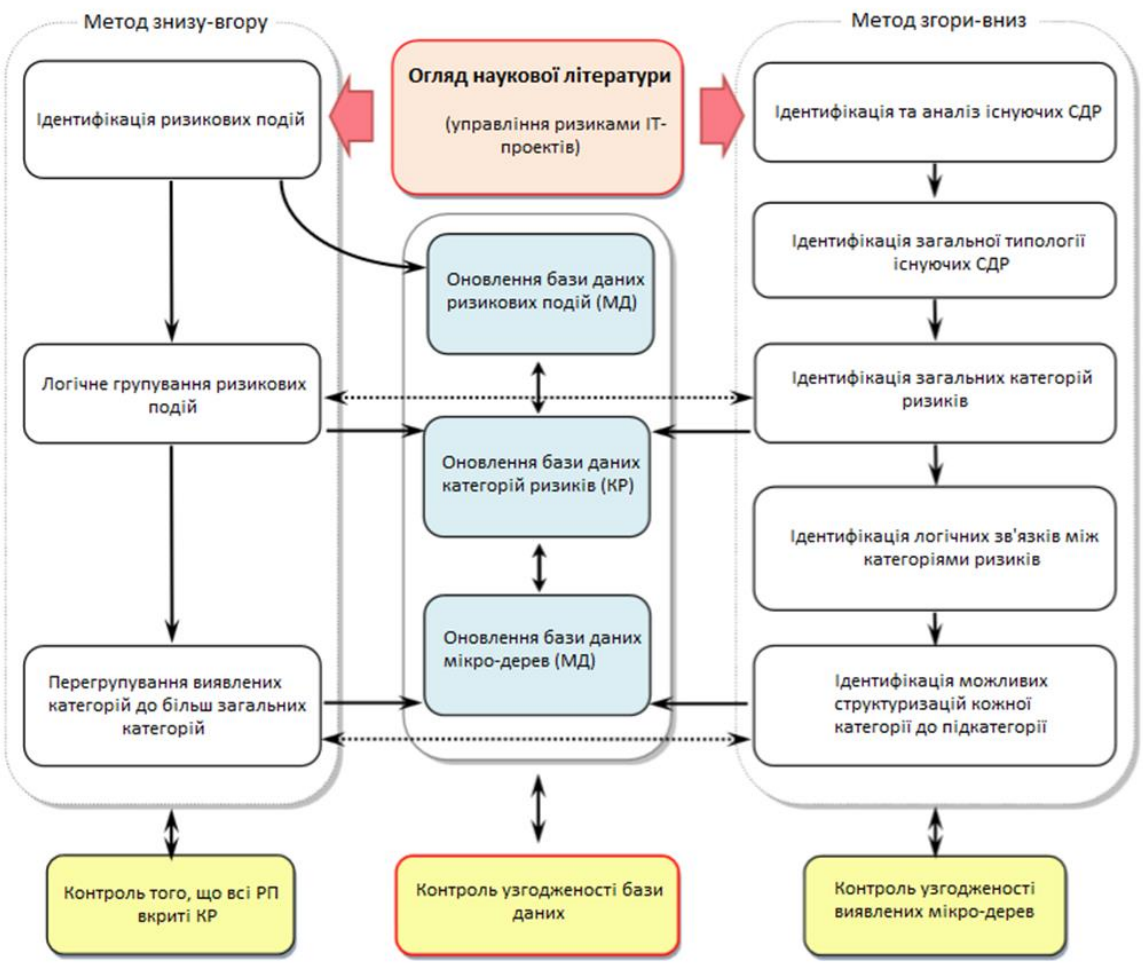



Рисунок 2.9 – Розробка бази даних ризикових подій, категорій ризиків і мікродерев

Метою було не отримання вичерпності, яка, очевидно є недосяжною, а однорідно покрити основні області ризиків в ІТ-проєктах. Цей аналіз дав змогу виявити багато плутанини і протиріч. Наприклад, в [6] ризики проєкту поділяються на внутрішні і зовнішні ризики, далі останній розкладається на три підкатегорії: контрактних документів, виконання власником і проблем з місцевою владою. Наприклад, важливі ризикові події, пов’язані з управлінням проєкту, продуктивність та внутрішні фінансові проблеми інших зацікавлених сторін проєкту не можуть бути покриті будь-якою з цих трьох категорій, тоді як всі з них будуть розглядатися як внутрішні ризики проєкту.

Підхід заснований на комбінації знизу-вгору (від базової ризикової події (РП) до глобального проєктного ризику) і підходу зверху-вниз, де глобальний ризик

проєкту розбивається на кілька КР, кожен з яких потім розкладають до необхідного рівня, при якому РП можуть бути прикріплені до КР.

Синтез усіх цих даних, спрямований на створення бази даних, яка містить три інтерактивні компоненти (рис.2.10):

– бібліотеку ризикових подій;
– бібліотеку категорій ризиків;
– бібліотеку мікродерев.

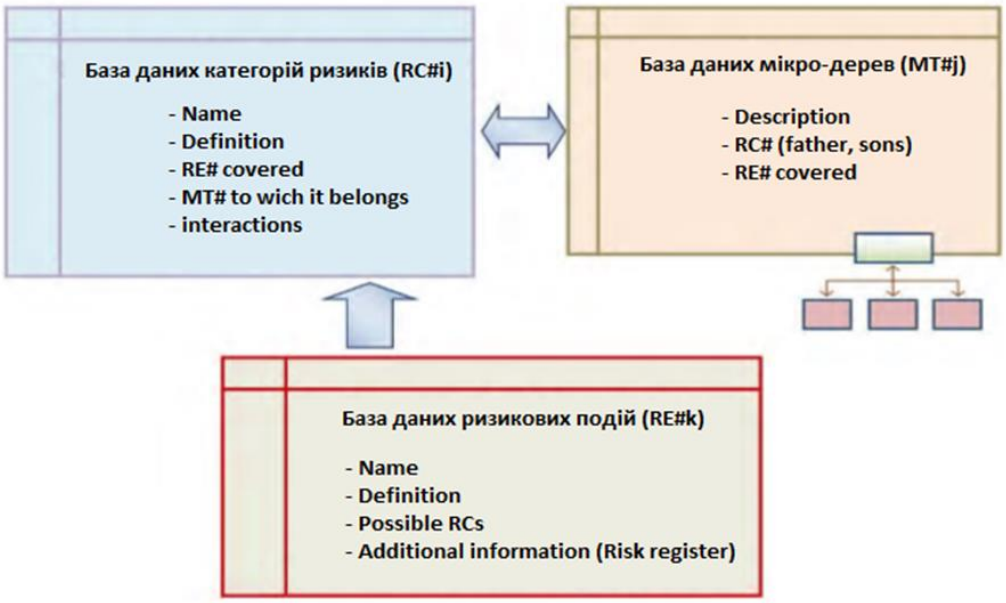



Рисунок 2.10 – Зв’язки між трьома компонентами бази даних

Ризикові події розглядаються як будь-який факт або подія, чия поява може мати деякий вплив/наслідки, принаймні на одну з цілей проєкту. Подія також може складатися з чогось, що не відбувається.

Аналіз ризиків призводить до великої кількості РП, які потім можна класифікувати. Етап класифікації полягає у визначенні всіх КР, до яких можуть належати РП. Однією з практичних трудностей є те, що база даних КР розвивається паралельно, таким чином, вимагає ітераційної перевірки. Табл.2.1 є невеликою частиною найчастіших ризикових подій, доступних в базі даних РП.

Таблиця 2.1 – Список найчастіших РП в IT-проєктах з деякими прикладами КР

| Категорія ризику | Приклад ризикової події |
|---|---|
| Графік | Розклад не реальний, тільки у «кращому випадку».<br>Важливе завдання відсутнє в розкладі.<br>Затримка в одній задачі призводить до затримок залежних задач.<br>Незнайомі області продукту займають більше часу, ніж очікувалося, щоб спроектувати і реалізувати. |
| Вимоги | Вимоги були чітко визначені, але продовжують змінюватися.<br>Вимоги погано визначені, і подальше визначення розширює задачі проекту.<br>Зазначені ділянки продукту вимагають більше часу, ніж очікувалося.<br>Вимоги лише частково відомі на початку проекту. |
| Проектне управління | Проектний менеджер має мало повноважень у структурі організації і мало особистої сили, щоб впливати на прийняття рішень і ресурси.<br>Зміна пріоритетів існуючої програми.<br>Ключові критерії успіху проекту не чітко визначені, щоб перевірити успішне завершення кожної фази проекту.<br>Проекти у рамках програми часто потребують одні й ті ж ресурси в той же час.<br>Мало уваги оцінці проектної команди. |
| Програмний продукт/технологія | Розробка неправильного користувальницького інтерфейсу в реконструкції та реалізації.<br>Розробка додаткових програмних функцій, які не потрібні, розширює графік.<br>Вимоги для взаємодії з іншими системами, що не знаходяться у задачах команди.<br>Залежність від технологій, які досі в стадії розробки, подовжує графік.<br>Обрана технологія мало збігається із проблемами або інтересами замовника. |
| Замовник | Замовник наполягає на нових вимогах.<br>Замовник оцінює/вирішує цикли планів, прототипів і технічних характеристик повільніше, ніж очікувалося.<br>Замовник наполягає на технічних рішеннях, які подовжують графік.<br>Замовник не братиме програмне забезпечення, що поставляється, хоча воно відповідає всім вимогам.<br>Замовник має надії на швидкості розробки, яку розробники не можуть забезпечити. |

| | |
|---|---|
| Трудові ресурси і підрядники | Критична задача розробки виконується одним розробником.<br>Деякі розробники можуть покинути проект, перш ніж він буде закінчений.<br>Процес найму займає більше часу, ніж очікувалося.<br>Персоналу потрібен додатковий час, щоб вивчити незнайомі програмні засоби, апаратні засоби і мови програмування.<br>Персонал може піти до завершення проекту.<br>Конфлікти між членами групи внаслідок поганої комунікації, поганого дизайну, помилок інтерфейсу і додаткового доопрацювання.<br>Персонал з критичними навичками, які необхідні для реалізації проекту, не можна знайти.<br>Підрядник не доставляє компоненти вчасно. |

У базі даних, кожна ризикова подія, яка ідентифікується унікальним кодом (RE#i) і має унікальне описове визначення, пов’язана з відповідними категоріями, управляється глобальною цілісністю бази даних.

Категорія ризику – це група з кількох ризикових подій. Всі категорії можуть бути розділені на підкатегорії, коли потрібно детальніше уявлення або навпаки згруповані з іншими категоріями, коли потрібний загальніший вигляд.

Розробка бази даних КР піднімає той же тип запитань, що і база даних РП. Бібліографічний аналіз привів до багатьох КР, вони були детально розглянуті, для забезпечення узгодженості. Процес моделювання знань в основному емпіричний і повторюваний, так як категорії ризику і їх відносна організація в мікродеревах визначаються разом. Насправді, на цьому етапі назви категорій виправлені так, щоб зменшити їх загальну кількість, тоді як вони охоплюють широкий спектр чинників ризику/подій.

У базі даних кожна КР ідентифікується унікальним кодом (RC#i) та іменем і має опис, який точно пояснює тип ризиків, які беруть участь. КР, які не є батьківським вузлом будь-якого МД в базі даних називаються «категорії нижнього рівня», до яких РП можуть бути повторно додані. Для всіх інших КР РП кріпляться побічно через зв’язок «батько-син». У заключних СДР, які будуть побудовані в комбінації МД, ці категорії не можуть бути більше структуровані, а тому представлені на останніх рівнях СДР. Це не внутрішня властивість КР, так як нові

МД можуть бути додані в базу даних, щоб структурувати нижню категорію, якщо це є корисним.

РП мають прямі зв’язки з категоріями нижнього рівня і непрямі зв’язки з іншими. У базі даних для кожної РП визначаються лише прямі посилання, а непрямі посилання генеруються зв’язком «батько-син» в МД. Як приклад, на рис.2.11 RE#f має прямий зв’язок з RC#i, яка є нижнім рівнем і непрямі посилання на RC#j та RC#k, так як вони є «батько» і «дідусь» цієї категорії. Не лише виявлені КР повинні відповідати локально в базі даних КР, а й узгодженість має контролюватися з іншими частинами (РП і МД).

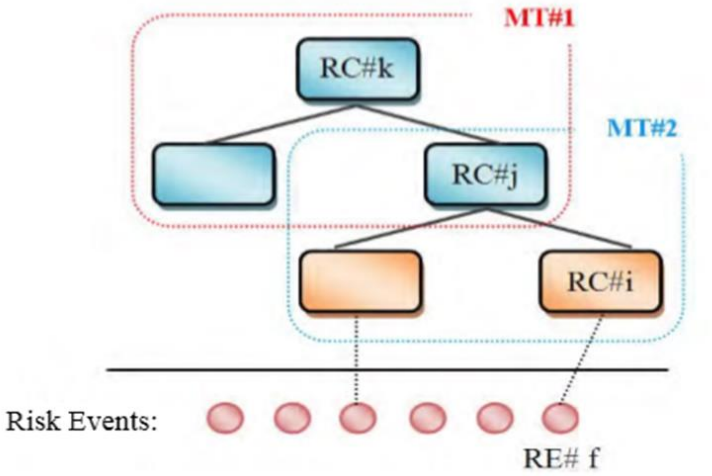



Рисунок 2.11 – Прямі і непрямі зв’язки РП із КР

Як вказувалося, можливості класифікації проєктних ризиків у літературі широкі: за діями, фазами проєкту, за природою тощо. Марно шукати єдину оптимальну структуру. Таким чином, підхід заснований на ідентифікації окремих категорій відповідних ризиків, а потім на їх ієрархічній організації у вигляді елементарних дерев (мікродерев).

Мікродерево визначається як структуризація кожної категорії ризику на підкатегорії або, іншими словами, зв’язок між «батьком» і «сином». Пошук елементарних дерев здійснюється на основі ретельного аналізу існуючих СДР, опублікованих у технічній та науковій літературі в галузі управління ризиками ІТ-проєктів. База існуючої СДР готується синтетично, зберігаючи всі ієрархічні зв’язки в деталях.

Табл.2.2 є прикладом синтезу існуючих СДР для знаходження логічних зв'язків КР. У цій таблиці представлено частковий аналіз категорії «Зовнішні ризики». Рівень категорій в СДР, «батьківський» вузол, «брати», підкатегорії і типологія загалом досліджуваних СДР є проаналізованими параметрами для кожної категорії.

Таблиця 2.2 – Синтез структуризації категорії ризиків «Зовнішні» в СДР

| Код СДР | Загальні властивості | | Підкатегорії | Рівні категорії |
|---|---|---|---|---|
| СДР1 | Назва категорії: | Зовнішні ризики | Політичні<br>Соціальні та культурні<br>Економічні<br>Природні<br>Інші | Внутрішні |
| | Рівень в СДР: | 1 | | |
| | Кількість підкатегорій: | 5 | | |
| | Кількість категорій одного рівня: | 1 | | |
| | Батьківський вузол: | Проектні ризики | | |
| СДР2 | Назва категорії: | Зовнішні ризики | Здійсненність<br>Дизайн<br>Реалізація<br>Експлуатація | Клієнт<br>Дизайнери<br>Підрядники<br>Поставник и<br>Уряд |
| | Рівень в СДР: | 1 | | |
| | Кількість підкатегорій: | 4 | | |
| | Кількість категорій одного рівня: | 5 | | |
| | Батьківський вузол: | Проєктні ризики | | |
| СДР4 | Назва категорії: | Зовнішні ризики | Дія третіх персон<br>Непередбачені обставини | Внутрішні |
| | Рівень в СДР: | 1 | | |
| | Кількість підкатегорій: | 3 | | |
| | Кількість категорій одного рівня: | 1 | | |
| | Батьківський вузол: | Проектні ризики | | |
| СДР5 | Назва категорії: | Зовнішні ризики | Законодавство<br>Курси валют<br>Конкуренція<br>Політика<br>Країна<br>Соціальний тиск<br>Форс-мажорні обставини | Технічний ризик<br>Ризик управління<br>Комерційн ий ризик |
| | Рівень в СДР: | 1 | | |
| | Кількість підкатегорій: | 11 | | |
| | Кількість категорій одного рівня: | 3 | | |
| | Батьківський вузол: | Проектні ризики | | |
| СДР6 | Назва категорії: | Зовнішні ризики | Непередбачені обставини<br>Політика<br>Економіка<br>Соціальні | Ризик управління<br>Проєктна реалізація<br>Плануванн я |
| | Рівень в СДР: | 1 | | |
| | Кількість підкатегорій: | 4 | | |
| | Кількість категорій одного рівня: | 3 | | |
| | Батьківський вузол: | Проєктні ризики | | |

| | | | | |
|---|---|---|---|---|
| СДР7 | Назва категорії: | Зовнішні ризики | Легальність<br>Політичні і соціальні<br>Субпідрядник і постачальник<br>Форс-мажорні обставини<br>Економічні | Організаційні ризики<br>Технічні ризики |
| | Рівень в СДР: | 1 | | |
| | Кількість підкатегорій: | 5 | | |
| | Кількість категорій одного рівня: | 2 | | |
| | Батьківський вузол: | Проектні ризики | | |
| СДР8 | Назва категорії: | Зовнішні ризики | Стихійні лиха<br>Злочинність<br>Непродуктивна праця<br>Війна | Внутрішні Ризик управління |
| | Рівень в СДР: | 1 | | |
| | Кількість підкатегорій: | 4 | | |
| | Кількість категорій одного рівня: | 2 | | |
| | Батьківський вузол: | Проєктні ризики | | |
| СДР38 | Назва категорії: | Зовнішні ризики | Політичні та економічні<br>Природні та екологічні чинники<br>Чинники третіх осіб | Внутрішні |
| | Рівень в СДР: | 1 | | |
| | Кількість підкатегорій: | 3 | | |
| | Кількість категорій одного рівня: | 1 | | |
| | Батьківський вузол: | Проєктні ризики | | |

Щоб зрозуміти логіку, яка склалася для розробки бази даних МД, є простий спосіб – дивитися на вищий рівень («рівень 0»), де три варіанти переважають для структуризації глобальних ризиків проєкту. Глобальні ризики найчастіше розбиваються на:

– внутрішні і зовнішні ризики, пов’язані з джерелом ризиків;

– ризики, пов’язані з фазами проєкту, і ризики інтерфейсів між фазами (категорія «ризики проєкту» розкладена на підкатегорії «техніко-економічна», «договір», «дизайн», «реалізація», «експлуатація» і «управління»);

– ризики, пов’язані з учасниками проєкту, і ризики інтерфейсів між ними (категорія «проєктні ризики» розкладається на підкатегорії «учасники проєкту», «зовнішні ризики» і «управління»).

В останніх двох випадках ризики інтерфейсів, які можна назвати як «управління проєктними ризиками» мають важливе значення. Добре відомо, що ризики часто з’являються на інтерфейсах, вони будуть з’являтися у випадку поганого управління. Ефективне управління зв’язками між проєктом та зацікавленими сторонами є важливим ключем до успіху проєкту.

Генерація кожного з цих мікродерев була заснована на аналізі наявної інформації в базі даних СДР (для зовнішніх ризиків, табл.2.2), щоб визначити всі ризики, які мають бути охоплені кожною категорією, виявляючи заплутані та суперечливі випадки в структурах, а потім запропонувати мінімальну кількість підкатегорій, які повністю покриють відповідні категорії ризиків. Також варто перевірити, чи пропоновані підкатегорії не перекриваються між собою. Так аналіз наведених у табл.2.2 даних призвів до знаходження багатьох неточностей. Наприклад, в СДР7 категорія «Субпідрядник і постачальник» розглядається як зовнішній ризик проєкту. У СДР5 підкатегорія «Зовнішні ризики», таких, законодавство, курси валют і політика перетинаються з категорією «Країна». Такий аналіз пропонує мікродерева, проілюстровані на рис.2.12.


Рисунок 2.12 – Декомпозиція «зовнішніх ризиків» (три різних мікродерева)

Інші приклади, якими можна проілюструвати декомпозицію глобальних ризиків проєкту:

– за фазами проєкту – «контрактна фаза» може бути розділена на наступному рівні: конфлікт в документах, затримки у вирішенні питань за контрактом, неоднозначність договору, нестандартні форми контракту, зовнішні ризики під час фази контракту;

– за учасниками проєкту – можна розглянути на другому рівні: власник/клієнт, фінансист, дизайнер, консультант, підрядник, постачальник.

## 2.3 Методологія виявлення та агрегації ризиків в структурній декомпозиції ризиків

Основна складність на етапі ретельної перевірки – уникнення множення можливостей. Оскільки багато існуючих СДР у відповідній документації не були побудовані з орієнтацією на певний «стандарт», можна знайти, наприклад, багато дерев, в яких «політичні ризики» знаходяться безпосередньо нижче «зовнішніх ризиків» [14], не будучи згруповані спочатку в проміжній категорії, як «державні ризики». Лише через багато порівнянь та ітерацій можна визначити обмежену кількість категорій і елементарних дерев, які охоплюють дуже великий відсоток наявних дерев [28].

У кінці процесу база даних містить список мікродерев і список КР, а також усі належні співвідношення, що визначають:

– для кожного МД всі КР, які він містить;

– для кожної КР, до якого МД вони належать (всі можливі батьківські вузли).

Ці правила забезпечують агрегацію приналежності властивостей з нижнього рівня на верхній рівень в СДР.

У базі даних в певний час містяться мікродерева, які можуть бути використані для відновлення великої кількості можливих СДР. Особливу увагу приділено контролю узгодженості цих МД на місцевому та глобальному масштабі. Рис.2.13 схематично ілюструє місцеві обмеження узгодженості бази даних МД. Правила для керованих елементів:

– МД повинно мати принаймні 2 підкатегорії;

– категорія може бути представлена як «батько» вузла МД лише за умови, що це підкатегорія іншого МД (винятком є «Проєктні ризики» – категорія на нульовому рівні);

– підкатегорія в МД не може бути «батьком» свого «батька» в іншому МД;

– категорія може бути представлена лише один раз як підкатегорія МД;

– категорія не може бути «батьком» і одночасно підкатегорією МД. Однак категорія може бути батьківським вузлом різних МД.

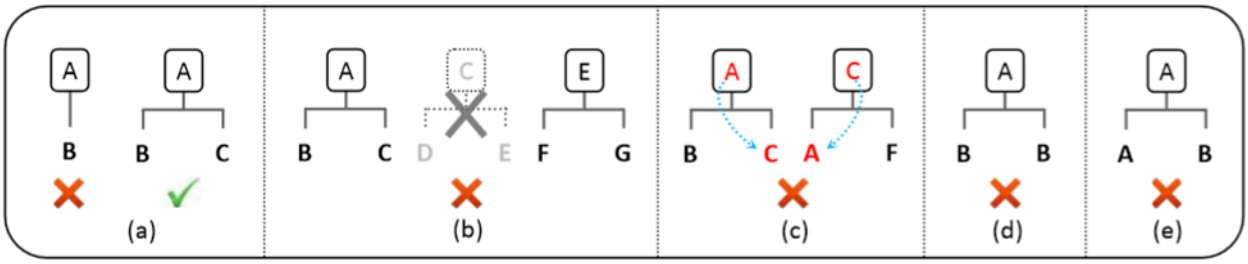



Рисунок 2.13 – Внутрішні обмеження на несуперечливість бази даних мікродерев

Зрозуміло, що рішення для покриття великої кількості існуючих СДР не є унікальним, і що вибір буде суб'єктивним. Цей вибір є результатом тривалого процесу, під час якого критеріями для прийняття рішень були: ліквідація непотрібних рішень, скорочення можливостей, перевірка узгодженості.

Розробка повної бази даних є повторюваним процесом, який вимагає ретельної уваги до деталей. Однак, оскільки в таких процесах швидко з'являється факторне зростання можливостей, необхідно розробити кілька автоматичних процедур для перевірки узгодженості бази даних. Загальна ідея полягає в тому, що в будь-яких СДР, які можуть бути побудовані шляхом збірки різних МД в декількох рівнях, або РП можуть бути приєднані один раз (і тільки один раз) до однієї з КР, що належать до нищого рівня. Таким основним обмеженням є: якщо RC#i «батьківський вузол» і набір RE#j, які належать до цієї RC#i дані, то будь-яка декомпозиція батька (RC#i) на підкатегорії повинна бути послідовною. Потім треба ретельно перевірити, що для кожного MT#k, чиїм батьківським вузлом є RC#i, кожна RE#j може бути приєднана до однієї (і тільки однієї) з підкатегорій в цьому мікродереві (рис.2.13). Будь-яка неможливість підключення або будь-який можливий подвійний результат показує деяку невідповідність, яка має бути усунена.

Як це обмеження запобігає виникненню проблеми, коли РП будуть поширюватися на генеровані СДР, можна побачити на рис.2.14. Якщо в базі даних користувач підключає RE#i до КР#k і RC#q, перша узгодженість для MT#i, яке

знаходиться на верхніх рівнях СДР, не діє через більш ніж одне підключення РП до його підкатегорій (які тут є непрямими посиланнями). Таким чином, це обмеження не дає змогу зберегти ці два нові посилання в базу даних і запобігає проблемам, що можуть виникнути. Тому «ризикова подія не може бути приєднана до більше за одну КР в СДР», коли перше обмеження контролюється для всіх МД.

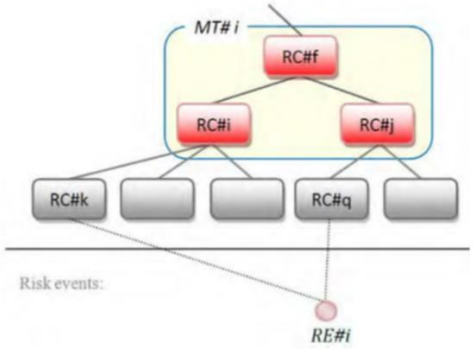



Рисунок 2.14 – Ризикова подія не може бути приєднана
до більш ніж однієї КР в СДР

Друге обмеження пов’язане з мікродеревами одного батьківського вузла. Обмеження полягає в тому, що коли кілька МД розглянуті відповідно різними декомпозиціями категорії, і якщо ризикова подія може бути прикріплена до першого МД, вона також має бути (необов’язково) прикріплена до інших МД. Ці два обмеження схематично показано на рис.2.15. Автоматизація процесу розроблена таким чином, щоб приступити до автоматичної перевірки цих обмежень, і чітко пояснити, де знаходяться конфлікти, що полегшує розробку бази даних. Оскільки ця перевірка автоматична, подальші зміни в базі даних будуть легшими.

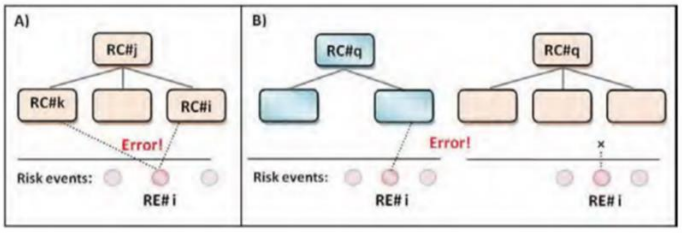



Рисунок 2.15 – Узгодженість управління інформацією в базі даних
а) будь-яка РП може впливати один раз (і лише один раз) на одну з підкатегорій МД;
б) для МД з одним і тим самим батьківським вузлом, якщо один з них може охопити РП, інші повинні (обов’язково) покрити його

Розробка первісної бази даних означає додавання нових РП, нових КР або нових МД, щоб охопити ширший спектр застосування або покриття заданого поля на детальнішому рівні. З початкової бази даних легко перевірити узгодженість будь-якого доданого елемента, так як він впливає лише на дуже обмежену частину з усієї бази даних. Це важливо, оскільки розроблені бази даних розглядаються як перший варіант бази знань. Розширення бази даних для покриття найзагальніших ризикових подій ІТ-проєкту вирішують це питання.

Третє обмеження полягає в тому, що РП може мати прямі посилання тільки на категорії ризику нижнього рівня. Категорія нижнього рівня не має підкатегорії в базі даних або іншими словами, нижня КР не може бути «батьком» будь-якому МД у базі даних. Це обмеження контролюється, коли воно визначає з’єднання РП з відповідною КР у базі даних.

Тепер виникає питання – як визначити процес, що дає змогу розробити і вибрати «зручні» СДР, які будуть використовуватися в процесі управління проєктними ризиками. Будь-яка СДР розглядається як набір МД, в якому кожен «син» КР може бути додатково структурований, поки є батьківським вузлом іншого МД. База даних у певний час містить мікродерева, які відповідають великій кількості можливих СДР. Усі згенеровані СДР ранжуватимуться за основними критеріями якості СДР та з урахуванням загальних вимог і цілей користувача і вибраних РП, які повинні бути об’єднані через СДР. Найзручніша СДР відносно глобальних, обрана котра з найвищим рейтингом. Тоді якість цієї СДР буде покращена шляхом подальшої розробки категорій ризиків і видалення незначних і неважливих гілок щодо рівня деталізації та критичності. Основні етапи генерації, ранжування і вибір найзручнішої СДР зображені на рис.2.16.

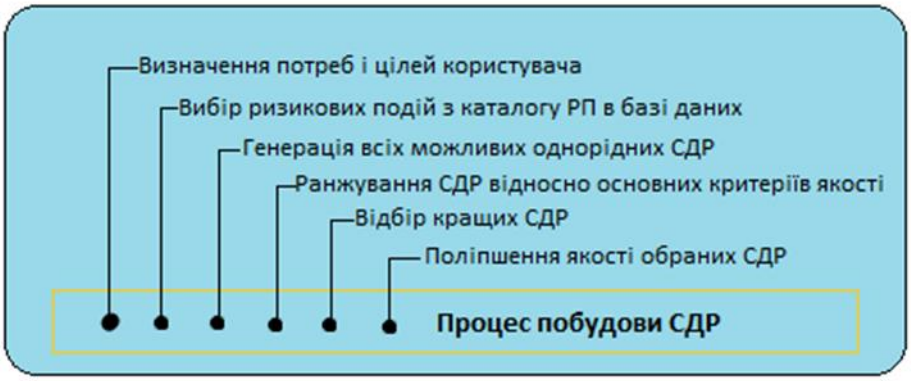



Рисунок 2.16 – Процес побудови СДР

Першим кроком є визначення основних вимог користувача для фаз проєкту, учасників проєкту та основних завдань управління проєктними ризиками. Користувачеві може бути цікаво зосередитися на одному з етапів проєкту (ініціація, договір, проєктування, впровадження, експлуатація) чи на всьому життєвому циклі проєкту. Структурна декомпозиція може становити певну перспективу одного з учасників проєкту (дизайнера, фінансиста, власника / клієнта, підрядника / субпідрядника, постачальника, консультанта) або може бути загальним інструментом для об’єднання різних перспектив проєктних ризиків. Цілі можуть управляти часом, вартістю, якістю, або навіть ними всіма. Кінцева СДР повинна бути сумісна з усіма цими вимогами.

Висновки до розділу 2

1. У цьому розділі структурна декомпозиція ризиків визначається як вельми практичний інструмент на різних етапах управління ризиками. Було роз’яснено, чому це може бути потужною допомогою в ідентифікації, оцінюванні та представленні проєктних ризиків. Зазначені його переваги та недоліки і показано існування різноманітних класифікацій ризиків, які розроблялися без дотримання будь-яких інструкцій.

2. Пояснено концепцію взаємодії ризиків, представлені різні доступні методи для їх врахування в процесі аналізу ризиків.

3. Встановлено, що у зв’язку з характером ІТ-проєктів, ітераційний процес управління ризиками повинен застосовуватися на всіх стадіях життєвого циклу проєкту. Це причина, чому було розроблено інноваційний метод для генерації індивідуальних СДР для ефективнішого управління ризиками в ІТ-проєктах.

# 3 ПРОГРАМНА РЕАЛІЗАЦІЯ ЗАПРОПОНОВАНОГО ПІДХОДУ

## 3.1 Вибір програмних засобів формування структурної декомпозиції ризиків

Створення СДР передбачає використання різних інструментальних засобів для визначення, класифікації та аналізу ризиків ІТ-проєктів. Ці інструменти можна умовно розділити на кілька груп (табл.3.1):

Таблиця 3.1 – Інструментальні засоби для визначення, класифікації та аналізу ризиків

| № | Група | Методи | Зміст |
|---|---|---|---|
| 1 | Методи мозкового штурму | Традиційний мозковий штурм | Групова техніка для створення широкого діапазону ідей щодо потенційних ризиків без початкової оцінки |
| | | Інтелектуальна карта | Візуальне представлення, яке допомагає організувати та зв’язати різні елементи ризику та їхні зв’язки |
| 2 | Інтерв'ю та опитування | Інтерв'ю з експертами | Поглиблені обговорення з експертами з певної тематики для визначення ризиків у їхній конкретній сфері |
| | | Опитування зацікавлених сторін | Збір відгуків і думок зацікавлених сторін щодо потенційних ризиків, які вони передбачають |
| 3 | Контрольні списки та шаблони | Контрольний список ризиків | Попередньо визначений список потенційних ризиків на основі історичних даних або галузевих стандартів |
| | | Шаблони RBS | Попередньо встановлені структури, які допомагають систематично розподіляти ризики за категоріями |
| 4 | Методи аналізу | SWOT-аналіз | Визначення сильних і слабких сторін проекту, можливостей і загроз для розпізнавання потенційних ризиків |
| | | Аналіз відмов і наслідків (FMEA) | Систематичне оцінювання потенційних відмов та їх впливу на проект. |
| | | Аналіз причин і наслідків (діаграма Ішікави) | Виявлення та класифікація причин, що сприяють потенційним ризикам |
| 5 | Кількісні інструменти | Моделювання Монте-Карло | Техніка статистичного моделювання, яка використовується для аналізу впливу ризику та невизначеності в графіках або бюджетах проєкту |
| | | Дерева рішень | Візуальні інструменти, які використовуються для розрахунку та |

| | | | |
|---|---|---|---|
| | | | оцінювання можливих результатів рішень, прийнятих під ризиком |
| 6 | Експертне оцінювання | Групи експертів | Збір думок кількох експертів для оцінки та визначення пріоритетів ризиків на основі їхніх спільних знань |
| | | Метод Delphi | Ітеративний метод для досягнення консенсусу між експертами через контрольовані раунди зворотного зв'язку |
| 7 | Технологічні рішення | Програмне забезпечення для управління ризиками | Інструменти для полегшення процесів ідентифікації, оцінювання та управління ризиками за допомогою спеціалізованих програмних рішень |
| | | Аналітика даних та інструменти на основі ШІ | Використання розширеної аналітики та алгоритмів ШІ для виявлення потенційних ризиків на основі моделей історичних даних |
| 8 | Семінари та фокус-групи | Семінари з ризиків | Спільні сесії за участю зацікавлених сторін для спільного мозкового штурму та визначення ризиків |
| | | Фокус-групи | Невеликі групи, зосереджені на обговоренні та аналізі конкретних сфер ризику в рамках проекту |

Кожна з цих категорій охоплює спеціальні інструменти та методології, які можна використовувати залежно від характеру проєкту, наявних ресурсів і складності ризиків, які необхідно визначити в структурі аналізу ризиків. Вибір правильної комбінації інструментів часто передбачає врахування унікальних характеристик проєкту та досвіду осіб, залучених до процесу ідентифікації ризиків.

Серед наведених засобів нас цікавитимуть насамперед технологічні рішення, які дають змогу виявлені структурні елементи ризиків оформити у вигляді бази даних з можливістю подальшого керування цими шляхом доповнення, коригування, пошуку і опрацювання.

Сьогодні найпоширенішими є реляційні SQL СУБД двох типів:

– великі СУБД комерційного характеру, призначені зберігати величезні обсяги інформації;

– компактні СУБД, вільно поширювані, котрі можуть використовуватися і для БД обсягом усього лише в десятки кілобайт.

У табл.3.2 згруповано опис СУБД першої групи.

Таблиця 3.2 – Найвідоміші великі комерційні СУБД

| Назва | Призначення | Функції | Використання |
|---|---|---|---|
| Oracle | Домінуючий гравець на ринку баз даних, відомий своєю масштабованістю та надійністю | Пропонує повний набір функцій для складного керування даними, високої доступності, безпеки та масштабованості | широко використовується на підприємствах, особливо в таких секторах, як фінанси, телекомунікації та великомасштабні програми |
| Microsoft SQL Server | Універсальна СУБД із сильною присутністю в екосистемі Windows | Легко інтегрується з продуктами та інструментами MS. Надає ряд функцій для керування даними, аналітики, бізнес-аналітики та можливостей хмари | Зазвичай використовуються в корпоративних середовищах і галузях, які потребують надійних рішень для обробки даних |
| IBM Db2 | Відома своєю надійністю, масштабованістю та продуктивністю в програмах корпоративного рівня | Пропонує розширену аналітику, інтеграцію штучного інтелекту та підтримку різних типів даних | Переважно використовують в таких секторах, як фінанси, охорона здоров’я та галузі з високими вимогами до даних |
| SAP HANA | СУБД у пам’яті, орієнтована на обробку та аналітику даних у реальному часі | Розроблено для високошвидкісних транзакцій і аналітики з використанням обчислень у пам’яті | Часто використовуються в програмах SAP для аналітики та обробки даних у реальному часі |
| Teradata | Спеціалізується на сховищах даних і аналітиці | Відома своєю масштабованістю та обробкою великих обсягів даних | Часто використовується в галузях, що потребують важкої аналітики |
| Amazon RDS | Частина AWS, що пропонує послуги керованої БД, у т.ч. опції для Oracle, MySQL, SQL Server, … | Надає параметри масштабування в хмарному середовищі | Широко застосовується компаніями, які використовують AWS для своїх потреб у БД |
| Informix | Пропонує надійне керування даними з акцентом на Інтернеті речей (IoT) і даних часових рядів | Відома своїми можливостями ефективної обробки потоків даних IoT | Зазвичай зустрічаються в галузях, пов’язаних з IoT, наприклад у виробництві та комунальному господарстві |

Друга група мобільних, компактних і вільно розповсюджуваних СУБД включає кілька популярних варіантів, які підходять для баз даних невеликого обсягу та сценаріїв, де простота, портативність і легкість використання є ключовими міркуваннями. Нижче наведено огляд шести відомих СУБД у цій категорії (табл.3.3). Ці варіанти СУБД пропонують гнучкість, простоту використання та портативність, що робить їх придатними для сценаріїв, де вимоги до бази даних є відносно невеликими або де перевагу надають легким, автономним рішенням. Їм часто віддають перевагу через їхню простоту, сумісність з різними платформами та відкритий код.

Таблиця 3.3 – Найвідоміші невеликі компактні СУБД

| Назва | Призначення | Функції | Використання |
|---|---|---|---|
| SQLite | Самодостатній, безсерверний механізм бази даних SQL без конфігурації | Надзвичайно легкий і призначений для вбудованих систем і невеликих програм. Не вимагає окремого серверного процесу, простий у налаштуванні та дуже портативний | Широко використовується в мобільних програмах, вбудованих системах, браузерах і невеликих проектах завдяки своїй простоті, надійності та портативності |
| MySQL Community Edition | Популярна реляційна СУБД з відкритим кодом | Підходить як для невеликих програм, так і для веб-сайтів великого обсягу; широко використовується у веб-розробці | Зазвичай використовується стартапами, додатками малого та середнього розміру та веб-проєктами завдяки простоті використання та широкому застосуванню |
| PostgreSQL | Надійна СУБД з відкритим кодом, відома своєю відповідністю стандартам SQL | Розширюваність за допомогою спеціальних функцій, таких як підтримка JSON | Широко використовується в різних галузях завдяки розширеним функціям і надійності |
| MariaDB | Відгалуження MySQL, зосереджене на розробці з відкритим | Висока сумісність з MySQL, підвищення продуктивності та додаткові механізми зберігання. Підходить | Часто вибирають як альтернативу MySQL через його природу з відкритим вихідним |

| | | | |
|---|---|---|---|
| | вихідним кодом та інноваціях спільноти | для програм невеликого та корпоративного рівня | кодом і розробку, керовану спільнотою |
| Firebird | Реляційна СУБД з відкритим вихідним кодом, яка пропонує високу продуктивність і сумісність з кількома платформами | Доступна вбудована версія, підтримує збережені процедури, тригери та методи множинного доступу. Підходить для додатків малого та середнього розміру | Використовується у вбудованих системах, невеликих проєктах і програмах, які вимагають полегшеної бази даних |
| HSQLDB (DB HyperSQL) | Швидка реляційна СУБД з відкритим кодом, написана на Java | Компактна і може вбудовуватися у програми Java. Підтримка БД у пам’яті та стандартного синтаксису SQL | Зазвичай використовується в програмах на основі Java, освітніх середовищах і як вбудована база даних |

На наш погляд, Microsoft SQL Server може бути найкращим вибором для СДР завдяки наступним перевагам:

– стійкість і надійність – забезпечує надійність і узгодженість даних, стабільністю та постійною продуктивністю, що має вирішальне значення для ефективного управління ризиками;

– масштабованість і продуктивність – може обробляти як малі, так і великі бази даних, пристосовуючись до зростання даних, пов’язаних із ризиком; також використовує передові методи оптимізації для запитів і обробки даних, що забезпечує ефективну роботу СДР;

– інтеграція з екосистемою Microsoft – добре працює в екосистемі Microsoft, полегшуючи інтеграцію з іншими інструментами та програмами, такими як Excel, SharePoint і Power BI, допомагаючи у візуалізації та аналізі даних для управління ризиками;

– розширені заходи безпеки – пропонує надійні функції безпеки, як-от шифрування, контроль доступу та аудит, що має вирішальне значення для захисту конфіденційної інформації, пов’язаної з ризиком;

– розширена аналітика та звітність – служби аналітики охоплюють такі потужні інструменти, як SQL Server Analysis Services (SSAS) для багатовимірної аналітики і поглибленого аналізу ризиків, а служби звітності SQL Server (SSRS) допомагають створювати вичерпні звіти та візуалізацію даних про ризики;

– простота використання та управління – надає інтуїтивно зрозумілі інструменти керування та користувацькі інтерфейси для адміністрування бази даних, що робить її доступною для розробки та обслуговування СДР, а також надає функції для автоматичного резервного копіювання, планів обслуговування та моніторингу, зменшуючи адміністративне навантаження;

– підтримка та спільнота – оскільки продукт широко використовується, він має велику спільноту та обширну документацію, що полегшує пошук несправностей і підтримку. Корпорація Майкрософт регулярно випускає оновлення, виправлення та нові функції, забезпечуючи постійні вдосконалення та покращення безпеки;

– розширені функціональні можливості – пропонує широкий спектр функцій, процедур та інструментів, що полегшує складні обчислення та маніпулювання даними, необхідні для оцінювання ризику.

Отже, проєктним командам, які працюють у середовищі Microsoft або віддають перевагу комплексному та добре інтегрованому рішенню для розробки СДР, надійність, масштабованість, можливості інтеграції, функції безпеки та широкі функціональні можливості Microsoft SQL Server роблять його вагомим вибором для ефективного керування та аналізу даних, пов’язаних із ризиками.

Спеціально для платформи .NET Microsoft була розроблена нова мова програмування C#, синтаксис якої дуже схожий на синтаксис Java (але не ідентичний йому).

Середовище розробки Visual Studio.NET надає розробникам потужні та зручні засоби написання, коригування, компіляції, налагодження і запуску додатків, що базуються на використанні .NET-сумісних мов. Оскільки платформа .NET – відкрите середовище, то компілятори для неї можуть поставляти й сторонні розробники. Наразі розроблено багато таких компіляторів.

Всі .NET-сумісні мови мають відповідати вимогам специфікації Common Language Specification (CLS), де описано набір загальних характеристик. Це дає змогу використовувати для розробки додатки кількома мовами програмування і проводити повноцінне міжмовне налагодження. Незалежно від мови, всі застосунки працюють на одних і тих же базових класах бібліотеки .NET.

Для побудови проведено формалізацію задачі, що є необхідним етапом розробки завдання і полягає в побудові структури таблиць для зберігання інформації, схеми їх взаємозв'язків і опису алгоритмів обробки. Розроблена схема даних зображена на рис.3.1.

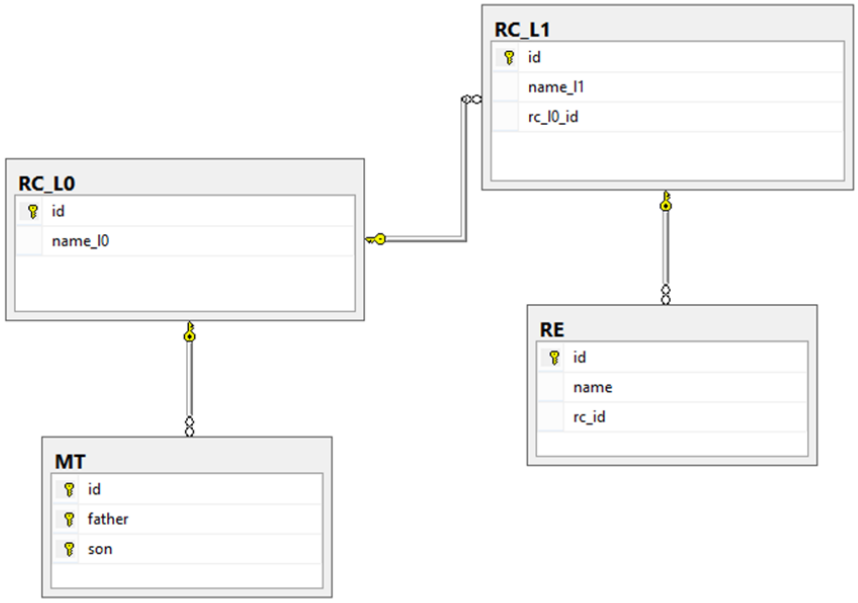



Рисунок 3.1 – Схема даних розробленої БД

Для створення бази даних, таблиць і збережених процедур написано SQL-сценарій.

Як правило, розробка проєкту реалізації завдання виконується в кілька етапів і починається з аналізу тієї інформації, яка є вихідною (таблиці Microsoft SQL Server), підсумкова (кінцева) форма для Microsoft Visual Studio (C# .NET). Тільки після з'ясування структури і складу цієї інформації, формулювання запитів для отримання звітів можна зробити висновок про структуру і склад таблиць даних.

Необхідним етапом формалізації задачі є нормалізація бази даних, яка, по суті, являє собою процес оптимізації зберігання та використання інформації в таблицях.

У відповідності до поставленого завдання і аналізу предметної області, розробка формування структурної декомпозиції ризиків проводиться на основі принципів та елементів систем управління базами даних, логічним є збереження даних у вигляді файлів таблиць бази даних певного типу, вибір і обробку інформації виконувати на основі запитів, для введення і відображення даних використовувати діалогові екранні форми.

Для розробки програми обрано мову C#, технологію Microsoft .NET і середовище розробки Microsoft Visual Studio 2022, з використанням Microsoft SQL Server 2019.

Середовище розробки Microsoft Visual Studio 2022 призначене для розробки сучасного програмного забезпечення, однією з можливих мов написання програмних додатків є мова програмування C#. Використання мовою C# багатофункціональної бібліотеки класів і шаблонів Net Framework дає змогу розробляти складні програмні продукти в короткі строки.

Для розробки БД обрано середовище розробки SQL Server Management Studio (SSMS). Середовище SSMS є інтегрованим середовищем для доступу, налаштування, адміністрування, розробки всіх компонентів SQL Server і управління ними. У середовищі SSMS велика вількість графічних засобів поєднується з набором повнофункціональних редакторів скриптів для доступу розробників й адміністраторів з будь-яким рівнем знань до SQL Server.

Середовище SSMS об’єднує в єдиному інтерфейсі можливості програм Enterprise Manager, Query Analyzer і Analysis Manager, що входили до складу ранніх випусків SQL Server. Крім того, SSMS працює з усіма компонентами SQL Server, наприклад зі службами Reporting Services та Integration Services. Розробники отримують знайоме середовище, а адміністратори баз даних – єдину повнофункціональну програму, що об’єднує прості у використанні графічні засоби і багаті можливості для створення сценаріїв.

## 3.2 Динамічне формування структури ризиків ІТ-проєкту

ІТ-проєкти характеризуються як досить складні, де невизначеність надходить від багатьох джерел. Ці проєкти оточують різні зацікавлені сторони, які мають різні точки зору та цілі, які приходиться брати до уваги. Крім того, складні та мінливі умови привносять деякий ступінь невизначеності в кожен проект, що може вплинути на графік, якість, безпеку та остаточну вартість роботи.

Тому розроблено загальний метод побудови СДР, щоб ефективно визначати і організовувати ризики в ІТ-проєктах. Однією з цілей є те, що для кожного нового проєкту різні партнери, слідуючи загальним настановам, мають можливість будувати свою власну СДР відповідно до їхніх цілей та особистих поглядів на проєктні ризики, тоді як загальна думка про ризики також залишиться. Це зробить можливим «мультимасштабний» підхід, де кожен партнер може зосередитися на деяких особливих ризиках і розвивати СДР ще кількома підкатегоріями в спеціальних областях.

Нами було розроблено програмне забезпечення (ПЗ) для полегшення застосування цієї методології в реальних проєктах для керівництва проєкту. Це ПЗ є інтеграцією всіх концепцій і алгоритмів цього інноваційного методу, з дружнім інтерфейсом користувача. ПЗ може бути використане як фахівцем з управління ризиками, так і проєктними менеджерами. Разом з тим, кожен, хто має основну інформацію про управління ризиками проєкту може легко використовувати це ПЗ.

Вказане програмне забезпечення є корисним інструментом для ідентифікації, аналізу та ієрархічного представлення ризиків. Воно може допомогти менеджеру проєкту знайти відповіді на багато питань, таких як:

- які основні ризики проєкту?
- який тип ризиків?
- хто або що є джерелом небезпеки?
- в якій фазі проєкту це може статися?
- це значний ризик?
- який партнер або фаза проєкту є більш ризикованим?

Кожен користувач може створити свою власну базу даних ризикових подій, категорій ризику і мікродерев, а ПЗ контролює узгодженість даних на кожному етапі. Неможливо зробити зміни в базі даних, коли вони можуть призвести до суперечливої ситуації. Також користувач може використовувати базу даних інших користувачів. Вони можуть обмінюватися інформацією бази даних.

Була підготовлена база ризиків, пов'язаних з ІТ-проєктами, яка є корисною для користувачів цього програмного продукту. БД ризиків ІТ-проєктів охоплює найчастіші ризики, упродовж усього життєвого циклу проєкту. Однак вони не є вичерпними, адже в кожному новому проєкті можуть бути виявлені багато нових ризиків, вони можуть бути легко додані в базу даних, тоді як програмне забезпечення контролює їх узгодженість з наявними даними в БД. Ця база даних була розроблена на основі ретельного аналізу і огляду літератури і випадків керування ризиками. Поєднання такої бази даних і програмного забезпечення оснащує менеджера корисним інноваційним інструментом, який може допомогти краще управляти ризиками проєкту.

Використовуючи це програмне забезпечення, користувач може визначити можливі ризики певного проєкту з довгого списку ризикових подій. ПЗ буде класифікувати ці ризикові події, які можуть допомогти кращому розумінню ризиків. Цей процес відбувається згідно зі спеціальними вимогами користувача. Ризики аналізуються з точки зору яких партнерів проєкту? Ризики, відповідні якій фазі проєкту? Що є основною метою управління проєктними ризиками? Відповіді на ці питання дають необхідну інформацію для алгоритму, щоб підібрати найзручніші СДР.

Невизначеність, яка наявна в проєкті, спричиняє ризики у ньому, відповідно усуваючи невизначеність усуваються ризики. На цьому шляху насамперед проводиться ідентифікація ризиків, яка передбачає порівняння ризиків за важливістю і вибір найадекватнішої стратегії для з кожного з них.

Зокрема, ризики з високим рейтингом варто усунути з проєкту за умови економічної доцільності (іноді вартість уникнення ризику може бути дорожчою за

наслідки його появи). Тоді як для низькорейтингових ризиків варто скористатися стратегією прийняття, оскільки ухиляння від них є недоцільним.

Важливість ризиків проєкту переважно оцінюють за двома показниками: імовірність виникнення та його вплив на проєкт. Завдяки ним можна скористатися формулою для обчислення важливості ризику:

*Важливість ризику* = *Імовірність* x *Вплив*.

Щоб розрахувати ймовірність виникнення ризику можна скористатися двома найпоширенішими підходами – експертним методом і використанням статистики.

Далі описано процес роботи з розробленим програмним забезпеченням.

Після відкриття програми завантажується вікно, яке має вигляд (рис.3.2):

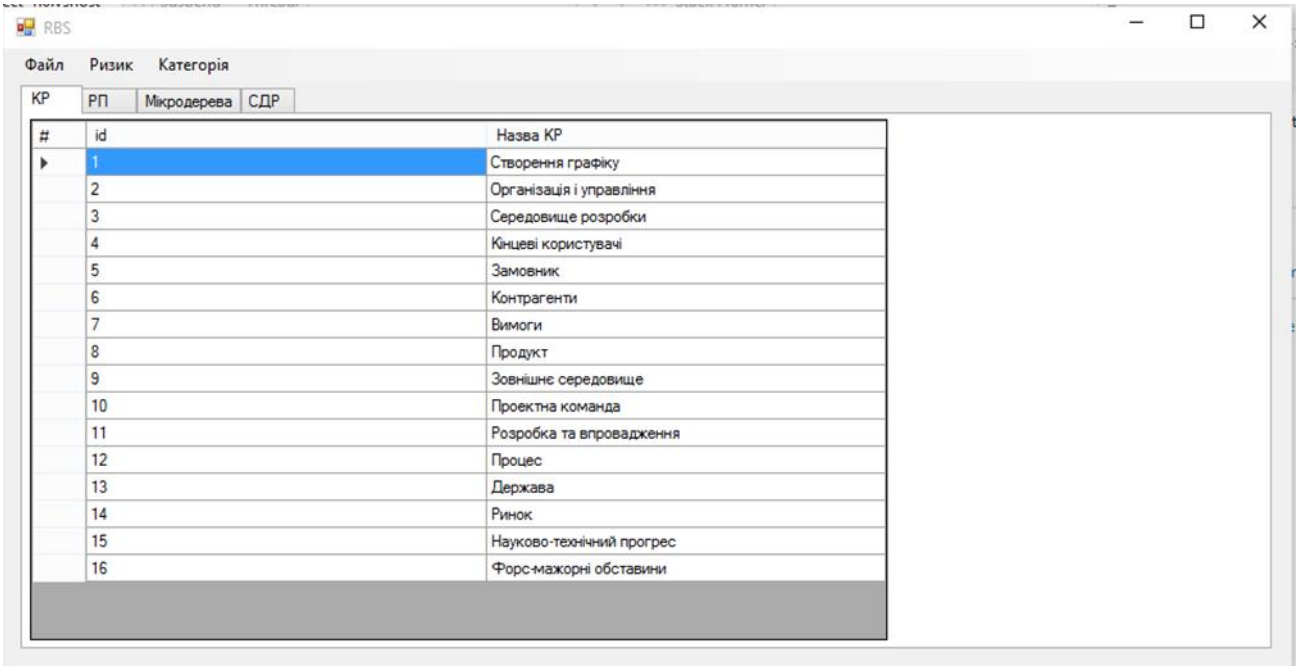



Рисунок 3.2 – Головне вікно програми

Зверху знаходиться панель з функціональними кнопками, основні дії виконуються за їх допомогою.

Вкладка «КР» представляє категорії ризиків бази даних (рис.3.3). Як показано, кожен має: «id», тобто унікальний номер; тип, який може бути загальним або розширеним; ім’я і опис. Це чотири основні атрибути кожної категорії ризику. За замовчуванням, сторінка призначена тільки для читання і користувач не може нічого змінювати.

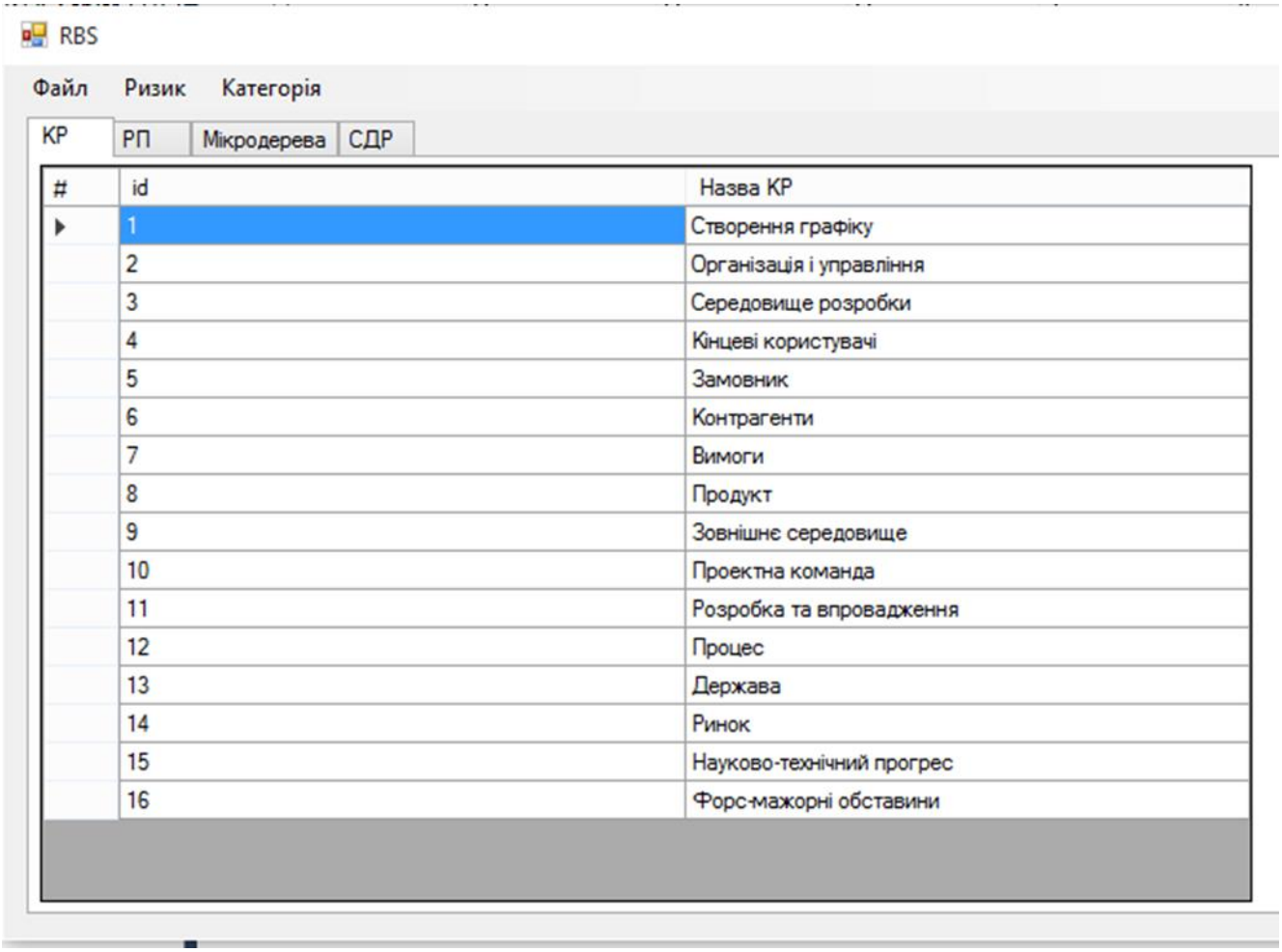



Рисунок 3.3 – База даних категорій ризиків

Щоб додати нову категорію ризику потрібно перейти до кнопки «Категорія» та вибрати кнопку «Додати нову категорію» (рис.3.4). На формі, що з’явиться (рис.3.5), необхідно ввести правильний код КР (унікальний у цій базі даних), вибрати тип, ввести ім’я (унікальне в базі даних) і текст для опису.

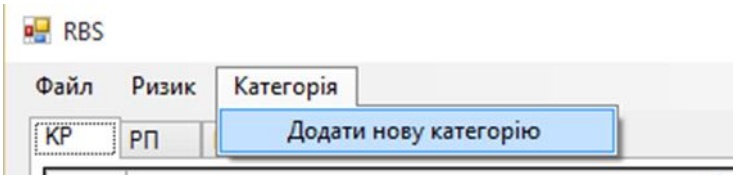



Рисунок 3.4 – Додавання нової категорії

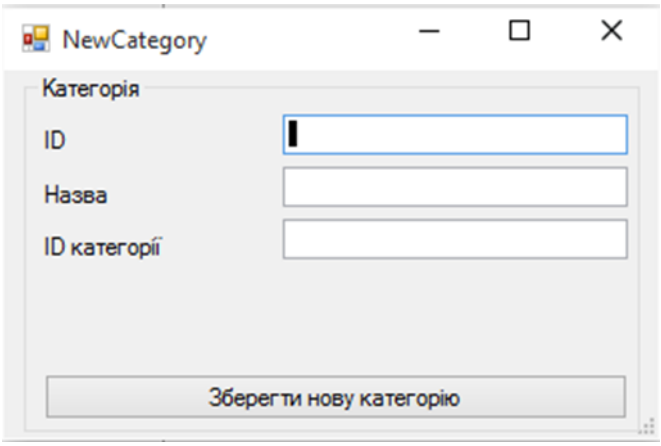
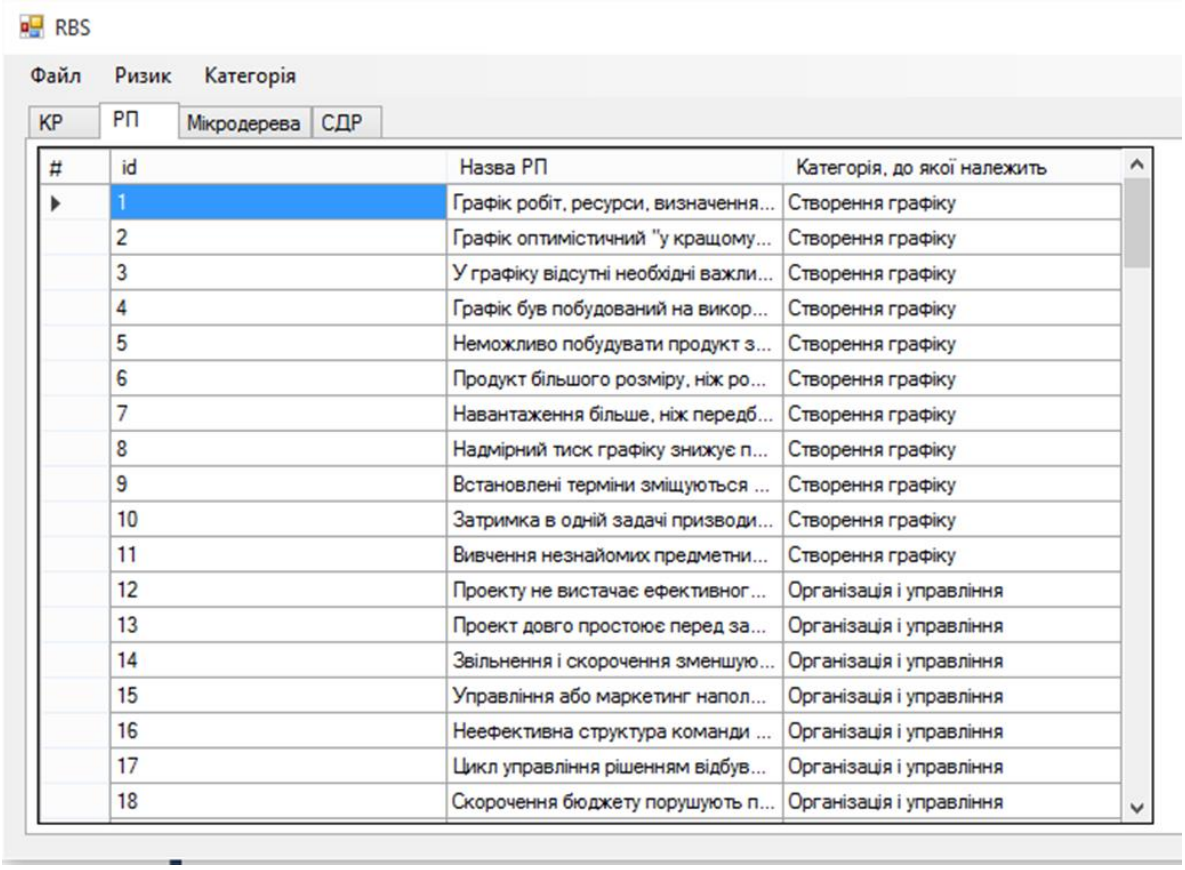



Рисунок 3.5 – Форма нової категорії

Вкладка «РП» представляє ризикові події бази даних (рис.3.6). Як показано, кожен має «id», ім’я, категорію, до якої належить, значення імовірності і три значення чиників впливу. Це п’ять основних елементів кожної ризикової події. По замовчуванню, сторінка призначена тільки для читання і користувач не може нічого змінювати.




| # | id | Назва РП | Категорія, до якої належить |
|---|---|---|---|
| ▶ | 1 | Графік робіт, ресурси, визначення... | Створення графіку |
| | 2 | Графік оптимістичний "у кращому... | Створення графіку |
| | 3 | У графіку відсутні необхідні важли... | Створення графіку |
| | 4 | Графік був побудований на викор... | Створення графіку |
| | 5 | Неможливо побудувати продукт з... | Створення графіку |
| | 6 | Продукт більшого розміру, ніж ро... | Створення графіку |
| | 7 | Навантаження більше, ніж передб... | Створення графіку |
| | 8 | Надмірний тиск графіку знижує п... | Створення графіку |
| | 9 | Встановлені терміни зміщуються ... | Створення графіку |
| | 10 | Затримка в одній задачі призводи... | Створення графіку |
| | 11 | Вивчення незнайомих предметни... | Створення графіку |
| | 12 | Проекту не вистачає ефективног... | Організація і управління |
| | 13 | Проект довго простоює перед за... | Організація і управління |
| | 14 | Звільнення і скорочення зменшую... | Організація і управління |
| | 15 | Управління або маркетинг напол... | Організація і управління |
| | 16 | Неефективна структура команди ... | Організація і управління |
| | 17 | Цикл управління рішенням відбув... | Організація і управління |
| | 18 | Скорочення бюджету порушують п... | Організація і управління |

Рисунок 3.6 – База даних ризикових подій

Щоб додати нову ризикову подію потрібно перейти до кнопки «Ризик» та вибрати кнопку «Додати новий ризик» (рис.3.7). На формі, що з’явиться (рис.3.8), ввести правильний код РП (унікальний у цій базі даних), ввести ім’я (унікальне в базі даних), значення ймовірності може змінюватися в діапазоні (0, 1), але для значень впливу, прийнятний діапазон залежить від функції аналізу ризику, який буде обраний.

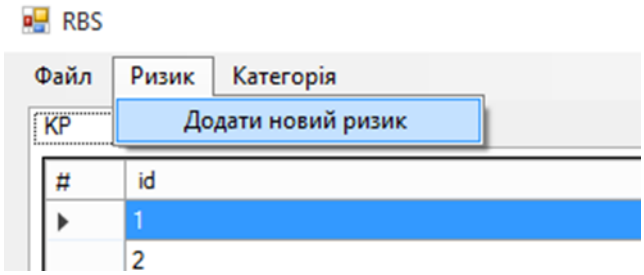



Рисунок 3.7 – Додавання нового ризику

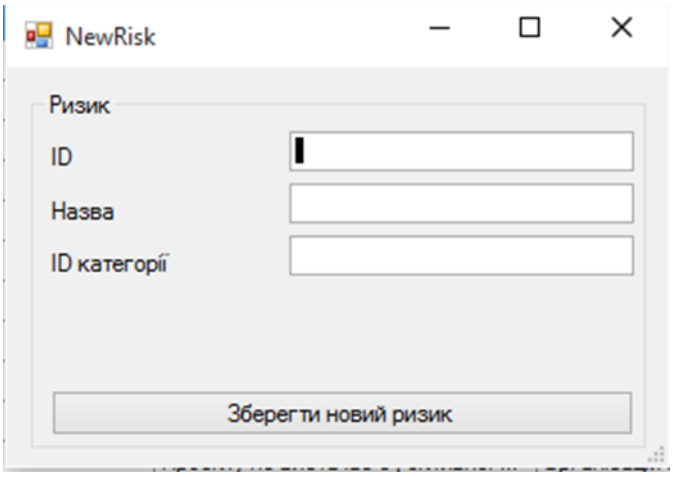



Рисунок 3.8 – Форма нового ризику

Якщо введені значення більше 1, з’явиться повідомлення про помилку і програма не дозволить збереження нової РП. Аналогічно, якщо введене ім’я чи код РП уже існує в базі даних, з’явиться повідомлення про помилку.

Вкладка «Мікродерева» представляє мікродерева бази даних (рис.3.9). Як показано, кожен має «id», «батька» і «сина». За замовчуванням сторінка виставлена лише для читання і користувач не може нічого змінювати.

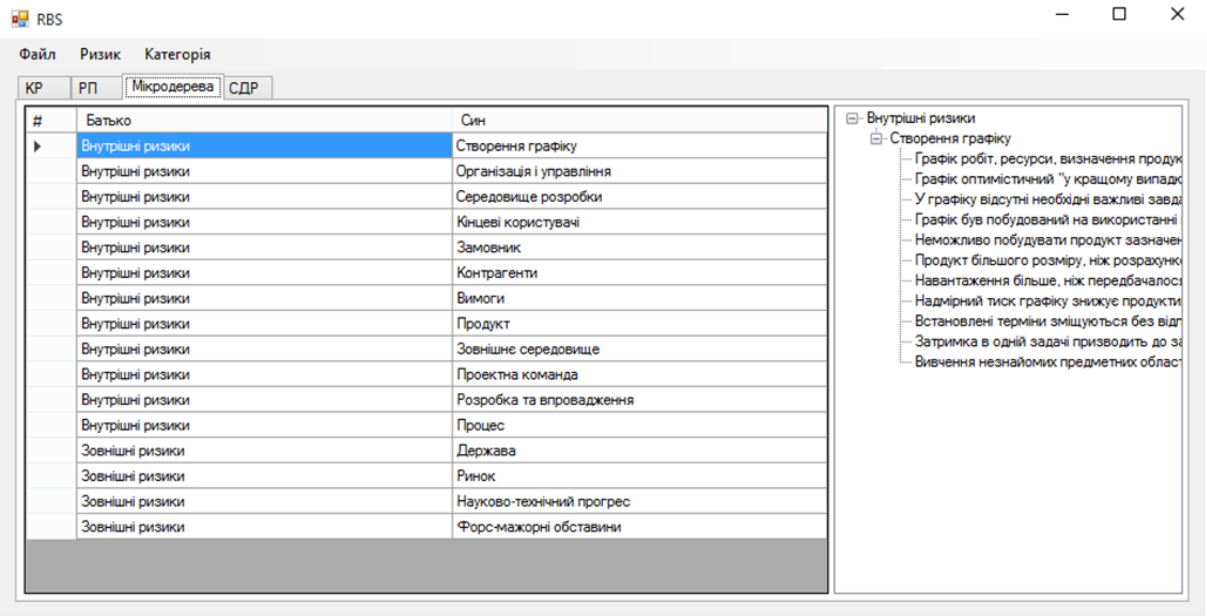



Рисунок 3.9 – База даних мікродерев

Вибравши клацанням миші певну частину мікродерева, його схематична форма з’являється в правій частині вікна (рис.3.10). У цьому схематичному вигляді назва батьківського вузла і підкатегорій наведені в ієрархічному вигляді.

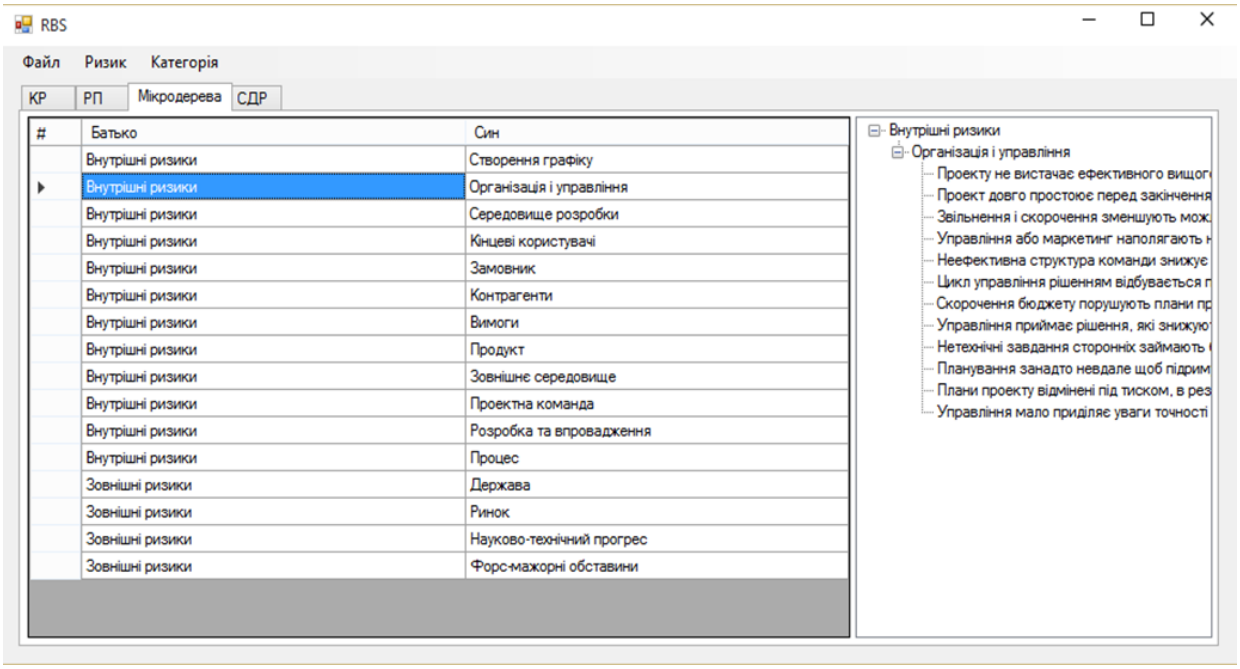



Рисунок 3.10 – Сформоване мікродерево

Щоб додати нове мікродерево, потрібно перейти до останнього рядка списку і додати правильний код МД (який є цілим числом, і унікальний у цій базі даних),

вибрати тип КР. Щоб увійти в батьківський вузол, натиснути на відповідну комірку і з’явиться вікно списку. Далі вибирають батьківський вузол зі списку. У такий же спосіб обираються підкатегорії.

Нове МД повинне мати, принаймні унікальний і дійсний код, батьківську КР і підкатегорії, в іншому випадку програма не дозволить додати дані в базу даних.

На вкладці «СДР» генеруються всі можливі СДР (рис.3.11).

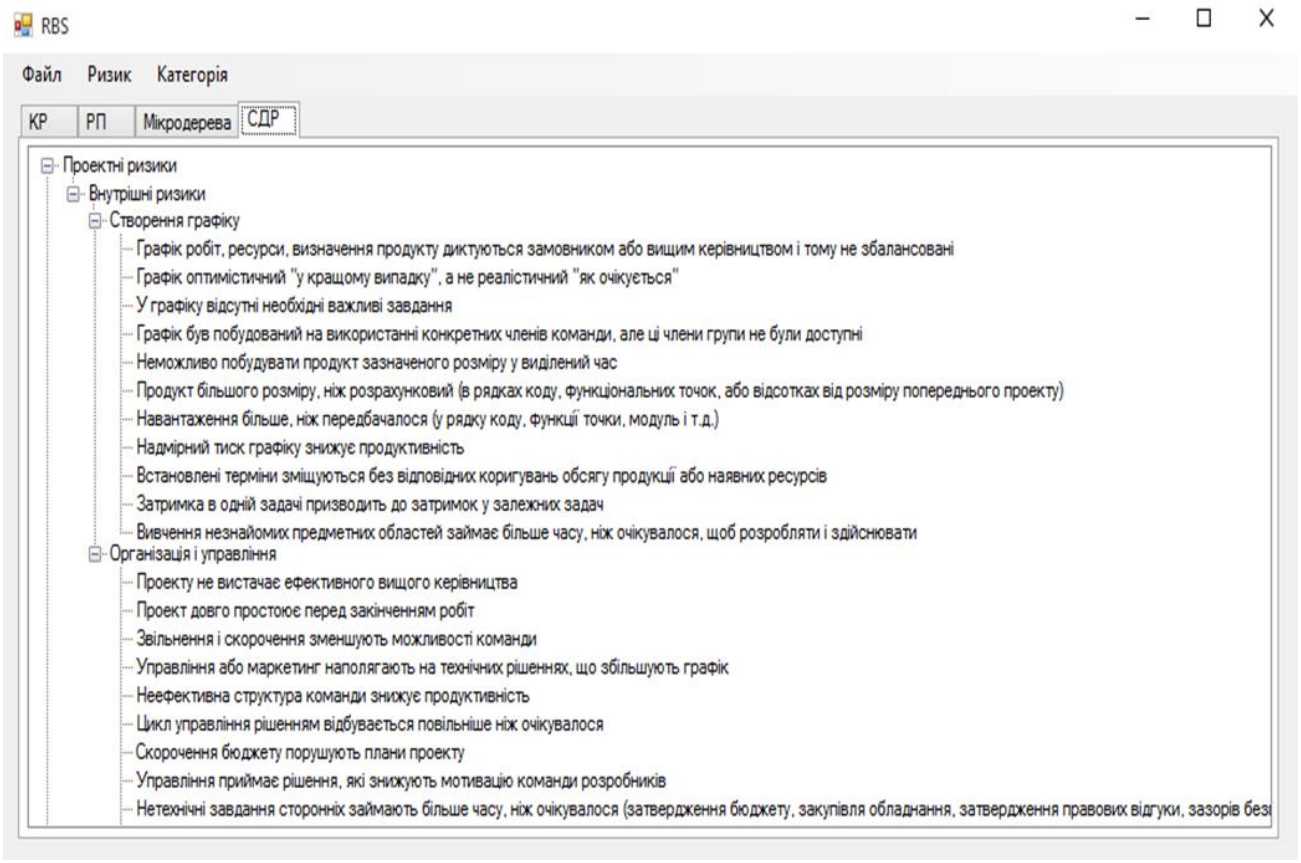



Рисунок 3.11 – Сформована структурна декомпозиція ризиків

Ці дерева побудовані шляхом поєднання різних мікродерев, наявних у базі даних. Також ці дерева є однорідними, а це означає, що всі гілки були поширені на тому ж рівні (якщо є МД для декомпозиції підкатегорій).

## Висновки до розділу 3

У розділі досліджено та проаналізовано засоби для побудови програмного забезпечення, що реалізує запропонований підхід, описаний в розділі 2.

1. Розділ розпочинається з опису та аналізу мов програмування та середовищ розробки програмного забезпечення, які були застосовані при розробці ПЗ, що реалізує застосування пропонованої методики в реальних проєктах. Програмне забезпечення включає в себе всі поняття і алгоритми методу з дружнім інтерфейсом користувача.

2. Процес управління проєктними ризиками розпочинається з первинної ідентифікації ризиків і оцінювання ймовірних РП, пов’язаних з етапом техніко-економічного обґрунтування. Потім було показано, як виявлення СДР можуть бути індивідуально проаналізовані, незалежно від їх загального впливу на цілі проєкту.

3. Варто зазначити, що для апробації у ІТ-проєкті використовувалась лише доступна інформація про ІТ-проєкт, щоб показати здатність запропонованої методології.

# ВИСНОВКИ

1. Як і у всіх складних видах діяльності, в ІТ-проєктах залучаються багато партнерів з різними цілями, котрі зазнають різноманітних ризиків за умов невизначеності. Управління цими ризиками вкрай важливе, оскільки дає змогу заздалегідь ідентифікувати, оцінити та зменшити можливі негативні наслідки для проєкту, забезпечуючи ефективне управління витратами, строками та якістю реалізації, а також мінімізуючи втрати через виникнення непередбачених проблем. Саме тому удосконалення процесу управління ризиками є ключовим викликом у сфері ІТ-проєктів.

2. У роботі проаналізовано ризики ІТ-проєктів, виявлено їхні особливості, а також розглянути існуючі підходи до класифікації цих ризиків на предмет їх подальшої структуризації.

3. Запропонована в роботі СДР є структурою, яка системно класифікує та організовує ризики в межах проєкту. Вона є цінним інструментом в управлінні ризиками, який допомагає ідентифікувати, аналізувати та інформувати про потенційні ризики у структурований та зрозумілий спосіб. Суть концепції СДР полягає в її здатності розбивати складні ризикові сценарії на менші, керованіші компоненти, що полегшує зацікавленим сторонам оцінювання та ефективне зниження ризиків.

4. Розроблено метод для управління ризиками ІТ-проєкту, заснований на застосуванні спеціально розроблених структур ризиків, які добре адаптовані до стадії і ступеня розвитку проєкту, конкретних вимог і завдань учасників проєкту, і мають необхідний рівень деталізації.

5. Автором розроблено програмне забезпечення для полегшення застосування цієї методології в реальних проєктах. Вказане програмне забезпечення є корисним інструментом для ідентифікації, аналізу та ієрархічного представлення ризиків і може допомогти менеджерам проєкту ефективно керувати ризиками.

6. Використовуючи запропонований метод, кожен з учасників проєкту, на кожному з етапів проєкту і на свій власний погляд на ризики може побудувати свою власну специфічну СДР. Таку СДР також варто адаптувати як загальну підтримку всіх зацікавлених сторін проєкту з метою полегшення розуміння та обговорення проєктних ризиків.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Bartlett J. The Essentials of Managing Risk for Projects and Programmes. Taylor & Francis, 2017. 120 p.

2. Кузьмін О. Є., Подольчак Н. Ю., Подольчак Н. І., Вербицька Л. Г. Управління ризиками в інноваційній діяльності: навч. посіб. Львів: Видавництво Львівської політехніки, 2012. 240 с.

3. Управління проектами: навчальний посібник / Уклад.: Л. Є. Довгань, Г. А. Мохонько, І. П. Малик. Київ: КПІ ім. Ігоря Сікорського, 2017. 420 с.

4. Eriksson P., Westerberg M. Effects of cooperative procurement procedures on construction project performance: A conceptual framework. *International Journal of Project Management*. 2011. Vol.29. P.197–208.

5. Березуцький В. В., Адаменко М. І. Небезпечні виробничі ризики та надійність: навчальний посібник. Харків: ФОП Панов А. М., 2016. 385 с.

6. Chapman C., Ward S. Project Risk Management: Processes, Techniques and Insights, Second edition. John Wiley & Sons, 2003. 322 p.

7. Боровик М. В. Ризик-менеджмент: конспект лекцій для студентів магістратури. Харків: ХНУМГ ім. О. М. Бекетова, 2018. 65 с.

8. Сьоме видання Настанови до зводу знань з управління проєктами (Настанова PMBOK) та Стандарт з управління проєктами. Project Management Institute. 2021.

9. Hillson D. The Risk Management Handbook: A Practical Guide to Managing the Multiple Dimensions of Risk. Kogan Page; 2nd edition. 2023. 416 p.

10. Mulcahy R. PMP Exam Prep, Eighth Edition - Updated: Rita's Course in a Book for Passing the PMP Exam. Eighth Edition. RMC Publications, 2015. 611 p.

11. Hubbard D. The Failure of Risk Management: Why It's Broken and How to Fix It. Wiley, 2009. 240 p.

12. Portny S. Project Management for Dummies. 4th edition. For Dummies, 2013. 408 p.

13. Батенко Л. П., Загородніх О. А., Ліщинська В. В. Управління проектами: навч. посібник. Київ: КНЕУ, 2003. 231 с.

14. Азаренкова Г. М. Аналіз моделювання і управління ризиком (в схемах та прикладах): Навч. посібник. Львів: Новий світ-2000, 2011. 240 с.

15. Berkeley D., Humphreys P. C., Thomas R. D. Project Risk Action Management. *Construction Management and Economics*. 1991. Vol.9(1). P.3-17.

16. Flanagan R., Norman G., Chapman R. Risk management and construction. 2nd ed. John Wiley & Sons Incorporated, 2006. 240 p.

17. BS/IEC 62198:2001 Project risk management – Application guidelines. London, UK: British Standards Institute.

18. Hertz D. B., Thomas H. Risk analysis and its application. Wiley, Chichester, 1983.

19. Del Cano A., de la Cruz M. P. Integrated Methodology for Project Risk Management. Journal of Construction Engineering and Management. 2002. Vol.128, P.473-485

20. Madsen S. 9 Steps to Managing Risk for Your Projects. – URL: https://www.liquidplanner.com/blog/9-steps-risk-management-process/ (дата відвідання: 21.11.2023).

21. Cagliano A. C., Grimaldi S., Rafele C. Choosing project risk management techniques. A theoretical framework. *Journal of Risk Research*. 2015. Vol.18, N.2. P.232-248.

22. A guide to the project management body of knowledge (PMBOK Guide), 6th ed. Project Management Institute, Newtown Square, PA. 2017. 756 p.

23. Del Cano A., de la Cruz M. P. Integrated Methodology for Project Risk Management. *Journal of Construction Engineering and Management*. 2002. Vol.128, P.473-485.

24. Patterson F. D., Neailey K. A Risk Register Database System to aid the management of project risk. *International Journal of Project Management*. 2002. P.365-374.

25. Project Risk Management. Guidance for WSDOT Projects. Washington State Department of Transportation, 2010. – 96 p.

26. Assaf S. A., Al-Hejji S. Causes of delay in large construction projects. *International Journal of Project Management*. 2006. Volume 24, Issue 4. P.349-357.

27. Project Management Institute. Practice Standard for Risk Management. – Newtown Square, PA: PMI, 2009. – 128 p.

28. ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови (ISO 31000:2018, IDT). Київ: УкрНДНЦ.

29. ДСТУ ISO/TR 31004:2018 Менеджмент ризиків. Настанова з впровадження ISO 31000 (ISO/TR 31004:2013, IDT). Київ: УкрНДНЦ.

30. ДСТУ ISO Guide 73:2013 Керування ризиком. Словник термінів (ISO Guide 73:2009, IDT). Київ: УкрНДНЦ.

31. ДСТУ IEC/ISO 31010:2013 Керування ризиком. Методи загального оцінювання ризику (IEC/ISO 31010:2009, IDT). Київ: УкрНДНЦ.

32. Carr V. Tah J. H. M. A fuzzy approach to construction project risk assessment and analysis: construction project risk management system. *Advances in Engineering Software*. 2001. P.847-857.

33. ISO 21511:2018(en) Work breakdown structures for project and programme management.

34. Institute Project Management. What Is a Work Breakdown Structure (WBS)? – URL: https://instituteprojectmanagement.com/blog/work-breakdown-structure/ (дата відвідання: 21.11.2023).

35. Lutkevich B. HIPAA (Health Insurance Portability and Accountability Act). – URL: https://www.techtarget.com/searchhealthit/definition/HIPAA. (дата відвідання: 21.11.2023).

36. Magnusson A., Brown S. SOX Compliance: 2023 Complete Guide. – URL: https://www.strongdm.com/sox-compliance (дата відвідання: 21.11.2023).

37. Hillson D. Understanding risk exposure using multiple hierarchies. Paper presented at PMI Global Congress 2007 – EMEA, Budapest, Hungary. Newtown Square, PA: Project Management Institute. – URL:

https://www.pmi.org/learning/library/understanding-risk-exposure-multiple-hierarchies-7367 (дата відвідання: 21.11.2023).

38. Pipattanapiwong J., Watanabe T. An Effective Risk and Uncertainty Management Process for Infrastructure Projects: Development of Multi-Party Risk and Uncertainty Management Process. *Society for Social Management Systems*. Vol.5 (1), 2009.

39. Marle F., Vidal L. A., Bocquet J. C. Interactions-based risk clustering methodologies and algorithms for complex project management. *International Journal of Production Economics*. 2013. Vol.4. P.225-234

40. Chauveau E. Management des risques dans les projets et les processus logiciel. Ph.D. thesis. University Bordeaux 1, 2006.

41. Risk Classification. A Complete Guide - 2021 Edition. Risk Classification Publishing, 2020. 316 p.

42. Rejda G. E., McNamara M. Principles of Risk Management and Insurance, 13th Edition. Pearson, 2016.

43. Marks N. World-Class Risk Management. 2015. 236 p.

44. Vose D. Risk Analysis: A Quantitative Guide. 3rd Edition. Wiley, 2012. 750 p.

45. Гладій Г. М. Методологія розробки структурної декомпозиції ризиків проекту. *Труды международной научно-практической конференции «Математическое моделирование процессов в экономике и управлении инновационными проектами (ММП-2014)»*. Харьков: ХНУРЭ, 2014. С.41-43.

46. Hladiy G., Tomyn I. The Concept of Forming a Hierarchical Structure of IT Project Risks. Proceedings of the III International Scientific and Practical Conference Problems of creating scientific ideas about world development" (October 03-06, 2023) Ottawa, Canada. P.90-94.

47. Hladiy G., Tomyn I. Identification of IT Project Risks. Proceedings of the VII International Scientific and Practical Conference «Global problems of improving scientific inventions». Copenhagen, Denmark. 2023. P.132-137.

48. Корнелюк О. М. Лекції з дисципліни «Проектний практикум». Національний університет кораблебудування ім. адмірала Макарова. Херсон, 2015.

49. Бобров С. В., Романченко О. А., Утюшев М. К., Педан Ф. П. Визначення рейтингу ризиків проєкту. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. 2019. №2(66). С.68-72.

50. Комар М. П., Саченко А. О., Васильків Н. М., Гладій Г. М., Турченко І. В. Методичні рекомендації до виконання кваліфікаційної роботи з освітньо-професійної програми «Управління проєктами» спеціальності 122 «Комп'ютерні науки» за другим (магістерським) рівнем вищої освіти. – Тернопіль: ЗУНУ, 2021. – 32 с.

Додаток А

Копія публікацій автора