ТОВ «ТЕХНІЧНИЙ УНІВЕРСИТЕТ «МЕТІНВЕСТ ПОЛІТЕХНІКА»
Факультет автоматизації виробництва та цифрових технологій
Кафедра цифрових технологій та проєктно-аналітичних рішень

«Допущено до захисту»
Гарант ОПП

Павло САГАЙДА

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня магістра

за підсумками виконання
освітньо-професійної програми
«Комп'ютерні науки та цифровий інтелект»
за спеціальністю 122 Комп`ютерні науки

на тему «Дослідження методів, моделей та інформаційних технологій при розробці автоматизованої системи аналізу управління ризиками бізнес-процесів»

Керівник роботи — Ірина ГЕТЬМАН

Консультант від бази практики — Олександр ВИБОРНОВ

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Здобувач — Максим СМИРНОВ

Підсумкова оцінка за атестацію			

Голова ЕК — Олена ПАВЛЕНКО

КРИВИЙ РІГ 2024

ТОВ «ТЕХНІЧНИЙ УНІВЕРСИТЕТ «МЕТІНВЕСТ ПОЛІТЕХНІКА»

Факультет	автоматизації виробництва та цифрових технологій
Кафедра	цифрових технологій та проектно-аналітичних рішень
Ступінь вищої освіти	магістр
Спеціальність	122 Комп'ютерні науки
ОПП	Комп'ютерні науки та цифровий інтелект

ЗАТВЕРДЖУЮ
Гарант ОПП

Павло САГАЙДА
«06» листопада 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

Смирнову Максиму Юрійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема роботи *Дослідження методів, моделей та інформаційних технологій при розробці автоматизованої системи аналізу управління ризиками бізнес-процесів* керівник роботи *Гетьман Ірина Анатоліївна, доцент, канд. техн. наук*,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом Університету від 29.08. 2023 р. №137.1/29.08.2023
2. Термін подання роботи *10.01.2024 р.*
3. Вихідні дані до роботи *Навчальна література, державні стандарти, методична література з спеціальних дисциплін та дипломування, науково-дослідницькі роботи з тематики автоматизації обробки й аналізу даних та методів цифрового інтелекту, літературні джерела, результати власних експериментів та досліджень, технологічні інструкції тощо*
4. Зміст пояснювальної записки (перелік питань) *Реферат. Зміст. Вступ. 1. Аналіз стану питання, предметної області, концепцій з проблеми, що розглядається (літературний огляд, недоліки існуючих систем, сучасні тенденції). 2. Розробка математичної моделі об'єкта (предметної області) та методики дослідження. 3. Розробка програмно-методичного комплексу для аналізу даних та інформаційної підтримки діяльності у процесі автоматизації системи аналізу управління ризиками бізнес-процесів. 4. Проведення та аналіз результатів теоретичних та експериментальних досліджень за індивідуальним завданням. 5. Економічне обґрунтування запропонованих технічних рішень. Висновки. Перелік використаних джерел. Додатки.*5. Перелік графічного (демонстраційного) матеріалу (з точним зазначенням обов'язкових креслень): *Актуальність, мета, об'єкт, предмет та завдання дослідження; розроблені або удосконалені математичні моделі, методика*

дослідження; діаграми проекту програмно-методичного комплексу в нотації UML (діаграми прецедентів, класів, послідовностей, діяльності); результати розробки та експериментальних досліджень; результати економічних розрахунків; висновки до роботи; публікація результатів дослідження.

6. Консультанти по роботі, із зазначенням розділів роботи, що стосуються їх.

Розділ	Прізвище, ініціали та посада консультанта
1	Гетьман І.А., доц. каф. ЦТПАР
2	Гетьман І.А., доц. каф. ЦТПАР
3	Гетьман І.А., доц. каф. ЦТПАР
4	Гетьман І.А., доц. каф. ЦТПАР
5	Гетьман І.А., доц. каф. ЦТПАР

7. Дата видачі завдання *06.11.2023*

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи
1	Розділ 1. Аналіз стану питання, концепцій з проблеми, що розглядається	25.12.2023 - 30.12.2023
2	Розділ 2. Розробка математичної моделі об'єкта (предметної області) та методики дослідження	25.12.2023 - 30.12.2023
3	Розділ 3. Розробка програмно-методичного комплексу для аналізу даних та інформаційної підтримки діяльності у процесі автоматизації системи аналізу управління ризиками бізнес-процесів	25.12.2023 – 02.01.2024
4	Розділ 4. Проведення та аналіз результатів теоретичних та експериментальних досліджень за індивідуальним завданням	03.01.2024 - 07.01.2024
5	Розділ 5. Економічні розрахунки	03.01.2024 - 07.01.2024
6	Висновки, перелік посилань, вступ, зміст, реферат	07.01.2024 – 08.01.2024
7	Подання завершеної роботи. Перевірка на академічний плагіат	10.01.204 – 16.01.2024
8	Остаточне оформлення роботи, презентаційного матеріалу, автореферату	17.01.2024 – 19.01.2024
9	Рецензування завершеної роботи. Захист	19.01.2024 – 24.01.2024

Здобувач (Максим СМИРНОВ)

Керівник роботи (Ірина ГЕТЬМАН)

РЕФЕРАТ

Кваліфікаційна робота: 119 с., 10 рис., 7 табл., 5 додатків, 32 літературних джерела.

Актуальність теми автоматизації управління ризиками визначається складним та змінюваним бізнес-середовищем, конкурентним тиском, розширенням технологічних можливостей та високими вимогами до корпоративного управління.

Метою дослідження – підвищення ефективності та безпеки бізнес-процесів завдяки впровадженню автоматизованої системи аналізу управління ризиками надійності контрагентів.

Об'єкт дослідження – система аналізу управління ризиками надійності контрагентів, що включає в себе технічні рішення, процеси та методи, призначені для оцінки та мінімізації ризиків у співпраці з контрагентами.

Предметом дослідження – основні аспекти автоматизованої системи, такі як ідентифікація та оцінка ризиків, аналіз відкритих джерел даних та інтеграція з існуючими бізнес-процесами.

Методи дослідження: системний аналіз ризиків, можливості веб-скрапінгу для збору даних, аналізу великих обсягів даних, використання методів статистичного аналізу та моделювання.

Наукова новизна дослідження полягає в створенні динамічної системи, яка комбінує різні джерела інформації (внутрішні бази даних, веб-скрапінг, відкриті джерела) для комплексного аналізу контрагентів та поглиблення розуміння потенційних небезпек. Практичне значення отриманих результатів полягає в забезпеченні підприємства засобами для ефективного виявлення та управління ризиками взаємодії з контрагентами, мінімізує можливості виникнення негативних сценаріїв взаємодії, нівелює виникнення репутаційних та санкційних ризиків, що дозволяє зменшити втрати та збільшити надійність бізнес-процесів.

SUMMARY

Qualification work: 119 pages, 10 figures, 7 tables, 5 appendices, 32 literary sources.

The relevance of the topic of automation of risk management is determined by the complex and changing business environment, competitive pressure, the expansion of technological capabilities and high requirements for corporate governance.

The purpose of the study is to increase the efficiency and security of business processes thanks to the implementation of an automated system of risk management analysis of the reliability of counterparties.

The object of the study is a system of risk management analysis of the reliability of counterparties, which includes technical solutions, processes and methods designed to assess and minimize risks in cooperation with counterparties.

The subject of research is the main aspects of an automated system, such as identification and assessment of risks, analysis of open data sources and integration with existing business processes.

Research methods: systemic risk analysis, web scraping capabilities for data collection, analysis of large volumes of data, use of statistical analysis and modeling methods.

The scientific novelty of the study consists in the creation of a dynamic system that combines various sources of information (internal databases, web scraping, open sources) for a comprehensive analysis of counterparties and deepening the understanding of potential dangers. The practical significance of the obtained results is to provide the company with means for effective detection and management of risks of interaction with counterparties minimizes the possibility of negative scenarios of interaction, eliminates the occurrence of reputational and sanction risks, which allows reducing losses and increasing the reliability of business processes.

ЗМІСТ

ВСТУП

Автоматизовані системи аналізу управління ризиками бізнес-процесів використовуються для виявлення, оцінки, моніторингу та управління ризиками в організаціях. В сучасних реаліях такі системи важливі для ефективного управління та збереження стійкості в бізнесі.

Автоматизовані системи аналізу управління ризиками надають комплексний підхід до управління ризиками, що дозволяє підприємствам ефективно взаємодіяти з невизначеністю та забезпечувати стабільність у динамічному бізнес-середовищі.

Актуальність теми автоматизації управління ризиками визначається численними факторами, включаючи складне та змінюване бізнес-середовище, конкурентний тиск, розширення технологічних можливостей та високі вимоги до корпоративного управління.

Дослідження предметної області проведено на базі підприємства, яке працює у напрямку надання послуг у сфері економічної безпеки, а саме контролю ризиків безпеки контрагентів та комплаєнс-ризиків.

З метою вдосконалення надання комплаєнс-послуг, існує необхідність своєчасного отримання аналітичної інформації шляхом формування звітів у розрізі контрагентів для визначення ризикових факторів впливу на бізнес-процеси підприємств відповідно встановленим критеріям ризиків співпраці.

Крім того, через проведення військових дій на території України виникли додаткові ризики, що потребують підвищеної уваги, у зв'язку з можливим співробітництвом контрагентами, які перебували на тимчасово окупованих територіях, з країною-агресором.

Таким чином, розробка автоматизованої системи аналізу управління ризиками бізнес-процесів дозволить своєчасно та

ефективно відреагувати на вплив зовнішніх факторів та мінімізувати ризики.

Метою дослідження є підвищення ефективності та безпеки бізнес-процесів завдяки впровадженню автоматизованої системи аналізу управління ризиками надійності контрагентів.

Об'єктом дослідження є система аналізу управління ризиками надійності контрагентів, що включає в себе технічні рішення, процеси та методи, призначені для оцінки та мінімізації ризиків у співпраці з контрагентами.

Предметом дослідження є основні аспекти автоматизованої системи, такі як алгоритми ідентифікації та оцінки ризиків, аналіз відкритих джерел даних про контрагентів, інтеграція з існуючими бізнес-процесами.

Задачі дослідження: огляд та аналіз існуючих методів та технологій управління ризиками взаємодії з контрагентами, включаючи традиційні та інноваційні підходи; розробка алгоритмів ідентифікації потенційних ризикованих ситуацій у взаємодії з різними контрагентами; дослідити можливості використання відкритих джерел даних (веб-скрапінг) для збору інформації про контрагентів та їхню репутацію; розробити механізми інтеграції автоматизованої системи аналізу ризиків у вже існуючі бізнес-процеси підприємства.

Методи дослідження: використання методів системного аналізу, аналізу ризиків, веб-скрапінгу для збору даних, аналізу великих обсягів даних, використання методів статистичного аналізу та моделювання.

Наукова новизна дослідження полягає в створенні системи, яка комбінує різні джерела інформації (внутрішні бази даних, веб-скрапінг, відкриті джерела) для комплексного аналізу контрагентів. Крім того, проведено дослідження розробки динамічних моделей аналізу ризиків, які адаптуються до змін у бізнес-середовищі та поглиблюють розуміння потенційних небезпек.

Практичне значення отриманих результатів полягає в забезпеченні підприємства засобами для ефективного виявлення та управління ризиками взаємодії з контрагентами, мінімізує можливості виникнення негативних сценаріїв взаємодії, нівелює виникнення репутаційних та санкційних ризиків, що дозволяє зменшити втрати та збільшити надійність бізнес-процесів.

РОЗДІЛ 1. АНАЛІЗ СУЧАСНОГО СТАНУ ПИТАННЯ ТА КОНЦЕПЦІЙ З ПРОБЛЕМИ УПРАВЛІННЯ РИЗИКАМИ БІЗНЕС-ПРОЦЕСІВ

1.1 Аналіз та актуальність процесів автоматизованої системи аналізу та управління ризиками бізнес-процесів

У сучасному складному та постійно змінюваному бізнес-середовище на перші ролі визначається актуальність теми автоматизації управління ризиками процесів діяльності підприємства. Крім того, суттєвий вплив оказують такі фактори як конкурентний тиск, розширення технологічних можливостей та високі вимоги до корпоративного управління.

Основні аспекти, які роблять це питання актуальним:

– Глобалізація та змінюване середовище. У сучасному світі компанії взаємодіють на глобальному рівні, що вносить додаткову невизначеність та ризики. Системи аналізу ризиків допомагають компаніям адаптуватися до швидко змінюваного середовища та виявляти потенційні небезпеки.

– Інновації та технологічний прогрес. Високий темп технологічних змін може призводити до нових можливостей, але також створює нові види ризиків, пов'язаних з кібербезпекою, конфіденційністю даних, невдачами систем і т.д. Системи управління ризиками дозволяють ефективно реагувати на ці виклики.

– Висока конкуренція та тиск на витрати. Конкуренція в бізнесі є високою, і підприємства завжди шукають шляхи оптимізації процесів та зниження витрат. Управління ризиками дозволяє ефективно планувати та мінімізувати витрати.

– Підвищення вимог до корпоративного управління. Зростаюча

увага до корпоративного управління та вимоги щодо звітності від акціонерів та регуляторів створюють потребу в ефективному управлінні ризиками для забезпечення стійкості та відповідності.

– Публічні скандали та репутаційні ризики. Негативні події, пов'язані з корупцією, недобросовісністю або порушенням етичних стандартів, можуть призводити до серйозних репутаційних втрат. Системи управління ризиками допомагають уникати таких ситуацій та забезпечити дотримання етичних норм.

– Підвищення свідомості про кліматичні зміни. Зміни в кліматі та пов'язані з цим ризики можуть впливати на багато галузей, включаючи виробництво, логістику та інші. Управління такими екологічними ризиками є важливою частиною сталого розвитку.

– Необхідність відповідності до регуляторних вимог. Зростання обсягу регуляторних вимог і стандартів вимагає від підприємств вдосконалювати системи управління ризиками для відповідності нормативам та уникнення штрафів.

– Глобальні здійснення бізнесу. Підприємства здійснюють свою діяльність на різних ринках, що викликає унікальні геополітичні та економічні ризики. Ефективне управління ризиками дозволяє компаніям адаптуватися до різноманітних умов різних регіонів.

Таким чином, актуальність необхідності застосування системи аналізу управління ризиками бізнес-процесів для сучасного підприємства визначається потребою в комплексному та систематичному підході до управління всіма видами ризиків, що можуть впливати на успішність та стабільність діяльності бізнесу.

Автоматизовані системи аналізу та управління ризиками бізнес-процесів призначені для забезпечення ефективного виявлення, оцінки, моніторингу та керування ризиками, що можуть виникнути в діяльності підприємства.

Сутність таких систем включає в себе кілька ключових процесів:

1. Ідентифікація ризиків: Збір інформації про потенційні ризики, які можуть виникнути в рамках бізнес-процесів. Цей процес може включати аналіз діяльності компанії, виявлення слабких місць та ідентифікацію потенційних загроз.

2. Оцінка ризиків: Аналіз і визначення важливості та ймовірності виникнення ризиків. Оцінка ризиків дозволяє визначити їхній вплив на бізнес та визначити, яким чином їх слід обробляти.

3. Моніторинг та аналіз: Постійний моніторинг стану ризиків в реальному часі. Це може включати в себе аналіз виконання бізнес-процесів, збір даних та виявлення будь-яких нових або змінених ризиків.

4. Управління ризиками: Розробка стратегій та планів для управління ризиками. Це може включати прийняття заходів для зменшення ризиків, їх передачу за допомогою страхування, прийняття на себе ризику чи інші стратегії.

5. Застосування проактивних заходів: Застосування проактивних заходів для запобігання виникненню ризиків або зменшення ймовірності їхнього виникнення. Це може включати навчання персоналу, впровадження нових технологій та інші заходи.

6. Звітність та документація: Ведення документації та складання звітів щодо стану ризиків. Це може включати створення звітів для стейкхолдерів, аналіз ефективності заходів та регулярне оновлення планів управління ризиками.

7. Інтеграція з іншими системами: Взаємодія з іншими системами, такими як системи управління проєктами, системи моніторингу безпеки, для забезпечення цілісності та повноцінного аналізу ризиків.

8. Неперервне вдосконалення: Постійне вдосконалення методів аналізу та управління ризиками на основі вивчення досвіду та

реакції на зміни в діловому оточенні.

Ці процеси дозволяють підприємствам ефективно взаємодіяти з ризиками, щоб забезпечити стабільну та безпечну діяльність, а також підтримувати стратегічні та операційні цілі бізнесу.

1.2 Фреймворки та сучасні моделі аналізу та управління ризиками бізнес-процесів.

Існує ряд сучасних моделей та фреймворків для аналізу та управління ризиками бізнес-процесів:

- ISO 31000
- COSO ERM (Enterprise Risk Management)
- PMI Risk Management Framework
- FAIR (Factor Analysis of Information Risk)
- BowTie Risk Management
- Agile Risk Management
- FRAP (Facilitated Risk Analysis Process)
- NIST Risk Management Framework

Розглянемо основні принципи цих моделей.

ISO 31000

Міжнародний стандарт ISO 31000:2018 [1] надає загальний підхід до управління ризиками та встановлює принципи та загальні керівництва. Він визначає терміни, принципи та рамки для управління ризиками.

Основні принципи цього стандарту включають:

- загальний підхід: ISO 31000 пропонує загальний та універсальний підхід до управління ризиками, який може бути застосований до будь-якого виду організації та її контексту.

– інтеграція з управлінням організацією: Управління ризиками розглядається як невід'ємна частина загального управління організацією. Ризики повинні бути інтегровані в стратегічне планування та процеси прийняття рішень.

– визнання та власництво ризиків: Організація повинна чітко визнавати та розуміти свої ризики. Керівництво повинно приймати власництво ризиків, тобто нести відповідальність за їх управління.

– розподіл відповідальності: ISO 31000 визначає необхідність розподілу відповідальності за управління ризиками між різними рівнями та функціональними одиницями організації.

– контекст організації: Управління ризиками повинно враховувати контекст організації, включаючи її цілі, структуру, культуру, стратегії та стейкхолдерів.

– забезпечення інформацією: Забезпечення актуальною, достовірною та зрозумілою інформацією є ключовим аспектом ефективного управління ризиками.

– забезпечення всебічності та системності: Управління ризиками повинно охоплювати всі ризики, які можуть вплинути на досягнення цілей організації, і враховувати їх взаємозв'язок.

– індивідуальність та визнання відмінностей: Розпізнання різних підходів до управління ризиками, адаптація до специфічних умов та визнання індивідуальних відмінностей важливі для ефективного управління ризиками.

– постійне вдосконалення та виявлення нових ризиків: Управління ризиками — це процес, який повинен бути вдосконалюваний постійно. Це включає в себе виявлення нових ризиків та вдосконалення методів їх управління.

– забезпечення відповідності та згідності: Управління ризиками повинно бути відповідним стандартам та вимогам, які стосуються конкретної організації.

Ці принципи встановлюють загальний фреймворк для розробки, впровадження та оцінювання систем управління ризиками в організаціях.

COSO ERM

COSO ERM (Enterprise Risk Management) — це фреймворк для управління підприємством, який включає у себе елементи оцінки та управління ризиками. Він розроблений Комітетом організаційної структури (COSO) та визначає загальні засади управління ризиками на рівні підприємства. Основні принципи COSO ERM:

– створення та збереження значення: Управління ризиками повинно сприяти досягненню стратегічних цілей підприємства та забезпечувати створення та збереження цінності.

– визнання та інтеграція управління ризиками в організаційний процес: Управління ризиками повинно бути вбудоване в процеси управління та виконання стратегії організації.

– встановлення заздалегідь зрозумілих обов'язків та відповідальностей: Чітко визначені обов'язки та відповідальності для управління ризиками сприяють ефективному виконанню завдань та враховують стейкхолдерів.

– розуміння завдань та мети: Ризики повинні аналізуватися та оцінюватися в контексті досягнення цілей організації.

– зв'язок з зовнішніми та внутрішніми середовищами: Розуміння впливу зовнішніх та внутрішніх факторів на організацію та управління ризиками, пов'язаними з цими факторами.

– оцінка загального ризику: Визначення загального рівня ризику для оцінки, чи досягають організації своїх цілей та чи належним чином управляються ризиками.

– визнання та управління змінами: Управління ризиками повинно бути гнучким та пристосовуватися до змін у внутрішньому та зовнішньому середовищі організації.

– визначення та оцінка змоги: Розуміння можливостей, які можуть виникнути з управління ризиками, і їх використання для покращення результатів.

– належність до подання інформації: Належне подання інформації про управління ризиками стейкхолдерам та усім іншим зацікавленим сторонам.

– належне подання і використання інформації: Забезпечення належності та точності інформації про ризики для прийняття вчасних та належних рішень.

Ці принципи допомагають організаціям створювати систематичний та інтегрований підхід до управління ризиками та забезпечують їх взаємозв'язок з стратегічним управлінням та операційними процесами.

PMI Risk Management Framework

Project Management Institute (PMI) пропонує фреймворк для управління ризиками, який можна визначити через його стандарт PMI PMBOK (Project Management Body of Knowledge) та конкретно модуль "Project Risk Management" [3]. Основні принципи PMI Risk Management Framework включають:

– інтеграція з проектним управлінням: управління ризиками повинно бути тісно інтегроване з усіма процесами управління проєктом. Ризики визначаються, аналізуються та враховуються при прийнятті рішень на різних етапах проєкту.

– систематичний підхід: управління ризиками повинно бути систематичним та охоплювати всі аспекти проєкту. Це включає визначення, аналіз, планування відповідей на ризики та моніторинг ризиків протягом усього життєвого циклу проєкту.

– визначення та оцінка ризиків: визначення ризиків включає ідентифікацію потенційних подій та їх вплив на проєкт. Оцінка ризиків визначає ймовірність виникнення та вплив кожного ризику на цілі

проєкту.

– планування відповіді на ризики: розроблення планів відповіді на ризики для ефективного керування та мінімізації впливу виникаючих ризиків.

– моніторинг та контроль ризиків: систематичне відстеження ризиків, оновлення їх статусу та реалізація необхідних коректив заходів.

– залучення стейкхолдерів: важливість взаємодії з усіма зацікавленими сторонами (стейкхолдерами) для отримання інформації щодо ризиків та їх оцінки.

– співпраця та комунікація: співпраця між членами проектного команду та ефективна комунікація грають ключову роль у виявленні та управлінні ризиками.

– аналіз чутливості: врахування чутливості ризиків до змін у ключових параметрах проєкту та їх вплив на кінцеві результати.

– ітеративний процес: процес управління ризиками є ітеративним і може змінюватися на протязі життєвого циклу проєкту.

– документування та звітність: збір та збереження документації щодо ризиків, проведення аналізу та відповідей на ризики, а також регулярна звітність стейкхолдерам.

Ці принципи є частиною загального підходу PMI до управління проєктами та допомагають забезпечити ефективне управління ризиками в рамках проєкту.

FAIR

FAIR (Factor Analysis of Information Risk) є квантитативним методом для аналізу і оцінки ризиків, пов'язаних із інформаційною безпекою [4]. Його основні концепції включають ідентифікацію ризиків, оцінку вартості та ймовірності:

– дефініція ризику: FAIR визначає ризик як комбінацію ймовірності виникнення події та величини втрати внаслідок цієї події.

– квантитативний аналіз: FAIR наголошує на квантитативному, а не кваліативному, аналізі ризиків. Він використовує числові значення для оцінки ймовірності та втрат.

– елементи аналізу ризиків: FAIR визначає чотири основні елементи аналізу ризиків: Asset (актив), Threat (загроза), Vulnerability (вразливість) та Impact (вплив).

– структурований підхід: FAIR надає структурований підхід до аналізу ризиків, використовуючи деякі базові категорії та поняття.

– масштабованість: методологія FAIR може бути масштабована від простих оцінок до складних, враховуючи різні рівні деталей.

– об’єктивність: FAIR ставить перед собою завдання забезпечити об'єктивні та повторювані оцінки ризиків.

– використання метрик: FAIR використовує конкретні метрики, такі як Annualized Loss Exposure (ALE) та Annualized Rate of Occurrence (ARO), для вимірювання ймовірності та втрат.

– фокус на бізнес-подіях: FAIR орієнтований на аналіз конкретних бізнес-подій та їх вплив на організацію.

– адаптивність: FAIR прагне бути адаптивним до різних контекстів та типів організацій.

– роль стейкхолдерів: FAIR активно залучає стейкхолдерів для забезпечення більшої достовірності та повноти аналізу.

FAIR надає структуровану методологію для кількісного аналізу ризиків і може бути використана для розуміння впливу інформаційних ризиків на бізнес-процеси та цінності активів організації.

BowTie Risk Management

Методологія BowTie - це спосіб управління ризиками, який використовує візуальні зображення у вигляді "метелика" (англ. "bowtie") – діаграми бар'єрів для візуалізації ризиків та протиризикових заходів. Це спрощує розуміння ризиків та можливостей їх

управління [5]. Основні принципи BowTie Risk Management включають:

– визначення цілей та ризиків: ясне визначення цілей та ризиків, пов'язаних із здійсненням операцій чи здійсненням конкретних процесів.

– ідентифікація небезпек: визначення та ідентифікація конкретних небезпечень, які можуть призвести до виникнення ризиків.

– оцінка ймовірності та впливу: оцінка ймовірності та впливу ризиків для визначення їх важливості та пріоритету.

– визначення заходів безпеки: встановлення та деталізація заходів безпеки, які спрямовані на управління ризиками та запобігання виникненню небезпек.

– побудова метелика (BowTie): створення візуального зображення, що нагадує бабочку, з ймовірністю ризику на одному крилі та заходами безпеки на іншому.

– визначення контрольних точок (Barriers): визначення контрольних точок, які є важливими заходами безпеки для запобігання виникненню або обмеження наслідків ризиків.

– моніторинг та оцінка ефективності: систематичний моніторинг та оцінка ефективності заходів безпеки та їх впливу на управління ризиками.

– стейкхолдерський підхід: залучення всіх зацікавлених сторін, включаючи керівництво, робочий персонал та інших учасників, до процесу управління ризиками.

– комунікація та звітність: чітка комунікація та звітність щодо ризиків, заходів безпеки та їх стану для всіх стейкхолдерів.

– гнучкість та адаптивність: методологія BowTie надає гнучкість та можливість адаптації до різних умов та середовищ.

BowTie Risk Management використовується для управління ризиками в різних сферах, таких як промисловість, авіація, охорона здоров'я тощо. Вона надає візуальну та систематичну стратегію для

управління ризиками та забезпечення безпеки.

Agile Risk Management

Управління ризиками в *агільних* проєктах відрізняється від традиційних методологій. Воно акцентує на регулярних ретроспективах та невеликих ітераціях для швидкого виявлення та вирішення ризиків. Agile Risk Management - це підхід до управління ризиками, спрямований на ітеративний та гнучкий розвиток проєктів в рамках методологій Agile, таких як Scrum чи Kanban [6]. Основні принципи Agile Risk Management включають:

– раннє та постійне визначення ризиків: визначення ризиків вже на ранніх етапах проєкту та постійна актуалізація цього визначення на протязі всього життєвого циклу проєкту.

– інкрементальний та ітеративний підхід: використання ітерацій та інкрементального підходу для забезпечення неперервного вдосконалення та врахування нових ризиків.

– залучення команди та стейкхолдерів: взаємодія з командою та стейкхолдерами для ідентифікації та аналізу ризиків, врахування різноманітних точок зору та спільного вирішення проблем.

– прозора комунікація: створення ефективної системи комунікації для виявлення, обговорення та вирішення ризиків на всіх рівнях.

– гнучкі засоби впровадження: застосування гнучких та адаптивних засобів впровадження змін для забезпечення швидкого реагування на ризики.

– постійна оцінка ризиків: регулярна оцінка ризиків для визначення їх ступеня небезпеки та актуальності заходів управління.

– спільний підхід до ризиків та завдань: інтеграція управління ризиками в процес управління завданнями та плануванням, сприяючи одночасному вирішенню проблем та досягненню цілей.

– адаптивність та реагування на зміни: готовність до швидкого

адаптування до змін в середовищі, що дозволяє забезпечити реагування на нові ризики.

– культура відкритості та взаємодопомоги: розвиток культури відкритості, де команда може вільно обговорювати ризики та взаємно допомагати один одному у їх розв'язанні.

– фокус на постачанні цінності: зосередження на постачанні цінності для клієнта та відмова від надлишкової бюрократії, щоб забезпечити ефективність управління ризиками.

Ці принципи дозволяють ефективно інтегрувати управління ризиками в культуру Agile, що дозволяє забезпечити більшу гнучкість та ефективність у роботі з ризиками під час розробки та впровадження продуктів чи проєктів.

FRAP

FRAP (Facilitated Risk Analysis Process) є методом колективного аналізу ризиків, в якому беруть участь різні зацікавлені сторони для ідентифікації, аналізу та оцінки ризиків [7]. Основні принципи FRAP включають:

– груповий підхід: FRAP використовує груповий підхід, де група учасників, яка включає представників різних рівнів та фахівців, працює разом для визначення та аналізу ризиків.

– активне залучення учасників: учасники процесу активно залучаються до аналізу ризиків та взаємодіють для досягнення консенсусу.

– процес фасилітації: процес аналізу ризиків фасилітується незалежним фасилітатором або експертом для забезпечення об'єктивності та ефективності.

– швидкість та ефективність: FRAP покликаний бути швидким та ефективним, спрощуючи процес аналізу для швидшого виявлення та управління ризиками.

– визначення ключових аспектів: фокус на визначенні

ключових аспектів, які найбільше впливають на досягнення цілей організації.

– пріоритетизація ризиків: пріоритетизація ризиків для концентрації уваги на найважливіших та найімовірніших загрозах.

– використання простих інструментів: FRAP використовує прості та зрозумілі інструменти для аналізу ризиків, щоб зробити процес доступним широкому колу учасників.

– фокус на результаті: акцент на визначенні конкретних результатів та заходів для зменшення чи управління ризиками.

– консенсус та схвалення: досягнення консенсусу серед учасників щодо ідентифікації ризиків та прийняття рішень щодо управління ними.

– підтримка комунікації: забезпечення ефективної комунікації між учасниками для обміну інформацією щодо ризиків та заходів.

FRAP спрощує процес аналізу ризиків та робить його більш доступним для широкого кола учасників, забезпечуючи швидше виявлення та управління ризиками в організації.

NIST Risk Management Framework:

National Institute of Standards and Technology (NIST) пропонує свій фреймворк для управління ризиками, зокрема, у сфері кібербезпеки. Він включає в себе кроки і методи для ідентифікації, захисту, виявлення, відгуку та відновлення від кіберризиків. NIST RMF – це стандарт із управління ризиками, розроблений Національним інститутом стандартів і технологій (NIST) США [8]. Основні принципи RMF включають:

– кишеньковий підхід: RMF застосовує кишеньковий підхід до управління ризиками, зосереджуючись на конкретних потенційних загрозах та вразливостях в інформаційних системах.

– інтеграція у життєвий цикл системи: RMF інтегрується у життєвий цикл системи, включаючи розробку, впровадження,

експлуатацію та відмову.

– поверхневий підхід до управління ризиками: RMF використовує поверхневий підхід для ідентифікації та оцінки ризиків на рівні організації та інформаційної системи.

– постійний процес управління ризиками: RMF покликаний забезпечити постійний та систематичний процес управління ризиками, оскільки загрози можуть змінюватися з часом.

– оцінка впливу та ймовірності: важливою частиною RMF є оцінка впливу та ймовірності ризиків для прийняття обґрунтованих рішень з управління ризиками.

– керування заходами безпеки: RMF включає керування заходами безпеки для зменшення ризиків та захисту інформаційних систем.

– розгляд на рівні організації: розгляд ризиків відбувається на рівні організації, щоб врахувати стратегічні та бізнес-аспекти.

– узгодження з передовими практиками: RMF узгоджений із передовими практиками у сфері управління ризиками та інформаційної безпеки.

– фокус на захисті інформації: захист інформації визначається як основна мета RMF, і управління ризиками спрямоване на забезпечення цілісності, конфіденційності та доступності інформації.

– врахування стейкхолдерів: залучення стейкхолдерів для забезпечення широкого розуміння та підтримки управління ризиками.

RMF дозволяє організаціям ефективно інтегрувати управління ризиками у всі аспекти життєвого циклу інформаційних систем і забезпечує систематичний підхід до цього процесу.

Кожен з цих фреймворків чи моделей може бути використаний залежно від специфіки бізнес-потреб та галузі. Реалізація ефективної системи аналізу управління ризиками великою мірою залежить від унікальних вимог та характеристик конкретної організації.

1.3 Глосарій термінів

BPMN (англ. Business Process Model and Notation, модель та нотація бізнес-процесів) – система умовних позначень (нотація) для моделювання бізнес-процесів.

CSV (англ. comma-separated values ‘значення, розділені комою’) – файловий формат, котрий є відмежовувальним форматом для представлення табличних даних, у якому поля відокремлюються символом коми та переходу на новий рядок.

DOM (англ. Document Object Model) – об'єктна модель документа, специфікація прикладного програмного інтерфейсу для роботи зі структурованими документами (як правило, документами XML).

ERP (англ. enterprise resource planning system — Система планування ресурсів підприємства) – планування ресурсів підприємства (ERP-система) корпоративна інформаційна система (KIC), призначена для автоматизації обліку й керування.

IDEF0 (Function Modeling) – методологія функціонального моделювання і графічного опису процесів, призначена для формалізації і опису бізнес-процесів.

JavaScript - динамічна, об'єктно-орієнтована прототипна мова програмування.

MySQL - вільна система керування реляційними базами даних, яка була розроблена компанією «TcX» для підвищення швидкодії обробки великих баз даних.

UML (англ. Unified Modeling Language) – уніфікована мова моделювання, використовується у парадигмі об'єктно-орієнтованого програмування.

WBS (англ. work breakdown structure) – структура декомпозиції робіт, ієрархічна структура робіт у проєктному менеджменті та

системотехніці є орієнтованою на доконане виконання проєкту декомпозицією проєкту на менші частки.

База даних (англ. database) – сукупність даних, організованих відповідно до концепції, яка описує характеристику цих даних і взаємозв'язки між їх елементами.

Веб-скрапінг (англ. scraping — «вишкрібання», веб-збирання або витягнення веб-даних) - перетворення у структуровані дані інформації з веб-сторінок, які призначені для перегляду людиною за допомогою браузера.

Фреймворк (англ. Framework, каркас, платформа, структура, інфраструктура) – інфраструктура програмних рішень, що полегшує розробку складних систем.

Фронтенд та Бекенд (Front end та back end) – презентаційна частина інформаційної або програмної системи, її інтерфейс користувача і пов'язані з ним компоненти; застосовується у співвідношенні з базисною частиною системи, її внутрішньою реалізацією, яка називається в цьому випадку бекендом.

Висновки за розділом 1

Перши розділ присвячений аналізу сучасного стану питання та концепцій з проблеми управління ризиками бізнес-процесів.

В ході дослідження встановлено, що актуальність необхідності застосування системи аналізу управління ризиками бізнес-процесів для сучасного підприємства визначається потребою в комплексному та систематичному підході до управління всіма видами ризиків, що можуть впливати на успішність та стабільність діяльності бізнесу.

Автоматизовані системи аналізу та управління ризиками бізнес-процесів призначені для забезпечення ефективного виявлення, оцінки, моніторингу та керування ризиками, що можуть виникнути в діяльності підприємства.

Встановлені ключові процеси системи аналізу та управління ризиками бізнес-процесів: ідентифікація ризиків, оцінка ризиків, моніторинг та аналіз, управління ризиками, застосування проактивних заходів, звітність та документація, інтеграція з іншими системами, неперервне вдосконалення.

Досліджені основні сучасні моделі та фреймворки для аналізу та управління ризиками бізнес-процесів: ISO 31000, COSO ERM (Enterprise Risk Management), PMI Risk Management Framework, FAIR (Factor Analysis of Information Risk), BowTie Risk Management, Agile Risk Management, FRAP (Facilitated Risk Analysis Process), NIST Risk Management Framework.

Досвід застосування цих фреймворків чи моделей може бути використаний залежно від специфіки бізнес-потреб та галузі. Реалізація ефективної системи аналізу управління ризиками великою мірою залежить від унікальних вимог та характеристик конкретної організації.

РОЗДІЛ 2. РОЗРОБКА МАТЕМАТИЧНОЇ МОДЕЛІ ПРОЦЕСА АВТОМАТИЗАЦІЇ СИСТЕМИ АНАЛІЗУ УПРАВЛІННЯ РИЗИКАМИ БІЗНЕС-ПРОЦЕСІВ

2.1 Обґрунтування вибору методів теоретичних та експериментальних досліджень та програмного забезпечення систем аналізу та управління ризиками бізнес-процесів

Сучасні компанії можуть використовувати різноманітні методи та інструменти для аналізу ризиків, включаючи:

– аналіз фінансових даних: використання фінансових даних для оцінки фінансової стійкості компаній.

– моніторинг юридичного статусу: систематичний моніторинг змін у юридичному статусі підприємств.

– аналіз даних з реєстрів та баз даних: використання великих обсягів даних з різних реєстрів та баз даних для аналізу ризиків та ідентифікації аномалій.

– моделі машинного навчання та штучного інтелекту: використання алгоритмів машинного навчання для прогнозування ризиків та виявлення нетипового здійснення операцій.

– аналіз ринку та конкурентів: вивчення ринкових та конкурентних тенденцій для розуміння контексту та конкурентної ситуації.

– оцінка репутації та відгуків: аналіз відгуків клієнтів та рейтингів для оцінки репутації бізнес-партнерів.

Для автоматизації системи управління аналізом ризиків при перевірці надійності контрагентів використовують різноманітне

програмне забезпечення. Розглянемо деякі типові сучасні категорії програм та інструментів, які можна використовувати для цієї мети:

1. Системи Управління Ризиками (ERM - Enterprise Risk Management):

- Mega International - HOPEX Risk Intelligence: Ця платформа дозволяє інтегрувати різні аспекти управління ризиками в одну систему, включаючи оцінку ризиків контрагентів.

- IBM OpenPages: надає засоби для ідентифікації та управління ризиками включаючи ризики, пов'язані з контрагентами.

2. Фінансовий моніторинг та аналіз:

- Dun & Bradstreet: ця компанія надає послуги з аналізу фінансової стійкості та надійності контрагентів.

- CreditRiskMonitor: спеціалізується на моніторингу фінансового здоров'я підприємств та відстеженні змін в кредитоспроможності.

3. Аналітичні та ділові звіти:

- SAS Risk Management for Banking: надає рішення для аналізу та управління ризиками в банківській сфері, включаючи ризики контрагентів.

- Thomson Reuters Eikon: платформа, яка дозволяє вивчати та аналізувати фінансові дані, включаючи дані про підприємства та їх ризики.

4. Інструменти для збору та аналізу відкритої інформації:

- LexisNexis Risk Solutions: надає доступ до різноманітних джерел інформації для вивчення ризиків та надійності контрагентів.

- Reputation.com: використовується для аналізу онлайн-репутації підприємств та організацій.

Слід зазначити, що вибір конкретного програмного забезпечення може залежати від конкретних вимог підприємства, розміру бізнесу та інших факторів.

Управління ризиками та аналіз даних є ключовою складовою для компаній, які надають послуги з контролю за бізнес-партнерами та ринкової інтелектуальної діяльності. В Україні на даний час у цій галузі працює декілька веб-сервісів та компаній, які вважаються найбільш актуальними за наповненням та універсальним за охопленням бізнес-процесів. Основною метою таких сервісів є забезпечення користувачів даними про юридичних осіб, їхні фінансові стани, керівництво, судові рішення, афілійованість та інші релевантні дані.

Основні етапи роботи аналітичних веб-сервісів:

– Збір та агрегація даних: сервіс отримує доступ до різних джерел даних, таких як державні бази даних, юридичні звіти, судові рішення, та інші відкриті джерела.

– Аналіз та обробка: отримані дані аналізуються та обробляються для створення структурованої інформації про підприємства.

– Індексація та пошук: дані індексуються для швидкого та ефективного пошуку. Користувачі можуть здійснювати пошук за різними критеріями, такими як назва компанії, код ЄДРПОУ, ім'я керівника тощо.

– Представлення інформації: отримані та оброблені дані представляються користувачам через інтерфейс веб-сайту або інші зручні канали.

– Сервіси для бізнесу: у додаток до основних функцій пошуку, сервіси, можуть надавати додаткові сервіси для бізнес-аналізу, моніторингу, антифрауду та інші.

Слід зазначити, що практична реалізація програмного продукту для автоматизованої системи аналізу управління ризиками бізнес-процесів у вигляді веб-сервісу має суттєві переваги, наприклад у порівнянні з десктопною програмою або мобільного додатку (табл. 2.1).

Таблиця 2.1 Порівняння властивостей застосування різних форм кінцевого програмного продукту

Властивості	Веб-ресурс	Десктопна програма	Мобільний додаток
Доступність	Легкий доступ через браузер з будь-якого пристрою (комп'ютер, планшет, смартфон).	Залежить від платформи (Windows, macOS, Linux).	Залежить від операційної системи (iOS, Android)
Оновлення та сумісність	Оновлення здійснюються на сервері, не вимагають встановлення на кінцевих пристроях. Сумісний з різними браузерами	Потребує оновлень, може виникнути проблема зі сумісністю між різними версіями операційних систем	Вимагає оновлень та підтримки для різних версій операційних систем
Розподілений доступ	Зручний для розподіленого доступу до даних з будь-якого місця	Зазвичай використовується на конкретному пристрої	Також може забезпечувати розподілений доступ, але вимагає встановлення на кожному пристрої
Вартість розробки та підтримки	Може бути більш вартісним для розробки, але зазвичай дешевший у плані підтримки	Потребує вартості для кожної платформи та оновлень	Також може бути вартісним для кожної операційної системи.
Інтеграція та обмін даними	Легко інтегрується з іншими веб-сервісами, обмін даними здійснюється через мережу	Може вимагати спеціальних зусиль для інтеграції та обміну даними	Зручний для інтеграції з функціональністю мобільного пристрою
Кросплатформеність	Робиться кросплатформеним через браузери	Залежить від вибраної технології розробки	Також залежить від технології та обраної платформи
Системи автентифікації та безпеки	Зручний для реалізації систем автентифікації та заходів безпеки	Також потребує врахування аспектів безпеки	

Загалом, веб-ресурс може бути оптимальним вибором для багатьох сценаріїв, зокрема, якщо важлива доступність, розподілений доступ та ефективність інтеграції з іншими веб-сервісами. Варто також

враховувати потреби цільової аудиторії та специфіку бізнес-задач проєкту.

2.2 Математична модель оцінювання величини показника ризику

На підприємстві, що забезпечує дослідження предметної області та аналізу даних, сформована політика якісного оцінювання критеріїв ризиків, рівень яких впливає на процес взаємодії з контрагентом. Згідно встановлених норм, ранжування утворюючих ризик факторів співвідноситься трьом групам рівня ризику: чорний, червоний, жовтий.

Розглянемо встановлені на базовому підприємстві критерії ризиків оцінки співпраці з контрагентом.

Рівень ризику – критичний (чорний):

– A1 - актуальне кримінальне переслідування посадових осіб контрагента за статтями КК України: розділ "Злочин проти засад національної безпеки України".

– A2 - реєстрація контрагента за даними Єдиного державного реєстру юридичних осіб, фізичних осіб підприємців та громадських формувань припинено.

– A3 - контрагенти причетні до захоплення підприємств на тимчасово окупованій території України, а також контрагенти, пов'язані з експлуатацією таких активів або реалізацією їх продукції та іншими контактами

– A4 - контрагенти, які вчинили шахрайські дії щодо компанії.

– A5 - блокуючі санкції України, ЄС, США, міжнародних організацій, інших країн застосовані хоча б до однієї з таких осіб: контрагенту, прямому або опосередкованому акціонеру, кінцевому бенефіціару контрагента незалежно від частки його володіння.

Рівень ризику – високий (червоний):

– В1 - актуальне кримінальне переслідування посадових осіб контрагента за статтями КК України: ст. 201 (Контрабанда), ст. 205 "Фіктивне підприємництво", ст. 209 "Легалізація (відмивання) доходів, отриманих злочинним шляхом" та інших.

– В2 - місцезнаходження (реєстрація) відокремлених підрозділів контрагента на тимчасово окупованій території України, на яких органи державної влади тимчасово не здійснюють своїх повноважень.

– В3 - афілійованість контрагента з відповідальними співробітниками підприємства та/або з іншими учасниками бізнес-процесів (конфлікт інтересів).

– В4 - наявність актуального кримінального переслідування посадових осіб контрагента за порушення податкового законодавства у сфері фінансово-господарської діяльності.

– В5 - контрагент відповідає ознакам "податкова яма", "вигодонабувач" або "транзитер" (в розумінні порядку взаємодії підрозділів ДФС, що рекомендується, при комплексному відпрацюванні податкових ризиків з податку на додану вартість).

– В6 - контрагент зареєстрований в Ірані, Північній Кореї, Судані, Південному Судані, Сирії, Лівії або в іншій юрисдикції/території з високим ризиком санкції.

Рівень ризику – середній (жовтий):

– С1 - місцезнаходження відокремлених підрозділів контрагента та/або його виробничих потужностей на тимчасово окупованій території України, на яких органи державної влади України тимчасово не здійснюють своїх повноважень, або здійснення контрагентом господарських операцій з юридичними особами, місцезнаходження яких є тимчасово окупованою територією України.

– С2 - контрагент перебуває у стадії припинення чи банкрутства за даними Єдиного державного реєстру юридичних.

– С3 - повне чи часткове зупинення діяльності контрагента за рішенням органу державного нагляду (контролю).

– С4 - наявність у контрагента корпоративних суперечок.

– С5 - наявність інформації про протиправне заволодіння майном контрагента (рейдерське захоплення).

– С6 - з дати проведення державної реєстрації контрагента закінчилося менше 6 місяців та/або контрагент не здійснював фінансово-господарську діяльність з дня державної реєстрації.

– С7 - контрагент не має матеріально-технічної бази, кваліфікованого персоналу, виробничих потужностей, відповідної дозвільної документації для провадження господарської діяльності, і як наслідок - виконання умов договору.

– С8 - наявність сум податкового боргу.

– С9 - щодо контрагента відкрито виконавче провадження.

– С10 - протягом останніх 5 років був притягнутий до відповідальності за порушення санкцнонних режимів (хоч би один із): контрагент; прямий чи опосередкований акціонер контрагента, який здійснює контроль за ним; кінцевий бенефіціар контрагента

– С11 - член виконавчого органу, прямий або опосередкований учасник/акціонер, який володіє часткою від 25% і вище, кінцевий власник власника або їх близькі родичі є державними службовцями.

– С12 - контрагент, кінцевий бенефіціарний власник, прямий або опосередкований учасник/акціонер, що володіють часткою від 25% і вище, зареєстрований у офшорній юрисдикції.

– С13 - основний вид діяльності контрагента не збігається з характером послуг, що їм надаються за договором (у контрагента немає належної кваліфікації для надання послуг за договором, матеріальною базою, іншими елементами, необхідними для виконання договірних зобов'язань).

Оцінювання величини показника ризику від ймовірності появи ризикових подій та величини можливих наслідків реалізації ризику (загрози) для бізнесу дуже важливий етап в процесі управління аналізу ризиків бізнес-процесів.

Встановим величини можливих наслідків та ймовірність появи ризикових подій.

Величина можливих наслідків:

– Мінімальна (1 бал): фінансові збитки, дестабілізація бізнесу.

– Низька (2 бали): фінансові втрати, втрата доходу, невиконання договірних зобов'язань.

– Середня (3 бали): залучення до кримінального переслідування, обшуки, вилучення документів, переривання операційної діяльності, державні штрафи, судові позови

– Висока (4 бали): державні штрафи, судові позови, порушення внутрішньо корпоративних принципів.

– Максимальна (5 балів): залучення до кримінального переслідування, скасування виданих дозволів та ліцензій, блокування фінансово-господарської діяльності, втрата виробничих потужностей, значні збитки, втрата доходу.

Ймовірність появи ризикових подій:

– Слабо-ймовірна (1 бал): Це вказує на те, що ймовірність виникнення ризикової події дуже низька. Така подія може бути малоймовірною, і їй приділяють невелику увагу, оскільки вважається, що ймовірність виникнення низька.

– Малоймовірна (2 бали): Це також вказує на низьку ймовірність. Ризикова подія, яка є малоймовірною, може вважатися малоймовірною, але тем не менш, слід здійснювати відслідковування та контроль.

– Ймовірна (3 бали): Ймовірна ризикова подія має певний рівень ймовірності виникнення. Це може вказувати на те, що ймовірність

висока достатньо, щоб варто було взяти цей ризик до уваги та розглядати стратегії управління ризиками.

– Вельми ймовірна (4 бали): Цей термін вказує на те, що ймовірність виникнення ризикової події велика. Така подія є ймовірною, і вона може потребувати активного управління ризиками та прийняття заходів.

– Майже можлива (5 балів): Цей термін може вказувати на те, що ймовірність дуже висока, практично на межі реалізації. Такі ризики слід ретельно вивчати та вживати відповідних заходів для їх управління.

Для оцінювання ймовірності впливу ризикових подій на процес взаємодії з контрагентом потрібно використати показник ризику, який дає змогу визначити величину можливих наслідків (у балах) від настання негативних ситуацій. Також цей показник дає можливість комплексно оцінити заходи реагування на ризикові події та рівень їхньої загрози загалом. Показник ризику обчислюють за формулою (2.1):

$$R = I * B\ , \tag{2.1}$$

де: $I = f_1(x)$ - ймовірність появи ризикових подій (у балах);

$B = f_2(y)$ - величина можливих наслідків (у балах);

$f_1(), f_2()$ – таблично-задані функції, що визначають перехід від значень оцінок x та y, обчислених на підставі даних про процес взаємодії з контрагентом, до ціло-чисельних бальних оцінок (табл. 2.2).

Таблиця 2.2 – Оцінювання величини показника ризику від ймовірності появи ризикових подій та величини можливих наслідків

Ймовірність появи ризикових подій		Величина можливих наслідків				
		1	2	3	4	5
Слабо-ймовірна	1	1	2	3	4	5
Малоймовірна	2	2	4	6	8	10
Ймовірна	3	3	6	9	12	15
Вельми ймовірна	4	4	8	12	16	20
Майже можлива	5	5	10	15	20	25

Якісні оцінки ідентифікованих ризиків можна виразити через ймовірність появи цих подій (І) і величину можливих наслідків (В), які в сукупності характеризують ступінь їх впливу на подальший хід процесу взаємодії з контрагентом. Для цього використовуємо таку якісну шкалу градації, як високий, середній і низький ступінь впливу ризиків. Також важливо визначити кількісне значення ступеня впливу кожного ризику, для чого використовуємо шкалу від 1 до 25 балів. Водночас, показник ризику дає змогу оцінювати величини можливих наслідків (в балах), які визначаємо за допомогою матриці "Ймовірність-Наслідки", що дає можливість робити деякі висновки про відповідну ступінь впливу ризику та певні рівні їхньої загрози (рис. 2.1).

Процедура оцінювання ідентифікованих ризиків процесу взаємодії з контрагентом ґрунтується на ефективності запланованих заходів реагування на ризикові події за ступенем їхнього впливу згідно з поточним значенням показника ризику (R). На підставі значення цього показника самі ризикові події класифікують за ступенем їхнього впливу на стан виконання проєкту і за рівнем їхньої загрози подальшим етапам реалізації всього проєкту.

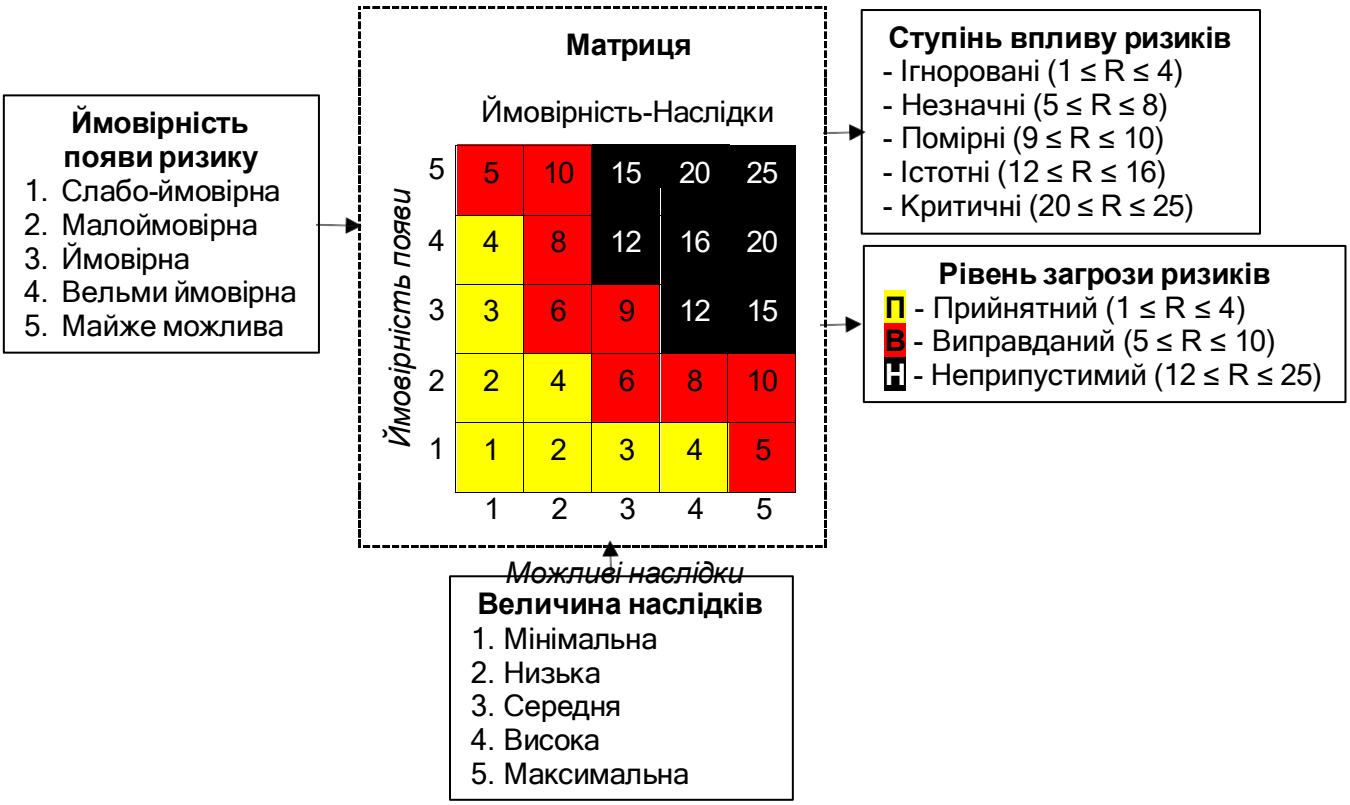


Рисунок 2.1 - Оцінювання ідентифікованих ризикових подій на процес взаємодії з контрагентом

Класифікація ризикових подій за ступенем їхнього впливу процес взаємодії з контрагентом має такий вигляд:

1. ігноровані ризики (1 ≤ R ≤ 4):

– мало відчутний вплив на процес взаємодії з контрагентом;

– незначне збільшення тривалості виконання деяких процесів взаємодії з контрагентом;

2. незначні ризики (5 ≤ R ≤ 8):

– збільшення тривалості виконання запланованих процесів взаємодії з контрагентом;

– потрібно виконати деякі додаткові дії в межах стандартних процесів взаємодії з контрагентом;

– недотримання деяких функціональних вимог, які не вимагаються для погодження взаємодії із контрагентом;

– незначна затримка надання необхідних документів контрагентом для погодження процесів співпраці;

3. помірні ризики ($9 \leq R \leq 10$):

– збільшення тривалості виконання багатьох процес взаємодії з контрагентом;

– потрібно виконати багато додаткових досліджень щодо контрагента поза межами запланованих термінів завершення;

– присутні багато невідповідностей та неточностей від контрагента, усунення яких у поточному процесі вимагають додаткових зусиль його виконавців;

– недотримання контрагентом багатьох узгоджених домовленостей, особливо функціональних вимог, зміни яких вимагають деяких додаткових тривалих погоджень;

– значне зниження ефективності виконання процесів взаємодії з контрагентом;

4. істотні ризики ($12 \leq R \leq 16$):

– значне збільшення тривалості виконання багатьох процес взаємодії з контрагентом;

– потрібно виконати значну кількість додаткових досліджень щодо контрагента поза межами запланованих термінів завершення;

– присутня значна кількість невідповідностей та неточностей від контрагента, усунення яких у поточному процесі вимагають додаткових зусиль його виконавців;

– недотримання контрагентом більшості узгоджених домовленостей, особливо функціональних вимог, зміни яких вимагають деяких додаткових тривалих погоджень;

– загальне зниження ефективності виконання процесів взаємодії з контрагентом;

– припинення виконання процесів взаємодії з контрагентом через можливість втрати значної частки прибуток;

5. критичні ризики (20 ≤ R ≤ 25):

– припинення виконання процесів взаємодії з контрагентом через можливість втрати всього прибутку;

– припинення виконання процесів взаємодії з контрагентом через можливість втрати частки майна компанії.

Класифікація ризикових подій за рівнем їхньої загрози подальшим етапам виконання процесів взаємодії з контрагентом має такий вигляд:

1. прийнятний ризик (1 ≤ R ≤ 4) :

– розглядається до прийняття проектних рішень, в т.ч. вимог до ПЗ;

– рівень загрози ризику має періодично переоцінюватися керівником проєкту;

2. виправданий ризик (5 ≤ R ≤ 10):

– визначається як вторинний для оброблення та аналізу;

– ризик має мати певну стратегію його оброблення, аналізу та реагування;

– ризик потрібно обробляти доти, доки рівень його загрози не знизиться до прийнятного;

– ризик має знаходитися під постійним контролем керівника проєкту;

– рівень загрози ризику має постійно переоцінюватися керівником проєкту;

3. неприпустимий ризик (12 ≤ R ≤ 25):

– ризик визначається як первинний для оброблення, аналізу та реагування;

– ризик має мати певну стратегію його оброблення, аналізу, реагування та моніторингу;

– ризик потрібно наполегливо і без зупинки обробляти доти, доки рівень його загрози не знизиться до виправданого;

– ризик має знаходитися під постійним і безпосереднім контролем керівника проєкту;

– рівень загрози ризику має систематично переоцінюватися керівником проєкту.

Залежно від отриманого значення показника ризику (R) для кожної з можливих ризикових подій потрібно встановити ступінь її впливу на подальший хід реалізації програмного проєкту залежно від категорії ризику та визначити заплановані заходи реагування на них. В обґрунтованих випадках визначені тривалості та вартості виконання завдань проєкту можуть бути скореговані на величину очікуваних результатів, пов'язаних з цими завданнями.

Висновки до розділу 2

У другому розділі проведена розробка математичної моделі процесу автоматизації системи аналізу управління ризиками бізнес-процесів.

В ході роботи розглянути різноманітні методи та інструменти для аналізу ризиків, досліджено порівняльну характеристику властивостей застосування різних форм кінцевого програмного продукту.

В результаті встановлено, що практична реалізація програмного продукту для автоматизованої системи аналізу управління ризиками бізнес-процесів у вигляді веб-сервісу має суттєві переваги.

Згідно сформованої політики якісного оцінювання критеріїв ризиків, рівень яких впливає на процес взаємодії з контрагентом, встановлено докладне ранжування утворюючих ризик факторів із співвідношенням до трьох груп ризику: чорний, червоний, жовтий.

На підставі дослідження проведено оцінювання величини показника ризику від ймовірності появи ризикових подій та величини можливих наслідків. В результаті розроблена класифікація ризикових подій за ступенем їхнього впливу процес взаємодії з контрагентом.

РОЗДІЛ 5. ЕКОНОМІЧНІ РОЗРАХУНКИ

Оцінка вартості розробки програмного забезпечення — це важливий етап у плануванні проекту. Щоб розцінити витрати, можна використовувати кілька підходів та інструментів. Нижче наведені кілька методів і факторів, які можна врахувати:

1. Розбір робочих завдань:

– Аналіз функціональності: Розбийте проєкт на конкретні завдання та функціональність, яку потрібно реалізувати.

2. Оцінка ресурсів:

– Робочі години: Визначте, скільки робочих годин буде потрібно для виконання кожного завдання.

– Інтенсивність праці: Врахуйте інтенсивність праці розробників, тестувальників, аналітиків та інших учасників проєкту.

3. Розцінка робочих годин:

– Ставки заробітної плати: Визначте робочі ставки для кожного фахівця, який бере участь у розробці.

– Вартість години роботи: Обчисліть вартість робочої години кожного учасника.

4. Фактори, що впливають на вартість:

– Складність завдань: Врахуйте складність та технічні виклики, які можуть збільшити робочі години.

– Терміни виконання: Короткі терміни можуть вимагати більше зусиль та прискорити роботу, що може збільшити вартість.

5. Використання стандартів та готових рішень:

– Готові бібліотеки та фреймворки: Використання готових рішень може значно скоротити час розробки та витрати.

6. Оцінка ризиків та невизначеності:

– Запаси часу: Додайте запаси на випадок можливих затримок або змін у завданнях.

7. Оцінка витрат на обладнання та програмні засоби:

– Ліцензії на програмне забезпечення: Врахуйте витрати на придбання ліцензій на необхідне програмне забезпечення.

– Обладнання та інфраструктура: Визначте вартість обладнання та інфраструктури, яку потрібно для розробки та тестування.

8. Визначення загальної вартості:

– Сумування вартостей: Сумуйте вартості робочих годин для кожного учасника, додайте витрати на обладнання, програмне забезпечення та інші витрати.

9. Оцінка та аудит оцінки:

– Проведення аудиту: Періодично переглядайте та аудитуйте оцінки вартості для виявлення можливих відхилень та коригувань.

Важливо зазначити, що точність оцінок може залежати від рівня деталізації завдань та реальних умов виконання проєкту. Рекомендується використовувати методології, такі як Agile, які дозволяють гнучко реагувати на зміни та уточнення у процесі розробки.

Враховуючи специфіку галузі з економічної безпеки та діяльності базового підприємства, реалізація проєкту можлива тільки власною командою розробників, без залучення сторонніх фахівців.

З метою виявлення економічної доцільності розробки програмного продукту визначимо наявність економічного ефекту від запровадження веб-додатку автоматизованої системи аналізу управління ризиками бізнес-процесів. Для цього проведемо розрахунки затрат на розробку програмного продукту та експлуатаційних витрат при впровадженні програмного продукту.

Проведемо розрахунок затрат на розробку проєкту у розрізі наступних витрат:

- на основну заробітну плату розробників проекту;
- на додаткову заробітну плату розробників;
- нарахування на заробітну плату;
- амортизація комп'ютерної техніки, яка використовується процесі розробки проекту;
- на матеріали, які використані в процесі розробки;
- на силову електроенергію;
- інші витрати.

Затрати на основну заробітну плату команди розробників проекту визначаються виходячи із складу та чисельності команди, розмірів місячної заробітної плати кожного з учасників команди, а також із загальної трудомісткості розробки програмного забезпечення.

Розрахунок величини основної заробітної плати розробників проекту проводиться за формулою:

$$З_о = (М/Т_р)*t, \qquad (5.1)$$

де М – місячний посадовий оклад конкретного розробника, грн.;

$Т_р$ – число робочих днів у місяці (коливається в межах 21 – 23 робочі дні), дн.;

t – число днів роботи конкретного розробника проєкту.

Місячно заробітна плата визначається із середнього рівня заробітної плати на ринку праці даної категорії працівника.

Над розробкою програмного продукту планується залучити двох працівників компанії: керівник проєкту та програміст-розробник. Місячний оклад керівника складає 45000 грн. Місячний оклад розробника складає 30000 грн. (суми вказані в якості прикладу для

розрахунків).

Роботи з розробки веб-додатку (складання та узгодження технічного завдання, проектування, написання коду, тестування) згідно умов технічного завдання повинні бути виконані за шість місяців. Розробник Керівник проєкту виконує контроль, надає рекомендації, консультації та перевіряє виконання етапів робіт один раз на тиждень протягом половини робочого дня та при потребі додаткові консультації. Програміст-розробник в зв'язку з виконанням об'ємом робіт згідно посадової інструкції виконує роботи по проєкту три робочих дня в тиждень.

Виходячи з вищенаведених даних, заробітна плата розробника проєкту $З_{ор}$ та керівника проєкту $З_{ок}$ складає:

$З_{ор} = (30000/22)*72 = 98208$ грн.

$З_{ок} = (45000/22)*24 = 49080$ грн.

Таким чином, загальні витрати на заробітну плату склали 147288 грн. (табл. 5.1).

Таблиця 5.1 – Витрати на заробітну плату

Робітник	Місячний оклад, грн.	Заробітна плата за 1 робочий день, грн.	Трудомісткість робіт, дні	Витрати на заробітну плату
Програміст-розробник	30000	1363	72	98208
Керівник проєкту	45000	2045	24	49080
			Всього	147288

Витрати на додаткову заробітну плату команди розробників включає виплати, передбачені чинним законодавством про працю і визначається за формулою:

$$З_д = (З_о * Н_д)/100\%, \quad (5.2)$$

де $З_о$ – витрати на основну заробітну плат розробників проєкту, грн.;

$Н_д$ – норматив додаткової заробітної плати, який прийнято у межах 10%.

Тоді

$$З_д = 147288/10*100 = 14728,8 \text{ грн.}$$

До розрахунку кошторису витрат на розробку програмного забезпечення включають відрахування на державне соціальне страхування у вигляді єдиного соціального внеску, який здійснюється від суми всіх витрат на оплату праці розробників проекту, зайнятих безпосередньо вказаними роботами.

Нормативи, за якими здійснюється відрахування, встановлюються на державному рівні. На теперішній час ЄСВ згідно з чинними законодавчими актами України становить 22%.

Відрахування на соціальні потреби проводяться за формулою:

$$В_{сз} = ((З_о + З_д)*22\%)/100\% \quad (5.3)$$

Тобто, відповідно до проєкту розробки веб-додатку

$В_{сз} = ((147288 + 14728,8)*22\%)/100\% = 35643,7$ грн.

Амортизаційні відрахування визначаються за формулою:

$$А = (Ц/Т_к)*(Т/12), \quad (5.4)$$

де Ц – балансова вартість одиниці обладнання, на якому проводиться розробка проєкту, грн.;

$T_к$ – термін корисного використання обладнання (5 років), р.;

Т – термін використання обладнання для проведення розробки проєкту, міс..

У роботі по створенню веб-додатку використовується один персональний комп'ютер з операційною системою Windows 11 (вартість 30000 грн.).

А = (30000/5)*(6/12) = 3000 грн.

Витрати на матеріали розраховуються за формулою:

$$M = (H_i * Ц_i * K_i) * n, \quad (5.5)$$

де H_i - кількість матеріалу і-го найменування, од.;

$Ц_i$ - ціна матеріалу і-го найменування, од.;

K_i - коефіцієнт транспортних витрат, що приймається у межах 1,1.

Витрати по матеріалам, використаних у процесі роботи над проєктом відображено в таблиці 5.2.

Таблиця 5.2 – Витрати на матеріали

Назва матеріалів	Ціна, грн.	Кількість, од.	Коефіцієнт транспортних витрат	Вартість витратного матеріалу, грн.
Флеш-накопичувач	800	1	1,1	880
Батарея АА для миші	50	2		110
Папір А4	200	1		220
Тонер для принтера	150	1		165
			Всього	1375

Витрати на електроенергію визначаються за формулою:

$$B_e = В * П * Ф * K_п, \quad (5.6)$$

де, В – вартість однієї кВт*год електроенергії, грн.;

П – установлена потужність обладнання, кВт;

Ф – фактична кількість годин робот комп’ютера, год.;

$K_п$ – коефіцієнт використання потужності.

Станом на теперішню дату тариф електроенергії дорівнює 2,64 грн./кВт*год.

Установлену потужність комп’ютера приймаємо рівною 0,08 кВт.

Фактична кількість годин робот комп’ютера розраховуємо як добуток кількості днів та кількості годин його фактичного використання:

Ф = 72*8 = 576

Коефіцієнт використання потужності приймаємо рівним 0,9.

Тоді,

B_e = 2,64*0,08*576*0,9 = 109,50 грн.

Витрати на оренду приміщення та комплектуючи для обладнання відсутні.

Окрім того, розраховуються інші витрати на розробку програмного забезпечення, до яких відносять витрати як напряму пов’язані з розробкою проекту, так і витрати, пов’язані з функціонуванням організації розробника в цілому (наприклад, витрати на послуги Internet, освітлення, опалення приміщень, вартість послуг на зв'язок та інші додаткові витрати).

Оскільки розроблюване програмне забезпечення буде використовуватися для власних потреб та розробляється власними силами, багато статей інших витрат відсутні (до прикладу, витрати на службові відрядження та ін.). Інші витрати приймаємо рівними 70% від суми основної та додаткової заробітної плати учасників проекту.

B_i = (147288 + 14728,8)*0,7 = 113411,76 грн.

Загальні витрати на розробку програмного продукту розраховується як сума усіх попередніх статей витрат:

$$В = З_о + З_д + В_{сз} + А + М + В_е + В_і \quad (5.7)$$

В = 147288 + 14728,8 + 35643,7 + 3000 + 1375 + 109,5 + 113411,76 =
= 315556,76 грн.

Таким чином, загальна вартість затрат становить 315556,76 грн. (табл. 5.3).

Таблиця 5.3 – Витрати на розробку програмного забезпечення

Стаття витрат	Сума, грн.
Основна заробітна плата команди розробників	147288
Додаткова заробітна плата команди розробників	14728,8
Відрахування у фонд соціального забезпечення	35643,7
Амортизаційні відрахування	3000
Витрати на матеріали	1375
Витрати на електроенергію	109,5
Інші витрати	113411,76
Загальна сума витрат на розробку	315556,76

Тепер проведемо розрахунок експлуатаційних витрат при використання програмного продукту, які включають наступні статті:

- заробітна плата обслуговуючого персоналу;
- додаткова заробітна плата обслуговуючого персоналу;
- нарахування на заробітну плату обслуговуючого персоналу в;
- витрати на силову електроенергію;
- інші витрати.

Заробітна плата обслуговуючого персоналу (менеджерів), який буде використовувати продукт, ($З_{мен}$) розраховується по формулі:

$$З_{мен} = 12*М*β, \quad (5.8)$$

де 12 – кількість місяців у році, од.;

М – місячний посадовий оклад менеджера (в середньому 30000 грн.) грн.;

β – частина часу, який витрачає менеджер на обслуговування нового програмного забезпечення в загальному часі своєї роботи (приймаємо рівним 0,2).

$З_{мен}$ = 12*30000*0,2 = 72000 грн./рік

Додаткова заробітна плата менеджера по обслуговуванню нового програмного забезпечення розраховується як 10% від основної заробітної плати:

$$З_д = З_{мен}*0,1, \quad (5.9)$$

$З_д$ = 72000*0,1 = 7200 грн.

Нарахування на заробітну плату менеджера приймається рівним 22% від основної та додаткової заробітної плати, тому нарахування визначаються за формулою:

$$Н_{зп} = (З_{мен} + З_д)*0,22 \quad (5.10)$$

$Н_{зп}$ = (72000 + 7200)*0,22 = 17424 грн.

Витрати на силову електроенергію можна визначити за формулою:

$$В_е = В*П*Ф*К_п*β, \quad (5.11)$$

де, В – вартість однієї кВт*год електроенергії (2,64 грн.), грн.;

П – установлена потужність обладнання (0,09 кВт), кВт;

Ф – фактична кількість годин робот комп'ютера (8 годин на день, 22 робочих дня в місяці, 12 місяців в году), Ф = 2112 год.;

$К_п$ – коефіцієнт використання потужності комп'ютера, дорівнює 0,9;

β – доля часу, який витрачає менеджер на обслуговування нового програмного забезпечення в загальному часі своєї роботи (приймаємо рівним 0,2).

Витрати на силову електроенергію становлять:

$В_е$ = 2,64*0,09*2112*0,9*0,2 = 90,33 грн./рік.

Розрахунок інших витрат приймається, як 10% від загальної суми попередніх витрат та розраховується за формулою:

$$І_в = (З_{мен} + З_д + Н_{зп} + В_е)*0,1 \quad (5.12)$$

$І_в$ = (72000 + 7200 + 17424 + 90,33)*0,1 = 9671,43 грн.

Величина експлуатаційних витрат при використанні програмного забезпечення розраховується, як сума всіх попередніх статей витрат за формулою:

$$Е_2 = З_{мен} + З_д + Н_{зп} + В_е + І_в \quad (5.13)$$

$Е_2$ = 72000 + 7200 + 17424 + 90,33 + 9671,43 = 106385,76 грн.

Розрахуємо річний економічний ефект для споживача від провадження програмного забезпечення. Даний розрахунок ведеться за формулою:

$$\Delta E = (E_1/Q_1 - E_2/Q_2)*Q_2 \quad (5.14)$$

де E_1 - експлуатаційні витрати перед впровадженням програмного забезпечення;

E_2 - експлуатаційні витрати після впровадження програмного забезпечення;

Q_1 - обсяг робіт за рік, який виконується без використання програмного забезпечення;

Q_2 - обсяг робіт за рік, який виконується з використанням програмного забезпечення.

Розрахунок експлуатаційних витрати перед впровадженням програмного забезпечення проведемо аналогічно E_2 по формулам 5.8 - 5.13, приймаючи до розрахунку зміну показника β - приймаємо рівним 0,4.

E_1 = 144000 + 14400 + 34848 + 179,28 + 19342,73 = 212770 грн.

Розрахунок умовного обсягу робіт без використання та з використанням програмного продукту проводимо за формулою:

$$Q = (F*60*\beta)/t, \quad (5.15)$$

де F – фонд часу роботи за рік, F = 2112 год.;

показника β - доля часу, 0,4 для Q_1 та 0,2 для Q_2;

t – час виконання аналогічних функцій без використання програмного продукту та з його використанням, t_1 = 30 хв., t_2 = 4 хв.

Виходячи з наведених даних, річний економічний ефект від впровадження програмного продукту становитиме:

ΔE = (212770/1689,6 - 106385,76/6336)*6336 = 691501,8 грн.

Оскільки річний економічний ефект від впровадження програмного продукту становить 691501,8 грн. на противагу загальній сумі витрат на його розробку, що становлять 315556,76 грн., можна зробити висновок про доцільність розробки та впровадження даного програмного продукту.

Висновки до розділу 5

В п’ятому розділі досліджено економічні процеси розробки та впровадження автоматизованої системи аналізу управління ризиками бізнес-процесів.

Враховуючи специфіку галузі з економічної безпеки та діяльності базового підприємства, реалізація проєкту можлива тільки власною командою розробників, без залучення сторонніх фахівців.

З метою виявлення економічної доцільності розробки програмного продукту визначена наявність економічного ефекту від запровадження веб-додатку автоматизованої системи аналізу управління ризиками бізнес-процесів. Для цього проведено розрахунки затрат на розробку програмного продукту та експлуатаційних витрат при впровадженні програмного продукту.

Отриманий результат розрахунків річного економічного ефекту від впровадження програмного продукту дозволяє зробити висновок про доцільність розробки та впровадження даного програмного продукту.

ЗАГАЛЬНІ ВИСНОВКИ

В ході кваліфікаційної роботи проведено дослідження методів, моделей та інформаційних технологій при розробці автоматизованої системи аналізу управління ризиками бізнес-процесів.

Автоматизовані системи аналізу управління ризиками надають комплексний підхід до управління ризиками, що дозволяє підприємствам ефективно взаємодіяти з невизначеністю та забезпечувати стабільність у динамічному бізнес-середовищі.

Встановлена актуальність теми автоматизації управління ризиками, яка визначається численними факторами, включаючи складне та змінюване бізнес-середовище, конкурентний тиск, розширення технологічних можливостей та високі вимоги до корпоративного управління.

В ході роботи досліджено сучасні моделі та фреймворки для аналізу та управління ризиками бізнес-процесів з метою їх застосування в сучасних реаліях та особливо вагомих факторах ризиків, таких як надійність контрагентів, репутаційних та санкційних ризиків.

Встановлені ключові процеси системи аналізу та управління ризиками бізнес-процесів, такі як ідентифікація ризиків, оцінка ризиків, моніторинг та аналіз, управління ризиками, застосування проактивних заходів, звітність та документація, інтеграція з іншими системами, неперервне вдосконалення.

В ході роботи розглянути різноманітні методи та інструменти для аналізу ризиків, досліджено порівняльну характеристику властивостей застосування різних форм кінцевого програмного продукту. В результаті встановлено, що практична реалізація програмного продукту для

автоматизованої системи аналізу управління ризиками бізнес-процесів у вигляді веб-сервісу має суттєві переваги.

Згідно сформованої політики якісного оцінювання критеріїв ризиків, рівень яких впливає на процес взаємодії з контрагентом, встановлено докладне ранжування утворюючих ризик факторів із співвідношенням до трьох груп ризику: чорний, червоний, жовтий.

На підставі дослідження проведено оцінювання величини показника ризику від ймовірності появи ризикових подій та величини можливих наслідків. В результаті розроблена класифікація ризикових подій за ступенем їхнього впливу процес взаємодії з контрагентом.

По результатам роботи розроблено алгоритм дій програмного продукту по автоматизації системи управління аналізу ризиків бізнес-процесів в розрізі перевірки надійності контрагентів.

Також встановлено функціонал програмного продукту, який дозволяє ефективно та автоматично проводити аналіз ризиків та перевірку контрагентів, забезпечуючи користувачеві інформацію для прийняття надійних бізнес-рішень.

В ході роботи розроблено структура автоматизованої системи аналізу управління ризиками бізнес-процесів та виділено кілька ключових компонентів та модулів.

Розроблена концепція та основні характеристики проєкту:

1. Власні бази даних: реалізація системи передбачає використання власних баз даних для зберігання та управління інформацією про контрагентів.

2. Веб-Скрапінг: в системі передбачено модуль веб-скрапінгу для автоматичного отримання ризикової інформації з відкритих джерел.

3. Веб-сервіс: розробка вед-додатка на мові програмування JavaScript для обробки та аналізу отриманих даних, виявлення потенційних ризиків та генерації звітів.

4. Механізми оцінки ризиків: впровадження алгоритмів машинного навчання для прогнозування ризиків на основі історії взаємодії з іншими контрагентами.

5. Звіти та висновки: автоматична генерація звітів з висновками щодо ризиків, їхніх характеристик та рекомендацій для управлінських рішень.

6. Інтерфейс користувача: Забезпечення зручного інтерфейсу для користувачів системи з можливістю перегляду звітів, введення параметрів оцінки ризиків та моніторингу стану бізнес-процесів.

Вибір мови програмування JavaScript для веб-додатка, який має взаємодіяти з внутрішніми базами даних MySQL та використовувати веб-скрапінг, обумовлено наявністю наступними перевагами: браузерна інтеграція та веб-скрапінг; використання бібліотек Node.js; фреймворки для веб-розробки.

Крім того встановлено особливості та проблематика реалізації проєкту, що висловлюється у юридичних аспектах впровадженні модулю веб-скрапінгу.

З метою виявлення економічної доцільності розробки програмного продукту визначена наявність економічного ефекту від запровадження веб-додатку автоматизованої системи аналізу управління ризиками бізнес-процесів. Для цього проведено розрахунки затрат на розробку програмного продукту та експлуатаційних витрат при впровадженні програмного продукту.

Отриманий результат розрахунків річного економічного ефекту від впровадження програмного продукту дозволяє зробити висновок про доцільність розробки та впровадження даного програмного продукту.

ПЕРЕЛІК ПОСИЛАНЬ

1. A Comparative Study on Web Scraping. 2015. URL: http://ir.kdu.ac.lk/bitstream/handle/345/1051/com-059.pdf?sequence=1&isAllowed=y (дата звернення 05.01.2024)

2. About the business process model and notation specification. Version 2.0. BPMN™ Version: 2.0 Publication Date: 12.2010. URL: https://www.omg.org/spec/BPMN/2.0/ (дата звернення 28.12.2023)

3. Anderson E.J. Business Risk Management: Models and Analysis. Wiley, 2013. 384 c.

4. Becker, G. M. (2004). A practical risk management approach. Paper presented at PMI® Global Congress 2004—North America, Anaheim, CA. Newtown Square, PA: Project Management Institute.

5. C.J. DateAn Introduction to Database / C.J. DateAn // Pearson. 2003. C. 1024

6. Committee of Sponsoring Organizations of the Treadway Commission (COSO) "Enterprise Risk Management — Integrated Framework". Executive Summary, September 2004. C. 7-13.

7. David A. Black The Well-Grounded Java / A. David. Manning Publications Co., 2009. 483 c.

8. David A. Black The Well-Grounded Java second edition / A. David. Manning Publications Co., 2014. 538 c.

9. Fielding, Roy Thomas (2000). "Chapter 5: Representational State Transfer (REST)". University of California, Irvine. URL: https://ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm (дата звернення 27.12.2023)

10. Hopper, Carolyn H. (2007). "Mapping". Practicing College Learning Strategies (4th ed.). Boston: Houghton Mifflin. pp. 139-143.

11. ISO 31000:2018 Risk management Guidelines URL:

https://www.iso.org/ru/standard/65694.html (дата звернення 26.12.2023)

12. Java – java Manual 7.0 [Електроннийресурс]. – java is the officially supported ODM (Object-Document-Mapper) framework for java in Java. URL: https://docs. java.com/java/master (дата звернення 06.01.2024)

13. Java -Doc.org: Documenting the Java Language – Core API docs for Ruby 2.5.1 This is the current official release. URL: https://ruby-doc.org/core-2.5.1/.(дата звернення 06.01.2024)

14. Martin Fowler UML Distilled: A Brief Guide to the Standard Object ModelingLanguage/ Martin Fowler // Addison-Wesley Professional. 2003. C 208.

15. Mary Carmichael, CRISC, CISA, CPA, Member of ISACA Emerging Trends Working Group. Making Risk Management for Agile Projects Effective. Date Published: 20 February. 2023. URL: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/making-risk-management-for-agile-projects-effective (дата звернення 26.12.2023)

16. NIST Risk Management Framework, December 13, 2023. URL: https://csrc.nist.gov/projects/risk-management/about-rmf (дата звернення 26.12.2023)

17. Olston, C. and Najork, M. Web crawling. 2010. Foundations and Trends in Information Retrieval 3:175-246.

18. Rumbaugh J., Jacobson I., Booch G. (1999). The unified modeling language reference manual. Addison Wesley Longman, Inc. P. 24-45.

19. Sean Salleh, Risk analysis using FRAP: is it just silo thinking? July 19, 2013. URL: https://lumina.com/blog/risk-analysis-using-frap-is-it-just-silo-thinking/#:~:text=FRAP%20or%20the%20Facilitated%20Risk,in%20common%20with%20expert%20elicitation. (дата звернення 26.12.2023)

20. Subbu Allamaraju RESTful Web Services Cookbook / Subbu Allamaraju//O'Reilly Media / Yahoo Press. 2010. С 316.

21. The bowtie method. URL: https://www.wolterskluwer.com/en/solutions/enablon/bowtie/expert-insights/barrier-based-risk-management-knowledge-base/the-bowtie-method (дата звернення 26.12.2023)

22. Web Scraping Tools to Extract Online Data. 2019. URL: https://www.hongkiat.com/blog/web-scraping-tools/ (дата звернення 05.01.2024)

23. What Is Factor Analysis Of Information Risk (FAIR)? URL: https://www.wallarm.com/what/what-is-factor-analysis-of-information-risk-fair (дата звернення 26.12.2023)

24. ДСТУ IEC/ISO 31010:2013 Керування ризиком. Методи загального оцінювання ризиком (IEC/ISO 31010:2009,IDT). [Чинний від 2013-12-11]. Вид. офіц. Київ: Мінекономрозвитку України. 2015. 80 с.

25. Журман С., Шишкіна О. Систематизація наукових підходів до розуміння природи ризику. Проблеми і перспективи економіки та управління. 2018. № 3 (15). С. 155-163.

26. Косович Б. Діджиталізація як інноваційний тренд у забезпеченні сталого розвитку. Цифровізація економіки як фактор економічного зростання : колективна монографія / За заг. ред. проф. О. Л. Гальцової. Запоріжжя / Херсон : Вид. дім «Гельветика», 2021. С.185-199.

27. Куликова Е.Е. Управление рисками: инновационный аспект. - М.: Бератор-Паблишинг, 2008. 112 с.

28. Лесохин В.З. Разработка бизнес-процессов совместных инвестиций с применением ППП МАТЛАБ – нейронные сети. СПб. : Изд-во СПбГУЭФ, 2011. 90 с.

29. Литюга Ю. В., Ревуцька Н. В. Ризики інноваційної діяльності та сучасні аутсорсингові моделі її здійснення / Ю. В. Литюга, Н. В. Ревуцька

// Стратегія економічного розвитку України : зб. наук. праць / голов. ред. А. П. Наливайко. К. : КНЕУ, 2012. № 30. С. 61-67.

30. Оптимізація бізнес-процесів: навч. посіб. / Г.О. Швиданенко, Л.М. Приходько. К.: КНЕУ, 2012. 487 с.

31. Підручник з Umbrello UML Modeller. Автори Umbrello UML Modeller. Переклад українською: Юрій Чорноіван, версія 2.11.0 (1 червня 2013 року). URL: https://docs.kde.org/stable5/uk/umbrello/umbrello/index.html (дата звернення 28.12.2023)

ДОДАТОК А. ВІДОМІСТЬ РОБОТИ

п/п	Назва документу	Найменування об’єкта або виробу	Формат	Кількість сторінок
1	Пояснювальна записка	КЦТПАР.122-22-1М.01.00.КР.ПЗ	А4	
Графічна частина				
2	Оцінювання ідентифікованих ризикових подій на процес взаємодії з контрагентом	КЦТПАР.122-22-1М.02.00.КР.ПЛ	А4	1
3	Загальна структура автоматизованої системи аналізу управління ризиками бізнес-процесів	КЦТПАР.122-22-1М.03.00.КР.ПЛ	А4	1
4	Діаграма послідовності у форматі прецедентів Mermaid	КЦТПАР.122-22-1М.04.00.КР.ПЛ	А4	1
5	Контекстна діаграма в нотації IDEF0	КЦТПАР.122-22-1М.05.00.КР.ПЛ	А4	1
6	UML діаграма діяльності	КЦТПАР.122-22-1М.06.00.КР.ПЛ	А4	1
7	Модель системи в нотації BPMN	КЦТПАР.122-22-1М.07.00.КР.ПЛ	А4	1
8	Модель системи у вигляді діаграми Mind Mapping	КЦТПАР.122-22-1М.08.00.КР.ПЛ	А4	1
9	Модель системи у Use Case діаграми	КЦТПАР.122-22-1М.09.00.КР.ПЛ	А4	1
10	Приклад коду JavaScript з бібліотекою Puppeteer	КЦТПАР.122-22-1М.10.00.КР.ПЛ	А4	1
11	Приклад коду JavaScript для отримання інформації з веб-сайту та бази даних MySQL	КЦТПАР.122-22-1М.11.00.КР.ПЛ	А4	1

ДОДАТОК Б

Технічне завдання до проєкту «Автоматизація системи аналізу управління ризиками бізнес-процесів»

1. Загальний опис (Overall Description)

1.1 Перспектива продукту (Product Perspective)

Система в автоматичному режимі дозволить формувати звіт по підприємству, який укладатиметься з критеріїв ризиковості співробітництва та формуватиметься на основі баз даних, що постійно наповнюються, з урахуванням поточної ситуації. Одним із джерел інформації для звіту буде виступати розроблена підприємством інформаційно-аналітична система, яка містить аналітичні матеріали, отримані у процесі оцінювання ризиків благонадійності контрагентів, комплаєнсу, безпеки угод, а також результати конкурентного аналізу, корпоративних розслідувань та аудиторських перевірок.

1.2 Класи та характеристики користувачів (User Classes and Characteristics)

Короткий опис користувачів системи наведено в таблиці:

Користувач	**Короткий опис**
Адміністратор системи	здійснює налаштування нейронної мережі здійснює автентифікацію оператора системи
	отримає інформацію від системи про ризикові

Оператор системи	фактори співпраці з контрагентом формує запит на звітність та отримує звітність

1.3 Операційне середовище (Operating Environment)

Клієнт-серверна архітектура на основі веб-технологій Операційна система: Windows Server, 2019.

База даних – веб-застосунок на базі фреймворка Vaadin з використанням JavaScript-бібліотеки.

Бекенд (Node.js): для розробки бекенду буде використовуватися JavaScript, зокрема Node.js 21.6.0. Також знадобитися використовувати JavaScript разом із засобами веб-скрапінгу, такими як бібліотека Puppeteer (це бібліотека для Node.js, яка дозволяє автоматизувати браузер Google Chrome)

Фреймворк для бекенду: передбачити використання фреймворка Express для розробки бекенду.

База даних: планується використовувати MySQL з необхідністю використання ORM (Object-Relational Mapping) для спрощення взаємодії з базою даних.

Фронтенд: визначення фреймворку чи бібліотеки для використання (React, Angular, Vue.js).

RESTful API або GraphQL: - визначення способу взаємодії між фронтендом та бекендом (RESTful API або GraphQL).

середовище розробки: вказати інтегроване середовище розробки, яке планується використовувати (Visual Studio Code).

Система моніторингу та резервного копіювання на основі хмарних

технологій для забезпечення безпеки (System Center Operations Manager, SCOM)

1.4 Обмеження щодо проектування та впровадження (Design and Implementation Constraints)

Обмеження визначні використанням систем, зазначених в п. 2.4 Операційне середовище

1.5 Документація користувача (User Documentation)

Інструкція для адміністратора та оператора системи

1.6 Припущення та залежності (Assumptions and Dependencies)

Припущення:

- аналітичні висновки системи щодо доцільності подальшої співпраці з контрагентом мають рекомендаційний характер;
- система може використовувати інформацію суб'єктивного характеру зовнішнього джерела щодо наявності ризикових факторів діяльності контрагента;
- інформація, що використовується системою, має суворо конфіденційний характер і застосовується лише для службового користування.

Функціонування системи може залежати від:

- від якості та коректності інформації, що вноситься в базу даних для ідентифікації контрагента (повне найменування, мова, тощо);
- своєчасності наповнення інформації бази даних ТОВ «БСГ»;
- швидкості передачі даних.

2. Вимоги до зовнішнього інтерфейсу (External Interface Requirements)

2.1 Інтерфейси користувача (User Interfaces) -(UINT)

Інтерфейс користувача для Оператора системи:

Ідентифікатор вимог до інтерфейсів	**Опис**
UINT-1.01	користувач має можливість зайти в систему за допомогою логіну та паролю оператора системи (аутентифікація)
UINT-1.02	користувач повинен вводити умови запиту та надсилати запит на отримання звітності
UINT-1.03	користувач повинен отримувати на екрані звітність, сформовану за результатами запиту
UINT-1.04	користувач повинен вивантажувати звітність в файл Excel
UINT-1.05	користувач повинен надсилати звітність у форматі Excel через Outlook
UINT-1.06	інтерфейс користувача повинен бути представлений на українській мові

Інтерфейс користувача для Адміністратора системи:

Ідентифікатор вимог до інтерфейсів	**Опис**
UINT-2.01	користувач має можливість зайти в систему за допомогою логіну та паролю адміністратора системи (аутентифікація)
UINT-2.02	користувач повинен здійснювати реєстрацію та

	авторизацію оператора системи
UINT-2.03	користувач повинен додавати інформацію відносно контрагента для підготовки навчальної вибірки
UINT-2.04	користувач повинен маркувати ризикові критерії діяльності контрагента для підготовки навчальної вибірки
UINT-2.05	користувач повинен налаштовувати навчання нейронної мережі
UINT-2.06	користувач отримує результат навчання нейронної мережі на екран
UINT-2.07	інтерфейс користувача повинен бути представлений на українській мові

2.2 Апаратні інтерфейси (Hardware Interfaces) - (HINT))

Серверна частина:

Ідентифікатор вимог до інтерфейсів	**Опис**
HINT-1.01	хмарний сервер Microsoft Azure серії NC A100 версії 4 (Standard_NC24ads_A100_v4)
HINT-1.02	маршрутизатор Cisco C1113-8P (2 од)

Клієнтська частина:

Ідентифікатор вимог до інтерфейсів	Опис
HINT-2.01	процесор AMD Ryzen 3 4300U with Radeon Graphics, 2.70 GHz
HINT-2.02	монітор 49" Samsung Odyssey Neo G9 S49AG95
HINT-2.03	відеокарта MSI Nvidia GeForce RTX 4090 VENTUS 3X 24G OC
HINT-2.04	мережева карта HP Ethernet 1Gb 2-port 332T Adapter
HINT-2.05	оперативна пам'ять DDR4 16GB (2x8GB) 3000 MHz Sniper X G.Skill
HINT-2.06	жорсткий диск Kingston NV2 500GB M.2 2280 NVMe PCIe 4.0 x4

2.3 Інтерфейси програмного забезпечення (Software Interfaces) - (SwINT)

Ідентифікатор вимог до інтерфейсів	Опис
SwINT-01	Використання Application Programming Interface

2.4 Інтерфейси зв'язку (Communications Interfaces) -(CINT)

Ідентифікатор вимог до інтерфейсів	Опис

CINT-01	Система повинна забезпечувати можливість підключення до баз даних через стандартизовані мережеві інтерфейси, такі як T-SQL, ODBC, JDBC, ADO.NET

3. Особливості системи (System Features)

Вимоги можуть будуть розміщені згідно пріоритетам, що базуються на техніці MoSCoW, котра розділяє вимоги на наступні категорії:

Рейтинг пріоритетів	**Опис**
П - Повинен мати	Описує вимоги, що повинні бути задоволені у фінальному представлені рішення для досягнення успіху
В - Варто було б мати	Представляє високо-пріоритетні деталі (пункти), що повинні бути добавлені у рішення, якщо це можливо. Дуже часто це вирішальні вимоги, проте кожен з них може бути задоволений інших шляхом, якщо суворо необхідно
М - Можливо мати	Описує вимоги котрі вважаються бажаними, але не обов'язковими. Вони будуть включені, якщо дозволять час і ресурси
Х - Хотілося б мати	Представляє вимоги, які були погоджені зацікавленими сторонами , що не будуть додаватися до анонсування, проте можуть бути розглянуті у подальшому

3.1 Функція системи 1 (System Feature 1)

3.1.1 Опис і пріоритет (Description and Priority)

Система виконує ідентифікацію ризикових факторів діяльності контрагента на основі обробки внесеної інформації. Має високий пріоритет

3.1.2 Послідовності стимулів/відповідей (Stimulus/Response Sequences)

Система отримує дані щодо наявності критеріїв ризику.

Система інформує оператора про виявлені ризики співпраці.

3.1.3 Функціональні вимоги (Functional Requirements)

ID функціональної вимоги	FR-01
Тип вимоги	функціональна
Пріоритет	П
Опис вимоги	Система виконує ідентифікацію ризикових факторів на основі обробки даних
Перехресне посилання на вимоги бізнесу	BR-07. Ідентифікація ризикових факторів
Бізнес правило	У випадку ідентифікації: • повідомлення про наявність ризикового фактору виводиться на екран оператора: «Виявлено ризики»; У випадку не ідентифікації: • повідомлення про не виявлення ризикового фактору виводиться на екран оператора:

	«Ризики не виявлено»
Джерело	Зовнішні та внутрішні бази даних

3.2 Системна функція 2 (System Feature 2)

3.2.1 Опис і пріоритет (Description and Priority)

Система виконує оцінку виявлених факторів ризику діяльності контрагента на бізнес-процеси співпраці з підприємствами Групи на основі. Має високий пріоритет

3.2.2 Послідовності стимулів/відповідей (Stimulus/Response Sequences)

Система оцінює вплив наявних критеріїв ризику на співпрацю з контрагентом.

Система інформує оператора про результати оцінки.

3.2.3 Функціональні вимоги (Functional Requirements)

ID функціональної вимоги	FR02
Тип вимоги	функціональна
Пріоритет	П
Опис вимоги	Система оцінює виявлені фактори ризику
Перехресне посилання на вимоги бізнесу	BR-08. Оцінка факторів ризику
Перехресне посилання на використання	За результатами оцінки система встановлює ризики співпраці. В залежності від типу ризику на екран оператора виводяться повідомлення про результати оцінки: • «Виявлені репутаційні ризики співпраці» • «Виявлені ризики невиконання договірних зобов'язань» • «Виявлені ризики постачання неякісної продукції» • «Виявлені ризики зриву строків постачання продукції» • «Виявлені ризики постачання продукції не в повному обсязі» • «Виявлені ризики фінансової неспроможності контрагента» • «Виявлені ризики порушень встановлених регламентів та політик ведення бізнесу» • «Виявлені ризики по лінії безпеки» • «Виявлені ризики іншого характеру»

Бізнес правило	Функціональна
Джерело	-

4.3. Системна функція 3 (System Feature 3)

4.3.1 Опис і пріоритет (Description and Priority)

Система формує звітність на підставі запиту оператора системи. Має середній пріоритет.

4.3.2 Послідовності стимулів/відповідей (Stimulus/Response Sequences)

Система отримує запит оператора на формування звітності.

Система формує звітність на підставі та в об’ємі зазначеним у запиті. Система виводить сформовану звітність на екран оператору.

Система може вивантажити сформовану звітність в файл Excel..

Система може відсилати сформовану звітність у форматі Excel через Outlook

4.3.3 Функціональні вимоги (Functional Requirements)

ID функціональної вимоги	FR-03
Тип вимоги	функціональна
Пріоритет	П
Опис вимоги	Система формує звітність на підставі запиту оператора
Перехресне посилання на вимоги бізнесу	BR-11. Формування звітності

Бізнес правило	На підставі запиту оператора, система виводить сформовану звітність на екран оператора. Додатково по команді оператора, система вивантажує сформовану звітність в файл CSV. Додатково по команді оператора, система відсилає сформовану звітність у форматі CSV через Outlook
Джерело	-

4.4. Системна функція 4 (System Feature 4)

4.4.1 Опис і пріоритет (Description and Priority)

Адміністратор авторизує оператора системи. Має високий пріоритет.

4.4.2 Послідовності стимулів/відповідей (Stimulus/Response Sequences)

Адміністратор проводить ідентифікацію оператора (встановлення логіну та паролю для оператора).

Система проводить аутентифікацію оператора (порівняння введеного логіна та пароля з даними, збереженим у базі даних).

Адміністратор проводить авторизацію оператора (надання доступу для виконання функціоналу оператора).

4.4.3 Функціональні вимоги (Functional Requirements)

ID функціональної вимоги	FR-04
Тип вимоги	функціональна
Пріоритет	П
Опис вимоги	Авторизація оператора системи
Перехресне	BR-12. Аутентифікація оператора системи

посилання на вимоги бізнесу	
Бізнес правило	Ідентифікація оператора: • адміністратором встановлюється логін та пароль для оператора; • логін у форматі «name@name.com» • вимоги до паролю: не менше 10 знаків (символи, літери, цифри) • занесення логіну та паролю в базу даних системи Аутентифікація оператора: • порівняння введеного логіна та пароля з даними, збереженим у системі. Авторизація оператора: • надання доступу для виконання функціоналу оператора.

4.5. Системна функція 5 (System Feature 5)

4.5.1. Опис і пріоритет (Description and Priority)

Здійснення маркування ризикових критеріїв діяльності контрагента для навчання нейронної мережі. Має високий пріоритет.

4.5.2. Послідовності стимулів/відповідей (Stimulus/Response Sequences)

Адміністратор здійснює маркування ризикових критеріїв діяльності контрагента.

Запускається процес навчання нейронної мережі.

Результат навчання нейронної мережі виводиться на екран. При необхідності адміністратор здійснює зміну налаштування та запускає процес навчання нейронної мережі повторно.

4.5.3. Функціональні вимоги (Functional Requirements)

ID функціональної вимоги	FR-05
Тип вимоги	функціональна
Пріоритет	П
Опис вимоги	Маркування ризикових критеріїв діяльності контрагента для навчання нейронної мережі
Перехресне посилання на вимоги бізнесу	BR-03. Маркування ризикових факторів
Бізнес правило	Підготовка навчальної вибірки: • формулювання та градація ризикових критеріїв для маркування; Навчання нейронної мережі: • адміністратор налаштовує параметри навчання нейронної мережі; • адміністратор запускає процес навчання; Вивід результатів навчання нейронної мережі на екран оператора. Система запитує оператора чи погоджується з результатом навчання. При необхідності адміністратор здійснює зміну налаштування та запускає процес навчання

	нейронної мережі повторно. Схема бізнес правила описана за допомогою діаграми діяльності (додаток В: Моделі аналізу (Analysis Models), рис. 4)
Джерело	-

4. Нефункціональні вимоги (Other Nonfunctional Requirements)

Функція: Надійність

ID нефункціональної вимоги	NFR-01
Тип вимоги	нефункціональна
Пріоритет	П
Опис вимоги	Надійність системи
Перехресне посилання на бізнес-вимогу	бізнес-вимога не визначена
Перехресне посилання на використання	FR-01, FR-02, FR-05
Бізнес правило	• швидкість передачі даних; • час обробки даних; • доступність (функціонування та доступність ПЗ, коли воно потрібне); • відмовостійкість (можливість роботи ПЗ як

	передбачалося, незважаючи на наявність апаратних або програмних збоїв). Залежність від відмовостійкості серверу. Забезпечення безперебійного (альтернативного) інтернет-зв'язку; • відновлюваність (можливість відновлення «постраждалих» даних та відновлення бажаного стану ПЗ у разі переривання або невдачі)
Джерело	-

Функція: Зручність використання

ID нефункціональної вимоги	NFR-02
Тип вимоги	нефункціональна
Пріоритет	B
Опис вимоги	Зручність використання системи з точки зору користувача
Перехресне посилання на бізнес-вимогу	BR13. Наявність зручного та зрозумілого інтерфейсу
Перехресне посилання на використання	FR-03, FR-04
Бізнес правило	• керованість (наявність атрибутів, які дають змогу легко керувати ПЗ та контролювати його); • захист від помилок користувача (ступінь захисту від

	помилкових рішень); • доступність (можливість використання користувачами з найширшим діапазоном характеристик та можливостей)
Джерело	-

Функція: Сумісність

ID нефункціональної вимоги	NFR-03
Тип вимоги	нефункціональна
Пріоритет	B
Опис вимоги	Сумісність роботи системи з іншими системами
Перехресне посилання на бізнес-вимогу	бізнес-вимога не визначена
Перехресне посилання на використання	FR-04, FR-05
Бізнес правило	• співіснування (ефективність виконання функцій програмним забезпеченням під час спільного використання ресурсів з іншим ПЗ); • взаємодія (можливість обміну інформацією з іншим ПЗ та використання одержаної інформації).
Джерело	-

Функція: Модифікованість

ID нефункціональної вимоги	NFR-04
Тип вимоги	нефункціональна
Пріоритет	B
Опис вимоги	Модифікованість системи
Перехресне посилання на бізнес-вимогу	бізнес-вимога не визначена
Перехресне посилання на використання	FR-01, FR-02, FR-05
Бізнес правило	• можливість ефективної зміни ПЗ без введення дефектів та без зниження якості; • можливість проводити перенавчання нейронної мережі на нових даних та можливе заміна самої нейронної мережі
Джерело	-

Функція: Валідація даних

ID нефункціональної вимоги	NFR-05
Тип вимоги	нефункціональна
Пріоритет	B
Опис вимоги	Валідація даних

Перехресне посилання на бізнес-вимогу	бізнес-вимога не визначена
Перехресне посилання на використання	FR-01, FR-02, FR-05
Бізнес правило	• підтвердження того що дані є достовірними та отримані відносно конкретного контрагента
Джерело	-

Функція: Адаптованість

ID нефункціональної вимоги	NFR-06
Тип вимоги	нефункціональна
Пріоритет	B
Опис вимоги	Адаптованість системи
Перехресне посилання на бізнес-вимогу	бізнес-вимога не визначена
Перехресне посилання на використання	FR-01, FR-02, FR-05
	• можливість ПЗ ефективно адаптуватись до різного

Бізнес правило	апаратного і програмного забезпечення або до різних оперативних середовищ. Можливість адаптувати програмний продукт до більш «свіжих» операційних систем
Джерело	-

Функція: Тестованість

ID нефункціональної вимоги	NFR-07
Тип вимоги	нефункціональна
Пріоритет	B
Опис вимоги	Тестованість системи
Перехресне посилання на бізнес-вимогу	бізнес-вимога не визначена
Перехресне посилання на використання	FR-01, FR-02, FR-05
Бізнес правило	• ефективність, з якою критерії випробувань можуть бути встановлені для ПЗ. Вимога ручного тестування
Джерело	-

Функція: Цілісність даних

ID нефункціон	NFR-08

альної вимоги	
Тип вимоги	нефункціональна
Пріоритет	П
Опис вимоги	Забезпечення цілісності даних
Перехресне посилання на бізнес-вимогу	BR-03, BR-05, BR-06, BR-12
Перехресне посилання на використання	FR-03, FR-05
Бізнес правило	• можливість запобігання несанкціонованому доступу і зміні ПЗ та даних. Дані захищені за допомогою системи доступив. Доступ к даним та налаштуванням нейронної мережі має тільки адміністратор
Джерело	-

4.1 Вимоги до продуктивності (Performance Requirements) - (PER)

Окремо не визначені

4.2 Вимоги щодо неушкодженості (техніки безпеки) (Safety Requirements)

Окремо не визначені

4.3 Вимоги безпеки(Security Requirements)- (SEC)

Ідентифікатор вимог безпеки	Опис вимоги
SEC-01	Розмежування прав доступу користувачів
SEC-02	Авторизація оператора системи
SEC-03	Період резервного копіювання даних - щотижня

4.4 Атрибути якості програмного забезпечення (Software Quality Attributes)

Доступність. Запланований час, протягом якого система доступна для використання і повністю працездатна.

Ефективність. Безпомилкова обробка кожного запиту стосовно ризиковості контрагенту.

Надійність. Вірогідність роботи ПЗ без збоїв протягом певного періоду часу.

5. Інші вимоги (Other Requirements)

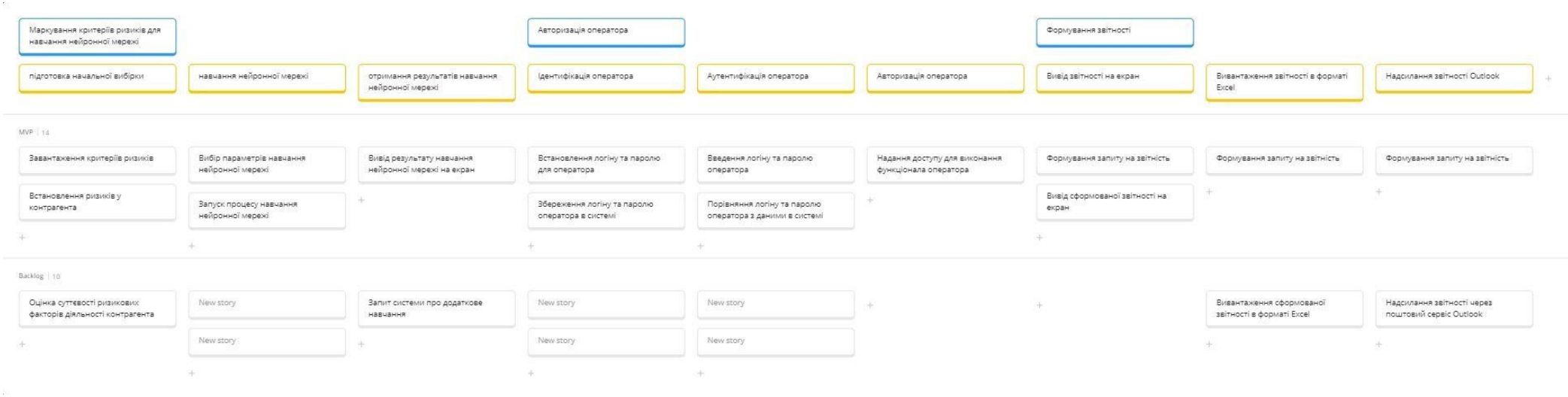
Не визначені

Додаток А: Глосарій (словник) (Glossary)

Визначення, термінологія, скорочення та абревіатури	Визначення/Опис
АС – автоматизована система	організаційно-технічна система, що забезпечує вироблення рішень на основі автоматизації інформаційних процесів
БД – база даних	сукупність даних, організованих відповідно до концепції, яка описує характеристику цих даних і взаємозв'язки між їх елементами, ця сукупність підтримує щонайменше одну з областей застосування
НВ – навчальна вибірка	деяка підмножина досліджуваної загальної (генеральної) сукупності. На основі вивчення навчальної вибірки висновки про генеральну сукупність
Підприємство	Організація-замовник, яка виконую послуги в сфері економічної безпеки підприємствам Групи Метінвест.

ДОДАТОК В

Story Mapping у системі Miro



ДОДАТОК Г

Gantt Chart Template

Project Name: Дослідження методів, моделей та інформаційних технологій при розробці автоматизованої системи аналізу управління ризиками бізнес-процесів

Task Name	Start (Date)	End (Date)	Duration (Days)
1.1.1 Чітке визначення цілей та завдань проєкту	06.11.2023	08.11.2023	2
1.1.2 Визначення ключових учасників проєкту	08.11.2023	10.11.2023	2
1.1.3 Попередня оцінка цінності проєкту для компанії	10.11.2023	12.11.2023	2
1.2.1 Підготовка статуту	12.11.2023	14.11.2023	2
1.2.2 Затвердження статуту	14.11.2023	15.11.2023	1
2.1.1 Визначення цільових критеріїв ризиковості операцій з контрагентами при співпраці з Активами Метінвест	15.11.2023	16.11.2023	1
2.1.2 Формування переліку зовнішних джерел та способів отримання інформації	16.11.2023	17.11.2023	1
2.1.3 Позначення напрямків отримання даних із внутрішніх джерел	17.11.2023	18.11.2023	1
2.2 Визначення форми та віду інформації у звітності, сформованої за підсумками аналізу ризиків співпраці з контрагентами	18.11.2023	21.11.2023	3
2.3 Визначення типу наданних рекомендацій бізнесу	21.11.2023	23.11.2023	2
2.4 Формування та узгодження переліку осіб, маючих доступ до програмного продукту	23.11.2023	25.11.2023	2
2.5 Опрацювання плану управління ризиками реалізації проєкту	25.11.2023	27.11.2023	2
3.1 Формування специфікації вимог до програмного продукту	27.11.2023	29.11.2023	2
3.2 Визначення операційного середовища	29.11.2023	30.11.2023	1
3.3 Розробка програмного продукта згідно сформованих вимог	30.11.2023	21.12.2023	21
3.4 Налаштування надання прав доступу для виконання функціоналу	21.12.2023	23.12.2023	2
3.5 Налаштування системи моніторингу та резервного копіювання	23.12.2023	24.12.2023	1
3.6 Налаштування формування звіту	24.12.2023	25.12.2023	1
4.1 Проведення тестувальних робіт працездатності системи	25.12.2023	08.01.2024	14
4.2 Оцінювання функціональності системи	08.01.2024	15.01.2024	7
4.3 Підготовка супровідної документації	15.01.2024	22.01.2024	7
5.1 Підготовка документації дипломної роботи	22.01.2024	31.01.2024	9
5.2 Підготовка презентації	31.01.2024	02.02.2024	2

5.3 Захист дипломної роботи	02.02.2024	03.02.2024	1

ДОДАТОК Д

Project Name	Дослідження методів, моделей та інформаційних технологій при розробці автоматизованої системи аналізу управління ризиками бізнес-процесів
Project Manager	Смирнов Максим Юрійович
Date	01.11.2023
Version	1.001

ProjectManager

WORK BREAKDOWN STRUCTURE TEMPLATE - TASKS

Task No.	Task Description	Task Owner	Dependency	Resources Needed	Task Status	Cost	Start Date	Estimated Completion	Finish Date	Notes
1	**Initiation Phase**									
1,1	Визначення необхідності, актуальності мети та цінності проєкту	Смирнов М.Ю.					06.11.2023	6	12.11.2023	
1.1.1	Чітке визначення цілей та завдань проєкту	Смирнов М.Ю.					06.11.2023	2	08.11.2023	
1.1.2	Визначення ключових учасників проєкту	Смирнов М.Ю.					08.11.2023	2	10.11.2023	
1.1.3	Попередня оцінка цінності проєкту для компанії	Смирнов М.Ю.					10.11.2023	2	12.11.2023	
1.2	Підготовка та затвердження статуту проєкту	Смирнов М.Ю.					12.11.2023	3	15.11.2023	
1.2,1	Підготовка статуту	Смирнов М.Ю.					12.11.2023	2	14.11.2023	
1.2,2	Затвердження статуту	Смирнов М.Ю.					14.11.2023	1	15.11.2023	
2	**Planning Phase**									
2,1	Структуризація етапів робіт по проєкту	Смирнов М.Ю.					15.11.2023	3	18.11.2023	
2.1.1	Визначення цільових критеріїв ризиковості операцій з контрагентами при співпраці з Активами Метінвест	Смирнов М.Ю.					15.11.2023	1	16.11.2023	
2.1.2	Формування переліку зовнішніх джерел та способів отримання інформації	Смирнов М.Ю.					16.11.2023	1	17.11.2023	
2.1.3	Позначення напрямків отримання даних із внутрішніх джерел	Смирнов М.Ю.					17.11.2023	1	18.11.2023	

2,2	Визначення форми та віду інформації у звітності, сформованої за підсумками аналізу ризиків співпраці з контрагентами	Смирнов М.Ю.					18.11.2023	3	21.11.2023	
2.3	Визначення типу наданних рекомендацій бізнесу	Смирнов М.Ю.					21.11.2023	2	23.11.2023	
2.4	Формування та узгодження переліку осіб, маючих доступ до програмного продукту	Смирнов М.Ю.					23.11.2023	2	25.11.2023	
2.5	Опрацювання плану управління ризиками реалізації проєкту	Смирнов М.Ю.					25.11.2023	2	27.11.2023	
3	**Execution Phase**									
3,1	Формування специфікації вимог до програмного продукту	Смирнов М.Ю.					27.11.2023	2	29.11.2023	
3,2	Визначення операційного середовища	Смирнов М.Ю.					29.11.2023	1	30.11.2023	
3,3	Розробка програмного продукта згідно сформованих вимог	Смирнов М.Ю.					30.11.2023	21	21.12.2023	
3,4	Налаштування надання прав доступу для виконання функціоналу	Смирнов М.Ю.					21.12.2023	2	23.12.2023	
3,5	Налаштування системи моніторингу та резервного копіювання	Смирнов М.Ю.					23.12.2023	1	24.12.2023	
3,6	Налаштування формування звіту	Смирнов М.Ю.					24.12.2023	1	25.12.2023	
4	**Control Phase**									
4,1	Проведення тестувальних робіт працездатності системи	Смирнов М.Ю.					25.12.2023	14	08.01.2024	
4,2	Оцінювання функціональності системи	Смирнов М.Ю.					08.01.2024	7	15.01.2024	
4,3	Підготовка супровідної документації	Смирнов М.Ю.					15.01.2024	7	22.01.2024	
5	**Close Phase**									
5,1	Підготовка документації дипломної роботи	Смирнов М.Ю.					22.01.2024	9	31.01.2024	
5,2	Підготовка презентації	Смирнов М.Ю.					31.01.2024	2	02.02.2024	
5,3	Захист дипломної роботи	Смирнов М.Ю.					02.02.2024	1	03.02.2024	