Сумський державний університет

Міністерства освіти і науки України

Кваліфікаційна наукова
праця на правах рукопису

ГРАБІНА КАТЕРИНА ВІКТОРІВНА

УДК 004.4 : 005.8 : 005.334

ДИСЕРТАЦІЯ

МОДЕЛІ ТА МЕТОДИ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ УПРАВЛІННЯ РИЗИКАМИ В ІТ-ПРОЄКТАХ

122 – комп’ютерні науки

Подається на здобуття наукового ступеня доктора філософії

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

_____К. В. Грабіна

Науковий керівник –
Шендрик Віра Вікторівна
кандидат технічних наук,
доцент

Суми – 2024

АНОТАЦІЯ

Грабіна К. В. **Моделі та методи інформаційної технології управління ризиками в ІТ-проєктах.** – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 122 Комп'ютерні науки (12 Інформаційні технології). Сумський державний університет, Міністерство освіти і науки України, Суми, 2024.

В дисертаційній роботі вирішено актуальне науково-прикладне завдання, що полягало в розробці та вдосконаленні створення теоретичних та практичних основ підвищення ефективності функціонування ІТ-компаній шляхом побудови та застосування моделей та методів інформаційної технології управління ризиками (загрозами та можливостями) в ІТ-проєктах. Розроблені моделі та методи інформаційної технології управління ризиками в ІТ-проєктах дозволяють забезпечити ефективне управління та мінімізацію негативних впливів, а також використання можливостей, що виникають у ході реалізації ІТ-проєктів. Впровадження цих моделей та методів сприяє зниженню ризиків, покращенню показників проєкту та, як результат, може привести до підвищення конкурентоспроможності ІТ-компаній на ринку.

У першому розділі роботи було проаналізовано особливості управління ІТ-проєктами, оглянуті класифікації ризиків в ІТ-проєктах, а також сучасні моделі та методи інформаційних технологій управління ризиками (загрозами та можливостями) в ІТ-проєктах. За результатами проведеного аналізу існуючих моделей та методів управління ризиками загалом та в ІТ-сфері, було показано у роботі, що існує потреба у розробці та вдосконаленні саме підходів, моделей та методів управління ризиками в ІТ-проєктах з урахуванням впливу загроз та можливостей. Томущо існуючі інформаційні технології в управлінні ризиками проєктів частково можуть бути застосовані для управління ризиками ІТ-проєктів з урахуванням загроз та можливостей. Як результат цього автором пропонується розроблення інформаційної технології управління ризиками в ІТ-проєктах, яка б враховувала вплив загроз та можливостей.

У даній роботі розроблено концептуальну модель управління ризиками в ІТ-проєктах з урахуванням загроз та можливостей, яка ґрунтується на тому, що будь-який проєкт може бути описаний в просторі найголовніших метрик – час, гроші, обсяг та якість. Побудовані нові моделі управління ризиками в ІТ-проєктах з урахуванням загроз та можливостей, які дозволяють враховувати вплив можливих ризиків та можливостей ззовні та зсередини проєкту, що має цінність для компаній та організацій в цілому. Зокрема запропонована модель RIO-RIT-REO-RET-аналізу дозволяє на етапі ідентифікації ризиків провести аналіз проєкту з точку зору кожного з аспектів: сильних чи слабких сторін, сприятливих можливостей та загроз. Також у другому розділі роботи представлені таргетні моделі управління проєктами, що ґрунтуються на аналогії медицини та управління проєктами. На основі таргетної моделі інтегрованого управління ризиками в ІТ-проєктах, будуються графіки, за допомогою яких формуються обмеження проєкту, які є найбільш чутливими та вимагають належного управління. Запропоновані графіки таргетних моделей водночас найбільш ризиковані та сповнені можливостей, вони можуть призвести до запланованого результату проєкту та принести певні переваги проєкту. За допомогою цих графіків керівник проєкту може прийняти швидке і точне рішення, яке відповідає початковим обмеженням проєкту.

У роботі удосконалено інтелектуальну модель вибору оптимальної стратегії управління ризиками (загрозами та можливостями), що враховує графи розвитку подій, синергію можливих загроз та можливостей. Вибір оптимального рішення забезпечується оптимізацією витрат, для яких запропоновано критерії, цільову функцію. Застосовується розподіл загроз та можливостей у вигляді розробленої таргетної моделі за введеними вагами загроз та можливостей на основі експертних оцінок. Враховується як вартість реалізацій стратегій, так і загальні витрати на їх реалізацію, використовується обережний підхід до заощадливого використання ресурсів, що дозволяє балансування вигоди від реалізації можливості та витрат від загрози при обмежених наявних ресурсах.

У другому розділі роботи описана математична модель управління загрозами та можливостями в ІТ-проєктах, що ґрунтується на розрахунку синергетичного ефекту ІТ-проєкту з урахуванням таких показників як бюджет, тривалість, його сумарний ризик та можливість, та дозволяє оцінити ефективність управління ІТ-проєктом й порівняти її з ефективністю управління проєктом з урахуванням окремих груп ризиків та можливостей. Таке порівняння дозволяє обрати найбільш оптимальну та успішну модель управління ризиками з урахуванням загроз та можливостей, що дозволяє менеджеру успішно керувати проєктом, а ІТ-компанії розумно оптимізувати витрати.

Автором запропоновано удосконалення методу інтелектуального вибору оптимальної стратегії управління ризиками (загрозами та можливостями), що дозволяє за допомогою інтелектуального аналізу даних обирати оптимальну стратегію управління загрозами та можливостями з метою підвищення ефективності управління ІТ-проєктом. У третьому розділі роботи отримав подальший розвиток метод інтегрованого управління загрозами та можливостями в ІТ-проєктах, який на відміну від існуючих, враховує ідентифікацію, оцінку та реагування на ризики, як для загроз, так і для можливостей. Такий розвиток дозволяє підвищити ефективність управління ризиками з метою зниження впливу загроз та врахування впливу можливостей.

У четвертому розділі розроблена структура інформаційної бази інтегрованого управління загрозами та можливостями в ІТ-проєкті, яка дає можливість реалізувати моделі та методи управління ризиками в ІТ-проєкті з метою забезпечення накопичення статистичної та експертної інформації щодо управління загрозами та можливостями. Для інформаційної технології інтегрованого управління загрозами та можливостями в ІТ-проєктах була побудована структура відповідної інформаційної бази, що поділяється на довідникову базу інтегрованого управління загрозами та можливостями, інформаційну базу інтегрованого управління загрозами та можливостями в ІТ-проєкті, інформаційну базу оцінки загроз та можливостей в ІТ-проєкті та на інформаційну базу управління загрозами та можливостями в ІТ-проєкті.

Розроблена структура інформаційної бази інтегрованого управління загрозами та можливостями в ІТ-проєкті дає можливість реалізувати моделі та методи управління ризиками в ІТ-проєкті з метою забезпечення накопичення статистичної та експертної інформації щодо управління загрозами та можливостями. Це дає змогу керівнику ІТ-проєкту та його команді застосовувати та реалізувати розроблені автором відповідні моделі та методи з метою забезпечення успішної та своєчасної реалізації ІТ-проєкту для задоволення потреб стейкхолдерів та виконання обмежень та вимог проєкту.

Автором було виконано застосування розроблених у роботі моделей, методів та інформаційної технології інтегрованого управління загрозами та можливостями в ІТ-проєктах на практиці у двох різних ІТ-компаніях, зокрема: компанії AMC Bridge, BROCODERS (акти впровадження додані у Додаток Б).

У четвертому розділі на прикладі реалізованого ІТ-проєкту однієї з ІТ-компаній було показано практичне застосування моделей, методів та інформаційної технології інтегрованого управління загрозами та можливостями в ІТ-проєкті. За допомогою методу інтегрованого управління загрозами та можливостями в ІТ-проєктах був проведений аналіз загроз та можливостей, з урахуванням застосування моделі RIO-RIT-REO-RET-аналізу, яка дозволила провести їхню ідентифікацію. У результаті було проведено ранжування загроз та можливостей на критичні, середні та низькі. В результаті застосування методу інтелектуального вибору оптимальної стратегії управління ризиковими подіями: загрозами та можливостями були запропоновані методи боротьби/посилення критичних та середніх загроз й можливостей, а також запропоновані заходи профілактики для усіх загроз та можливостей. Означені результати дали змогу підвищити ефективність прийняття рішень керівником ІТ-проєкту щодо стратегій реагування на загрози та врахування можливостей ІТ-проєкту.

Результати апробації показали, що розроблені моделі та методи інформаційної технології управління ризиками в ІТ-проєктах дозволили знизити рівень непередбачених витрат на 7,3% порівняно з іншими подібними проєктами

без застосування даних моделей та методів інформаційної технології управління IT-проєктами.

Ключові слова: ризик, можливість, загроза, ризикова подія, IT-проєкт, ризик менеджмент, управління ризиками, управління проєктами, інформаційна технологія, проєктний менеджмент.

ABSTRACT

Hrabina K. V. **Models and methods of information technology risk management in IT-projects. – Qualifying scientific work on manuscript rights.**

Dissertation for obtaining the scientific degree of Doctor of Philosophy in the specialty 122 Computer Sciences (12 Information Technologies). Sumy State University, Ministry of Education and Science of Ukraine, Sumy, 2024.

In the dissertation, an actual scientific and applied task was solved, which consisted in the development and improvement of the creation of theoretical and practical foundations for increasing the efficiency of the functioning of IT companies by building and applying models and methods of information technology for managing risks (threats and opportunities) in IT-projects. The developed models and methods of information technology for managing risks (threats and opportunities) in IT-projects allow for effective management and minimization of negative impacts, as well as the use of opportunities that arise during the implementation of IT-projects. The implementation of these models and methods helps to reduce risks, improve project performance and, as a result, can lead to an increase in the competitiveness of IT companies in the market.

In the first part of the work, the features of IT-project management were analyzed, risk classifications in IT-projects were reviewed, as well as modern models and methods of information technologies for managing risks (threats and opportunities) in IT-projects. According to the results of the analysis of existing models and methods of risk management in general and in the IT sphere, it was shown in the work that there is a need to develop and improve approaches, models, and methods of risk management in IT-projects, taking into account the impact of threats

and opportunities. Because existing information technologies in project risk management can be partially applied to IT-project risk management considering threats and opportunities. As a result, the author proposes the development of information technology for risk management in IT-projects, which would consider the impact of threats and opportunities.

It has been developed a conceptual model of risk management in IT-projects, taking into account threats and opportunities, which is based on the fact that any project can be described in the space of the most important metrics - time, money, volume and quality. New models of risk management in IT-projects have been built, taking into account threats and opportunities, which allow taking into account the impact of possible risks and opportunities from outside and inside the project, which has value for companies and organizations as a whole. In particular, the proposed RIO-RIT-REO-RET analysis model allows at the risk identification stage to analyze the project from the point of view of each of the aspects: strengths and weaknesses, favorable opportunities, and threats. Also, in the second section of the work, target models of project management based on the analogy of medicine and project management are presented. Based on the target model of integrated risk management in IT-projects, graphs are built, with the help of which project limitations are formed, which are the most sensitive and require proper management. The proposed target model graphs are at the same time the most risky and full of opportunities, they can lead to the planned result of the project and bring certain benefits to the project. With the help of these graphs, the project manager can make a quick and accurate decision that meets the initial constraints of the project. An intelligent model for choosing the optimal strategy for managing risks (threats and opportunities) has been improved, which considers the graphs of the development of events, the synergy of possible threats and opportunities. The mathematical model of managing threats and opportunities in IT-projects is described in the second section of the work.

An intelligent model for choosing the optimal strategy for managing risks (threats and opportunities) has been improved, which takes into account the graphs of the development of events, the synergy of possible threats and opportunities. The

choice of the optimal solution is ensured by cost optimization, for which the criteria and the objective function are proposed. The distribution of threats and opportunities is applied in the form of a developed target model based on the entered weights of threats and opportunities based on expert assessments. Both the cost of implementation of strategies and the total costs of their implementation are taken into account, a careful approach to the economical use of resources is used, which allows balancing the benefit from the implementation of the opportunity and the costs from the threat with limited available resources.

The second part of the work describes a mathematical model of managing threats and opportunities in IT-projects, which is based on the calculation of the synergistic effect of the IT-project, taking into account such indicators as the budget, duration, its total risk and opportunity, and allows evaluating the effectiveness of IT-project management and comparing it with the effectiveness of project management, taking into account individual groups of risks and opportunities. Such a comparison makes it possible to choose the most optimal and successful model of risk management, considering threats and opportunities, which allows the manager to successfully manage the project, and the IT company to intelligently optimize costs.

The author proposed the improvement of the method of intelligent selection of the optimal strategy for managing risks (threats and opportunities), which allows using intelligent data analysis to choose the optimal strategy for managing threats and opportunities in order to improve the efficiency of IT-project management. In the third section of the work, the method of integrated management of threats and opportunities in IT-projects was further developed, which, unlike the existing ones, considers the identification, assessment and response to risks, both for threats and for opportunities. Such development makes it possible to increase the effectiveness of risk management in order to reduce the impact of threats and take into account the impact of opportunities.

In the fourth chapter, the structure of the information base of the integrated management of threats and opportunities in the IT-project is developed, which makes it possible to implement models and methods of risk management in the IT-project in

order to ensure the accumulation of statistical and expert information on the management of threats and opportunities. For the information technology of the integrated management of threats and opportunities in IT-projects, the structure of the relevant information base was built, which is divided into the reference base of the integrated management of threats and opportunities, the information base of the integrated management of threats and opportunities in the IT-project, the information base of the assessment of threats and opportunities in IT-projects and on the information base of management of threats and opportunities in the IT-project. The developed structure of the information base of the integrated management of threats and opportunities in the IT-project will make it possible to implement risk management models and methods in the IT-project in order to ensure the accumulation of statistical and expert information on the management of threats and opportunities. This enables the IT-project manager and his team to apply and implement appropriate models and methods developed by the author to ensure successful and timely implementation of the IT-project to meet stakeholder needs and meet project constraints and requirements.

The author implemented the application of the models, methods, and information technology of integrated management of threats and opportunities in IT-projects developed in the work in practice in two different IT companies, in particular: AMC Bridge, BROCODERS (implementation acts are attached to Appendix B).

In the fourth chapter, the practical application of models, methods, and information technology of integrated management of threats and opportunities in the IT-project was shown on the example of the implemented IT-project of one of the IT companies. Using the method of integrated management of threats and opportunities in IT-projects, an analysis of threats and opportunities was carried out, taking into account the application of the RIO-RIT-REO-RET analysis model, which allowed their identification. As a result, threats and opportunities were ranked as critical, medium, and low. As a result of the application of the method of intelligent selection of the optimal strategy for managing risks: threats and opportunities, methods of combating/strengthening critical and medium threats and opportunities were proposed,

as well as preventive measures were proposed for all threats and opportunities. The identified results made it possible to increase the effectiveness of decision-making by the IT-project manager regarding strategies for responding to threats and considering the opportunities of the IT-project.

The test results showed that the developed models and methods of information technology for risk management in IT-projects made it possible to reduce the level of unforeseen costs by 7.3% compared to other similar projects without the use of these models and methods of IT-project management information technology for project management.

Keywords: risk, opportunity, threat, risk event, IT-project, risk management, risk management, project management, information technology.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації:

Статті у наукових фахових виданнях України

1. Грабіна К.В., Шендрик В.В. Огляд процесів управління ризиками в IT-проєктах в контексті стандартів проєктного менеджменту. *Управління розвитком складних систем*. Київ: КНУБА, 2020. Вип. 43. С. 26-32. DOI: https://www.doi.org/10.32347/2412-9933.2020.43.26-32. URL: http://mdcs.knuba.edu.ua/article/view/219812/219536. *Фахове видання України* (включена до Index Copernicus, BASE, Google Scholar, Ulrich’s Periodicals Directory).

Особистий внесок: проведено огляд та порівняння етапів процесу управління ризиками, що включає визначення і види ризиків, поняття загрози та можливостей, їх загальну класифікацію, притаманні стандартні характеристики, їх особливості й відмінності, найвідоміші методи аналізу ризиків та їх сучасні техніки й інструменти в контексті найбільш поширених і відомих стандартів ризик-менеджменту (0,86 друк. арк.).

2. Hrabina K., Shendryk V. Intelligent model of choosing the optimal risk events management strategy: threats and opportunities. *Artificial Intelligence*. Київ, 2022. № 2. P. 84-90. DOI: https://doi.org/10.15407/jai2022.02. URL: http://jai.in.ua/index.php/ua/issues?paper_num=1558. *Фахове видання України* (включена до Google Scholar, ICI Journals Master List, Ulrich's Periodicals Directory, Journal Factor, World Cat, Academia Edu, Internet Archive, Autor AID, ACM Digital Library, Open Academic Journals Index, Info Base Index, The IAEA'S NUCLEUS).

Особистий внесок: запропонована інтелектуальна модель для вибору та застосування оптимальної стратегії управління ризиковими подіями, як загрозами, так і можливостями, сучасних невеликих IT-проєктів при обмежених ресурсах та неявних чи невизначених факторах впливу (0,7 друк. арк.).

3. Грабіна К.В., Шендрик В.В. Метод управління ризиками IT-проєктів з врахуванням загроз та можливостей. *Управління розвитком складних систем*. Київ: КНУБА, 2023. Вип. 55. С. 18-28. DOI: TBD. URL: https://doi.org/10.32347/2412-9933.2023.55.18-28. *Фахове видання України* (включена до Index Copernicus, BASE, Google Scholar, Ulrich's Periodicals Directory).

Особистий внесок: запропоновано розглядати у рамках невизначеності не тільки загрози, а ще й можливості, для забезпечення успішності реалізації управління ризиками (0,8 друк. арк.).

4. Hrabina Kateryna, Shendryk Vira. Information technology of integrated management of threats and opportunities in IT-projects. *Herald of Advanced Information Technology*. Odessa: 2023. №6(4). P.363-374. DOI: https://doi.org/10.15276/hait.06.2023.24. *Фахове видання України* (включена до Index Copernicus, Research Bible, Academia, Directory of Open Access Scholarly Resources (ROAD), Google Academia, Ulrich's Periodicals Directory).

Особистий внесок: запропоновано розглядати алгоритм інформаційної технології інтегрованого управління загрозами та можливостями в IT-проекті

відповідно до розроблених моделей та методів інтегрованого управління загрозами та можливостями в IT-проекті (0,83 друк. арк.).

Статті у виданнях іноземних держав, які включені до міжнародних наукометричних баз

5. Hrabina K., Danchenko O., Shendryk V. Target models of integrated risk management for IT-projects. *The scientific heritage*. Budapest, 2021. Vol. 1, № 71 (71). p. 55-61. DOI: https://www.doi.org/10.24412/9215-0365-2021-71-1-55-61. URL: http://www.scientific-heritage.com/wp-content/uploads/2021/08/The-scientific-heritage-No-71-71-2021-Vol-1.pdf (включена до Index Copernicus; Google Scholar).

Особистий внесок: запропоновано таргетну модель інтегрованого управління ризиками в IT-проєктах та розроблено математичну модель для її розрахунку (0,7 друк. арк.).

Опубліковані праці апробаційного характеру

6. Danchenko O., Shendryk V., Hrabina K. Opportunity Management overview in terms of the Risk Management in the software development industry standards. *Управління проєктами: стан та перспективи*. Матеріали XV міжнародної науково-практичної конференції (м. Миколаїв, 10-13 вересня 2019 року). Миколаїв: НУК, 2019. С. 88-89.

Автором розглянуто управління можливостями у стандартах управління IT-проєктів.

7. Грабіна К.В., Шендрик В.В. Аналіз та порівняння методів управління ризиками проектів сервісних IT-компаній. *Математичне моделювання процесів в економіці та управлінні проектами і програмами (ММП-2020)*. Міжнародна науково-практична конференція (смт. Коблево, 14-18 вересня 2020 р.). Харків: ХНУРЕ, 2020. С. 49-53. 1

Автором проведено аналіз та порівняння методів управління ризиками проєктів сервісних IT-компаній.

8. Грабіна К.В., Шендрик В.В., Данченко О.Б. Синергетичний ефект від управління загрозами та можливостями в IT-проєктах. *Project, Program, Portfolio*

Management. Матеріали п’ятої Міжнародної науково-практичної конференції (м. Одеса, 04-05 грудня 2020 року). Одеса: ОНПУ, 2020. С. 26-30.

Автором запропоновано математичне уявлення визначення синергетичного ефекту від управління загрозами та можливостями в IT-проєктах.

9. Грабіна К.В., Шендрик В.В. Ризик менеджмент як інструмент планування успішних IT-проєктів. *Інформатика, математика, автоматика, IMA-2021*. Міжнародна науково-технічна конференція студентів та молодих учених (Суми-Нур-Султан, 19-23 квітня 2021 року). Суми, СумДУ: 2021. С. 76-77.
URL:https://drive.google.com/file/d/1c4OYoy7HoYGPrliSb851gXYv_wRwUk3o/view.

Особистий внесок: запропоновано враховувати вплив можливих загроз та можливостей в момент планування проєкту, що дозволяє забезпечити успішність реалізації IT-проєкту (0,7 друк. арк.).

10. Грабіна К.В., Шендрик В.В., Данченко О.Б., Мазуркевич А.Г. Застосування SWOT-аналізу для ідентифікації ризиків проекту. *Управління проектами у розвитку суспільства*. Тези доповідей XVIII Міжнародної науково-практичної конференції (м. Київ, 15 травня 2021 року). Київ: КНУБА, 2021. С. 133-137.

Автором запропоновано застосовувати SWOT-аналіз для ідентифікації ризиків проєкту.

11. Грабіна К.В., Шендрик В.В., Данченко О.Б. Складові управління ризиками IT-проєктів. *Інформатика. Культура. Технології, ІКТ-2021*. Матеріали VIII Міжнародної науково-практичної конференції (м. Одеса, 13-14 травня 2021 р.). Одеса: Одеська політехніка, 2021. С. 124-126.

Автором було проведено аналіз терміну «ризик» в розрізі позитивних можливостей та негативних загроз, що дало змогу виділити складові управління ризиками та їхній вплив на успіх проєкту.

12. Грабіна К.В., Шендрик В.В. Формування інтелектуальної моделі для вибору оптимальної стратегії управління ризиками. *Управління проєктами у розвитку суспільства*. Тези доповідей XX Міжнародної науково-практичної конференції (м. Київ, 12 травня 2023 року). Київ: КНУБА, 2023. С. 78-81.

Автором запропонована інтелектуальна модель для вибору оптимальної стратегії управління ризиками, яка забезпечує декомпозицію процесу на три підпроцеси та враховує графи розвитку подій, ризики та можливості.

13. Грабіна К. В., Шендрик В. В., Івашова Н. В. Алгоритм методу управління ризиками та можливостями в ІТ проєктах. *Теоретичні та практичні аспекти розвитку науки та освіти.* Тези доповідей X міжнародної науково-практичної конференції (м. Львів, 9-10 січня 2024 року). Львів: 2024, С. 77-80.

Автором запропоновано алгоритм методу управління ризиками та можливостями в ІТ-проєктах.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IT – інформаційні технології

ВВП – валовий внутрішній продукт

ІКТ – інформаційно-комунікаційні технології

PMI – Інститут управління проєктами

PMBoK – Project Management Body of Knowledge

ФВА – Функціонально-вартісний аналіз

SP – SharePoint (програмний продукт компанії Microsoft)

SDE (TL) – Software Development Engineer (Team Leader), інженер з розробки програмного забезпечення (лідер команди)

QAE – Quality Assurance Engineer, інженер з перевірки якості, тестувальник)

BA – Business Analyst, бізнес аналітик

PM – Project Manager, проєктний керівник

HR – Human Resource, людський ресурс, відділ кадрів

CAD – Computer aided design, система автоматизованого проєктування

САПР – система автоматизованого проєктування і розрахунку

GDPR – General Data Protection Regulation, загальний регламент про захист даних

STEP – Standard for the Exchange of Product Data, розширення файла, що активно використовується в комп’ютерному проектуванні і 3D

API – Application Programming Interface, опис взаємодії одної програми з іншою

BPCS – Business Planning and Control System, система планюванню та контролю

ERP – Enterprise Resource Planning, система планування ресурсів пвдприємства

ВСТУП

Прискорені темпи інформатизації суспільства і розвитку інформаційних технологій (ІТ), швидко змінювані потреби користувачів вимагають від компаній оптимізації зовнішніх та внутрішніх умов господарювання та організаційних процесів. Підвищення ефективності управління організацією або кампанією шляхом спроможності пристосовуватися до швидких змін в ІТ-галузі, які постійно виникають на глобальному рівні, задоволення потреб клієнтів та насичення ринку якісними ІТ-продуктами в стислі терміни й економічно вигідно є одним із головних аспектів забезпечення конкурентоспроможності на ринку ІТ-послуг. Швидкі темпи розвитку галузі інформаційних технологій та відповідне зроостання складності і масштабів її проєктів потребує застосування сучасних й перспективних підходів, моделей, методів та інструментів управління проєктами.

Враховуючи гостру конкуренцію на ринку ІТ-послуг та процеси глобалізації, керівництву ІТ-компаній необхідно постійно забезпечувати вдосконалення організаційних процесів їхньої діяльності. З метою забезпечення свого перспективного та ефективного розвитку, ІТ-компаніям необхідно швидко та гнучко реагувати часом на слабо передбачувані зміни, які відбуваються у зовнішньому та внутрішньому середовищах, виклики та ризики. Виходячи із цього, актуальним постає питання дослідження, розроблення та впровадження нових, інноваційних й передових підходів та інструментів до управління організаціями та їх проєктами, що дозволить ІТ-компаніям працювати швидше, ефективніше та економічно вигідно в умовах турбулентності їх внутрішнього та зовнішнього оточення, запобігати можливим загрозам та використовувати можливості розвитку.

Значний внесок в становлення та розвиток науково-методичних основ управління проєктами зробили С.Д. Бушуєв, Н.С. Бушуєва, Д.А. Бушуєв, Т.А. Воркут, В.Д. Гогунський, О.Б. Данченко, І.В. Кононенко, К.В. Кошкін,

О.В. Малєєва, В.М. Молоканова, В.В. Морозов, В.І. Польшаков, В.А. Рач, Ю.М. Тесля, С.К. Чернов, І.В. Чумаченко та ряд інших дослідників.

Питання управління ризиками проєктів, зокрема й застосування протиризикового підходу, розглядали у своїх працях такі науковці, як: С.Д. Бушуєв, Д.І. Бедрій, В.Д. Гогунський, Є.А. Дружинін, О.Б. Данченко, К.В. Колеснікова, К.В. Кошкін, М.О. Латкін, В.А. Рач, І.Б. Семко, С.К. Чернов та інші науковці.

Дослідження впровадження та удосконалення інформаційних технологій в управлінні проєктами у різних сферах діяльності проводили С.Д. Бушуєв, Н.С. Бушуєва, А.О. Білощицький, С.В. Білощицька, В.Д. Гогунський, О.Б. Данченко, Н.Ю. Єгорченкова, О.Є. Колесніков, О.Ю. Кучанський, В.В. Морозов, Л.В. Ноздріна, С.В. Палій, Н.О. Петренко, Ю.М. Тесля, С.В Цюцюра, М.І. Цюцюра, А.О. Хлевний та ряд інших дослідників.

Зважаючи на те, що ІТ-проєктам притаманні стандартні риси проєкту в класичному визначенні, такі як велика кількість взаємозалежних дій, що потребують координації та синхронізації, обмеженість у часі та ресурсах з визначеними початковими даними, а також мінливе середовище зовні та з середини проєкту, виникає необхідність управління ризиками з урахуванням загроз та можливостей для вдосконалення процесу управління ІТ-проєктами.

Вищенаведене свідчить про актуальність цього дослідження, тому актуальним науковим завданням є створення теоретичних та практичних основ підвищення ефективності функціонування ІТ компаній за допомогою підвищення ефективності управлінських рішень завдяки розробки моделей, методів та інформаційної технології управління ризиками в ІТ-проєктах.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження виконано в рамках науково-дослідних робіт «Інтелектуальна інформаційна технологія проактивного управління енергетичною інфраструктурою в умовах ризиків та невизначеності», № держреєстрації 0123U101852 та «Моделі та методи інформаційних технологій для аналізу та синтезу структурних, інформаційних і функціональних моделей

об’єктів і процесів, що автоматизуються», № держреєстрації 0120U103071, відповідно до тематичного плану науково-дослідних робіт Сумського державного університету. У цих дослідженнях автор був виконавцем частини 1, розділу 1. 3 за темою «Основні припущення та математична модель».

Мета і основні завдання наукового дослідження. Метою дисертаційної роботи є підвищення ефективності управління ІТ-проєктами шляхом розроблення та вдосконалення моделей, методів та інформаційної технології управління ризиками в них (з врахуванням як ризиків-загроз, так і ризиків-можливостей).

Для досягнення поставленої мети необхідно виконати наступні наукові завдання:

− проаналізувати предметну галузь, зокрема: особливості управління ІТ-проєктами, сучасні моделі, методи та інформаційні технології управління ризиками (загрозами та можливостями) в ІТ-проєктах;

− розробити концептуальну модель управління ризиками в ІТ-проєктах з урахуванням загроз та можливостей;

− побудувати нові моделі управління ризиками в ІТ-проєктах з урахуванням загроз та можливостей;

− розробити методи управління ризиками в ІТ-проєктах з урахуванням загроз та можливостей;

− розробити інформаційну технологію управління ризиками в ІТ-проєктах з урахуванням загроз та можливостей;

− апробувати результати досліджень у практиках управління ІТ-проєктами.

Об'єктом дослідження є процеси управління ризиками в ІТ-проєктах з урахуванням загроз та можливостей.

Предмет дослідження – моделі, методи та інформаційна технологія управління ризиками в ІТ-проєктах з урахуванням загроз та можливостей.

Методи дослідження. Методологічною основою дисертаційної роботи є загальнонаукові принципи проведення досліджень, фундаментальні положення

системного підходу, методологія управління проєктами та процесний підхід. У роботі були використанні такі методи досліджень: системний аналіз при виявленні особливостей управління ІТ-проєктами, а також їхніх ризиків; процесний підхід для підвищення ефективності процесів управління ризиками ІТ-проєктів; методи ризик-менеджменту для ідентифікації ризиків, загроз та можливостей, їх оцінки та планування реагування на них; математичне моделювання ризиків; методи інтелектуального аналізу даних для вибору оптимальної стратегії управління ризиками, загрозами та можливостями в ІТ-проєктах; метод експертного аналізу для проведення аналізу та оцінки ризиків, загроз та можливостей в ІТ-проєктах; SWOT-аналіз для виявлення загроз та можливостей в ІТ-проєкті; моделі розвитку подій на основі дерева Байеса; теорії графів, теорії матриць, теорії прийняття рішень, теорії інтелектуального управління, методи математичного програмування та оптимізації.

Наукова новизна одержаних результатів.

Вперше:

− розроблено концептуальну модель управління ризиками в ІТ-проєктах з урахуванням загроз та можливостей, яка ґрунтується на тому, що будь-який проєкт може бути описаний в просторі найголовніших метрик – час, гроші, обсяг та якість, і дозволяє заздалегідь врахувати вплив можливих ризиків з урахуванням загроз та можливостей в момент планування проєкту, завдяки чому проєктний менеджер є більш підготовленим до швидкоплинних реалій проєктної діяльності, які в свою чергу містять велику кількість незапланованих явищ, робіт, або іншими словами – змін;

− запропоновані моделі управління ризиками в ІТ-проєктах (модель RIO-RIT-REO-RET-аналізу ризиків проєкту, яка дозволяє на етапі ідентифікації ризиків провести аналіз проєкту з точки зору кожного з аспектів: сильних чи слабких сторін, сприятливих можливостей та загроз; таргетна модель інтегрованого управління ризиками в ІТ-проєктах, яка ґрунтується на аналогічних підходах в медицині та управлінні проєктами, і дозволяє створити новий альтернативний підхід до управління ризиками проєкту, як загрозами, так

і можливостями; математична модель управління загрозами та можливостями в ІТ-проєктах, яка ґрунтується на розрахунку синергетичного ефекту ІТ-проєкту з урахуванням таких показників як бюджет, тривалість, його сумарний ризик та можливість, та дозволяє оцінити ефективність управління ІТ-проєктом й порівняти її з ефективністю управління проєктом з урахуванням окремих груп ризиків та можливостей).

Удосконалено:

− інтелектуальну модель вибору оптимальної стратегії управління ризиковими подіями: загрозами та можливостями, яка забезпечує декомпозицію процесу на три підпроцеси, які враховують графи розвитку подій, синергію можливих загроз та можливостей, що на відміну від існуючих моделей управління ризиками дозволить балансувати вигоди від реалізації можливості та витрат від загрози при обмежених наявних ресурсах;

− метод інтелектуального вибору оптимальної стратегії управління ризиковими подіями: загрозами та можливостями, що дозволяє за допомогою інтелектуального аналізу даних обирати оптимальну стратегію управління загрозами та можливостями, що на відміну від існуючих методів забезпечить більше підвищення ефективності управління ІТ-проєктами за рахунок використання підходів штучного інтелекту в процесі вибору.

Отримав подальший розвиток:

− метод інтегрованого управління загрозами та можливостями в ІТ-проєктах, що дозволяє підвищити ефективність управління ризиками за рахунок зниження витрат часу та фінансових ресурсів на проект, та, на відміну від існуючих методів, враховує ідентифікацію, оцінку та реагування на ризики, як для загроз, так і для можливостей проекту.

Практичне значення одержаних результатів. Отримані наукові результати дозволили розробити гнучку інформаційну технологію управління ризиками в ІТ-проєктах з урахуванням загроз та можливостей, яка реалізує методику управління ризиками в ІТ-проєктах.

Практичне значення результатів роботи підтверджується впровадженням їх в процес управління ІТ-проєктами, зокрема: компанії AMC Bridge, BROCODERS (акти впровадження додані у Додаток Б).

Особистий внесок здобувача. Усі наукові результати, що виносяться на захист, одержані здобувачем самостійно. У публікаціях виконаних у співавторстві, особисто дисертанту належать: у [1] − проведено огляд та порівняння етапів процесу управління ризиками, що включає визначення і види ризиків, поняття загрози та можливостей, їх загальну класифікацію, притаманні стандартні характеристики, їх особливості й відмінності, найвідоміші методи аналізу ризиків та їх сучасні техніки й інструменти в контексті найбільш поширених і відомих стандартів ризик-менеджменту; у [2] − запропонована інтелектуальна модель для вибору та застосування оптимальної стратегії управління ризиковими подіями, як загрозами, так і можливостями, сучасних невеликих ІТ-проєктів при обмежених ресурсах та неявних чи невизначених факторах впливу; у [3] − запропоновано розглядати у рамках невизначеності не тільки загрози, а ще й можливості, для забезпечення успішності реалізації управління ризиками; у [4] − запропоновано розглядати алгоритм наповнення інформаційної технології інтегрованого управління загрозами та можливостями в ІТ-проекті відповідно до розроблених моделей та методів інтегрованого управління загрозами та можливостями в ІТ-проекті; у [5] − запропоновано таргетну модель інтегрованого управління ризиками в ІТ-проєктах та розроблено математичну модель для її розрахунку; у [6] − проведено огляд управління можливостями в стандартах управління ІТ-проєктами; у [7] − проведено аналіз та порівняння методів управління ризиками проєктів сервісних ІТ-компаній; у [8] − запропоновано математичне уявлення визначення синергетичного ефекту від управління загрозами та можливостями в ІТ-проєктах; у [9] − запропоновано враховувати вплив можливих загроз та можливостей в момент планування проєкту, що дозволяє забезпечити успішність реалізації ІТ-проєкту; у [10] − запропоновано застосовувати SWOT-аналіз для ідентифікації ризиків проєкту; у [11] – був зроблен аналіз терміну «ризик» в розрізі позитивних можливостей та

негативних загроз, що дало можливість виділити складові управління ризиками та їхній вплив на успіх проєкту; у [12] − запропонована інтелектуальна модель для вибору оптимальної стратегії управління ризиками, яка забезпечує декомпозицію процесу на три підпроцеси та враховує графи розвитку подій, можливі ризики та можливості; у [13] – запропоновано алгоритм методу управління ризиками та можливостями в ІТ-проєктах.

Апробація роботи. Результати досліджень дисертаційної роботи доповідалися та обговорювалися на таких національних та міжнародних конференціях: XV Міжнародна науково-практична конференція «Управління проєктами: стан та перспективи» (м. Миколаїв, 2019, 2021 рр.); Міжнародна науково-практична конференція «Математичне моделювання процесів в економіці та управлінні проектами і програмами» (смт. Коблево, 2020 р.); V Міжнародна науково-практична конференція «Project, Program, Portfolio Management» (м. Одеса, 2020, 2022 рр.); XVIII та XX Міжнародна науково-практична конференція «Управління проєктами в розвитку суспільства» (м. Київ, 2021-2023 рр.); Міжнародна науково-технічна конференція студентів та молодих учених «Інформатика, математика, автоматика» (Суми-Нур-Султан, 2021 р.); VIII Міжнародна науково-практична конференція «Інформатика. Культура. Технології» (м. Одеса, 2021 р.); X Міжнародна науково-практична конференція «Теоретичні та практичні аспекти розвитку науки та освіти» (м. Львів, 9-10 січня 2024 року).

Публікації. За темою дисертаційної роботи опубліковано 13 наукових праць, з них: статей у наукових фахових виданнях України – 4, з яких 4 включені до міжнародних наукометричних баз; у наукових періодичних виданнях інших держав – 1, з яких 1 включена до міжнародних наукометричних баз, та публікацій за матеріалами конференцій – 8.

Структура дисертації. Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та трьох додатків. Загальний обсяг дисертації – 181 стор., у тому числі 137 стор. основного тексту,

список використаних джерел за розділами загалом на 23 стор., 3 додатки на 7 стор. Дисертація містить 41 рисунка та 18 таблиць.

РОЗДІЛ 1. ОГЛЯД СУЧАСНОГО СТАНУ УПРАВЛІННЯ РИЗИКАМИ В ІТ-ПРОЄКТАХ

1.1. Особливості управління ризиками в ІТ-проєктах

Керівництво будь-якої компанії під час планування діяльності постійно зіштовхується із відповідними управлінськими проблемами – як спланувати роботи в часі, які будуть потрібні ресурси, скільки ресурсів та коли саме, скільки це буде коштувати, коли відбуватимуться розрахунки та інші. Вирішення цих проблем буде набагато якіснішим з використанням проєктного підходу [1], який сьогодні є невід'ємною частиною діяльності усіх успішних компаній та організацій. Ефективна система управління проєктами дедалі більшою мірою визначає успіх діяльності суб'єктів підприємництва та забезпечує їх фінансову стабільність, а отже, зміцнює позиції на ринку. Проте для побудови такої ефективної системи управління проєктами слід враховувати ряд особливостей, пов'язаних із станом розвитку галузі, в якій функціонує компанія, з видом та специфікою її проєктів [2]. Це стосується також, і галузі інформаційних технологій (ІТ) та ІТ-проєктів зокрема.

Світові зміни спричинені пандемією коронавірусної хвороби у 2019 році та запровадження правового режиму воєнного стану в Україні з 24 лютого 2022 року стало переламною датою для України та датою нового історичного відліку для всього світу. Війна принесла численні виклики та випробування, але в таких складних умовах ІТ-індустрія, разом з усією країною, демонструє феноменальну стійкість [3]. Індустрія залишається єдиною експортною галуззю України, яка повноцінно працює у воєнний час та тримає економічний фронт країни. ІТ-індустрії доводиться гнучко реагувати на непередбачувані виклики та загрози, шукати можливості для забезпечення сталості і стійкості ІТ-проєктів.

ІТ-компанії продовжують працювати та виконувати проєкти навіть за умови блекаутів, своєчасно сплачують податки, збільшують присутність на глобальному ринку та залучають нових клієнтів. Саме завдяки таким унікальним

вмінням та досвіду, українська ІТ-галузь має передумови стати основним драйвером відбудови України після закінчення війни. Ризик-менеджмент в умовах невизначеності при обмеженних ресурсах стає надзвичайно важливою умовою виживання ІТ-бізнесу.

ІТ є однією з провідних індустрій української економіки, яка стрімко зростала до 2022 року та показала незначне падіння у воєнний час (рис. 1.1.) [3, 4, 5]. За даними з 2015 по 2022 роки частка експорту комп'ютерних послуг у Валовому внутрішньому продукті (ВВП) зросла з 1,8% до 4, 6%, а в експорті послуг – з 13,4% до 45,5%.

Рисунок 1.1 - Динаміка надання комп'ютерних послуг з 2015 по 2023 роки

Також аналізуючи масштаби ІТ-галузі, необхідно подивитися кількість зайнятих у сфері інформаційно-комунікаційних технологій (ІКТ) згідно даним до 2022 року - 300 тис. осіб, що становить ~ 1,9% від усіх зайнятих осіб (рис. 1.2.) [3, 4, 5]. Опираючись на дослідження Digital Tiger: the Power of Ukrainian IT, підготовленого ІТ-асоціацією - кількість ІТ-фахівців, які працюють в Україні, 2023 року зросла приблизно на 2,7% - до 346,2 тис. осіб [5].

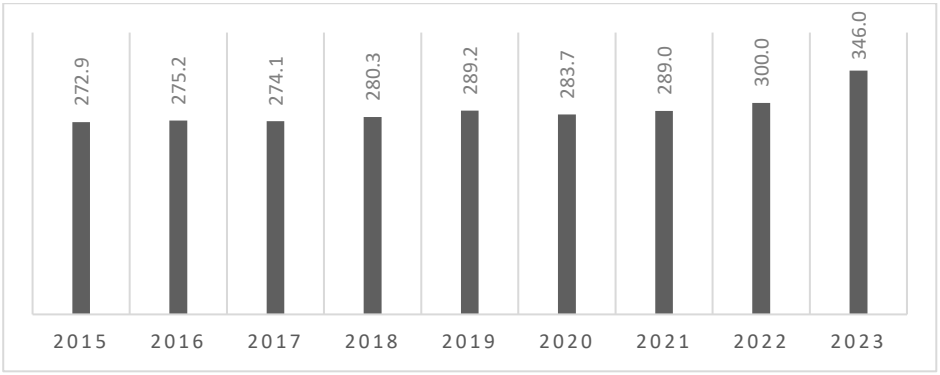


Рисунок 1.2. - Динаміка кількості зайнятих у сфері ІКТ у віці 15-70 років у період з 2015 по 2023 роки, тис. осіб

Дані щодо кількості ІТ-компаній в Україні мають велику розбіжність. Тим паче наш ринок насичений різними видами ІТ-компаній, такими як сервісні, аутсорсингові, продуктові та змішані, які в свою чергу працюють з різними видами проєктів. Можна побачити дані з Держстату [3] про 8,8 тис. діючих юридичних осіб з ІТ-КВЕДами у 2021 р. Але слід зауважити, що часто компанії складаються з декількох юридичних осіб, з цієї причини портал Tech Ecosystem дає оцінку в 2,4 тис. ІТ-компаній на початку грудня 2022 р., коли у той же час за експертними розрахунками 1,8-2 тис. з них перебувають активними на ринку праці. Слід відмітити, що ринок суттєво має зниження показників у 2022 р., після повномасштабного вторгнення (рис. 1.3.) [3, 4, 5].

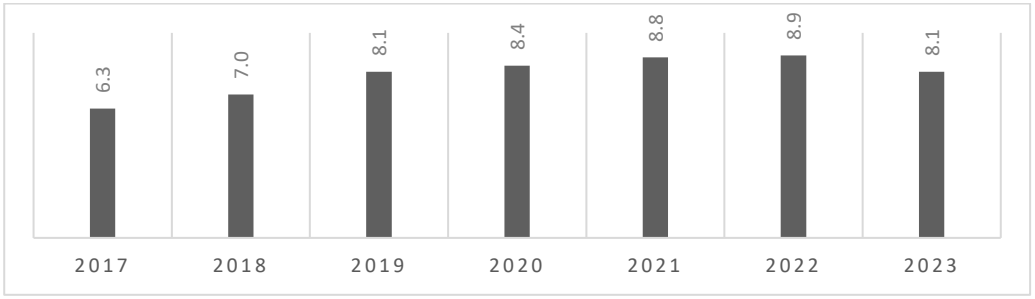


Рисунок 1.3. - Динаміка за кількістю активних юридичних осіб з ІТ-КВЕДами у період з 2017 по 2023 роки, тис. юр. осіб

Основним ресурсом ІТ-компанії є фахівці, а саме розробники, тестувальники, аналітики, дизайнери тощо. Тому активний розвиток ІТ-галузі

зумовлює зростання кількості ІТ-фахівців. Загалом протягом 2018-2023 років кількість працівників в ІТ-галузі зросла на 78,4%. Найбільший приріст відзначався серед фахівців, які працюють в ІТ за Гіг-контрактом у Дія Сіті. Їхня кількість у 2023 році склала 23,2 тис. Це в 3,9 раза більше від 2022 року. Для порівняння: у 2022 році налічувалося 5,9 тис. таких працівників (рис. 1. 4) [3, 4, 5, 7].

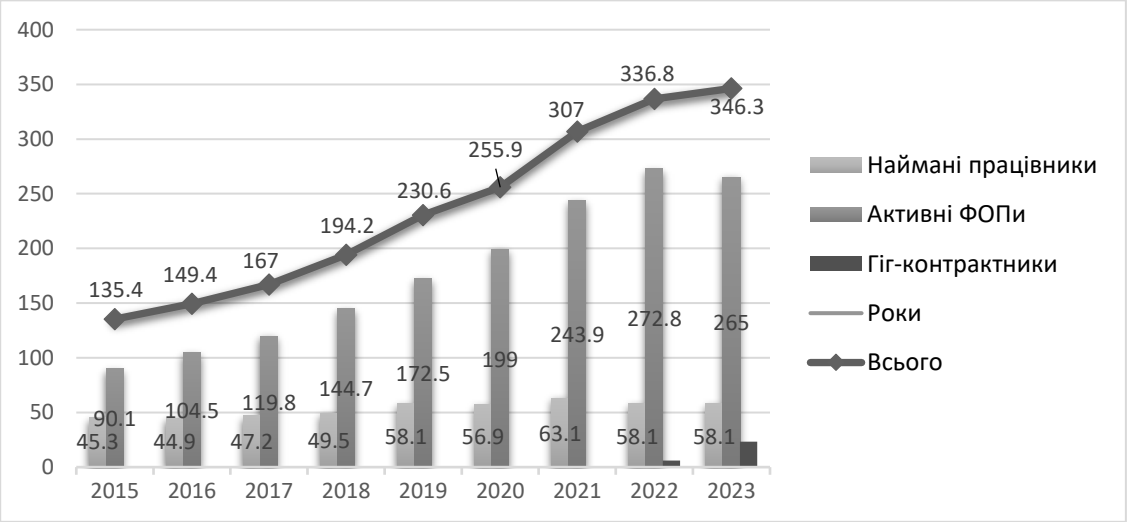


Рисунок 1.4. - Динаміка чисельності ІТ-фахівців в Україні у період з 2015 по 2023 роки, тис. осіб

Щороку традиційна ІТ-освіта готує 16-17 тис. бакалаврів. У 2022 р. кількість випускників зменшилась через повномасштабне вторгнення, адже частина студентів вимушено призупинила навчання (рис. 1.5.) [3]. Згідно дослідження експертів незалежного експертно-аналітичного центру офісу ефективного регулювання BRDO, у найближчі роки кількість випускників-бакалаврів ІТ-спеціальностей в українських вишах зросте - у 2024 році диплом бакалавра отримають більше 20 тисяч осіб у сфері ІТ, це на 23% більше, ніж у 2020 - 2022 роки [6].

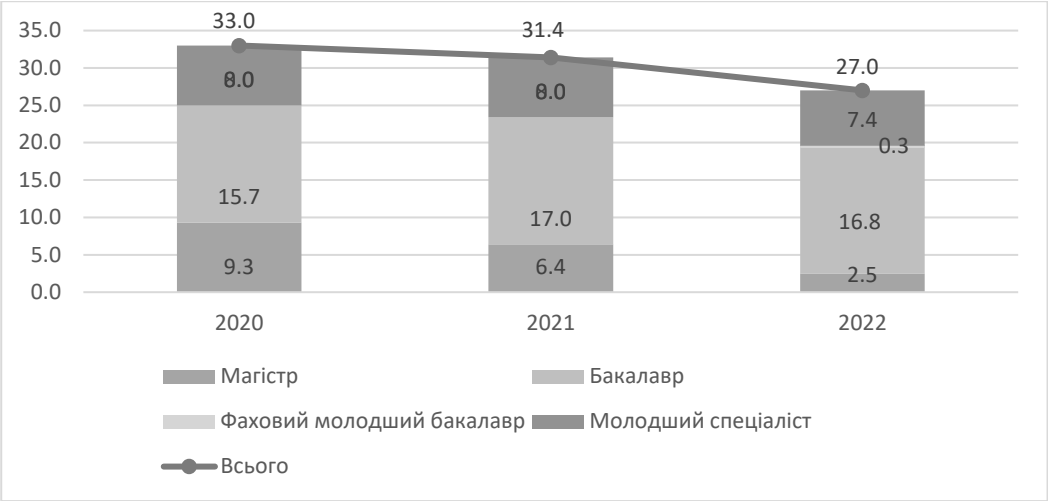


Рисунок 1.5. - Динаміка кількості випускників ІТ-спеціальностей у період з 2020 по 2022 роки, тис. осіб

В умовах сьогодення, зокрема із-за повномасштабного вторгнення ІТ-галузь зіткнулася з великою кількістю проблем. На діяльність ІТ-компаній найбільше вплинули наступні виклики:

- заборона виїзду ІТ-фахівців (чоловіків 18-60 років) за кордон;
- міграція робітників з їх сім’ями за кордон та в межах України;
- призов за мобілізацією ІТ-фахівців до лав Збройних сил України;
- валютне регулювання та обмеження при проведенні фінансових операцій;
- проблеми в роботі із клієнтами, враховуючи специфіку різноманітності культури та ведення бізнесу, різниця у часових поясах.
- виклики, пов'язані із релокацією бізнесу;
- активні бойові дії;
- окупація територій;
- зміни у податковому законодавстві, а саме впровадження Дія City.

Крім того, починаючи з 10 жовтня 2022 р. були завдані масовані ракетні удари по об’єктах енергетичної інфраструктури, які призвели до порушення електропостачання майже по всій території України. Це стало черговим викликом для галузі, тому що блекаут (це повна відсутність електроенергії) чи

навіть стабілізаційні вимкнення потребують введення нових антикризових заходів, зокрема [2, 3, 4]:

- придбання генераторів;
- використання Starlink;
- закупівля палива;
- створення системи інформування/окремого каналу для запитів;
- фінансова компенсація витрат при релокації працівників в інші регіони;
- диверсифікація інтернет-провайдерів;
- закупівля павербанків;
- переведення даних «у хмару» та забезпечення віддаленої роботи;
- облаштування офісів з можливістю проживання команди;
- оплата коворкінгу.

Враховуючи вищенаведене, можна дійти висновку, що діяльність ІТ-сфери та прийняття рішень в цій сфері здійснюється в колосальних умовах невизначеності та турбулентності, які мають властивість бути наповненими ризизками, тому питання управління ризиками є актуальним та потребує подальшого дослідження.

Також за даними KPMG (міжнародної аудит-консалтингової корпорації) за 2023 рік – 70% організацій зіткнулися щонайменше з одним провалом проекту за останні 12 місяців. KPMG провела опитування менеджерів проектів, результати якого показали, що серед головних провалів проєкту було саме неефективне управління ризиками [4, 5].

Управління ризиками є однією із компонент методології управління проєктами, яка відіграє позитивну роль під час прийняття рішень у сфері інноваційних розробок, або ж ІТ-проєктів [1, 2]. Варто дати визначення цьому терміну з огляду так званої проєктної тріади – обмежень, що накладаються на проєкт – час, бюджет, якість [1].

Визначення 1.1. ІТ-проєкт – це комплекс робіт, спрямований на розробку унікального продукту чи надання сервісу, що має чітко визначений термін

виконання, обмеження по ресурсах, свої критерії якості і поняття про успішне завершення [8].

ІТ-проєкти є комплексними, відрізняються від інших видів проєктів такими характеристиками як: складність, масштабність та різноманітність.

ІТ-проєктам властивий ряд особливостей, що впливають на формування ефективної системи управління, зокрема:

− нестандартний життєвий цикл, який може включати в себе також тестовий, гарантійний, післягарантійний етапи розробки та кастоматизацію розробки на боці замовника;

− необхідність чіткого визначення, вже на етапі ініціації, виявлення функціональних та нефункціональних вимог до ІТ-проєктів незважаючи на швидку зміну деяких напрямків в ІТ-сфері;

− необхідність оперативного внесення змін на етапі тестування, що створює складнощі, з якими стикаються практично всі керівники ІТ-проєктів, внаслідок чого відбувається відставання від запланованих термінів або необхідність зміни методології на більш гнучку;

− робочі пакети через специфіку технологій та архітектури розглядаються ієрархічно, а послідовність або паралельність їх виконання залежить від застосованих технологій та гнучкості методології розробки;

− робота з багаторівневими цілями: цілі різних рівнів разом з аналізом інтересів учасників і оцінкою їх впливу на проєкт часто включаються в концепцію реалізації проєкту;

− ІТ-проєкти не можуть розглядатися поза бізнес-проєктом клієнта і менеджмент з самого початку орієнтований на вибудовування складної комунікації;

− матрична організаційна структура управління проєктами (рис. 1.6), важливу роль в якій відіграє координатор проєктів або проєктний менеджер (керівник проектів) для кожної команди або співробітника М, Н, З та П.

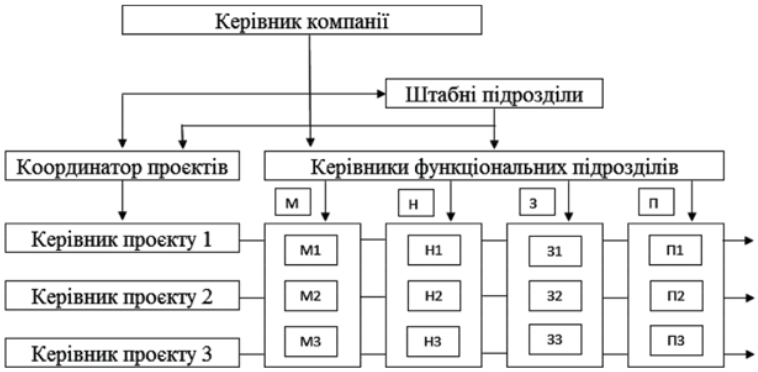


Рисунок 1.6. - Матрична структура управління проєктами

Варто зазначити, що терміни проєкту з розробки нового продукту повинні бути обмежені часом повернення інвестицій – концепція Time-To-Profit. Ця ідея досить серйозно конфліктує з усталеною думкою, що такий проєкт повинен закінчуватися при виведенні нового продукту на ринок. У разі виведення IT-продукту на ринок, ще немає ніяких серйозних підстав судити про успішність проєкту. Оскільки невирішеними залишаються питання: як він буде продаватися; наскільки будуть задоволені замовники або користувачі; чи потрібно вносити зміни.

Що стосується продуктових кампаній то критерієм успішності IT-проєкту зі створення нового продукту не може бути одне лише успішне впровадження – необхідно забезпечити комплексну експлуатацію розробленої IT-системи на підприємстві, тобто реалізувати розвиток і супровід IT-системи на повному життєвому циклі протягом п'яти – десяти років. І це перегукується зі згаданою концепцією Time-To-Profit, яка стверджує: «Недостатньо випустити – потрібно ще продати», стосовно IT-сфери: «Недостатньо впровадити – потрібно ще забезпечити тривалий розвиток, щоб залишитися конкурентноспроможним на ринку» [2, 8, 9].

Водночас кожен перехід IT-проєкту на нову стадію ознаменується істотним переглядом концепції (у зв'язку зі зміною цілей і пріоритетів), застосовуваних моделей якості (у зв'язку зі зміною пріоритетів) і способів комунікації з клієнтом, а значить, без вмілого застосування гнучких методологій і практик роботи з

динамічно змінюваними вимогами тут теж ніяк не обійтися, що є потенційно наповненою зоною ризиків проєкту [2, 9, 10].

В умовах сьогодення управління проєктами в індустрії розробки програмного забезпечення вимагає більш складних інструментів та методів у кожній області для успішного досягнення цілей проєкту на конкурентному ринку. Правильно реалізовані сфери управління проєктами допомагають на всіх етапах від представлення компанії на ринку, продажу продуктів і послуг, покращення кінцевих результатів проєктів до збільшення прибутку компанії. Галузеві стандарти розробки програмного забезпечення накопичують і осягають знання для всіх областей управління проєктами, зокрема й управління ризиками. Враховуючи все вищепредставлене, зростає тенденція до того, що компанії-розробники програмного забезпечення намагаються дотримуються найкращих галузевих стандартів [1, 11, 12, 13].

Визначення 1.2. Ризики – це невизначена подія або умова, що у разі настання матиме позитивний або негативний вплив на одну чи більше цілей проєкту [1, 21].

Визначення 1.3. Загроза – подія або умова, яка у випадку настання негативно впливає на одну або кілька цілей проєкту [1, 21].

Визначення 1.4. Можливість – подія або умова, яка у випадку настання позитивно впливає на одну або кілька цілей проєкту [1, 21].

Як було наведено вище, то ризики можуть мати як негативні, так і позитивні наслідки, тому окрім управління загрозами необхідно охоплювати ще й елементи управління можливостями в галузевих стандартах розробки програмного забезпечення.

Термін можливості широко використовується в стандартах для управління проєктами індустрії розробки програмного забезпечення [1,21]. Його можна визначити з точки зору управління ризиками як різновид ризиків або як окремий підрозділ управління можливостями.

Слід зазначити, що чітко визначене управління можливостями не представлено окремо або повністю в наступних галузевих стандартах:

- настанова до Зводу знань з управління проєктами (PMBOK® Guide) [1];
- стандарт управління ризиками в портфелях, програмах і проєктах [14];
- CMMI (інтеграція моделі зрілості можливостей) [15];
- CMMI для розвитку (CMMI-DEV) [16];
- база індивідуальних компетенцій для управління проєктами, програмами та портфоліо (IPMA ICB) [17];
- посібник з управління проєктами та програмами для корпоративних інновацій (P2M) [18].

Інститут управління проєктами (PMI) має один із відомих фундаментальних стандартів, присвячених управлінню ризиками – Стандарт управління ризиками в портфелях, програмах і проєктах [14]. Відповідно до цього стандарту управління можливостями допомагає розпізнавати та розуміти можливі способи більш успішного досягнення цілей проєкту. Таким чином, можливості протилежні загрозам, які мають традиційний погляд на ризик як на руйнівника цінності, модифікований на бачення ризику як потенційного підсилювача цінності [14]. Відповідно до PMI, стратегії та підходи до роботи з можливостями подібні до негативних ризиків.

CMMI (інтеграція моделі зрілості можливостей) – це інтегрований набір найкращих практик, який покращує продуктивність та ключові можливості для організацій, які розробляють продукти, компоненти та послуги [15].

CMMI for Development [16] – ця модель містить область управління ризиками, яка визначається як розширена область управління проєктами. Її мета полягає в тому, щоб визначити потенційні проблеми до того, як вони виникнуть, щоб заходи щодо управління ризиками могли бути сплановані та задіяні в міру необхідності протягом життєвого циклу продукту або проєкту для пом’якшення негативного впливу на досягнення цілей. Будь-які компоненти області управління ризиками в CMMI для розвитку не охоплюють управління можливостями та присвячені лише підготовці організації діяльності лише до негативних ризиків.

Стандарт IPMA ICB [17] окреслює управління ризиками та можливостями в одній лінії, підкреслюючи, що управління обома є важливим для успіху проєкту. Управління ризиком перекладається на людину, особу, що приймає рішення. Відповідно до цього стандарту людина повинна мати перспективні компетенції, які стосуються контекстів проєктів і людей, компетенції людей, які стосуються особистих та соціальних тем, й практичні компетенції, які стосуються конкретних практичних компетенцій для управління проєктами. «Ризик і можливість» є одним із елементів серед 14 елементів «Практичних компетенцій» у IPMA ICB, мета яких полягає в тому, щоб дати людині змогу зрозуміти та ефективно керувати ризиками та можливостями, включаючи реагування та загальні стратегії. Базовий показник IPMA Project Excellence Baseline (IPMA PEB) і IPMA Organizational Competence Baseline (IPMA OCB) також згадують блок можливостей у відповідності з ризиком.

Японський стандарт Керівництво з управління проектами та програмами для корпоративних інновацій (P2M) [18] описує управління ризиками з точки зору управління галуззю. Управління галуззю – це управління конкретними функціями або областю знань управління проєктами. Відповідно до стандарту P2M, впровадження управління ризиками в проєкти призводить до контролю багатьох подій ризику та може призвести до реалізації можливості, яка забезпечує кращі результати та розвиток. Можна помітити, що управління можливостями слабо представлено з точки зору стандарту P2M, тоді як акцент зосереджений переважно на прогнозуванні негативних ризиків, їх контролі та протидії.

Отже, за результатами огляду стандартів управління проєктами з точки зору їхнього застосування в IT-сфері, можна дійти висновку, що не всі вони мають відокремлену та сформульовану область управління можливостями, проте все більше компаній мають потребу зосередитися на можливостях досягнення цілей проєкту в умовах конкурентного середовища. Управління можливостями описано в IPMA ICB відповідно до Управління ризиками як елемент практичної компетенції для окремих осіб, однак відомі стандарти PMI та японський стандарт

P2M не містять окремо галузь управління можливостями, тоді як CMMI-DEV взагалі не охоплює можливості. Огляд показує, що управління можливостями залишається цікавою темою для дослідження через його невизначену присутність у більшості стандартів управління проєктами.

Таким чином, можна дійти висновку, що питання управління ризиками в IT-проєктах є актуальним та потребує подальшого дослідження.

1.2. Огляд міжнародних стандартів управління ризиками

Сфера інформаційних технологій почала швидкий темп розвитку наприкінці XIX століття і не вщухає й сьогодні, залишаючись передовою та суміжною для інших сфер, оскільки розвиток обчислювальної техніки дав змогу використовувати, зберігати та розповсюджувати інформацію й дані так, як то потрібно замовнику. Швидкість передачі інформації й ефект від її накопичення та аналізу змушує виконувати оцифрування усіх сфер людської діяльності задля забезпечення конкурентоспроможності. Тому IT-індустрія невпинно розвивається у світі. За підсумками 2019 р. та протягом останніх років IT індустрія України є найбільш прибутковою та потужною для її економіки [19]. Отже, вдосконалення управління IT-проєктами за допомогою нових методів має позитивно вплинути на економіку України і може бути комерційно цікавим для власників IT-компаній.

Одним зі способів удосконалення результатів будь-якого проєкту є своєчасне і доречне управління його загрозами для того, щоб мінімізувати втрати бюджету і ресурсів, до яких вони можуть призводити, або, навпаки, вміло збільшити ефект від позитивних загроз (можливостей), щоб досягати проєктних цілей й вдоволеності та очікування зацікавлених сторін проєкту у рамках заданих проєктних обмежень. Управління проєктами формувалося з історією людської діяльності та набувало структурованих і стандартизованих форм майже останні сто років [20]. Нині представлена велика кількість методів і стандартів

для усіх сфер проєктного управління. Вони регламентовані і використовуються інститутами та організаціями у всьому світі.

Огляд розпочнемо з Project Management Institute (PMI) – це інститут управління проєктами, який є провідною у світі асоціацією для тих, хто вважає управління проєктами, програмами чи портфелями своєю професією [21]. Загрозам і можливостям PMI присвячує однойменний розділ Risk Management у "Біблії" проєктного управління – PMBoK [1], який являє собою довідник з усіх процесів управління проєктами. Більш того, PMI відокремив ризик-менеджмент як фундаментальний стандарт для декількох рівнів управління – The Standard for Risk Management in Portfolios, Programs, and Projects.

За викладом всесвітнього банку у докладі про світовий розвиток будь-яку людську діяльність оточують ризики [22], PMI пропонує таке визначення ризика: проєктний ризик – це невизначена подія чи умова, яка (якщо настає) позитивно чи негативно може вплинути на цілі проєкту [1, 21]. Проєкт своєю чергою є унікальною ініціативою з різними рівнями складності, яке має чітко сформовані часові рамки, виділені ресурси та поставлені цілі. Тому доречно відмітити, що будь-який проєкт схильний до виникнення ризиків, а будь-яка галузь або сфера, до якої належить проєкт, має свої специфічні особливості, а тому їх мають і ризики. Але основна теорія і методи управління проєктами є базисом для будь-якої галузі.

Ризик також може бути і тягарем, і можливістю [1, 21], а отже, ризики поділяються на загрози та можливості. Загроза – невизначена подія чи умова, яка, якщо настає, негативно може вплинути на цілі проєкту. Можливість – невизначена подія чи умова, яка, якщо настає, позитивно може вплинути на цілі проєкту (рис. 1.7.) [23, 24].

Необхідно відмітити, що, на жаль, світові стандарти з управління проєктами акцентують менше уваги на управлінні можливостями. Також про це свідчить і аналіз стандартів управління ризиками, в яких здебільшого приділяється увага загрозам [11].

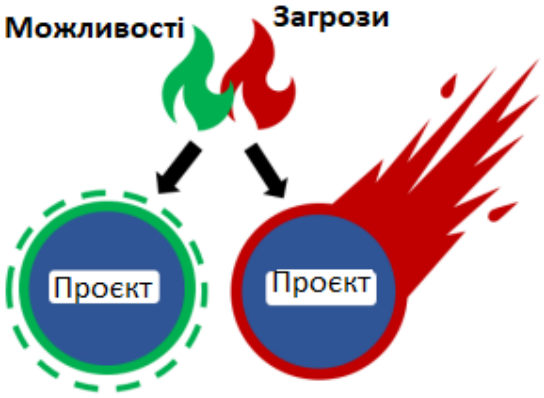


Рисунок 1.7. - Ілюстрація впливу загроз та можливостей на проєкт

Некомерційна європейська професійна організація International Project Management Association (IPMA) сприяє розвитку компетенцій спеціалістів сфери проєктного управління. Багато стандартів IPMA ICB, IPMA PEB та IPMA OCB згадує, що управлінець повинен мати компетенції щодо прогнозування і своєчасної ідентифікації загроз та можливостей [17]. А ось у японському стандарті Guidebook of Project and Program Management for Enterprise Innovation (P2M) ризик-менеджмент розглядається як окремий розділ, присвячений переважно роботі лише з ризиками, а не можливостями (рис. 1.8.) [25].

Англійський метод управління IT-проєктами Projects in Controlled Environments (PRINCE) має вже другий зареєстрований розділ PRINCE2 і може бути використаним для будь-яких проєктів. У PRINCE2 ризики розглядаються у рамках стадій проєктів, наприклад, ініціації та планування, а також як окрема компонента ризик-менеджменту [21, 26]. Capability Maturity Model Integration (CMMI) – набір стандартизованих підходів для покращення процесів від рівня проєктів до рівня організації в цілому.

Серед усіх процесних областей CMMI відокремлює Risk Management, де розглядається визначення потенційних проблем до їх виникнення. Специфіку ризик-менеджменту по CMMI можна розглянути, але модель являє собою набір обов’язкових елементів, які можуть бути виконані у будь-якій формі та використовуючи будь-які інструменти [16, 21].

Рисунок 1.8. - Огляд ризик-менеджменту згідно P2M

Тобто CMMI регламентує, що повинно бути у рамках області та практик процесів, але не дає чітких інструкцій, як це зробити (рис. 1.9.).

SG 1 Підготовка до управління ризиками
- SP 1.1 Визначення джерела та категорії ризику
- SP 1.2 Визначення параметрів ризику
- SP 1.3 Встановлення стратегії управління ризиком

SG 2 Ідентифікація та оцінка ризиків
- SP 2.1 Ідентифікація ризиків
- SP 2.2 Оцінка, класифікація та пріоритезація ризиків

SG 3 Зменшення ризиків
- SP 3.1 Розроблення плану зменшення ризиків
- SP 3.2 Реалізація плану зменшення ризиків

Рис. 1.9. - Практики та цілі ризик менеджменту згідно CMMI

Неурядова міжнародна організація International Organization for Standardization (ISO) сприяє розвитку стандартів у всьому світі. Ця організація має стандарт ISO 31000, який містить принципи, структуру та процес управління ризиками (рис. 1.10.) [21, 27].

Рисунок 1.10. - Діаграма процесу управління ризиками згідно ISO 31000

Аналізуючи перелічені стандарти, легко побачити, що більшість з них структурують та стандартизують роботу з ризиками в контексті життєвого циклу проєкту. Тому ці рекомендації можуть бути застосовані на будь-якому рівні управління: портфоліо, програма чи проєкт. Всі практики, компетенції, рекомендації або необхідні дії щодо управління ризиками в рамках проєкту повинні відбуватися своєчасно щодо життєвого циклу проєкту. PMI розділяє процес управління ризиками на такі підпроцеси (рис. 1.11.) [14, 21]. У рамках підпроцесу планування визначаються ступінь, методи та інструменти для роботи з ризиками. Все це залежить від методології та специфіки проєкту, його пріоритету на рівні портфеля, програми, або рівня компанії, його розміру, цілей та кількості і складності зацікавлених сторін.

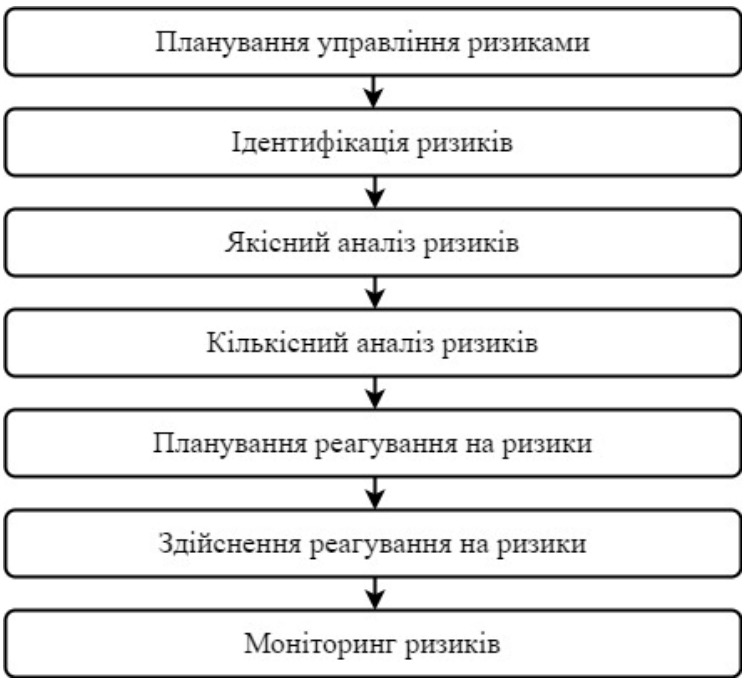


Рисунок 1.11. - Діаграма процесу управління ризиками згідно [14]

AGILE (Agile Manifesto) [28] розроблений та прийнятий 17 розробниками 11-13 лютого 2001 року на лижному курорті The Lodge at Snowbird в горах Юти, США. Маніфест був підписан представниками наступних методологій Extreme programming, Scrum, DSDM, Adaptive software development, Crystal Clear, Feature driven development, Pragmatic Programming. Цей стандарт призначений для застосування в інноваційних проєктах (наприклад, маркетингу, IT, організації подій, рекламної діяльності тощо). В підходах до управління проєктами Agile не говориться прямо про необхідність управління ризиками, але розглядаються наступні процеси: ідентифікація; аналіз та визначення пріоритетів; планування; моніторинг; коригування; аналіз результатів.

Стандарт FERMA [29, 30] є спільною розробкою Інституту ризик-менеджменту, Великобританія (The Institute of Risk Management, IRM), Асоціації ризик-менеджменту та страхування (The Association of Insurance and Management, AIRMIC) та національного форуму з управління ризиками у громадському секторі (The National Forum for Risk Management in Public Sector, ALARM). При його створенні метою була максимізація дохідності та скорочення незапланованих витрат. Впровадження цього стандарту більшою мірою

спрямоване на виробничу сферу чи реальні сектори економіки, але він може бути використан також і в системі управління ризиковими подіями будь-якого суб'єкта господарювання (рис. 1.12).

Рисунок 1.12. - Процес управління ризиками (структура FERMA)

Стандарт COSO [31, 32] «Управління ризиками організацій. Інтегрована модель» був розроблен Комітетом спонсорських організацій Комісії Тредвея, США, (Committee of Sponsoring Organizations of the Treadway Commission, COSO). Цей документ призначений для наступного, а саме: по-перше, це визначення рівня ризику, який буде відповідти обраній стратегії розвитку, по-друге, це удосконалення процесів прийняття рішень з урахуванням ризиків, що можуть виникнути; а також зменшення збитків від господарської діяльності; використовування капіталу найраціональніше.

Слід зауважити, що цей стандарт підходить у більшій мірі для корпорацій, які приймають участь у біржовох процесах. Як його недоліки слід виділити

недостатність методичних підходів до кількісних методів оцінювання ризикових подій (рис. 1.13.).

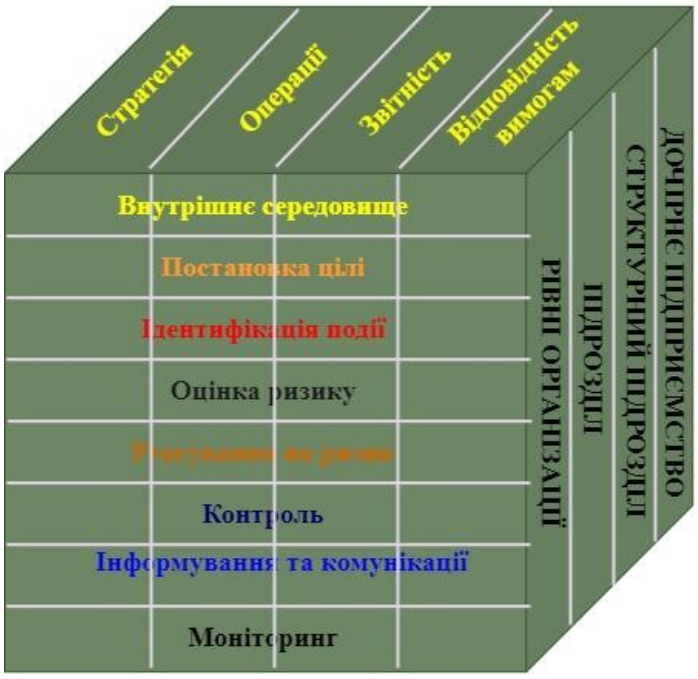


Рисунок 1.13. - Стандарт COSO (Структура ERF)

Стандарт ISO 31000:2018 [31, 33, 34] «Менеджмент ризиків. Принципи та керівні вказівки» (Risk Management – Principles and guidelines on implementation) є розробкою Міжнародної організації зі стандартизації (International Organization for Standardization, ISO) та Технічного комітету «Надійність Міжнародної електротехнічної комісії – МЕК (International Electrotechnical Commission, IEC). Цей стандарт є найбільш узагальнений, оскільки може бути застосований будь-яким суб'єктом господарювання незалежно від форми організації або виду діяльності. ISO 31000: 2018 може бути використаний протягом всього життєвого циклу організації. В документі зазначені принципи, структури та процеси, на яких базується управління ризиками. Вагомою перевагою саме цього стандарту є опис 31-го методу оцінювання ризиків з погляду сфери їх застосування, переваг та недоліків кожного з них. Варто зазначити, що саме цей стандарт є найбільш поширеним в практиці управління ризиками українських підприємств різних галузей (рис. 1.14.).

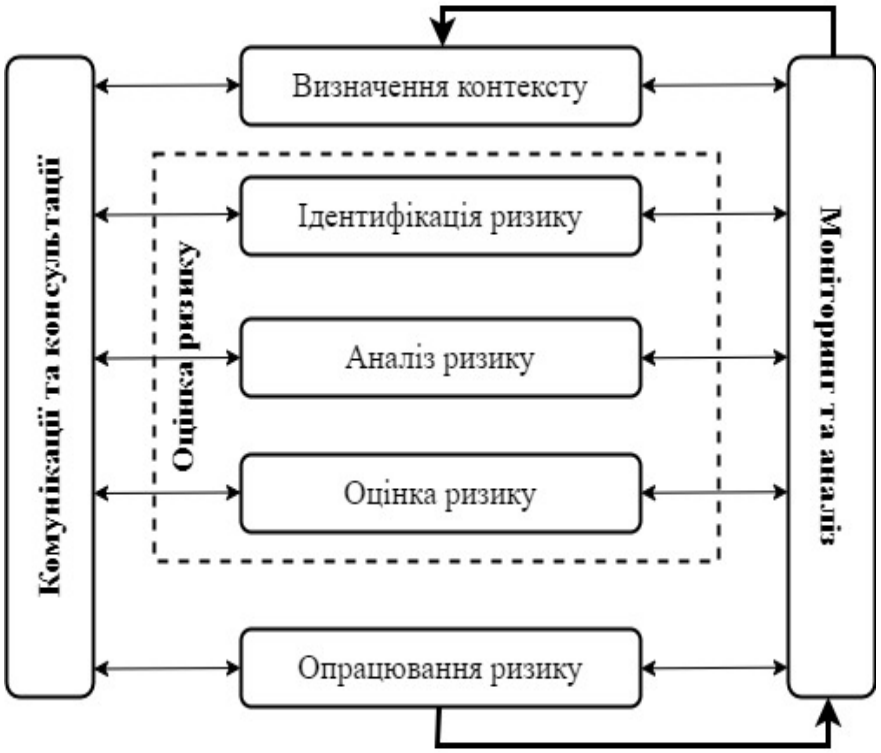


Рисунок 1.14. - Процес управління ризиками (на основі ISO 31000:2018)

Стандарт IWA 31:2020 «Управління ризиками – Настанови щодо використання ISO 31000 в системах управління» («Risk management – Guidelines on using ISO 31000 in management systems») [31, 35], що згідно [31] “містить вказівки щодо інтеграції та використання ISO 31000 в організаціях, які впровадили один або декілька стандартів системи управління ISO (ISEC) та IEC (MSS), або які вирішили здійснити проєкт із впровадження однієї або більше MSS, що включає ISO 31000”. Також цей документ не містить вказівок щодо впровадження системи управління в цілому, а дає основу для розуміння ISO 31000. Використання цього документа не позбавляє потреби використовувати інші стандарти для вирішення конкретних аспектів ризику”.

Роздивимося стандарт ISO/TR 31004:2013 «Управління ризиками – Керівництво з впровадження ISO 31000» (Risk management – Guidance for the implementation of ISO 31000) [31, 35, 36], що згідно роботі [31] “надає керівництву організації інструменти ефективного управління ризиками шляхом впровадження ISO 31000:2009; забезпечує структурований підхід до механізмів управління ризиками з метою узгодження з ISO 31000 з урахуванням

особливостей організації; пояснює основні концепції, принципи та системи управління ризиками, які описані ISO 31000. Документ може використовуватися будь-яким державним, приватним або громадським підприємством, об'єднанням, групою чи особою".

Стандарт IEC 31010:2019 «Управління ризиками – методи оцінки ризиків» (Risk management – Risk assessment techniques) [28, 32, 34], що згідно аналізу у [31] "опублікований як стандарт з подвійним логотипом разом з ISO та містить керівництво по вибору і застосуванню методів оцінки ризику в широкому діапазоні ситуацій. Ці методи використовуються для допомоги в прийнятті рішень в умовах невизначеності, для надання інформації про конкретні ризики і як частина процесу управління ризиками. Документ містить короткий виклад ряду методів з посиланнями на інші документи, в яких методи описані більш детально. Це друге видання скасовує та замінює перше видання, яке було опубліковане в 2009 році".

Ще є ряд стандартів, які орієнтовані на певну галузь впровадження.

Також цікавий факт згідно роботам [31, 38] "стандарти Базельського комітету з банківського нагляду вимірювання капіталу банків (Basel) використовують в фінансовій та банківській сферах. Стандарти групи Basel покликані встановити мінімальні вимоги до достатності банківського капіталу для створення більш стійкого фінансового сектору, посилення нагляду у банківській діяльності та закріплення дисципліни на ринку".

Стандарт «Вимоги (директива) про платоспроможність страхових компаній Європи» (ЄС та Великобританія), Solvency, розроблений у 1992-1993 рр. Available Solvency Margin, 1973, Risk-Based Capital – RBC (USA, Canada, Australia, Singapore, Japan) та спрямований на регулювання ризикових подій, що виникають у сфері страхування [31, 39].

Також слід відмітити згідно [31, 39], що "вагомий внесок в розвиток стандартизації внесли такі національні стандарти як: південно африканський «KING», Британський стандарт BS 31100:2011 Code of practice for risk management, австралійський стандарт AS/NZS 4360:2004 Risk management;

Канадський стандарт CSA Q 850:1997 Risk management Guidelines for Decision Makes, японський стандарт JIS Q 2001:2001 Guidelines for development or risk management system".

У зв'язку з існуванням різноманітного тлумачення термінів був введений в дію стандарт ДСТУ ISO Guide 73:2013 «Керування ризиком. Словник термінів» [40]. З метою надання інструментарію з методів оцінювання та управління ризиками імплементовано ДСТУ IEC/ISO 31010:2013 «Керування ризиком. Методи загального оцінювання ризику» [41].

Оскільки стандарти ISO є загальними та ґрунтуються на певних принципах, застосування способів та засобів управління ризиками зазвичай можуть істотно удосконалити будь-яку систему управління, її сприйняття, що, як правило, може значно покращити управлінські здібності керівника проєкту та основні аспекти життя.

Виходячи із наведених стандартів та підходів можна дійти висновку, що актуальним є управління ризиками, тому можна перейти до самих ризиків.

Вирізняють такі ризики – індивідуальний ризик та сукупний ризик проєкту залежно від виду аналізу ризиків, необхідного для проєкту [1, 21].

Індивідуальний ризик – це саме той ризик, що є невизначеною подією чи умовою, яка, якщо настає, позитивно чи негативно може вплинути на ціль проєкту або декілька цілей проєкту [1, 21].

Сукупний ризик проєкту – це вплив загальної невизначеності проєкту, яка є сумою усіх індивідуальних ризиків, інших джерел невизначеності, що являє собою вплив наслідку варіацій результатів проєкту на зацікавлені сторони проєкту [1, 21].

В теорії управління ризиками розрізняється якісний та кількісний аналіз. З індивідуальними ризиками виокремлюють за допомогою якісного аналізу, який дає можливість працювати із сукупним ризиком проєкту за допомогою кількісного аналізу, якщо це потрібно. Наприклад, невеликі проєкти, як правило, не потребують роботи із сукупним ризиком проєкту, тому що використання необхідних інструментів для сукупного ризика на короткому проміжку часу для

невеликих масштабів робіт не є доцільним. Якісний аналіз – це пріоритезація і надання індивідуальним ризикам характеристик з метою реагування на них вчасно. Індивідуальні ризики записують до реєстру ризиків [1, 21]. Виокремлюють такі базові характеристики індивідуального ризику проєкту:

- ймовірність виникнення ризику;
- вплив, що показує ступінь впливу ризику на проєкт;
- пріоритет – одна з характеристик оцінки ризику з урахуванням вірогідності ризику та його впливу (рис. 1.15.);
- тригер – це подія, стан, річ або предмет, який показує та сповіщає про те, що найімовірніше виникне ризик (або коли це вже факт, тому ймовірність ризику наближається до 100%);
- стратегія – це категоризована техніка управління ризиком;
- заходи – включає можливі дії щодо зменшення або усунення будь-яких негативних ризиків для проєкту при виникненні ризику або збільшення позитивних наслідків від можливості;
- власник – це особа, відповідальна за моніторинг ризиків та виконання заходів шодо ризиків, коли це доречно [1, 21].

Рисунок 1.15. - Правило формування пріоритету ризику

Слід зазначити, що визначення основних характеристик ризику – ймовірність, пріоритет та вплив є досить суб’єктивними, оскільки вони базуються на думці проєктної команди та зацікавлених сторін, що вносить деяку необ’єктивність в оцінювання ризиків, яку потрібно враховувати і робити поправку [1, 21].

Кількісний аналіз – це чисельний аналіз сукупного впливу пріоритетних ідентифікованих індивідуальних ризиків проєкту та інших джерел невизначеності на цілі проєкту загалом [1, 21].

Кількісний аналіз є доречним тільки для проєктів великих масштабів, з високим рівнем підготовки проєктної документації (з фіксованим об’ємом робіт з проєкту, з розкладом та вартістю) та з високим пріоритетом в рамках компанії. Він, як правило, потребує програмних продуктів для обчислювання великих масивів даних, а його надійність залежить від якості даних щодо індивідуальних ризиків проєкту (рис. 1.16.) [1, 21].

Серед найвідоміших методів аналізу даних: імітації, дерево рішення, діаграми впливу, аналізу чуттєвості або «торнадо». Кількісний аналіз може допомогти визначити діапазон можливих значень, наприклад, дати закінчення проєкту або фінальної вартості проєкту (будь-яка задана ціль проєкту) [49] (рис. 1.16.).

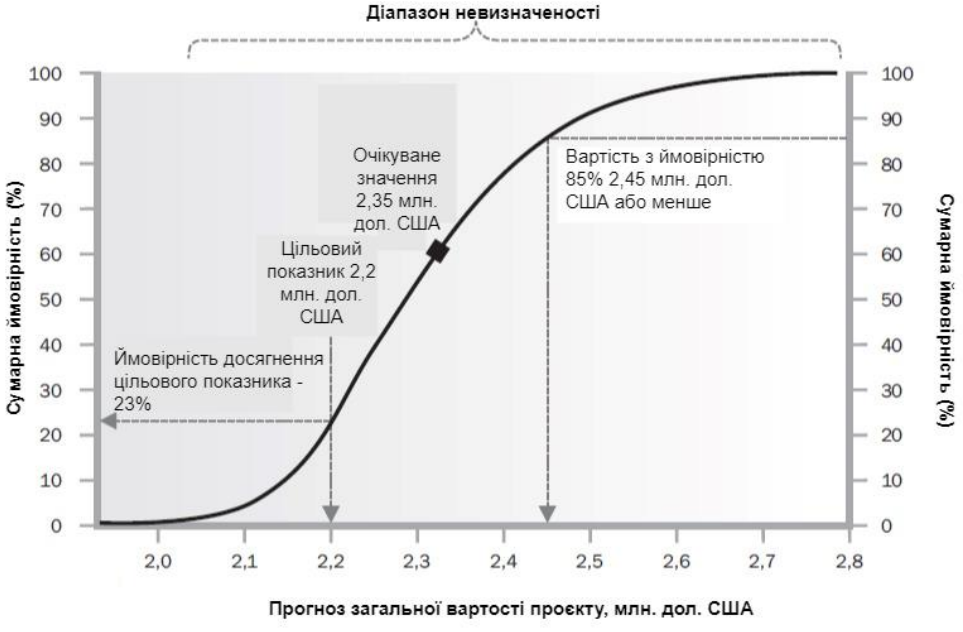


Рисунок 1.16. - Приклад S-кривої кількісного аналізу

Основні відмінності якісного та кількісного аналізу ризиків наведено у табл. 1.1.

Таблиця 1.1. Відмінності якісного та кількісного аналізу ризиків

Категорії	Якісний аналіз	Кількісний аналіз
Проєкти	Невеликі за масштабом проєкти; прості проєкти (нефіксований або фіксований обсяг робіт); низький рівень документації	Великі довгострокові проєкти з фіксованим обсягом робіт; складні проєкти; високий рівень документації; високий пріоритет
Ризики	Індивідуальні ризики; загрози; можливості	Індивідуальні ризики; будь-які джерела невизначеності; сукупний ризик; загрози; можливості
Інструменти	Реєстр ризиків	Використання результатів якісного аналізу; програмне забезпечення для чисельного аналізу
Методи	Мозкові штурми; інтерв'ю; контрольні списки; ієрархічні діаграми	Імітації (метод Монте-Карло); дерево рішення; діаграми впливу; діаграма аналізу чутливості
Залежності	Активні компанії	Використання результатів якісного аналізу; активи компанії

Зважаючи на вищенаведене, можна розглянути деякі підходи до ідентифікації ризиків в будь-якій сфері діяльності, зокрема й тих, які притаманні ІТ-галузі.

Це пов'язано із тим, що в умовах сьогодення інформаційні технології відіграють важливу, інколи вирішальну роль у всіх сферах діяльності, зокрема й у бізнесі. Тому потрібно приділяти увагу не тільки бізнес-ризикам, а також ризикам, притаманним ІТ-сфері, як їх невід'ємній частині. Беззаперечним є той факт, що застосування сучасних технологій потенційно створює передумови ризикам від втрати даних і кіберзлочинів і, як наслідок, економічного, екологічного, соціального та інших видів шкоди [42].

У роботі [43] визначено ризики ІТ-проєктів, класифіковано ключові ризики ІТ-проєктів та визначено основні джерела ризиків ІТ-проєктів. Також

представлено аналіз ризиків ІТ-проєктів при впровадженні інформаційної системи управління в реалізацію проектів компанії. З точки зору діяльності державної установи, авторами були ідентифіковані такі інформаційні ризики: невдала ІТ-структура; ризики штучного інтелекту; втрачені ІТ-активи; неефективний ІТ-аудит; недоступність послуги; дефіцит прибутку; помилки управління продуктивності; ризики конфігурації; юридичні ризики; невдачі партнерів; безповоротна втрата даних; автоматизація неточних рішень; збої інфраструктури; питання фізичної безпеки.

Авторами у роботі [44] розглянуто питання надійності та захисту інформаційних ресурсів, аналізу можливих негативних наслідків при настанні ризикових ситуацій. Автори визначили сутність та зміст поняття «інформаційний ризик» в умовах цифрової революції і нових технологій, відзначили необхідність комплексного підходу до ідентифікації, аналізу інформаційних ризиків та розробки плану управління інформаційними ризиками. Особливу увагу приділено інформаційним ризикам як окремій групі ризиків, що виникають при застосуванні інформаційних технологій.

У роботі [45] зроблено дослідження щодо управління ризиками в ІТ-проєктах по автоматизації. Визначено, що метою аналізу ризиків є оцінка всіх їх видів і визначення можливих шляхів їх зниження, доцільності реалізації проєкту за наявного ступеня ризику та способів його зменшення. Цей аналіз передбачає виявлення ризиків проєкту й їх оцінку з визначенням впливових чинників, пошук шляхів зниження ризику, врахування його за оцінки доцільності реалізації проєкт та способу його фінансування. Виявлено, що ризики ІТ-проєктів автоматизації ніколи не приймають нульового значення, адже середовище, в якому вони здійснюється, ніколи не є детермінованим та чітко визначеним. Автором зроблено висновок, що незважаючи на всі методи та заходи для зниження ризику, менеджер ІТ-проєкту повинен безперервно здійснювати моніторинг ситуації на кожному етапі, своєчасно реагуючи на "слабкі сигнали" ймовірного ризику. Якщо, пропустити початок розвитку ризикового події, то,

незважаючи на наступні правильні дії, збитки будуть значно вище, ніж у випадку попередження небезпеки, що насувається.

Автором у роботі [46] розглядаються основні підходи до ідентифікації та якісного аналізу ризиків ІТ-проєктів на прикладі проєкту впровадження автоматизованої системи. Проведення якісного аналізу ризиків в ІТ-проєктах дозволяє виявити всі ризики проєкту, визначити можливі наслідки їх реалізації та сконцентрувати увагу менеджера проєкту на ризиках, що мають найвищий показник впливу на проєкт. Всі ризики проєкту повинні підлягати контролю, проте реалізація стратегій управління ними залежить від певних додаткових витрат часу, ресурсів та бюджету проєкту. І категоризація загального реєстру ризиків по показнику впливу на проєкт шляхом проведення якісного аналізу, дозволить розставити пріоритети і відповідно призведе до економії ресурсів проєкту [68].

У роботі [47] автором запропоновано метод управління проєктом з інжинірингу ліквідації пожежі на об’єктах захисту, який ґрунтується на застосуванні математичної оптимізаційної моделі та ідентифікації ризиків виконання основних дій цього проєкту.

Як було викладено раніше, основна теорія і методи управління проєктами є базисом для будь-якої галузі, але ризики ІТ-проєктів та, наприклад, ризики проєктів матеріально-технічного забезпечення автотранспортних підрозділів Збройних Сил України [48] є концептуально різними та потребують доопрацювання в методах їх управління, які і дають поле діяльності для науковців.

Серед основних ризиків ІТ-проєктів виокремлюють такі категорії [21]:

- вади планування і документації;
- зміна вимог;
- плинність кадрів;
- порушення або неправильна трактовка специфікацій;
- низька продуктивність.

Загалом зрілі сертифіковані ІТ-компанії мають свої активи, які повинні включати стандартні інструменти для методів аналізу ризиків, архіви реєстрів ризиків та вивчених уроків. Тому управління ризиками ІТ-проєктів повинно перездійснюватися залежно від наявних активів, адаптуючи їх під тип проєкту, його цілі та пріоритет [21].

Управління ризиками є складним процесом з впливом невизначеності, оскільки ризики є випадковими подіями, що можуть або не можуть настати. Як будь-який складний процес, управління ризиками декомпозують на декілька підпроцесів, які своєю чергою мають різні методи та інструменти. Тому інструментарій для аналізу ризиків повинен обиратися й адаптуватися залежно від зрілості компанії, методології проєкту, його розміру, цілей та специфіки.

Ризик має багато класифікацій та характеристик, але для його якісного й кількісного управління необхідно знати основні – ймовірність, вплив, пріоритет та тригер. Необхідність і доречність застосування якісного і кількісного аналізу має чітку залежність від типу проєкту та його складності. Лише доцільне використання необхідних інструментів в управлінні ризиками має допомогти збільшити прибутки завдяки вмілому управлінню можливостями та уникненню або пом’якшенню загроз щодо фінансових і кадрових втрат ІТ-компаній.

1.3. Аналіз існуючих моделей та методів управління ризиками в ІТ-проєктах

Світова ІТ-галузь невпинно розвивається та росте, і основна частка світового ІТ-ринку припадає на США (36,8%), за ними – Китай (11,3%) і Велика Британія (5,8%) [49]. А тому питання ефективного управління ІТ-проєктами завжди стоїть перед власниками ІТ-бізнесу у всьому світі. Професіональне та ефективне управління проєктами призводить до задоволеності замовників завдяки успішності їхнього бізнесу та, як результат, збільшенню їхніх прибутків. Управління ризиками є однією із складових управління будь-якими проєктами, та відображено в усіх стандартах з управління проектами, їй присвячено багато

праць науковців та практиків [21, 50, 51]. Тем не менш специфіка ІТ-проєктів залишає велике поле для подальшої діяльності та інновацій в дослідженні та розробці ефективного управління ризиками для ІТ-проєктів.

Специфічність ІТ-проєктів полягає у створенні нематеріальних програмних продуктів, сервісів, або надання послуг командою високоосвічених фахівців – ІТ-спеціалістів, при умові швидкоплинних змін, що потребує гнучкості та налаштування за багатьма важливими для ІТ галузі критеріями [52]. Організація управління такими проєктами та командами потребує все більш ефективніших та практичних рішень, ніж представлені в стандартах з управління проєктами [21, 50, 51].

Управління проєктами націлене до зменшення показників тривалості та бюджету, а управління ризиками на зменшення втрат від можливих ризиків завдяки їх проактивному управлінню. Якщо подивитися на термін «ризик», а згідно PMBoK [1] ризик проєкту – це невизначена подія або умова, настання якої негативно або позитивно позначається на цілях проєкту, таких як зміст, розклад, вартість та якість, а цілями управління ризиками проєкту є підвищення ймовірності виникнення та посилення впливу сприятливих подій й зниження ймовірності виникнення та ослаблення впливу несприятливих подій в ході реалізації проєкту. Тому за ризик можна вважати як загрозу, так і можливість, де під терміном «загрози» потрібно розуміти тільки негативні ризики та їх значення приймати зі знаком мінус «–», а позитивні ризики – це «можливості», їх значення приймати зі знаком плюс «+».

PMBoK [1] розділяє процес управління ризиками на такі складові:

- планування управління ризиками,
- ідентифікацію ризиків,
- аналіз ризиків,
- планування реагування на ризики,
- реагування на ризики;
- моніторинг ризиків.

Відповідно до складових ризика (загрози та можливості) управління ризиками можна інтерпретувати як суму управління загрозами та управління можливостями, що циклічно проводиться проєктним менеджером протягом життєвого циклу проєкту [68]. Протягом всього проєкту необхідно мінімізувати ризики-загрози та збільшувати ефект від ризиків-можливостей (рис. 1.17.).

Рисунок 1.17. - Складові процесу управління ризиками проєкту

Виконання ІТ-проєкту вчасно та якісно, згідно бюджету та цілей проєкту з урахуванням повної задоволеності замовника та стейкхолдерів і вважається успіхом проєкту. Своєчасне та регулярне управління ризиками протягом всього проєкту можна інтерпретувати як управління загрозами та управління можливостями. Коли управління загрозами направлено на їх зменшення, а управління можливостями на будь-яке їх збільшення та отримання ефекту збільшення прибутків, виграшу у часі або якості. Регулярне та своєчасне виконання цих заходів і становить ефективне управління ризиками, яке частково призводить до успіху проєкту [68].

Автором у роботі [53] розроблено методологію інтегрованого управління відхиленнями в проєктах, що дала змогу керівнику управляти проєктами інтегровано й системно, та також одразу всіма причинами відхилень, наприклад, ризиками, змінами, конфліктами, проблемами, стресами, кризами). Після аналізу цієї роботи видно, що її результати дають інструменти для розроблення моделей

та методів управління ризиковими подіями, але не враховують особливостей ІТ-галузі.

У роботі [54] розроблено теоретико-методологічні основи інтегрованого протиризикового управління науковими проєктами в умовах невизначеності та переходу до циркулярної економіки. В рамках концептуальної моделі інтегрованого протиризикового управління науковими проєктами в умовах невизначеності та переходу до циркулярної економіки, яка побудована на основі моделі «Айсберга управління змінами», автором запропоновано управляти кадровими ризиками, конфліктами та факторами поведінкової економіки. Це дослідження стане у нагоді в процесі розроблення моделей та методів управління ризиками, зокрема загрозами та можливостями, в ІТ-проєктах [68].

Автором у роботі [55] розроблено метод аналізу проєктів створення нової техніки з урахуванням причинно-наслідкових зв'язків факторів ризику для підвищення достовірності оцінки часових і ресурсних витрат проєкту. Створено метод оцінки впливу зовнішніх факторів ризику на вартість ресурсів проєкту з урахуванням причинно-наслідкових зв'язків між факторами. Результати цього дослідження стануть у нагоді в процесі розроблення моделей та методів управління ризиками в ІТ-проєктах.

У роботі [56] розроблено методологічні засади, принципи, методи та моделі ризик-орієнтованого підходу, які забезпечують вирішення задач управління ризиками, ресурсами, фінансами, строками та якістю проєктів і програм розвитку техніки, стійких до ризиків. Сформовано підхід до структуризації страхових запасів проєкту, що ґрунтується на аналізі життєвого циклу та універсальності ресурсів, моделюванні основних показників проєкту за урахування процесів відновлення ресурсів, стану та витрат на їх зберігання. Інструменти ризик-орієнтованого підходу, які розроблені у цьому дослідженні стануть у нагоді в процесі розроблення моделей та методів управління ризиками в ІТ-проєктах.

Автором у роботі [57] обґрунтовано методологічні основи створення системи управління ризиками проєктів підприємства, а також системні моделі та

методи структурування, оцінювання, контролю проєктних ризиків для ефективного виконання підприємством проєктів з мінімальними витратами. Розроблено системні моделі ієрархічних структур проєктних ризиків, метод оцінювання тривалості та вартості виконання робіт проєкту з урахуванням негативного впливу ризиків. Створено методи оцінювання рівня проєктних ризиків, контролю його зміни, ефективності та вибору заходів реагування. Запропоновано системні моделі системи управління ризиками проєктів підприємства та методи її адаптації до прийнятих заходів реагування. Розроблено модель організаційної зрілості управління ризиками проєктів. Означене дослідження може стати підставою для ідентифікації та оцінки ризиків ІТ-проєктів під час розробки моделей та методів управління ризиками в ІТ-проєктах.

У роботі [58] розроблено методи вибору способів розрахунку основних показників проєктів створення нової техніки та забезпечення вірогідності результатів проєктного аналізу. Запропоновано методи ідентифікації, кількісної оцінки та управління ризиком одержання неточних результатів проєктного аналізу. Результати цього дослідження стануть у нагоді в процесі розроблення моделей та методів управління ризиками в ІТ-проєктах.

Автором у роботі [59] створено та досліджено моделі та методи протиризикового управління стейкхолдерами організаційного проєкту у сфері обслуговування літаків в умовах поведінкової економіки. Розроблено модель оточення організаційного проекту у сфері обслуговування літаків в умовах дії політичних, економічних, соціальних, технологічних, правових та екологічних факторів, а також з врахуванням факторів поведінкової економіки. Запропоновано таргетний метод протиризикового управління стейкхолдерами організаційного проекту у сфері обслуговування літаків, який полягає в управлінні кожним стейкхолдером шляхом зниження впливу їх ризиків та факторів поведінкової економіки на оточення проекту. Це дослідження буде корисне в процесі розробки моделей та методів управління ризиками в ІТ-проєктах.

У роботі [60] запропоновані моделі та методи ціннісно-орієнтованого управління портфелями наукомістких проєктів підприємств в поєднанні з мінімізацією їхніх ризиків, що сприяє підвищенню ефективності управління такими портфелями. Обґрунтовано методологічні аспекти вдосконалення моделей та методів ціннісно-орієнтованого протиризикового управління портфелями наукомістких проєктів підприємств на базі сучасної методології управління PMBoK і P2M та їхнього інструментального забезпечення. Зокрема, це використання підходів щодо оцінювання цінностей портфелів проєктів за стандартом P2M і процесів управління ризиками за стандартом PMBoK. Означене дослідження стане підґрунтям для розробки моделей та методів управління ризиками, зокрема загрозами та можливостями, в ІТ-проєктах.

У роботі [61] розглянуто питання управління ризиками, зокрема інформаційними, яке завжди було завданням номер один при розробці та впровадженні будь-якого проєкту. Проєкти ж діджиталізації особливо чуттєві до інформаційних ризиків, тому ризик-менеджмент постійно в пошуку механізмів захисту. Проаналізовано деякі методи управління ризиками, що запропоновані іншими науковцями, але разом із тим залишається ще ціла низка питань в напрямі управління інформаційними ризиками в процесі діджиталізації бізнесу. Серед методів, що дозволяють мінімізувати ймовірність настання ризикових подій є застосування методології реінжинірингу бізнес-процесів, яка була використана при розробці нового протиризикового методу. Для наочності розробниками методу надається алгоритм оптимізації бізнес-процесу з використанням модифікованого ФВА та який є складовою частиною методу управління інформаційними ризиками проєкту. Головна ідея методу полягає в тому, що на основі розробленої концептуальної моделі проєкту із своїми запланованим часом та вартістю, проводять ідентифікацію та аналіз можливих інформаційних ризиків, додатково планують визначені обсяги резервного часу та витрат на випадок загрози виникнення ризикових подій. Це дослідження стане у нагоді в процесі розробки підходів до управління ризиками ІТ-проєктів з урахуванням можливостей та загроз [68].

В роботі [62] подано концептуальну модель управління інформаційними ризиками проєкту впровадження інформаційної системи менеджменту та формалізовану на її основі математичну модель на основі визначення впливу інформаційних ризиків на державну установу, проєкт та середовище. Застосування означених моделей дозволить керівнику проєкту та його команді підвищити ефективність управління інформаційними ризиками компанії, проєкту та середовища. Це дослідження стане у нагоді під час розробки моделей та методів управління ризиками, зокрема загрозами та можливостями, в ІТ-проєктах.

Отже, як видно із проведеного аналізу існуючих моделей та методів управління ризиками в проєктах, зокрема й в ІТ-сфері, зрозуміло, що існує потреба у розробці саме підходів, моделей та методів управління ризиками в ІТ-проєктах.

1.4. Аналіз інформаційних технологій управління ризиками в ІТ-проєктах

На сьогоднішній день інформаційні технології відіграють важливу роль у підвищенні ефективності діяльності будь-якої компанії шляхом зосередження своєї уваги на тенденціях розвитку ринку, зниженні та посиленні конкуренції для отримання максимального прибутку [63]. Сучасні інформаційні системи управління спрямовані на збільшення можливостей та шляхів управління системою та покращення процесів керування компанією, що на кожному етапі управління зміцнюється впровадженням програмного забезпечення в сучасних ринкових умовах, є обставинами вдалого функціонування фірми в нинішніх умовах.

У світі та в Україні успішно впроваджується методологія управління проєктами, яка розглядає будь-яку ідею, функцію або кінцевий результат функціонування підприємства, що вже є самостійним проєктом [1]. В теперішніх умовах України після трансформації економіки розробляються нові методи та

механізми економічних відносин. Тому необхідно створити особливі підходи до управління проєктами підприємства для його подальшого отримання прибутку від своєї діяльності. Інформаційні технології допомагають вирішити питання із збільшенням складності розроблених підходів, збільшення вимог до термінів та якості виконання робіт, що обумовлюють потребу ефективного управління проєктами [63, 64].

При застосуванні сталого розвитку проєкт виглядає як якась ідея, сприйняття, перспективний стан або потребуючі предмети для його впровадження та реалізації. Основними ознаками проєкту є новизна, концептуальність, неповторність, адаптивність, кількісна вимірюваність, лімітованість часу та інші.

В розрізі сучасної динаміки управління проєктами можна зробити висновок, що роль інформаційних технологій збільшується, й саме вони здатні збільшити ефективність управління та зменшити частку незавершеності проєктів. Фактори інформаційних технологій: адаптація до змін, управління ресурсами, робочою командою, комунікацією, обмеженнями, мають значний вплив на проєкт.

При впровадженні інформаційних технологій, компанії мають змогу вдало керувати проєктами, налагоджувати зв’язок між учасниками проєкту, знаходити та оперативно реагувати на відхилення, складати звітність по всім етапам проєкту та мати змогу швидко здійснювати контроль [63, 64].

Інформаційна технологія – це поєднання процедур, що реалізують функції збору, накопичення, зберігання, обробки і передачі даних на основі використання відібраного комплексу технічних засобів за участі управлінського персоналу. Саме тому існує тісний зв’язок із програмним та технічним оточенням інформаційної технології.

Автоматизована інформаційна технологія має такі складові, як: технічні пристрої, персонал, програмне забезпечення та організаційно-методичні матеріали, що пов’язані у технологічну лінію. Дана лінія забезпечує збір, передачу, накопичення, зберігання, опрацювання, використання і поширення

інформації. Процеси трансформації вхідної інформації в результативну складають основу технології обробки даних. Головною метою інформаційної технології є досягнення необхідної інформації достатнього рівня якості на конкретному носії. І як результат, будь-яка інформаційна технологія завершується виробництвом інформаційного продукту [63, 64].

У роботі [65] розроблена інформаційна технологія, яка дозволяє реалізувати будівництво складних енергетичних об’єктів за найменш ризикованою топологією сітьового графіку проєкту, розклад виконання робіт якого буде мінімальним за критерієм ризику збільшення часу виконання і обсягу проєкту. Результати цього дослідження стануть у нагоді в процесі розроблення інформаційної технології управління ризиками в ІТ-проєктах.

Автором у роботі [53] розроблена структура інформаційної бази та інформаційна технологія інтегрованого управління відхиленнями в проєкті, яка дозволяє одночасно управляти ризиками, змінами, проблемами, конфліктами, стресами та кризами. Наведена інформаційна технологія інтегрованого управління відхиленнями в проєкті відрізняється від сучасних підходів до управління відхиленнями в методології управління проєктами і програмами та її реалізація призводить до зменшення негативних відхилень в проєкті. Це дослідження може бути у нагоді для розробки інформаційної технології управління ризиками в ІТ-проєктах з урахуванням загроз та можливостей.

У роботах [54, 66] розроблена інформаційна технологія інтегрованого протиризикового управління науковими проєктами в умовах невизначеності та переходу до циркулярної економіки, яка в умовах невизначеності дозволяє керівнику наукового проєкту та його команді реалізувати розроблену автором методологію інтегрованого протиризикового управління науковими проєктами в умовах невизначеності та переходу до циркулярної економіки з метою забезпечення успішної та своєчасної реалізації наукового проєкту для задоволення потреб його стейкхолдерів [68]. Результати цього дослідження стануть підґрунтям для розробки інформаційної технології управління загрозами та можливостями в ІТ-проєктах.

Автором у роботі [55] створено комп'ютерну систему для аналізу показників проєктів, що складається з підсистем оцінки впливу факторів зовнішнього середовища й імітаційного моделювання внутрішніх ризиків. Це дослідження стане у нагоді під час розробки інформаційної технології управління ризиками в ІТ-проєктах з урахуванням впливу загроз та можливостей.

У роботі [56] розроблено інформаційну технологію ризик-орієнтованого підходу, яка забезпечує вирішення задач управління ризиками, ресурсами, фінансами, строками та якістю проєктів і програм розвитку техніки, стійких до ризиків. Результати цього дослідження можуть стати підґрунтям для розроблення інформаційної технології управління ризиками, зокрема загрозами та можливостями, в ІТ-проєктах.

Автором у роботі [58] наведено аналітичні моделі помилок основних показників проєктів, продукційні моделі вибору способів розрахунку основних показників проєктів створення нової техніки, а також прикладну інформаційну технологію підтримки прийняття рішень стосовно процесу проєктного аналізу цього створення, що забезпечує підвищення ефективності й обґрунтованості вибору методів проєктного аналізу. Це дослідження стане підґрунтям для розробки моделей та методів управління загрозами та можливостями в ІТ-проєктах, які стануть основою для інформаційної технології управління ризиками в ІТ-проєктах.

У роботі [59] дістала подальшого розвитку інформаційна модель взаємодії стейкхолдерів організаційних проєктів у сфері обслуговування літаків за рахунок зменшення впливу ризиків кожного стейкхолдера з урахуванням факторів поведінкової економіки. Результати цього дослідження стануть у нагоді в процесі розробки інформаційної технології управління ризиками в ІТ-проєктах з урахуванням впливу загроз та можливостей.

Автором у роботі [67] створено інформаційну модель медичного проєкту з точки зору управління якістю проєкту у межах ціннісного підходу, яка дозволяє вирішити ряд завдань, таких як: вибрати ті зміни в медичному проєкті, які

забезпечуватимуть підвищення якості надання медичних послуг; ініціювати ті проєкти, які забезпечать необхідні зміни у якості надання медичних послуг; розробити такі схеми дій в ініційованих проєктах, які забезпечать необхідну модернізацію загальної системи якості надання медичних послуг. Означене дослідження стане у нагоді під час формування інформаційних зв'язків в процесі розробки інформаційної технології управління ризиками в ІТ-проєктах з урахуванням впливу загроз та можливостей.

Таким чином, можна зробити висновок, що існуючі інформаційні технології в управлінні ризиками проєктів частково можуть бути застосовані для управління ризиками ІТ-проєктів з урахуванням загроз та можливостей. Тому автором пропонується опрацювання інформаційної технології управління ризиками в ІТ-проєктах, яка б враховувала вплив загроз та можливостей.

1.5. Постановка задачі дослідження

Як було наведено вище, то інформаційні технології відіграють важливу, інколи вирішальну роль у всіх сферах діяльності, зокрема й у бізнесі, а у реаліях воєнного стану України – ІТ є однією з провідних індустрій української економіки. Тому необхідно приділяти увагу та розвивати підходи та інструменти ІТ-проєктів. Пандемія COVID-19 та російське вторгнення в Україну 2022 року показало, що в умовах такої непередбачуваної турбулентності саме ІТ-проєкти є економічно вигідними. Тому саме управляючи ризиками в таких проєктах та приймаючи рішення, більш можливо успішно завершити проєкт з задоволенням замовника та економічно вигідним результатом, що висвітлюється економічними показниками цієї галузі.

Після огляду сфери управління ризиками треба зазначити, що ризиками в ІТ-проєктах можна управляти так само, як і ризиками в інших галузях за кращими стандартами проєктного управління. Але постає цікава задача вдосконалення управління ризиками, зокрема загрозами та можливостями, притаманними саме ІТ-сфері. До особливостей реалізації ІТ-проєктів, які можуть

впливати на формування ефективної системи управління, можна віднести наступні: нестандартний життєвий цикл, який може включати в себе також тестовий, гарантійний та післягарантійний етапи розробки; необхідність чіткого визначення, вже на етапі ініціації, вимог до ІТ-проєктів незважаючи на рухливість та притаманність змін деяких напрямків в ІТ-сфері; необхідність оперативного внесення змін на етапі розробки та тестування, що створює складнощі, з якими стикаються практично всі керівники ІТ-проєктів, внаслідок чого відбувається відставання від запланованих термінів; робочі пакети завжди розглядаються ієрархічно, а послідовність або паралельність їх виконання залежить від можливостей технологій та ступеня гнучкості та адаптивності методології розробки; робота зі складними цілями проєктів, що мають багато рівнів: наприклад, цілі різних рівнів разом з аналізом інтересів учасників проєкту і оцінкою їх впливу на сам проєкт часто додаються в концепцію реалізації проєкту; також ІТ-проєкти не повинні розглядатися поза бізнес-проєктом клієнта і менеджмент компанії з самого початку орієнтований на вибудовування складної комунікації; матрична організаційна структура управління проєктами, важливу роль в якій відіграє координатор проєктів, менеджер, керівник проєктів або проєктний менеджер.

Таким чином, в процесі управління ризиками, як можливостями і загрозами, проектний менеджер, як особа, що приймає рішення, стикається зі складною проблемою прийняття рішень в умовах невизначеності. Для короткотривалих проектів незрілих компаній додатковою складною проблемою стає ідентифікація ризиків та неможливість виконати їх кількісну оцінку. На процес прийняття рішень негативний відбиток накладає і суб’єктивний характер рішення проектного менеджера при ідентифікації та управлінні ризиками. Також у загально відомих методологіях управління ризиками у більшості випадків ризики розглядаються лише як події, що носять негативний характер і не враховується додатковий вплив ризиків, як можливостей.

Виходячи із наведеного вище, автором пропонується розроблення моделей, методів та інформаційної технології управління ризиками в ІТ-проєктах з урахуванням впливу загроз та можливостей [68].

1.6. Висновки за першим розділом

За результатами проведеного дослідження у першому розділі можна зробити наступні висновки:

1. Керівництво будь-якої компанії, зокрема й в ІТ-сфері, під час планування діяльності постійно зіштовхується із відповідними управлінськими проблемами – як спланувати роботи в часі, які будуть потрібні ресурси, скільки ресурсів та коли саме, скільки це буде коштувати, коли відбуватимуться розрахунки та інші.

2. До особливостей реалізації ІТ-проєктів, які можуть впливати на формування ефективної системи управління, можна віднести, серед іншого, наступні: нестандартний життєвий цикл, який може включати в себе також тестовий, гарантійний та післягарантійний етапи розробки; необхідність чіткого визначення, вже на етапі ініціації, вимог до ІТ-проєктів незважаючи на рухливість і неоднозначність деяких напрямків в ІТ-сфері; необхідність оперативного внесення змін, що створює складнощі внаслідок чого відбувається відставання від запланованих термінів та незаплановане розростання обсягів проєкту; робочі пакети дуже часто розглядаються ієрархічно, а послідовність або паралельність їх виконання залежить від технологій та гнучкості методології розробки; робота з багаторівневими цілями: цілі різних рівнів разом з аналізом інтересів учасників і оцінкою їх впливу на проєкт часто включаються в концепцію реалізації проєкту; ІТ-проєкти не можуть розглядатися поза бізнес-проєктом клієнта і менеджмент з самого початку орієнтований на вибудовування складної комунікації; матрична організаційна структура управління проєктами, важливу роль в якій відіграє координатор проєктів або проєктний менеджер.

3. Виходячи із огляду стандартів управління проєктами з точки зору їхнього застосування в ІТ-сфері, можна дійти висновку, що не всі вони мають відокремлену та сформульовану область управління можливостями, проте все більше компаній мають потребу зосередитися на можливостях досягнення цілей проєкту в умовах конкурентного середовища. Управління можливостями описано в IPMA ICB відповідно до Управління ризиками як елемент практичної компетенції для окремих осіб, однак відомі стандарти PMI та японський стандарт P2M не містять окремо галузь управління можливостями, тоді як CMMI-DEV взагалі не охоплює можливості. Огляд показує, що управління можливостями залишається цікавою темою для дослідження через його невизначену присутність у більшості стандартів управління проєктами. Це свідчить про те, що питання управління ризиками в ІТ-проєктах є актуальним та потребує подальшого дослідження.

4. Одним зі способів удосконалення результатів будь-якого проєкту є своєчасне і доречне управління його загрозами для того, щоб мінімізувати втрати бюджету і ресурсів, до яких вони можуть призводити, або, навпаки, вміло збільшити ефект від можливостей, щоб досягати проєктних цілей й вдоволеності та очікування зацікавлених сторін проєкту у рамках заданих проєктних обмежень.

5. Ризик має багато класифікацій та характеристик, але для його якісного й кількісного управління необхідно знати основні – ймовірність, вплив, пріоритет та тригер. Необхідність і доречність застосування якісного і кількісного аналізу має чітку залежність від типу проєкту та його складності. Лише доцільне використання необхідних інструментів в управлінні ризиками має допомогти збільшити прибутки завдяки вмілому управлінню можливостями та уникненню або пом’якшенню загроз щодо фінансових і кадрових втрат ІТ-компаній.

6. За результатами проведеного аналізу існуючих моделей та методів управління ризиками в проєктах, зокрема й в ІТ-сфері, зрозуміло, що існує

потреба у розробці саме підходів, моделей та методів управління ризиками в IT-проєктах з урахуванням впливу загроз та можливостей.

7. Існуючі інформаційні технології в управлінні ризиками проєктів частково можуть бути застосовані для управління ризиками IT-проєктів з урахуванням загроз та можливостей. Тому автором пропонується розроблення інформаційної технології управління ризиками в IT-проєктах, яка б враховувала вплив загроз та можливостей [68].

Отже, необхідним завданням дисертаційної роботи є розроблення нових моделей, методів та інформаційної технології управління ризиками в IT-проєктах з врахуванням їх особливостей, загроз та можливостей і з метою оптимального планування ресурсів та витрачання коштів, а також врахування непередбачених витрат.

Результати досліджень першого розділу опубліковані у таких роботах [11, 21, 50, 51].

Список використаних джерел за першим розділом

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

2. Сметанюк О.А., Бондарчук А.В. Особливості системи управління проєктами в IT-компаніях. *Агросвіт*. 2020. № 10. С. 105-111. DOI: https://doi.org/10.32702/23066792.2020.10.105.

3. Дослідження Do IT Like Ukraine: IT-індустрія зростає попри все. Режим доступу: https://itukraine.org.ua/files/reports/2022/DoITLikeUkraine2022.pdf. Дата звернення: 15.04.2023.

4. Дослідження IT Research Ukraine 2023: Адаптивність та стійкість під час війни. Режим доступу: https://itcluster.lviv.ua/wp-content/uploads/2023/12/it-research-ukraine-2023-public-ua.pdf. Дата звернення: 02.06.2024.

5. Дослідження IT Ukraine Association: “Digital Tiger: the Power of Ukrainian IT”. Режим доступу: https://skilky-skilky.info/wp-

content/uploads/2024/03/Digital-Tiger-the-Power-of-Ukrainian-IT-research-for-2023.pdf. Дата звернення: 08.22.2024.

6. Офіс ефективного регулювання BRDO: Аналіз IT-освіти у вишах України. Режим доступу: https://brdo.com.ua/wp-content/uploads/2021/02/Analiz_IT_osvity_u_vyshah_Ukrai-ny_Print.pdf, https://brdo.com.ua/top/do-2024-roku-kilkist-it-fahivtsiv-v-ukrayini-zroste-na-23-doslidzhennya-brdo/. Дата звернення: 08.22.2024.

7. Архієреєв С.І., Ликова А.С. Роль людського капіталу сфери IT-послуг у розвитку зовнішньоекономічної діяльності України. *Соціальна економіка*. Харківський національний університет імені В.Н. Каразіна, 2019. Вип. № 58. С. 52-58. DOI: https://doi.org/10.26565/2524-2547-2019-58-07.

8. Глушенкова А.А. Особливості управління інноваційними проєктами в сфері телекомунікацій та інформатизації. *Економіка. Менеджмент. Бізнес*. 2015. № 4 (14). С. 72-77. URL: http://journals.dut.edu.ua/index.php/emb/article/view/1022.

9. Колянко О.В., Озимок Г.В. Використання жорсткої «Waterfall» та гнучкої «Agile» моделей управління проєктами. *Вісник Львівського торговельно-економічного університету. Економічні науки*. 2017. Вип. 52. С. 177-182. URL: http://journals-lute.lviv.ua/index.php/visnyk-econom/issue/view/64/66.

10. Крижановський Є.М., Ящолт А.Р., Жуков С.О., Козачко О.М. Моделювання бізнес-процесів та управління IT-проєктами: навч. посібн. [Електронний ресурс]. Вінниця: ВНТУ, 2018. 91 с. URL: https://ecopy.posibnyky.vntu.edu.ua/txt/2018/Kryzanovsk_yascholt_modelyuvanna_np_p024.pdf.

11. Danchenko O., Shendryk V., Hrabina K. Opportunity Management overview in terms of the Risk Management in the software development industry standards. *Управління проєктами: стан та перспективи*. Матеріали XV міжнародної науково-практичної конференції (м. Миколаїв, 10-13 вересня 2019 року). Миколаїв: НУК, 2019. С. 88-89.

12. Грицюк Ю.І., Жабич М.Р. Управління ризиками реалізації програмних проєктів. *Науковий вісник НЛТУ України*. 2018. Том 28. № 1. С. 150-162. URL: http://nbuv.gov.ua/UJRN/nvnltu_2018_28%281%29__32.

13. Шимкович В. Карьера в IT: должность Project Manager [Електронний ресурс] DOU.ua, 2013. URL: https://dou.ua/lenta/articles/projectmanager position/

14. The standard for risk management in portfolios, programs, and projects. Newtown Square: Project Management Institute, 2022. 175 p.

15. CMMI Institute. URL: https://cmmiinstitute.com/cmmi/dev.

16. CMMI for Development, Version 1.3, Product Team, Technical Report, Software Engineering Process Management Program. 2010. 482 p.

17. Marco, Peter et oth. Individual Competence Baseline for Project, Programme and Portfolio Management, Version 4.0, 2015. ISBN 978-94-92338-01-3.

18. S. Ohara, P2M - A Guidebook of Project & Program Management for Enterprise Innovation, Project Management Association of Japan (PMAJ), vol. 1, 2001. ISBN 978-4-90852-020-4.

19. Рощина Н.В., Черненко Н.О. До питання впливу IT-систем на економіку України. *Ефективна економіка*. 2016. № 4. URL: http://www.economy.nayka.com.ua/?op=1&z=4884.

20. Продіус О.І., Прокоф'єва В.К. Історичні передумови розвитку проєктного управління. *Економіка та підприємництво*. 2019. № 3(108). С. 141-146. URL: http://nbuv.gov.ua/UJRN/drep_2019_3_30.

21. Грабіна К.В., Шендрик В.В. Огляд процесів управління ризиками в IT-проєктах в контексті стандартів проєктного менеджменту. *Управління розвитком складних систем*. Київ: КНУБА, 2020. Вип. 43. С. 26-32. DOI: https://www.doi.org/10.32347/2412-9933.2020.43.26-32. URL: http://mdcs.knuba.edu.ua/article/view/219812/219536.

22. Герасименко О.М. Еволюція світового ризик-менеджменту. *Інвестиції: практика та досвід.* 2013. № 12. С. 26-31. URL: http://www.investplan.com.ua/pdf/12_2013/9.pdf.

23. Practice Standard for Project Risk Management. USA, PMI, 2019. 116 p.

24. Денчик О.Р. Моделі та методи інтегрованого управління ризиками проєктів в агропромисловому комплексі. : дис. … д-ра філос. : 073. Київ, 2020. 229 с.

25. A Guidebook of Program & Project Management for Enterprise Innovation. Japan: Project Management Association of Japan (PMAJ), 2017. 427 p.

26. Bentley, C. PRINCE2: A Practical Handbook – Third Edition. London, UK: Routledge, 2010. 322 p.

27. Risk Management Guidelines – Second Edition, ISO 31000: 2018.

28. Christopher, M. The agile supply chain: competing in volatile markets. Christopher, M. Agile supply chain – 2010.

29. Federation of European Risk Management Associations. URL: https://www.ferma.eu/.

30. Стандарт ризик-менеджменту Федерації європейських асоціацій з ризик-менеджменту (Risk Management Standard, FERMA – p. 6) [Електронний ресурс]. URL: http://www.ferma.eu/app/uploads/2011/11/a-Riskmanagement-standard-russian-version.pdf.

31. Овандер Н.Л. Огляд міжнародних та українських стандартів з управління ризиками з погляду сучасних викликів та загроз. *Економіка та суспільство.* 2021. Вип. 27. DOI: https://doi.org/10.32782/2524-0072/2021-27-26.

32. Committee of Sponsing of the Treadway Commission. URL: https://www.coso.org/Pages/default.aspx.

33. ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови (ISO 31000:2018 Risk Management – Principles and guidelines on implementation, IDT). [Чинний від 2019-01-01]. URL: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en.

34. B. Purwanggono, A. Margarette. Risk assessment of underpass infrastructure project based on ISO 31000 and ISO 21500 using fishbone diagram and RFMEA (project risk failure mode and effects analysis) method. *10P Conference Series: Materials Science and Engineering.* 2017. DOI: 10.1088/1757-899z/277/1/012039.

35. Офіційний сайт Міжнародної організації зі стандартизації (International Organization for Standardization, ISO). URL: https://www.iso.org/committee/629121/x/catalogue/.

36. ISO / TR 31004:2013 Risk management – Guidance for the implementation of ISO 31000 [Електронний ресурс]. URL: http://www.iso.org/iso/ru/catalogue_detail?csnumber=56610.

37. ДСТУ IEC/ISO 31010:2013 Керування ризиком. Методи загального оцінювання ризику (IEC/ISO 31010:2009, IDT). [Чинний від 2014-07-01]. Вид. офіц. Київ : Мінекономрозвитку України, 2015. 80 с.

38. Basel Committee on Banking Supervision. URL: https://www.bis.org/list/bcbs_all/sdt_1/index.htm. Дата звернення: 22.10.2021.

39. Герасименко О.М. Ризик-орієнтоване управління в системі економічної безпеки підприємства : дис. … д-ра екон. наук : 21.04.02. Київ, 2021. 667 с.

40. ДСТУ ISO Guide 73:2013. Керування ризиком. Словник термінів (ISO Guide 73:2009, IDT). [Чинний від 2014-07-01]. Вид. офіц. Київ : Мінекономрозвитку України, 2014. 17 с.

41. ДСТУ IEC/ISO 31010:2013 Керування ризиком. Методи загального оцінювання ризику (IEC/ISO 31010:2009, IDT). [Чинний від 2014-07-01]. Вид. офіц. Київ : Мінекономрозвитку України, 2015. 80 с.

42. Шевчук Ю., Васьків О. IT-ризики та їх зв'язок з бізнес-ризиками. URL: https://financial.lnu.edu.ua/wp-content/uploads/2015/10/Tezy_Vas-kiv_SHevchuk.pdf.

43. Elbaruni J.E., Bielova O., Melenchuk V. Analysis and prioritising risk minimizing techniques of IT-projects. *Управління розвитком складних систем*. Київ: КНУБА, 2020. Вип. 45. С. 6-12. DOI: 10.32347/2412-9933.2021.45.6-12.

44. Данченко О.Б., Ланських Є.В., Семко О.В. Інформаційні ризики цифрового формату. *Вісник Черкаського державного технологічного університету*. 2020. Вип. 3. С. 58-66. DOI: https://doi.org/10.24025/2306-4412.3.2020.200792.

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

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

47. Васильєв М.І. Моделі та методи ініціації проєктів протипожежного захисту об'єктів на основі оцінці ризиків: дис. … канд. техн. наук: 05.13.22. Львів. держ. ун-т БЖД. Львів, 2019.

48. Меленчук В. І. Моделі та методи управління проєктами матеріально-технічного забезпечення автотранспортних підрозділів Збройних Сил України: дис. … канд. техн. наук: 05.13.22. Львів. держ. ун-т БЖД. Львів, 2019.

49. IT в Україні: куди ми рухаємося : веб-сайт. URL: https://dou.ua/lenta/columns/future-of-it-ukraine/

50. Грабіна К.В., Шендрик В.В. Аналіз та порівняння методів управління ризиками проєктів сервісних ІТ-компаній. *Математичне моделювання процесів в економіці та управлінні проектами і програмами (ММП-2020)*. Міжнародна науково-практична конференція (смт. Коблево, 14-18 вересня 2020 р.). Харків: ХНУРЕ, 2020. С. 49-53.

51. Грабіна К.В., Шендрик В.В., Данченко О.Б. Складові управління ризиками ІТ-проєктів. *Інформатика. Культура. Технології, ІКТ-2021*. Матеріали VIII Міжнародної науково-практичної конференції (м. Одеса, 13-14 травня 2021 р.). Одеса: Одеська політехніка, 2021. С. 124-126.

52. ІТ-індустрія: тренди та прогнози розвитку: веб-сайт. URL: http://euinfocenter.rada.gov.ua/uploads/documents/29337.pdf/

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

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

55. Бабак І.М. Метод аналізу проектів з урахуванням причинно-наслідкових зв'язків факторів ризику: автореф. дис... канд. техн. наук: 05.13.22. Харків: Нац. аерокосм. ун-т ім. М.Є.Жуковського "Харк. авіац. ін-т", 2008. 19 с.

56. Дружинін Є.А. Методологічні основи ризик-орієнтованого підходу до управління ресурсами проектів і програм розвитку техніки: автореф. дис... д-ра техн. наук: 05.13.22. Харків: Нац. аерокосм. ун-т ім. М.Є.Жуковського "Харк. авіац. ін-т", 2006. 34 с.

57. Латкін М.О. Методологічні основи створення системи управління ризиками проектів підприємства: автореф. дис... д-ра техн. наук: 05.13.22. Харків: Нац. аерокосм. ун-т ім. М.Є.Жуковського "Харк. авіац. ін-т", 2009. 35 с.

58. Максименко О.В. Моделі та методи ризик-орієнтованого підходу, що забезпечують вірогідність результатів розрахунку основних показників проекту: автореф. дис... канд. техн. наук: 05.13.22. Харків: Нац. аерокосм. ун-т ім. М.Є.Жуковського "Харк. авіац. ін-т", 2005. 19 с.

59. Сепеда Гуаман Д.Ф. Протиризикове управління стейкхолдерами організаційних проектів в сфері обслуговування літаків в умовах поведінкової економіки: автореф. дис... канд. техн. наук: 05.13.22. Львів: ЛДБЖД, 2020. 20 с.

60. Савіна О.Ю. Ціннісно-орієнтоване протиризикове управління портфелями наукомістких проектів підприємств : дис. ... канд. техн. наук : 05.13.22. Миколаїв: НУК ім. адм. Макарова, 2019. 209 с.

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

62. Elbaruni J.E., Safar H., Bedrii D.I., Mann R. Risk management models of a project for the implementation of a management information system in the state institutions. Project, Program, Portfolio Management. Processing of the Five International Scientific and Practical Conference 04-05 December 2020. Book 2. Odesa, ONPU, 2020. P. ISSN 2522-9435. (Scopus).

63. Башинська І.О., Хрістова А.В. Використання сучасних інформаційних технологій в управлінні проєктами. *Економічний журнал Одеського політехнічного університету*. Одеса: ОНПУ, 2017. № 1(1). С. 16-22. URL: http://economics.opu.ua/ejopu/2017/No1/16.pdf.

64. Balan O.S., Berber O.V. Investment projects at industrial enterprises: accounting and implementation control. *Економіка: реалії часу. Науковий журнал*. 2013. № 2 (7). С. 126-134. URL: http://economics.opu.ua/files/archive/2013/n2.html.

65. Данченко О.Б. Інформаційна технологія формування протиризикових розкладів робіт при будівництві складних енергетичних об’єктів: дис. ... канд. техн. наук : 05.13.06. Черкаси: Черк. держ. технолог. ун-т, 2000. 201 с.

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

67. Гайдаєнко О.В. Інформаційна модель медичного проєкту. *Інформаційні управляючі системи та технології*. Матеріали VI міжнар. наук.-практ. конф. Одеса : ІУСТ, 2017. С. 340-342.

68. Грабіна К.В., Шендрик В. В. Метод управління ризиками ІТ-проєктів з врахуванням загроз та можливостей. *Управління розвитком складних систем.* Київ: КНУБА, 2023. Вип. 55. С. 18-28. DOI: https://doi.org/10.32347/2412-9933.2023.55.18-28. URL: http://mdcs.knuba.edu.ua/article/view/291119.

РОЗДІЛ 2.
МОДЕЛІ ІНТЕГРОВАНОГО УПРАВЛІННЯ ЗАГРОЗАМИ ТА МОЖЛИВОСТЯМИ В ІТ- ПРОЄКТАХ

2.1. Методологія та архітектура наукового дослідження

Виходячи із аналізу сучасного стану управління ризиками в ІТ-проєктах, що наведений у розділі 1 цього дослідження, можна перейти до формування методології цього дослідження.

В процесі наукових досліджень задачі управління ризиками, зокрема загрозами та можливостями, в ІТ-проєктах використані наступні підходи моделі та методи.

1. Системний підхід – це напрямок філософії та методології наукового пізнання, в основі якого лежить дослідження об’єктів як систем. Особливість системного підходу полягає в тому, що він орієнтований на розкриття цілісності об’єкта та механізмів, що його забезпечують, на виявлення різноманітних типів зв’язків складного об’єкта та зведення їх до єдиної теоретичної картини [1].

Принципи системного підходу поширюються практично на всі сфери наукового знання та практики. Системний підхід не існує у вигляді строгої методологічної концепції, будучи швидше за все – сукупністю принципів дослідження.

Системний підхід – це підхід, при якому досліджуваний об’єкт розглядається як система, тобто сукупність взаємопов’язаних елементів (компонентів), що має вихід (мета), вхід (ресурси), зв'язок із зовнішнім середовищем, зворотній зв'язок [2].

Системний підхід – це методологічний напрямок у науці, основне завдання якого полягає у розробці методів дослідження та конструювання складноорганізованих об’єктів – систем різних типів і класів [2, 3].

Отже, системний підхід в цьому дослідженні був застосований на етапі аналізу особливостей управління ризиками, класифікації ризиків, існуючих

моделей та методів управління ризиками, інформаційної технології управління ризиками в IT-проєктах. Завдяки системному підходу були виявлені особливості управління IT-проєктами, класифікація їхніх ризиків, а також виявлення загроз та можливостей, що мають вплив на процес планування та реалізації IT-проєктів.

2. Процесний підхід [4, 5, 6] використовується для:

1) забезпечення процедур в прийнятті рішень;

2) визначення рівня задоволення вимог;

3) підтримки управління ризиками;

4) дотримання прийняття рішень лише після розрахунку витрат, термінів, продуктивності та впливу ризиків на проєктування системи.

Процеси розробки логічної та фізичної архітектури системи використовують системний аналіз для оцінки характеристик або розробки властивостей варіантів архітектури, отримання аргументування для вибору найефективного варіанту з погляду витрат, ризиків та ефективності проєкту [4, 5]:

1) Визначення критеріїв вибору моделі:

− вибір критеріїв оцінки з нефункціональних вимог (продуктивність, умови функціонування, обмеження тощо) та/або опис властивостей;

− сортування та впорядкування критеріїв;

− визначення шкали порівняння для кожного оціночного критерію та визначення ваги кожного критерію відповідно до його рівня важливості щодо інших критеріїв.

2) Визначення варіантів рішень, пов'язаних із ними моделей та даних.

3) Оцінка варіантів з використанням раніше визначених методів та процедур:

− виконується аналіз витрат, ризиків, ефективності, розміщуючи всі альтернативні варіанти на шкалі для кожного критерію оцінки;

− оцінюються всі альтернативні варіанти по загальній шкалі оцінок.

4) Надання результатів процесу, що ініціював: критеріїв оцінки, вибір оцінок, шкали порівняння, результати оцінки для всіх варіантів, і можливі рекомендації з обґрунтуванням.

Рекомендується одночасно використовувати кілька різних типів моделей для порівняння результатів та врахування різних аспектів системи [4, 7, 8].

Вважається, що процесне управління ризиками розвитку підприємства є джерелом його конкурентоспроможності [4].

В роботах з управління якістю [5, 6] акцентується увага на процесному підході. В роботах [9, 10, 11, 12, 13] досліджено зв’язок управління якістю та процесного підходу. Організація роботи державних установ теж орієнтується на процесний підхід [14, 15, 16].

3. Проєктний підхід передбачає, що проєкт – це комплекс цілеспрямованих взаємопов’язаних робіт, для виконання яких виділяють відповідні ресурси та установлюють певні терміни.

З точки зору системного підходу проєкт являє собою модель процесу досягнення майбутніх змін. У загальному випадку для опису такої моделі використовується практично весь арсенал мовних засобів. За своєю сутністю весь процес управління проєктом, починаючи від етапу передпроєктних досліджень (генерації, аналізу та відбору ідей) до етапу закриття проєкту, є застосування методології системного аналізу до сфери людської діяльності, спрямованої на досягнення реальних змін у середовищі існування.

Ефективне управління проєктом потребує урахування й оптимізації психологічних, економічних, фінансових, технологічних, екологічних, організаційних, юридичних та інших факторів [17, 18].

Оцінка згенерованих ідей проєкту за своєю природою має евристичний і якісний характер, визначення оптимальної ідеї виявляється неможливим. Вибір ідеї, яку слід покласти в основу проєкту, звичайно щільно пов'язаний з плануванням робіт над проєктом, тобто календарним плануванням виконання завдань та завдань, необхідних для реалізації проєкту. Саме тут роль системного аналізу особливо відчутна. Планування робіт над проєктом передбачає також

детальне визначення організаційних взаємин з різними суб'єктами [19, 20]. Нині в сфері проєктної діяльності сформувалося чотири найважливіші концепції, що мають суттєвий вплив на розвиток теорії і практики управління проєктами: теорія наукового управління; теорія адміністративного управління; теорія управління з позицій психології людських відносин і теорія управління в контексті науки про поведінку. Процеси управління проєктами поділяють на п'ять основних категорій або груп [19, 21].

Процеси ініціювання слугують визначенню нового або нової фази наявного проєкту для отримання дозволу на початок його реалізації в цілому або окремої його фази.

Процеси планування та розроблення передбачають визначення загального змісту проєкту, уточнення цілей і виокремлення послідовності дій, достатніх для досягнення цілей проєкту.

Процеси виконання застосовують для проведення заходів, передбачених планом управління проєктом, а також для задоволення його специфікацій.

Процеси моніторингу і контролю необхідні для відстеження, аналізу і розуміння впливу на ефективність реалізації проєкту, виявлення недоліків, внесення змін для їх усунення від самого початку до повного завершення проєкту.

В діяльності ІТ-компаній методологія управління проєктами проявила себе дієвим та якісним інструментом для підвищення ефективності управління ІТ-проєктами з урахуванням їхніх особливостей, а також для виявлення ризиків з урахуванням загроз та можливостей. Крім того, надала змогу сформувати стратегії управління загрозами та можливостями в ІТ-проєктах.

4. Ризик-менеджмент/управління ризиками – один з напрямків сучасного менеджменту, що вивчає проблеми управління ризиками, що виникають в діяльності самостійної господарської організації [19, 22].

Ризик-менеджмент можна визначити як систему прийняття та виконання управлінських рішень, спрямованих на зменшення впливу наслідків реалізації ризиків на діяльність організації [22, 23].

Особливості ризик-менеджменту:

по-перше, ризик-менеджмент – система, що об’єднує осіб, які приймають рішення, і виконавців, що встановлює зв’язку між ними і порядок їх взаємодії;

по-друге, це дійсно менеджмент, тобто діяльність, в процесі якої приймаються і виконуються управлінські рішення;

по-третє, метою системи управління ризиками є зменшення впливу непередбачених подій на діяльність організації.

Ризик-менеджмент – в широкому сенсі – процес виявлення і оцінки ризиків, а також вибір методів та інструментів управління для мінімізації ризику [24, 25].

Ризик-менеджмент включає в себе:

– ідентифікацію, аналіз та оцінку ризиків;

– превентивну розробку програми заходів щодо ліквідації наслідків кризових ситуацій;

– розробку механізмів виживання;

– створення системи страхування;

– прогнозування розвитку підприємства з урахуванням можливої зміни кон’юнктури та інші заходи.

Структурні елементи ризик-менеджменту: ідентифікація ризику; оцінка ризику; контроль за ризиком; фінансування ризику (грошові витрати на ризик-менеджмент).

У теорії і практиці ризик-менеджменту можна виділити три основні напрями [25, 26]:

– перший, пов’язаний з розробкою системи заходів, спрямованих на попередження та профілактику ризиків;

– другий, стосується питань мінімізації негативних наслідків, які можуть заподіяти ризики організації;

– третій, пов’язаний з можливістю отримувати в ситуаціях ризику додаткові доходи або інші комерційні переваги.

У ризик-менеджменті прийнято виділяти кілька етапів:

– на першому відбувається виявлення ризику з супутньою оцінкою ймовірності його реалізації і масштабу наслідків;

– на другому здійснюється розробка ризик-стратегії з метою зниження ймовірності реалізації ризику і мінімізації можливих негативних наслідків;

– на третьому вибираються методи і інструменти управління виявленим ризиком;

– на четвертому проводиться безпосереднє управління ризиком;

– на заключному етапі оцінюються досягнуті результати і коригується ризик-стратегія.

Ключовим етапом ризик-менеджменту вважається вибір методів і інструментів управління ризиком [25, 26].

В цьому дисертаційному дослідженні методологія ризик-менеджменту була застосована для ідентифікації, оцінки, вироблення стратегій зниження та підвищення впливу та управління ризиками з урахуванням загроз та можливостей в управління ризиками в IT-проєктах.

5. Експертний аналіз. Сутність цього методу полягає в опитуванні й обробці думок експертів з проблеми, що вирішується [19, 27, 28]. Метод експертних оцінок раціонально поєднує процес інтуїтивно-логічного аналізу проблеми з кількісними і якісними методами обробки як для подання результату рішення, так і для управління самим процесом.

Експертні методи застосовуються за відсутності інформації по тих чи інших показниках аналогічних об'єктів, або за відсутності в об'єкту, що проєктується, аналогів. Методичний апарат проведення експертизи повинен забезпечувати виконання наступних основних етапів експертного оцінювання (незалежно від об'єкту експертизи): добір експертів; організація експертних опитувань; перевірка узгодженості оцінок експертів; обробка, оформлення і подання експертної оцінки для прийняття рішень по них [19, 28, 29].

Експертні методи у цьому дослідженні застосовуються автором для проведення оцінки ризиків з урахуванням загроз та можливостей в управлінні IT-проєктами.

6. Інтелектуальний аналіз даних. (Data Mining) – це сучасна концепція аналізу даних, яка припускає, що дані можуть бути неточними, неповними (містити пропуски), суперечливими, різнорідними, непрямими, і при цьому мати гігантські обсяги. Тому розуміння даних в конкретних програмах вимагає значних інтелектуальних зусиль [30, 31, 32].

В інтелектуальному аналізі даних застосовується математичний апарат для виявлення закономірностей і тенденцій, що існують в даних. Зазвичай, такого роду закономірності не можна виявити при традиційних методах перегляду даних, тому що їх зв'язки мають високий рівень складності, або із-за надмірного обсягу даних. Також слід зазначити, що побудова моделі інтелектуального аналізу даних є часткою більш масштабного процесу, в який входять всі завдання, від формулювання питань щодо даних і створення моделі для відповідей на ці питання до розгортання моделі в робочому середовищі. Інтелектуальний аналіз даних – це обробка інформації та виявлення в ній моделей і тенденцій, які допомагають проєктному керівнику приймати рішення [31, 32].

Необхідність інтелектуального аналізу даних виникла в кінці XX століття в результаті повсюдного поширення інформаційних технологій, що дозволяють детально протоколювати процеси бізнесу і виробництва. Великі обсяги даних, широту і різноманітність інформації привели до вибухового зростання популярності методів інтелектуального аналізу даних [30, 32].

Методи інтелектуального аналізу даних у цьому дослідженні були застосовані для вибору оптимальної стратегії управління ризиками, загрозами та можливостями в ІТ-проєктах.

7. SWOT-аналіз. З 60-х рр. XX ст. та до сьогоднішнього дня SWOT-аналіз широко застосовується у процесі стратегічного планування. Спочатку SWOT-аналіз застосовувався для структурування знань про поточну ситуацію та тенденції. Пізніше SWOT-аналіз став використовуватися у більш ширшому вжитку - для конструювання стратегій [28, 33, 34].

З появою SWOT моделі аналітики отримали інструмент для своєї інтелектуальної роботи. Відомі, але розрізнені та безсистемні уявлення про фірму та конкурентне середовище SWOT-аналіз дозволив сформулювати аналітикам у вигляді логічно погодженої схеми взаємодії сил, слабкостей, можливостей та загроз. У результаті виконання класичного SWOT-аналізу створюється структурована інформація у рамках єдиної SWOT моделі [28, 34, 35].

У 1965 році чотири професори Leraned E.P., Christensen C.R., Andrews K.R., Guth W.Q. запропонували технологію використання SWOT моделі для розроблення стратегії поведінки фірми. Була запропонована схема LCAG (за першими буквами прізвищ авторів), яка ґрунтується на послідовності кроків, які приводять до вибору стратегії [28, 33, 35].

У ряді підходів структурування інформація за кожним із напрямків - сили, слабкості, можливості, загрози - оцінюється кількісними мірами, на підставі яких за допомогою функцій корисності розраховується потенціал досліджуваного об’єкту за кожним напрямком (підхід розвивається у рамках Conjoint-аналізу).

У 1982 році професор Heinz Weihrich (Х. Вейріх) опублікував працю [35], у якій запропонував новий вигляд SWOT моделі. Свою SWOT модель він називає TOWS матрицю та розглядає її як “концептуальну основу систематичного аналізу, який полегшує співвідношення зовнішніх загроз та можливостей із внутрішніми слабкостями та силами організації” [35]. Професор Х. Вейріх запропонував будувати стратегії поведінки фірми на підставі систематичного співвідношення раніше розроблених переліків зовнішніх факторів із внутрішніми силами та слабкостями. Він також вказав на необхідність побудови SWOT матриць із певною періодичністю. Це повинно дозволити відстежувати зміни конкурентного середовища при побудові стратегій.

Пропонується використання цієї матриці у якості однієї із основ для оцінки варіантів стратегічного вибору у рамках того або іншого квадрата. Кожен фактор помічається або знаком «+» (що означає сильну відповідність сильних сторін

можливостям), або знаком «-» (що означає слабку відповідність сильних сторін можливостям або його повну відсутність) [35].

Читання матриці допоможе виявити стратегічні фактори, де сильні сторони фірми потенційно могли б відповідати можливостям зовнішніх умов зовнішнього середовища (зокрема, значення «+»). Матриця створена для порівняння оптимальності відповідностей для кожного квадрата [28, 34, 35].

У подальшому, в працях інших дослідників ця модель називається як розширена SWOT модель (extended SWOT matrix), або як інтегрована SWOT модель (integred SWOT matrix). Однак у більшості робіт із стратегічного планування все рівно можна зустріти термін “SWOT-аналіз”, хоча вони використовують модель Weihrich’a [28, 33, 34].

Процес стратегічного планування із застосуванням розширеної SWOT матриці було запропоновано організовувати як послідовність кроків:

- аналіз зовнішнього оточення;
- аналіз внутрішнього оточення;
- побудова стратегій та тактичних дій.

Мета побудови розширеної SWOT матриці полягає у тому, щоб сфокусувати увагу аналітика на побудові чотирьох груп, різних стратегій. Кожна група стратегій використовує певну парну комбінацію внутрішніх та зовнішніх обставин. Спільному аналізу піддаються пари наступних показників:

- сили - можливості (S-O);
- сили - загрози (S-T);
- слабкості - можливості (W-O);
- слабкості - загрози (W-T).

За результатами аналізу показників із кожної пари формується набір стратегій. Стратегії називаються за назвами досліджуваних внутрішніх та зовнішніх факторів.

У цьому дослідженні SWOT-аналіз був застосований для виявлення загроз та можливостей в ІТ-проєкті, а також для розробки моделей та методів управління ризиками в ІТ-проєктах з урахуванням загроз та можливостей.

Рисунок 2.1. - Архітектура наукового дослідження

2.2. Концептуальна модель управління ризиками в ІТ-проєктах з урахуванням загроз та можливостей

На підставі результатів дослідження сучасного стану управління ризиками в ІТ-проєктах, яке проведено у першому розділі цієї дисертаційної роботи, автор дійшов висновку про те, що питання підвищення ефективності управління цими проєктами є актуальним [36, 37]. Окрім того, у підрозділі 2.1. цього дисертаційного дослідження автором розглянуто методологію наукового дослідження та на її підставі побудована його архітектура (рис. 2.1.), які ґрунтуються на існуючих підходах, моделях та методах [36, 37, 38]. Управління ризиками в ІТ-проєктах з урахуванням загроз та можливостей дозволить підвищити ефективність управління означеними проєктами.

Концептуальна модель управління ризиками в ІТ-проєктах з урахуванням загроз та можливостей (рис. 2.2.) ґрунтується на тому, що будь-який проєкт може бути описаний в просторі найголовніших метрик – час (тривалість), гроші (бюджет), обсяг та якість [39, 40, 41]. Відповідно до останньої редакції «A Guide to the Project Management Body of Knowledge» (PMBoK Guide) [19] проєкт вважається успішним, якщо його результатами задоволені усі зацікавлені сторони проєкту та досягнуті усі проєктні цілі.

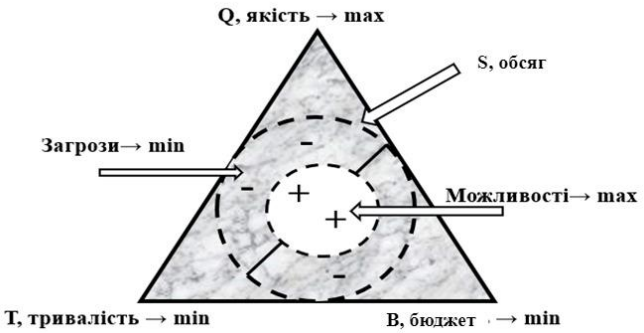


Рисунок 2.2. - Концептуальна модель управління ризиками в ІТ-проєкті з урахуванням загроз та можливостей

Означене можна відобразити у наступному вигляді (2.1):

$$F_p\left(T_p, B_p, S_p, Q_p\right) - F_a\left(T_a, B_a, S_a, Q_a\right) \to 0, \quad (2.1)$$

де $F_p\left(T_p, B_p, S_p, Q_p\right)$ – функція проєкту із запланованими змінними;

T_p – запланована тривалість проєкту;

B_p – запланований бюджет проєкту;

S_p – запланований обсяг робіт проєкту;

Q_p – встановлена якість продукту проєкту;

$F_a\left(T_a, B_a, S_a, Q_a\right)$ – функція проєкту із виконаними змінними;

T_a – фактична тривалість проєкту;

B_a – використаний бюджет проєкту;

S_a – виконаний обсяг робіт проєкту;

Q_a – фактична якість продукту проєкту.

Тобто необхідною умовою успішності проєкту є максимальне наближення запланованих параметрів до отриманих в результаті виконання проєкту [39, 42, 43]. Будь-яка подія, що призведе до від'ємної різниці між ними є потенційним ризиком, який загрожує виконанню проєкту із запланованими обмеженнями. Аналогічно, будь-яке позитивне відхилення – це можливість, яка зберігає час, гроші та ресурси. Можна зробити припущення, що майже не існує проєктів, у яких (2.2):

$$F_p = F_a. \quad (2.2)$$

Тоді можна зробити висновок, що (2.3):

$$F_a = F_p + C - D, \quad (2.3)$$

де C – сукупний вплив можливостей на виконаний проєкт;

D – сукупний вплив загроз на виконаний проєкт.

Функція виконаного проєкту дорівнює запланованій функції проєкту з урахуванням впливу сукупного ефекту від можливостей та загроз [39, 44, 45]. Саме управління загрозами та можливостями дає звести різницю між запланованою та фактичною величиною до нуля, тобто виконати проєкт по плану. Означене можна відобразити у вигляді наступного обмеження (2.4).

$$\begin{gathered} T_a \to \min, \\ B_a \to \min \\ S_a \to const, \\ Q_a \to \max \end{gathered} \tag{2.4}$$

Таким чином, ризик-менеджмент, як один із потужних засобів мінімізації втрат та збільшення прибутків, є дієвим та ефективним інструментом, що допомагає проєктним менеджерам успішно управляти проєктами та завершувати їх в рамках заданих обмежень часу, витрат, обсягу та якості (рис. 2.2.).

Враховуючи заздалегідь вплив можливих загроз та можливостей в момент планування проєкту, проєктний менеджер є більш підготовленим до швидкоплинних реалій проєктної діяльності, які в свою чергу містять велику кількість незапланованих явищ, робіт, або іншими словами – змін.

2.3. Моделі інтегрованого управління загрозами та можливостями в ІТ-проєктах

Виходячи із концептуальної моделі управління ризиками в ІТ-проєктах з урахуванням загроз та можливостей, яка наведена у підрозділі 2.2. цього дослідження, а також методології дослідження, наведеної у підрозділі 2.1., автором запропоновано управляти ризиками в ІТ-проєкті з урахуванням впливу на нього загроз та можливостей.

2.3.1. Модель RIO-RIT-REO-RET-аналізу

Управління ризиками являє собою комплексний процес, який потребує різних підходів та методів щодо його виконання. Одним з найвідоміших інструментів ідентифікації ризиків є SWOT-аналіз для аналізу даних [34, 35, 46]. Первісно даний метод був вперше застосований професором К. Ендрюсом на конференції з проблем бізнес-політики в Гарварді.

Через два роки професори Леранед, Крістенсен, Ендрюс і Гут запропонували технологію використання SWOT-моделі для розробки стратегії поведінки фірми та організацій в контексті стратегічного управління [34, 44]. Тому історично SWOT-аналіз є, перш за все, інструментом стратегічного управління.

Якщо ж розглядати використання SWOT-аналізу в проєктному менеджменті, то SWOT-аналіз дозволяє провести аналіз проєкту з точку зору кожного з аспектів: сильних чи слабких сторін, сприятливих можливостей та загроз.

Згідно [19] цей метод використовується при ідентифікації ризиків, щоб розширити ідентифікацію ризиків за рахунок ризиків, які виникають в середині самого проєкту [71].

Розглядаючи ризики для типового ІТ-проєкту, можна відзначити рівень їх виникнення: проєктний, організаційний (рівень компанії) чи галузевий. Приклад класифікації ризиків ІТ-проєкту за рівнем та джерелом виникнення наведено у табл. 2.1. [46, 47, 71].

Будемо вважати ризики проєктного рівня – внутрішніми (Internal), а ризики рівня компанії, організації чи галузі – зовнішніми (External). Тому введено класифікація за джерелом виникнення – внутрішні ризики (I) та зовнішні ризики (E).

Таблиця 2.1. Приклад ризиків ІТ-проєкту з класифікацією за рівнем та джерелом виникнення

Ризики	Рівень	Джерело виникнення
Поява альтернативного продукту на ринку	Галузь	І
Недотримання строків та термінів проєкту	Компанія	Е
Затримка фінансування проєкту	Галузь	Е
Вибір оптимальної технології	Проєкт	І
Порушення прав інтелектуальної власності	Галузь	Е
Експортні обмеження	Галузь	Е
Негнучкі закони про працю	Галузь	Е
Складнощі отримання візи	Галузь	Е
Зміни в податковому законодавстві можуть істотно зменшити заощадження	Галузь	Е
Негнучкі контракти	Компанія	Е
Порушення безпеки або конфіденційності	Проєкт	І
Політики загрожують податком ІТ-компаніям	Галузь	Е
Політична нестабільність всередині країни	Галузь	Е
Плинність кадрів розробників	Проєкт	І
Вигорання працівників	Компанія	Е
Низькі навички спілкування та комунікацій	Проєкт	І
Культурні різниці між співробітниками різних географічних локацій	Компанія	Е
Управління віддаленими командами	Проєкт	І
Різниця часових поясів	Компанія	Е
Календарна різниця в релігійних та національних святах	Компанія	Е
Координаційні подорожі	Компанія	Е
Слабка матеріальна база	Проєкт	І
Ненадійність ділових партнерів	Компанія	Е
Помилки в документації	Проєкт	І
Помилки проєктування	Проєкт	І
Недостатність кваліфікованого персоналу	Компанія	Е
Часті зміни вимог або технічного завдання	Проєкт	І
Збій апаратного і програмного забезпечення	Проєкт	І
Відсутність резервних копій даних	Проєкт	І
Виникнення незапланованих робіт та поява непередбачуваних витрат	Проєкт	І

В управлінні проєктом, в контексті управління ризиками, проєктний менеджер має мінімальні можливості управляти чи пом’якшувати або уникати

ризик (загрозу) галузевого рівня, в більшості випадків використовуючи підхід ухилення, якщо це можливо [19, 46]. Слід зазначити, що такими ризиками (можливостями) галузевого рівня потрібно вміло користуватися.

Якщо аналізувати необхідність та типову класифікацію ризиків для IT-проєктів, можна зробити висновок, що є потреба у адаптації класичного SWOT-аналізу, з урахуванням того, що ризики проєкту можуть представляти собою як загрозу, так і можливість, а також їх подальшого цільового використання.

Для кожного проєкту можна розділяти ризики на внутрішні можливості – Risks Internal Opportunities (RIO) та внутрішні загрози – Risks Internal Treats (RIT), зовнішні можливості – Risks External Opportunities (REO) та зовнішні загрози – Risks External Treats (RET) (рис. 2.3.).

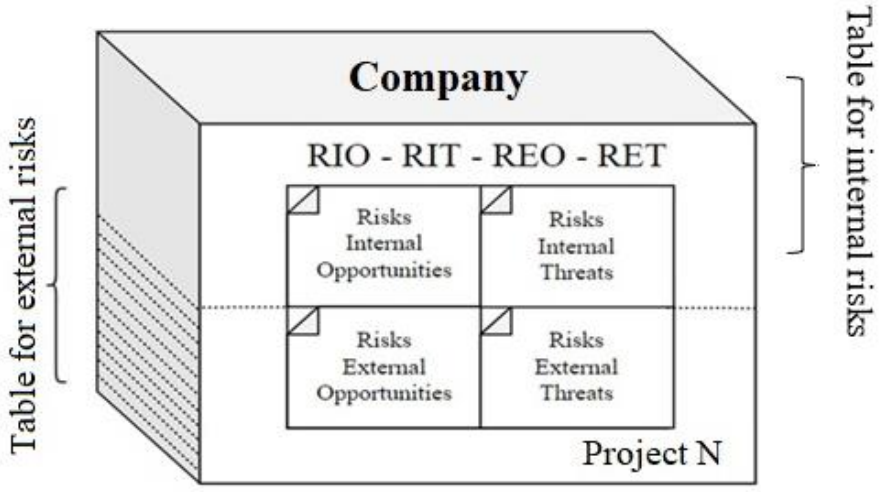


Рисунок 2.3. - RIO – RIT – REO – RET – аналіз

В такому випадку, зовнішні загрози та можливості (REO-RET) в цілому потенційно представляють цінність не лише для управління кожним проєктом компанії, але й для управління компанією чи організацією загалом.

Коли внутрішні загрози та можливості (RIO-RIT) є цінними в більшій мірі у ході перебігу проєкту та представляють собою історичні дані після закриття проєкту та можуть бути використані при ініціалізації наступного проєкту

схожого типу у подальшому [48]. Тому результати такого комплексного аналізу (RIO-RIT-REO-RET-аналіз) можуть бути використані як для проєкту, портфелю, так і для програм та управлінні компаній або організацій в цілому.

2.3.2. Таргетна модель інтегрованого управління ризиками в IT-проєктах

Існує велика різноманітність моделей управління ризиками, які допомагають досягти успіху проєкту [13, 48]. Однак у будь-якому проєкті є можливості для вдосконалення. Тому було вирішено дослідити комплексну природу ризиків, як загроз, так і можливостей, і використати підхід для таргетних моделей, що застосовуються до управління ризиками за аналогією з медициною. Таргетні моделі концепції інтегрованого управління ризиками виникли з таргетної терапії для лікування раку в медицині [49]. Кожен ризик, незалежно від того, чи це загроза, чи можливість, слід ранжувати та розмістити в таргетній моделі для кожного обмеження проєкту, щоб обчислити загальний ризик для кожного обмеження проєкту та прийняти рішення для управління проєктом.

Аналогія медицини та управління проєктами була встановлена в різних документах. Автори мають класифікацію відхилень на основі «хвороб» від загроз у проєктах, які побудовані за аналогією з класифікацією хвороб у медицині [50, 51, 52]. Також розроблено модель, яка дозволяє оцінити відносні та абсолютні синергетичні ефекти відхилень від загроз і можливостей у проєкті та загальний синергетичний ефект між загрозами та можливостями в IT-проєкті [36, 51]. Автор має певні аналогії між управлінням проєктами та медициною, а також особливості управління відхиленнями в проєктах, які допускають такі аналогії [53].

Класичний ризик-менеджмент визначає ризик як невизначену подію або стан, якщо воно відбувається, позитивно чи негативно впливає на цілі проєкту [19, 54]. Це твердження можна описати наступною формулою (2.5):

$$R_i = \sum_{i=1}^{n} P_i \cdot V_i \,, \tag{2.5}$$

де R_i – ризик у проєкті;

P_i – ймовірність виникнення ризику, що вимірюється від 0 до 1;

V_i – значення ефекту або впливу ризику на проєкт;

i – значення від 1 до n;

n – кількість ризиків у проєкті.

Відповідно до [19, 55], визначення ризику проєкту також охоплює невизначені події, які можуть мати негативний вплив на цілі проєкту, а також ті, що можуть мати позитивний ефект. Ці два типи ризиків називаються відповідно загрозами та можливостями. Важливо розглядати як загрози, так і можливості в рамках управління ризиками. Таке управління ризиками дозволяє досягти синергії та ефективності, наприклад розглядати обидва в одному аналізі та координувати відповіді на обидва, якщо вони збігаються або можуть посилювати один одного [52, 53, 55, 71]. Ось чому важливо розрізняти загрози та можливості в управлінні та прогнозуванні проєкту, природа яких може накладатися та посилювати одна одну та результати проєкту в цілому (2.6).

$$R = \{D; C\}, \tag{2.6}$$

де D – загрози проєкту;

С – можливості проєкту.

Кожен проєкт можна виміряти цілями проєкту або його обмеженнями. Обмеженнями проєкту є бюджет, час або строки, обсяг та якість [19, 55, 56].

Вони є найважливішими в управлінні проєктом та можуть допомогти керувати поточним статусом проєкту та повідомляти про нього. Таким чином, беручи до уваги важливість обмежень для успіху проєкту, будемо вважати, що кожен ризик або можливість впливає на кожне обмеження. Тому він має відповідний компонент, який показує вплив ризику на обмеження. Такий складний характер загрози та можливості можна представити формулами (2.7) та (2.8).

$$D_j = \sum_{j=1}^{m} P_{jd} \cdot \left(V_{jdb} + V_{jdt} + V_{jds} + V_{jdq} \right),$$

$$C_i = \sum_{i=1}^{n} P_{ic} \cdot \left(V_{icb} + V_{ict} + V_{ics} + V_{icq} \right), \qquad (2.8)$$

де j – значення від 1 до m;

m – кількість загроз у проєкті;

D_j – j-та загроза у проєкті;

P_{jd} – ймовірність появи j-ої загрози від 0 до 1;

V_{jdb} – значення впливу j-ої загрози на бюджет від -10 до 0;

V_{jdt} – значення впливу j-ої загрози на час або графік від -10 до 0;

V_{jds} – значення впливу j-ої загрози на обсяг від -10 до 0;

V_{jdq} – значення впливу j-ої загрози на якість від -10 до 0;

i – значення від 1 до n;

m – кількість можливостей у проєкті;

C_i – i-та можливість у проєкті;

P_{ic} – ймовірність появи i-ої можливості від 0 до 1;

V_{icb} – значення впливу i-ої можливості на бюджет від 0 до 10;

V_{ict} – значення впливу i-ої можливості на час або розклад від 0 до 10;

V_{ics} – значення впливу i-ої можливості на обсяг від 0 до 10;

V_{icq} – значення впливу i-ої можливості на якість від 0 до 10.

Усі значення (P_{jd}, P_{ic}, V_{jdb}, V_{jdt}, V_{jds}, V_{jdq}, V_{icb}, V_{ict}, V_{ics}, V_{icq}) для загроз та можливостей визначаються за допомогою застосування експертних оцінок.

Управління проєктами в галузі розробки програмного забезпечення вимагає більш складних інструментів і методів у кожній області для успішного досягнення цілей проєкту на конкурентному ринку. Правильно організовані сфери управління проєктами допомагають представити компанію на ринку, продавати продукти та послуги, покращувати вихідні результати проєктів і відповідно збільшувати дохід компанії [36]. Тому необхідно досліджувати нові підходи до покращення результатів ІТ-проєктів з урахуванням комплексного характеру цілей проєкту з точки зору комплексного управління ризиками (2.7) та (2.8).

Виходячи із (2.7), автором виявлено загрози, які пов’язані з ІТ-проєктом, результати наведено у табл. 2.2.

Таблиця 2.2. Виявлені загрози ІТ-проєктів

№, j	Ризики – загрози	P_{jd}	V_{jdb}	V_{jdt}	V_{jds}	V_{jdq}
1	2	3	4	5	6	7
1	Поява на ринку альтернативного продукту або нової більш відповідної технології	0.8	-9	-10	-4	0
2	Конфлікти між цілями проєкту та інтересами відділів	0.7	-9	-10	-5	-5
3	Конфлікти між зацікавленими сторонами та учасниками проєкту	0.5	-3	-7	-6	-3
4	Велика кількість одночасних питань і змін в проєкті	0.5	-8	-10	-4	-7
5	Відсутність управління змінами в проєкті	0.5	-10	-10	-10	-5
6	Відсутність управління ризиками в проєкті	0.5	-9	-7	-7	-9
7	Зміна клієнтів, спонсорів або зацікавлених сторін	0.2	-5	-1	-1	-9
8	Недостатня підтримка з боку вищого керівництва	0.1	10	-1	-1	0
9	Недотримання термінів в проєкті	0.4	0	-10	-1	0

Продовження табл. 2.2.

1	2	3	4	5	6	7
10	Негнучке трудове законодавство та зміни податкового законодавства можуть значно зменшити заощадження	0.5	-10	-5	0	0
11	Порушення безпеки або конфіденційності	0.5	-10	-9	0	-7
12	Політична нестабільність всередині країни	0.5	-10	-9	0	0
13	Оборот рідкісних ресурсів розробників	0.5	-10	-10	0	-9
14	Вигорання співробітників	0.6	-3	-10	0	-10
15	Низькі комунікативні навички, слабкі інформаційні зв'язки в проєкті	0.4	-3	-8	-1	-10
16	Різниця в часових поясах	0.6	-8	-10	-1	-3
17	Проблеми в документації, дизайні та специфікаціях	0.4	-9	-8	-7	-10
18	Часті зміни обсягу та стратегії проєкту	0.3	-10	-10	-10	-7
19	Збій апаратного та програмного забезпечення	0.2	-6	-8	-1	-4
20	Блокувальники з третьої сторони	0.7	-2	-10	0	-6

Базуючись на концепції таргетної терапії в медицині, де це вид лікування раку, який використовує ліки або інші речовини для точної ідентифікації та атаки певних типів ракових клітин [49], пропонується провести аналогію з управлінням ризиками та медицини [13, 49, 52]. Результати якої наведено у табл. 2.3.

Таблиця 2.3. Запропонована аналогія між таргетною терапією та управлінням ризиками

Медицина	Управління ризиками
Ракова клітина	Загроза
Здорова клітина	Можливість
Наркотики та психоактивні речовини	Реакція на ризик
Лікування	Управління
Частина тіла або орган	Обмеження проєкту (наприклад, бюджет, час, обсяг і якість)

Де цільові моделі для загроз і можливостей будуються для кожного обмеження, показуючи ступінь впливу ризику для кожного обмеження. Побудова таких таргетних моделей допомагає керівнику проєкту виділити основні напрямки проєкту з загрозами або можливостями. Таким чином, керівник проєкту може оцінити найнебезпечнішу або найприбутковішу та успішну сторону проєкту та підготувати найкраще лікування чи відповідь на ризик залежно від інших трагетних моделей. Ця інформація може допомогти управляти проєктом і досягти успіху проєкту залежно від потреб клієнтів або зацікавлених сторін.

Беручи до уваги аналогію, управління загрозами буде проведено в термінах таргетних моделей за кожним обмеженням проєкту: бюджет, час, обсяг і якість (рис. 2.4. – 2.7.). Де вони можуть бути описані відповідними формулами (2.9) – (2.12) на підставі (2.7) з урахуванням (2.5):

$$D_b = \sum_{j=1}^{m} P_{jd} \cdot V_{jdb} = -65.6\,, \tag{2.9}$$

$$D_t = \sum_{j=1}^{m} P_{jd} \cdot V_{jdt} = -82.8\,, \tag{2.10}$$

$$D_s = \sum_{j=1}^{m} P_{jd} \cdot V_{jds} = -27.9\,, \tag{2.11}$$

$$D_q = \sum_{j=1}^{m} P_{jd} \cdot V_{jdq} = -48.2\,, \tag{2.12}$$

Порівнюючи D_b, D_t, D_s та D_q, керівник проєкту міг би оцінити, яка область є більш ризикованою та вимагає додаткових дій і управління, див. рис. 2.8.

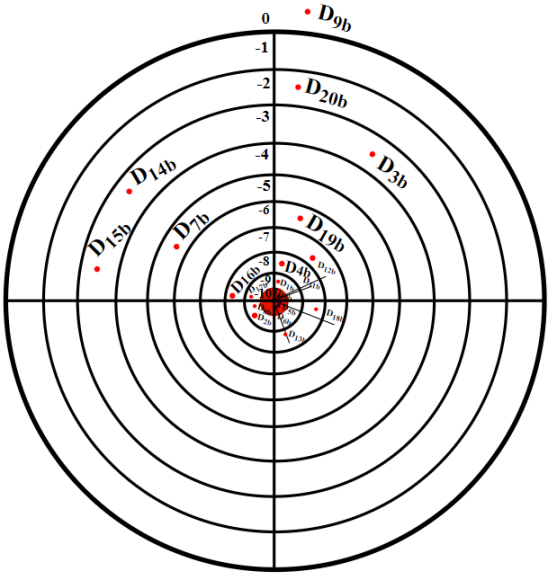


Рисунок 2.4. – Таргетна модель для загроз з впливом на бюджет ас

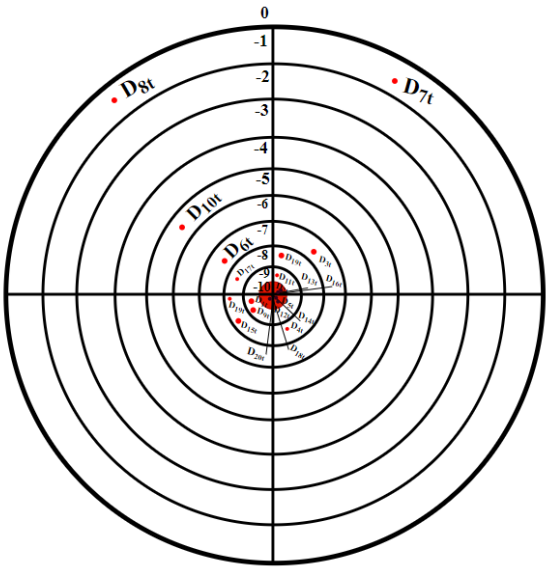


Рисунок 2.5. – Таргетна модель для загроз з впливом на час

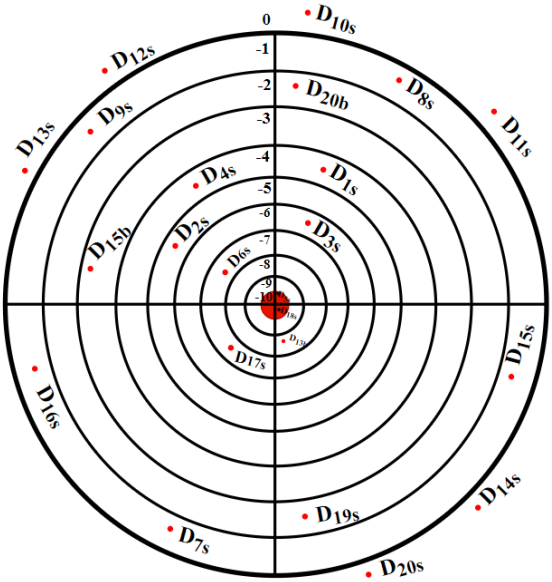


Рисунок 2.6. – Таргетна модель для загроз з впливом на обсяг

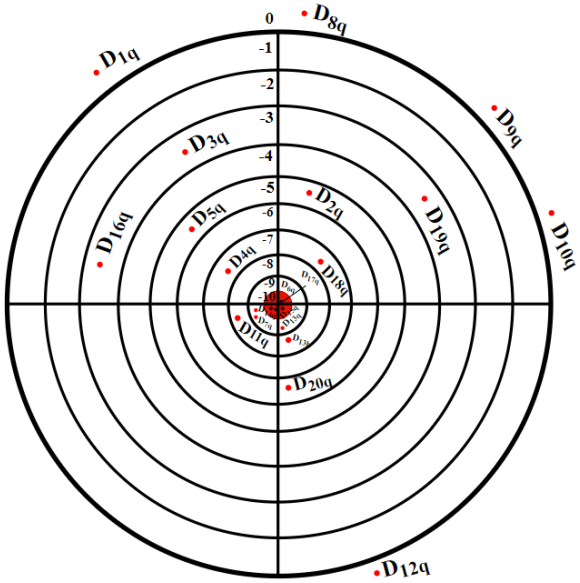


Рисунок 2.7. – Таргетна модель для загроз з впливом на якість

Графік проєкту найбільше страждає від загроз, які означають, що очікувані терміни виконання доставки не можуть бути дотримані своєчасно. Тоді бюджет проєкту може бути збільшений через вплив загрози, якщо не буде відповіді на ризик або необхідних дій. У той час як якість і обсяг досить стабільні та на них не впливають загрози проєкту. Час і бюджет є найважливішим обмеженням для

всіх проєктів [48, 54]. Будь-яка зміна чи загроза впливає на бюджет проєкту, питання лише в якій мірі.

Поряд із загрозами завжди існують можливості, якими повинен ретельно керувати керівник проєкту, отримуючи від них усі вигоди, основні можливості проєкту, виявлені експертами, наведені у табл. 2.4.

Таблиця 2.4. Виявлені можливості ІТ-проєктів

№, і	Ризики – можливості	P_{ic}	V_{icb}	V_{ict}	V_{ics}	V_{icq}
1	2	3	4	5	6	7
1	Поява на ринку альтернативного продукту або нової більш відповідної технології	0.8	8	7	3	1
2	Нові зв'язки з цілями проєкту та інтересами відділів	0.7	1	8	2	2
3	Міцні стосунки із зацікавленими сторонами та учасниками проєкту	0.8	1	9	1	9
4	Вигідні зміни в проєкті	0.7	8	7	10	4
5	Сильне управління змінами в проєкті	0.8	5	9	10	1
6	Сильне управління ризиками в проєкті	0.7	6	8	7	5
7	Клієнтам, спонсорам або стейкхолдерам вигідна зміна	0.7	5	2	4	1
8	Достатня і потужна підтримка з боку вищого керівництва	0.3	10	2	1	1
9	Дотримання термінів в проєкті	0.8	5	10	0	8
10	Гнучке трудове законодавство та зміни податкового законодавства	0.4	10	10	1	1
11	Надійна безпека або дотримання конфіденційності	0.6	8	10	3	10
12	Політична стабільність в країні та підтримка ІТ-сфери	0.5	10	10	1	4
13	Успішне збереження рідкісних ресурсів розробників	0.5	10	8	1	10
14	Задоволені працівники	0.5	5	10	0	10

Продовження табл. 2.4.

1	2	3	4	5	6	7
15	Професійні комунікативні навички, чудові інформаційні зв'язки в проєкті	0.5	5	10	0	10
16	Різниця в часових поясах, яка допомагає скоротити тривалість проєкту	0.4	8	10	7	1
17	Чітка документація, дизайн і технічні характеристики	0.6	5	10	4	10
18	Стабільний обсяг і стратегія проєкту	0.4	9	10	10	8
19	Надійність апаратного та програмного забезпечення	0.8	8	10	0	9
20	Швидка відповідь з третьої сторони	0.5	7	10	0	10

Підрахунок можливостей обмежень проєкту за допомогою відповідних формул (2.13) – (2.17):

$$C_b = \sum_{i=1}^{n} P_{ic} \cdot V_{icb} = 75.7\,, \tag{2.13}$$

$$C_t = \sum_{i=1}^{n} P_{ic} \cdot V_{ict} = 102.1\,, \tag{2.14}$$

$$C_s = \sum_{i=1}^{n} P_{ic} \cdot V_{ics} = 40\,, \tag{2.15}$$

$$C_q = \sum_{i=1}^{n} P_{ic} \cdot V_{icq} = 69.1\,, \tag{2.16}$$

Порівнюючи можливості основних обмежень, ми можемо побачити (2.17):

$$C_t > C_b > C_q > C_s\,, \tag{2.17}$$

Знову ж таки, одна з найбільш ризикованих сфер – своєчасність – повна можливостей. Це свідчить про те, що час і графік є найважливішою сферою управління проєктом для керівника проєкту з усіх точок зору. Перш за все, всіх замовників і стейкхолдерів цікавлять терміни та бюджет, а вже потім перевірятимуть, запитуватимуть та узгоджуватимуть обсяг й якість. Ці області є основними для кожного проєкту і спочатку використовуються для управління проєктом. Неможливо уявити керівника проєкту, який не використовує розклад для щоденних справ, як замовника, який не піклується про свій бюджет.

Можливості управління будуть розраховані на таргетні моделі за кожним обмеженням проєкту: бюджет, час, обсяг та якість, див. рис. 2.8 – 2.11.

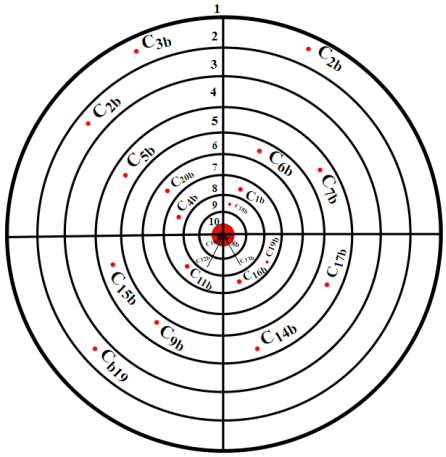


Рисунок 2.8. - Таргетна модель для можливостей з впливом на бюджет

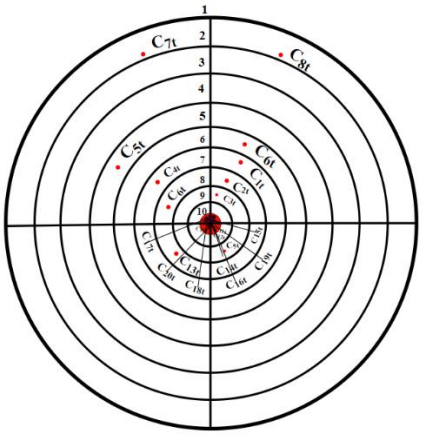


Рисунок 2.9. - Таргетна модель для можливостей з впливом на час

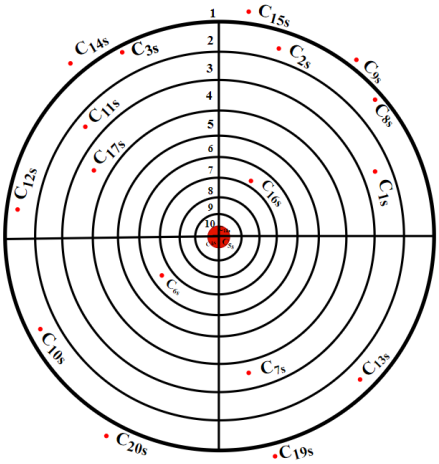


Рисунок 2.10. - Таргетна модель для можливостей з впливом на обсяг

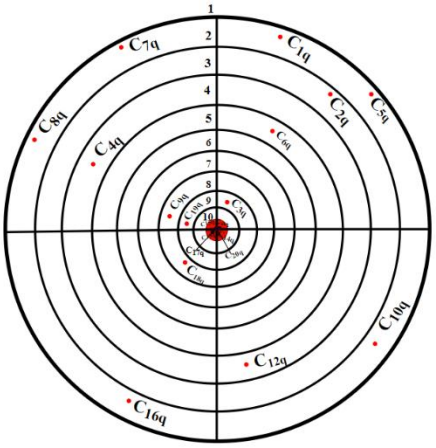


Рисунок 2.11. - Таргетна модель для можливостей з впливом на якість

Аналогія з медициною та управлінням проєктами може допомогти створити новий альтернативний підхід до управління ризиками проєкту, як загрозами, так і можливостями. На основі таргетної моделі інтегрованого управління ризиками, часовий графік (рис. 2.5 та 2.10) і бюджет (рис. 2.4 та 2.9), обмеження, які формують відповідну область проєкту, є найбільш чутливими і вимагають належного управління. Вони водночас найбільш ризиковані та сповнені можливостей, які можуть призвести до запланованого результату проєкту та принести певні переваги проєкту. За допомогою графіків таргетних моделей і обчислених даних керівник проєкту може прийняти швидке і точне рішення, яке відповідає початковим обмеженням проєкту.

2.3.3. Інтелектуальна модель вибору оптимальної стратегії управління ризиковими подіями: загрозами та можливостями

Процес побудови моделі оптимізації може бути розділений на три підпроцеси, кожний з яких може бути реалізований окремим модулем інтелектуальної рекомендаційної системи. Ці підпроцеси полягають у оцінці ризикової події, виборі критеріїв оптимізації та побудові можливих сценаріїв, виборі оптимального сценарію поведінки.

До основних блоків побудови інтелектуальної моделі можна віднести (рис. 2.12.) [57, 58, 59]:

1. Створення методів ідентифікації ризику як для загрози, так і для можливостей. Визначення класифікаційних ознак та віднесення ризикової події до відповідної категорії.
2. Кількісна та якісна оцінка ризику з визначенням ступеню впливовості. Визначення критеріїв, за якими проводиться аналіз ризикової події. Визначення критеріїв взаємного впливу (синергії) ризикових подій.
3. Приведення до єдиної шкали вимірювання критеріїв оцінки ризику.

4. Визначення мети управління ризиком, яка дозволить сформулювати стратегії поведінки при управлінні ризиком. Визначення можливих сценаріїв реагування на ризикову подію у відповідності до мети управління.

5. Вибір оптимальної стратегії поведінки для нівелювання впливу загрози чи розвитку можливості.

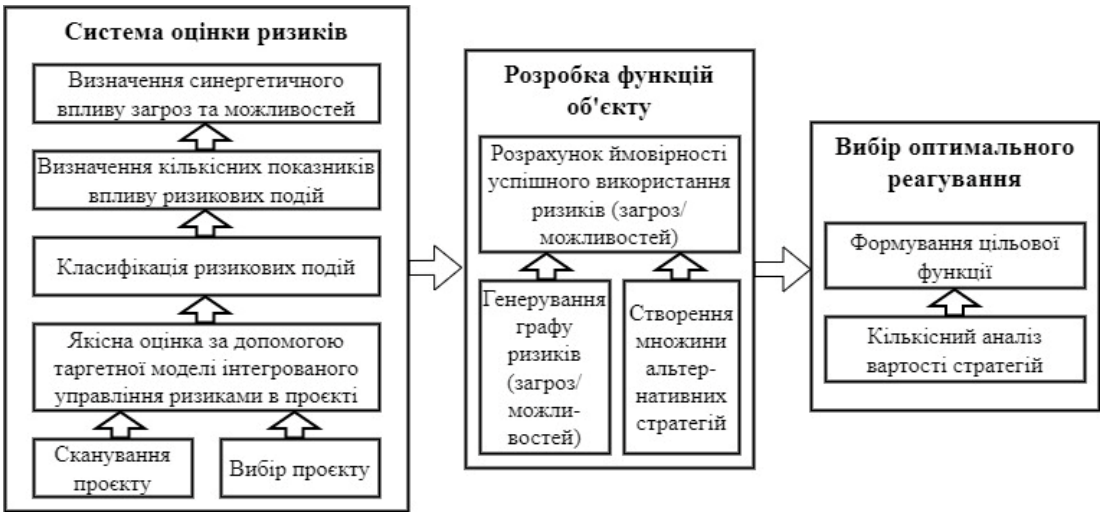


Рисунок 2.12. - Схема компонентів інтелектуальної моделі вибору оптимальної стратегії управління ризиковими подіями

Проаналізуємо кожний з процесів:

1) Оцінка ризикової події. На цій стадії виконується ідентифікація ризику, визначаються якісні характеристики ризикової події, за цими характеристиками подія класифікується як загроза або можливість, визначаються кількісні характеристики ризикової події, визначається взаємний вплив подій (синергія) на розвиток проєкту, виконується нормалізація критеріїв впливу;

2) Побудова цільової функції та можливих сценаріїв розвитку подій. Будується байєсовий граф можливого розвитку проєкту (сценарію) на основі історичної інформації для аналогічних подій у аналогічних проєктах, та інформації про наявні активи та ресурси. Формується набір альтернативних сценаріїв розвитку проєкту. Визначається критерій оптимальності, а саме обчислюється вигода від реалізації можливості і величина можливих втрат при загрозі.

3) Вибір оптимальної стратегії управління ризиковою подією. Реалізується алгоритм оптимізації, знаходиться оптимальний розв'язок для цільової функції за допомогою інтелектуальних алгоритмів, таким чином визначається оптимальний сценарій реагування на ризикову подію [54, 57, 60].

Беручи до уваги комплексний характер ризиків, як загроз, так і можливостей, та використовуючи підхід для цільових моделей кожен ризик, незалежно від того, чи це загроза, чи можливість, слід ранжувати та розмістити в цільовій моделі для кожного обмеження проєкту, щоб обчислити загальний ризик для кожного обмеження проєкту та прийняти рішення щодо вибору оптимальної стратегії.

Комплексний характер загрози та можливості можна представити наступними формулами (2.7) та (2.8) [53, 57, 58].

Розрахунок відносного синергетичного ефекту буде розглянуто більш детально у підрозділі 2.4. цього дисертаційного дослідження.

Для визначення найбільшої вирогідності розвитку тієї чи іншої ризикової події нам необхідно вирішити завдання колаборативної фільтрації. Для цього будемо створювати модель, яка буде визначати вирогідність розвитку того чи іншого сценарію на основі даних попередньої оцінки ризокової події. При цьому слід враховувати одночасно і поточну оцінку особи, що приймає рішення, і (за можливості) оцінку, отриману з попереднього досвіду з аналогічними проєктами.

Завдання колаборативної фільтрації можливо формалізувати у вигляді матриці, де кожний рядок відповідає оцінці, а стовпчик ризиковій події. Дані будуть складатися з множин $(k, b, r_{k,b})$, де k – комплексна оцінка ризику, b – ризикова подія, $r_{k,b}$ – рейтинг ризикової події відповідно до її оцінки. Вирішення завдання полягає у передбаченні невідомих елементів матриці, а саме тих елементів, які з найбільшою ймовірністю за можливими оцінками можуть виникнути.

Метод колаборативної фільтрації має ряд недоліків, які дозволить вирішити поєднання оцінок, отриманих від експертів на всіх етапах

ідентифікації та оцінки ризикової події, та оцінок, отриманих з попереднього досвіду в аналогічних проєктах. До найбільш значних недоліків колаборативної фільтрації слід віднести наступні:

- матриця рейтингів є дуже розрідженою, оскільки не всі ризикові події отримують адекватну оцінку, тому серед ризикових подій залишаються ті, які не мають відповідної оцінки.
- також існує проблема «холодного старту». Це проблема, коли виникає ризикова подія, яка не була попередньо ідентифікована і оцінена. В цьому випадку допомагає метод аналогій, який дозволяє надати ризиковій події оцінку найбільш подібної події досвіду виконання попередніх проєктів.

Таким чином, використання моделей, викладених у попередніх розділах, а також база попереднього досвіду дозволяє сформулювати систему правил для бази знань, що використовується під час колаборативної фільтрації.

Головним інструментом у даному випадку буде теорема Баєса:

$$\rho(\theta|D) = \frac{\rho(\theta)\rho(D|\theta)}{\rho(D)}, \tag{2.18}$$

де D — це відомі дані, рейтинги ризикових подій;

θ — це параметри моделі, яку ми бажаємо навчити;

$\rho(\theta|D)$ — це апостеріорна вирогідність, тобто розподіл вирогідностей параметрів моделі з урахуванням даних. Ризикові події не мають законів розподілу, тому, як правило, апостеріорну вирогідність необхідно знати;

$\rho(D|\theta)$ – вирогідність даних за умови зафіксованих параметрів моделі або так звана правдоподібність;

$\rho(\theta)$ — апріорна вирогідність, математична формалізацією знань про ризикову подію.

Таким чином, основне завдань байєсівського висновку - знайти апостеріорний розподіл на гіпотезах/параметрах: $\rho(\theta|D) \propto \rho(D|\theta)\ \rho(\theta)$ і знайти максимальну апостеріорну гіпотезу $\arg\max_{\theta} \rho(\theta|D)$.

Проблема полягає в тому, що отримуємо надто складні розподіли зазвичай, які складно максимізувати аналітично, оскільки між дуже багатьма змінними існують дуже складні зв'язки. Але при цьому у деяких випадках між ризиковими подіями відсутні зв’язки, тому для їх опису можемо використовувати структуру у вигляді незалежності $\rho(x, y) = \rho\ (x)\rho(y)$. У випадку слабких зв’язків можемо використовувати умовну незалежність $\rho(x, y|z) = \rho\ (x|z)\rho(y|z)$.

Для визначення можливих стратегій розвитку ризикової події будується баєсовий граф - це спрямований граф без спрямованих циклів, в якому вершини відповідають змінним у розподілі, а ребра з'єднують «пов'язані» змінні. У кожному вузлі заданий умовний розподіл вузла за умови своїх батьків. Байесів граф складається з елементарних графів, що означає, що великий спільний розподіл розкладається на добуток цих умовних розподілів.

В ідеальному випадку, який реалізує наявний Баєсів класифікатор, Баєсів граф буде мати вигляд рис. 2.13.

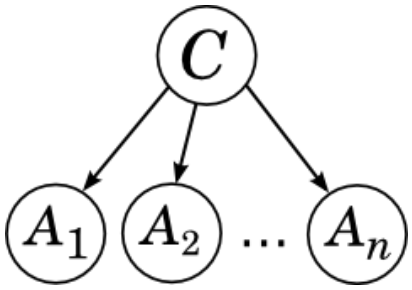


Рисунок 2.13. - Граф, що реалізує наївний класифікатор Баєса

У цьому подія С є батьківською і незалежною, тобто це безумовне розподілення $\rho(A_1, \dots, A_n, C) = \rho\ (C)\rho(A_1|C)\rho(A_2|C) \dots \rho(A_n|C)$. Подію С можна розкласти на незалежні події A_n. Всі атрибути A_i умовно незалежні при умові відповідності категорії С: $\rho\left(A_i, A_j\middle|C\right) = \ \rho(A_i|C)\rho\left(A_j\middle|C\right)$.

Між ризиковими подіями можуть бути зв’язки різних типів.

Розглянемо їх.

Послідовний зв’язок відображає послідовність, коли подія x впливає на подію y, а та, у свою чергу, впливає на подію z.

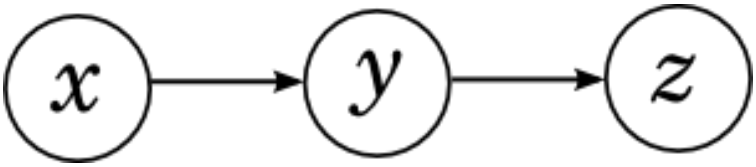


Рисунок 2.14. - Послідовний зв’язок

Формально це відповідає умовній незалежності x та z за умови y

$$p(x,z|y) = \frac{p(x,y,z)}{p(y)} = \frac{p(x)p(y|x)p(z|y)}{p(y)} = p(x|y)p(z|y), \quad (2.19)$$

де перше рівність – це визначення умовної ймовірності, друге – наше розкладання, а третє – застосування теореми Байєса.

Розбіжний зв'язок – зв'язок, коли x «впливає» і на y, і на z.

Такий граф зображує розкладання

$$p(x,y,z) = p(x)p(y|x)p(z\,|x) \quad (2.20)$$

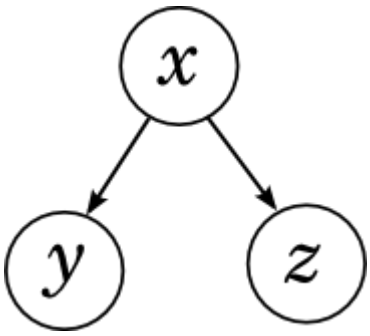


Рисунок 2.15. - Розбіжний зв’язок

Формально це відповідає умовній незалежності y та z при

$$p(y,z|x) = \frac{p(x,y,z)}{p(x)} = \frac{p(x)p(y|x)p(z|x)}{p(y)} = p(y|x)p(z|x) \quad (2.21)$$

При розбіжному зв'язку між трьома змінними «наслідки» умовно незалежні за умови своєї «загальної причини». Якщо причина відома, то

наслідки стають незалежними. Саме причина забезпечує наслідки, наслідки пов’язані саме через неї.

Збіжний зв'язок – зв'язок, що сходиться, коли x і y разом «впливають на» z.

$$p(x,y,z) = p(x)p(y)p(z\,|x,y) \tag{2.22}$$

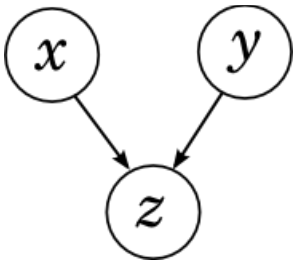


Рисунок 2.16. - Збіжний зв’язок

Це ситуація, в якій у того самого наслідку можуть бути дві різні причини.

Поки загальний наслідок невідомий, дві причини ніяк не пов'язані одна з одною

$$p(x,y) = \sum_z p(x,y,z) = \sum_z p(x)p(y)p(z|x,y) = p(x)p(y) \tag{2.23}$$

Таким чином, при збіжному зв'язку дві «причини» незалежні, але тільки доти, поки значення їх «загального наслідку» невідоме, якщо ж загальний наслідок отримує означення, причини стають залежними.

Байєсовий граф розвитку подій (сценарій) у загальній формі є направленим ациклічним графом, який можна задати як (2.24) [57, 58, 61]:

$$BAG = (S, E, A, P), \tag{2.24}$$

де $S = \{S_1, S_2, \ldots, S_n\}$ – множина вузлів всіх атрибутів графу;

$E = \{\ldots, E_{ij}, \ldots\}$ – множина всіх направлених ребер графу, де E_{ij} має два кінцевих вузла E_i та E_j, причому S_i – батьківський вузол, а S_j – дочірній вузол.

$A = \{A_1, A_2, \ldots, A_n\}$ – визначає альтернативи розвитку подій. A_1 = 1 означає, що альтернатива існує, інакше A_i = 0.

$P = \{P(S_1), P(S_2), \ldots, P(S_n)\}$ – множина ймовірностей того, що ризикова подія може виникнути на даному етапі. $P(S_i)$ визначає ймовірність успіху у проходженні ризикової події вузла атрибута S_i.

На байєсовий граф наноситься інформація про наявні активи та ресурси, яка дозволяє визначити критерій оптимальності. Критерій оптимальності є адитивним та характеризує вигоду від реалізації можливості і величину можливих втрат при загрозі.

Розрахунок ймовірності настання ризикової події відбувається з урахуванням індикаторів (2.25):

$$P(S_i) = V \cdot C \cdot U \,, \qquad (2.25)$$

де V – швидкість впливу (вплив ризикової події на короткому відрізку часу проєкту);

C – складності (характеризує собою рівень складності наслідків впливу);

U – аутентифікації ризикової події як загрози чи можливості.

Значення вказаних індикаторів, отриманих в результаті проведення серії експериментів, наведені у табл. 2.5.

Таблиця 2.5. Ідентифікатори

Індикатор	Рівень	Значення
V	висока	1
	середня	0,5
	низька	0
C	висока	1
	середня	0,5
	низька	0
U	загроза	1/0
	можливість	1/0

A є набором альтернативних сценаріїв розвитку подій, позначається як $A=\{A_1, A_2, \ldots, A_n\}$, де A_i – кожний окремий сценарій розвитку подій, який може бути реалізований на вузлі атрибуту S_i A_i = 1 означає, що стратегія буде реалізовуватися, у іншому випадку $A_i = 0$.

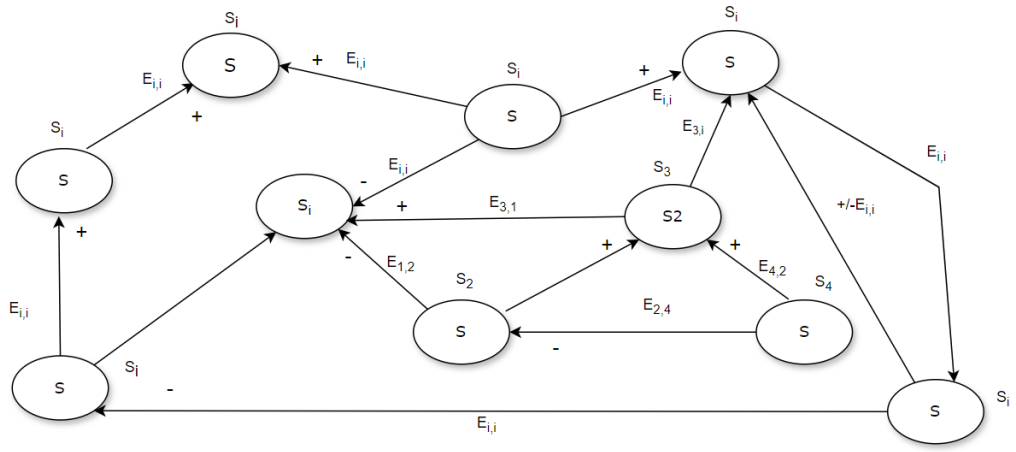


Рисунок 2.17. - Приклад можливого графа

Реалізація стратегій неминуче спричиняє витрати на запобігання загрозам та/чи реалізацію можливостей.

Вартість можна визначити множиною (2.26) [57, 62]:

$$COST = \{COST_1, COST_2, \ldots, COST_n\}, \tag{2.26}$$

де $COST_i$ – вартість реалізації стратегії A_i. Вартість кожної альтернативи можна визначити як (2.27):

$$COST_i = \omega_i \cdot value \cdot 100, \tag{2.27}$$

де ω_i – нормалізована вага стратегії, її значення вимірюється значенням активу.

Таким чином, загальні витрати на реалізацію стратегій $A=\{A_1, A_2, \ldots, A_n\}$ можна визначити за формулою (2.28):

$$C(A)=\sum A_i \cdot COST_i, \text{ де } i = 1. \quad (2.28)$$

Вигоду від реалізації можливості атрибуту S_i можна визначити як (2.29):

$$AG(S_i)=P(S_i)\cdot value. \quad (2.29)$$

Крім того, перевагу атрибуту при реалізації альтернативи стратегії можна визначити як (2.30):

$$AG(S_i|A)=P(S_i|A)\cdot value. \quad (2.30)$$

Таким чином, реалізація всіх можливих стратегій забезпечення можливостей (2.31) [57, 63]:

$$AG(M)=\sum S_i \in SAG(S_i|M). \quad (2.31)$$

Оскілки, у невеликих ІТ-проєктах втрати від загроз можуть значно переважати вигоди від можливостей, та їхня спільна реалізація може викликати конкуренцію у використанні ресурсів, то доцільно використати обережний підхід та заощадливо використовувати ресурси. Таким чином, пропонуємо мінімізувати як вигоду від можливостей, так і вартість витрат при загрозах [57, 64]. Цільова функція може бути визначена (2.32):

$$\min_{C(A)<B} \delta AG(A)+(1-\delta)C(A), \quad (2.32)$$

де δ та 1 – δ – вагові коефіцієнти переваги вигоди від можливості і вартість запобігання загрозі відповідно, та $0 \le \delta \le 1$; B – обмеження загальної вартості.

Запропоновано розглядати управління ризиковими подіями для невеликих ІТ-проєктів, як задачу оптимізації, що дозволяє виконувати вибір оптимальної стратегії управління ризиками, як загрозами, так і можливостями з урахуванням

їх синергетичного ефекту, вигоди від можливостей та мінімізації вартості витрат при загрозах та при обмежених наявних ресурсах проєкту. Розроблена інтелектуальна модель враховує складну природу ризику, зокрема загрози та можливості, яка впливає на основні обмеження проєкту, що призводить до проактивного та ефективного управління проєктами. Використання запропонованого підходу дозволить динамічно управляти нетиповими маломасштабними ІТ-проєктами, що не забезпечуються адекватною підтримкою при використанні стандартного програмного забезпечення для управління проєктами від світових лідерів.

Інтелектуальна модель забезпечує декомпозицію процесу на три підпроцеси, вона враховує графи розвитку подій, синергію можливих загроз та можливостей. Вибір оптимального рішення забезпечується оптимізацією витрат, для яких запропоновано критерії, цільову функцію. Застосовується розподіл загроз та можливостей у вигляді розробленої таргетної моделі за введеними вагами загроз та можливостей на основі експертних оцінок. Враховується як вартість реалізацій стратегій, так і загальні витрати на їх реалізацію, використовується обережний підхід до заощадливого використання ресурсів, що дозволяє балансування вигоди від реалізації можливості та витрат від загрози при обмежених наявних ресурсах.

2.4. Математична модель управління загрозами та можливостями в ІТ-проєктах

Сучасний світ характеризується сталим розвитком технологій, програм та продуктів. Компанії, які забезпечують цей розвиток у відповідь на запит сьогодення, мають риси цілісних систем з різною структурою та ієрархією, яка забезпечується та підтримується різноманітними зв’язками. Підходи до управління такими компаніями та їх проєктами залежить як від зв’язків в середині компанії, так і від зовнішніх зв’язків. Відомі та широко використовуються стандарти щодо організації, управління та функціонування

таких систем та їх підсистем: Project Management Institute (PMI), International Organization for Standardization (ISO), Capability Maturity Model Integration (CMMI), International Project Management Association (IPMA), A Guidebook of Project and Program Management for Enterprise Innovation (P2M), Projects in Controlled Environments (PRINCE2) [48, 53]. Більшість з них базується на суто менеджерському підході та найкращих практиках проєктного, програмного та портфоліо рівнях управління, що за своє сутністю є переліком умов, яким необхідно слідувати організаціям, компаніям та проєктам.

Спираючись на таке уявлення, цілком очевидно, що ІТ-компанію необхідно розглядати як цілісну систему, а ІТ-проєкти як її виокремлені внутрішні підсистеми. Визначенню або підбору методів управління, моделюванню і прогнозуванню поведінки системи, в першу чергу повинно передувати визначення властивостей досліджуваної системи, її місце і роль відносно до інших відомих систем [53, 65].

З одного боку, ІТ-компанія є зовнішнім середовищем для ІТ-проєкта, в першу чергу через те, що вона забезпечує фінансування, надходження ресурсів, інформації та підтримки до проєкту. З другого боку і одночасно з цим, компанія є складною системою з внутрішніми зв`язками між підсистемами – її ІТ-проєктами. В цьому є єдність та протиріччя. Необхідно зазначити, що властивості ІТ-компанії як системи залежать від її бізнес-моделі. Виділяють наступні види ІТ-компанії у відповідності до реалізованих у них бізнес-моделях [53, 66]:

- продуктові;
- сервісні;
- аутсорсингові;
- аутстаффінгові;
- центри розробки;
- гібридні та інші.

Як вже зазначалося, сама ІТ-компанія є складною системою, функціонування якої забезпечується великою кількістю складних взаємозв’язків,

які в свою чергу залежать від багатьох чинників, таких як тип структури, кількість співробітників, ієрархія управління та інші. На рис. 2.14. представлена матрична структура організації, яка характеризується взаємодією операційного та проєктного пулів через вертикальну та горизонтальну ієрархією управління відповідно.

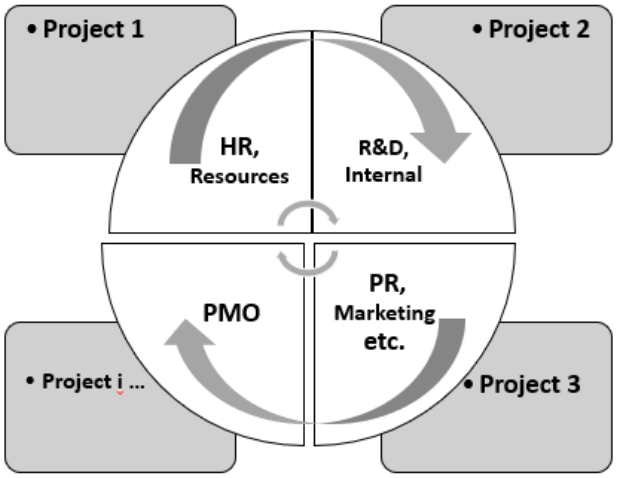


Рисунок 2.18. - Схема матричної структури IT-компанії або організації

Для успішного управління складними системами необхідно забезпечувати баланс між підсистемами. Через те, що досить часто виділяються найсильніші та найслабкіші ланки, потрібно врівноважувати дисбаланс розумним управлінням. Таким чином, використання ефекту синергізму є досить актуальним питанням для ефективного управління компаніями та проєктами.

Синергізм – в перекладі з грецької «той, що діє разом; співпраця». Одним з найголовніших принципів синергізму є взаємно-підсилююча дія декількох підсистем, що збільшує впорядкованість системи в цілому. Створення складної структури відбувається за рахунок трансформації простих узгоджених елементів, що є її складовими. Як результат отримується зростання ефективності діяльності, тобто виникає синергетичний ефект – сумарна віддача капіталовкладень організації стає більшою, ніж сума показників віддачі від кожного окремого напрямку [53, 67, 68, 71].

Управління ризиками з урахуванням загроз та можливостей – це вагома та добре досліджена частина управління проєктами, яка сформована та представлена в усіх стандартах проєктного менеджменту. Однак не так багато уваги в стандартах приділяється управлінню можливостями, що не задовольняє потребу IT-компаній у визначенні та використанні можливостей для досягнення цілей проєкту в умовах конкурентного ринку. Підходи до управління можливостями описано в IPMA ICB та розглядається, як еквівалент управління загрозами, що забезпечується практичними компетенціями професіоналів. У відомому стандарті PMI та японському стандарті P2M для управління можливостями відсутній окремий домен. Стандарт CMMI-DEV взагалі не охоплює можливості. Тому створення методології управління загрозами разом з управлінням можливостями, забезпечуючи їх спільний синергетичний ефект, представляє цікаву тему для досліджень, оскільки значно покращує конкурентні перспективи IT компаній [36, 53, 69, 70]. Сукупний ефект втрат від ризиків та дохід від можливостей в визначені інтервали часу визначається наступною формулою (2.33):

$$R_{it} = \sum_{t1=0}^{T} \sum_{i=0}^{n} c_{it1} - \sum_{t2=0}^{T} \sum_{j=0}^{m} d_{jt2}, \quad (2.33)$$

де c_{it1} – можливості проєкту, можна представити у наступному вигляді (2.34):

$$c_{it1} = \sum_{t1=0}^{T} \sum_{i=0}^{n} p_{it1} \cdot v_{it1}, \quad (2.34)$$

d_{it2} – загрози проєкту, можна представити у наступному вигляді (2.35):

$$d_{it2} = \sum_{t2=0}^{T} \sum_{j=0}^{m} p_{jt2} \cdot v_{jt2}, \quad (2.35)$$

де p_i, p_j – ймовірність виникнення загрози або можливості;

v_i, v_j – ступінь позитивного (i) та негативного (j) впливу;

t_1, t_2 – характеризує момент виникнення загрози або можливості;

T – тривалість проєкту.

Менеджер проєкту під час запровадження заходів управління також має можливість управляти і загрозами. Залучення експертів компанії для виявлення загроз та можливостей є невід'ємним інструментом досягнення синергизму. Використання накопиченого досвіду та аналізу попередніх помилок з реєстрів вивчених уроків на фазі планування, де наведений весь досвід схожих суміжних проєктів компанії. Позитивні та негативні уроки, винесені та проаналізовані проєктним менеджером з попередніх проєктів, можуть слугувати предметом обміркування для ідентифікації загроз або можливостей на поточному проєкті. Матриця RIO-RIT-REO-RET повинна враховувати не лише загрози, а й можливості, які створюють позитивний вплив на цілі проєкту в разі їх виникнення.

Відносний синергетичний ефект можна представити у вигляді відношення різниці показників доходу та запланованого бюджету з сумарними згрупованим ризиком та можливостю проєкту та різниці доходу та запланованого бюджету з сумою всіх *j*-их загроз та *i*-их можливостей проєкту. Яке моделюється наступним виразом (2.36):

$$E = \frac{\mathrm{F}-\mathrm{B}-(\sum_{i=0}^{n}\sum_{j=0}^{m}(\sum_{t2=0}^{T} p_{jt}v_{jt}-\sum_{t1=0}^{T} p_{it}v_{it}))}{F-B-\sum_{t2=0}^{T}\sum_{j=0}^{n} p_{jt}v_{jt}+\sum_{t1=0}^{T}\sum_{i=0}^{n} p_{it}v_{it}} > 1, \qquad (2.36)$$

де F – це очікуваний дохід від проєкту;

B – це бюджет проєкту.

Така умова (2.36) моделює позитивний синергетичний ефект від управління загрозами та можливостями одночасно, тому що сумарний результат

від управління ризиками вищий ніж від управління загрозами або можливостями окремо. Таку гіпотезу можна перевірити на моделі групування ризиків, зокрема загроз та можливостей у залежності від різних ознак [71].

Створення математичної моделі синергетичного ефекту ІТ-проєкту з урахуванням таких показників як бюджет, тривалість, його сумарний ризик та можливість, дозволяє оцінити ефективність управління ІТ-проєктом та порівняти її з ефективністю управління проєктом з урахування окремих груп ризиків та можливостей. Таке порівняння дозволить обрати найбільш оптимальну та успішну модель управління ризиками з урахуванням загроз та можливостей, що дозволить менеджеру успішно керувати проєктом, а компанії розумно оптимізувати витрати [71].

2.5. Висновки за другим розділом

За результатами проведених досліджень у другому розділі можна дійти таких висновків:

1. Запропоновані системний, процесний та проєктний підходи, ризик-менеджмент, експертний аналіз, інтелектуальний аналіз даних та SWOT-аналіз до проведення подальших наукових досліджень щодо розроблення моделей, методів та інформаційної технології управління ризиками з урахуванням загроз та можливостей в ІТ-проєктах.

2. Ґрунтуючись на методологічному базисі дисертаційного дослідження була побудована архітектура наукового дослідження.

3. Розроблена концептуальна модель управління ризиками в ІТ-проєктах з урахуванням загроз та можливостей ґрунтується на тому, що будь-який проєкт може бути описаний в просторі найголовніших метрик – час, гроші, обсяг та якість. Цей результат дозволяє заздалегідь врахувати вплив можливих ризиків з урахуванням загроз та можливостей в момент планування проєкту, завдяки чому проєктний менеджер є більш підготовленим до швидкоплинних реалій проєктної

діяльності, які в свою чергу містять велику кількість незапланованих явищ, робіт, або іншими словами – змін.

4. Запропонована автором модель RIO-RIT-REO-RET-аналізу дозволяє на етапі ідентифікації ризиків провести аналіз проєкту з точку зору кожного з аспектів: сильних чи слабких сторін, сприятливих можливостей та загроз. Результати такого комплексного аналізу (RIO-RIT-REO-RET-аналіз) можуть бути використані як для проєкту, портфелю, так і для програм та управління компаній або організацій в цілому. Зовнішні загрози та можливості (REO-RET) в цілому потенційно представляють цінність не лише для управління кожним проєктом компанії, але й для управління компанією чи організацією загалом. Внутрішні загрози та можливості (RIO-RIT) є цінними в більшій мірі у ході перебігу проєкту та представляють собою історичні дані після закриття проєкту та можуть бути використані при ініціалізації наступного проєкту схожого типу у подальшому.

5. Розроблена автором таргетна модель інтегрованого управління ризиками в IT-проєктах ґрунтується на аналогії медицини та управління проєктами, яка дозволяє створити новий альтернативний підхід до управління ризиками проєкту, як загрозами, так і можливостями. На основі таргетної моделі інтегрованого управління ризиками в IT-проєктах, будуються графіки, за допомогою яких формуються обмеження проєкту, які є найбільш чутливими та вимагають належного управління. Вони водночас найбільш ризиковані та сповнені можливостей, які можуть призвести до запланованого результату проєкту та принести певні переваги проєкту. За допомогою цих графіків керівник проєкту може прийняти швидке і точне рішення, яке відповідає початковим обмеженням проєкту.

6. Розроблена автором інтелектуальна модель вибору оптимальної стратегії управління ризиковими подіями: загрозами та можливостями забезпечує декомпозицію процесу на три підпроцеси, які враховують графи розвитку подій, синергію можливих загроз та можливостей. Вибір оптимального рішення забезпечується оптимізацією витрат, для яких запропоновано критерії,

цільову функцію. Застосовується розподіл загроз та можливостей у вигляді розробленої таргетної моделі за введеними вагами загроз та можливостей на основі експертних оцінок. Враховується як вартість реалізацій стратегій, так і загальні витрати на їх реалізацію, використовується обережний підхід до заощадливого використання ресурсів, що дозволяє балансування вигоди від реалізації можливості та витрат від загрози при обмежених наявних ресурсах.

7. Запропонована математична модель управління загрозами та можливостями в ІТ-проєктах ґрунтується на розрахунку синергетичного ефекту ІТ-проєкту з урахуванням таких показників як бюджет, тривалість, його сумарний ризик та можливість, та дозволяє оцінити ефективність управління ІТ-проєктом й порівняти її з ефективністю управління проєктом з урахуванням окремих груп ризиків та можливостей. Таке порівняння дозволить обрати найбільш оптимальну та успішну модель управління ризиками з урахуванням загроз та можливостей, що дозволить менеджеру успішно керувати проєктом, а компанії розумно оптимізувати витрати.

Результати досліджень другого розділу опубліковані у таких роботах [36, 37, 39, 46, 48, 53, 54, 57, 58].

Список використаних джерел за другим розділом

1. Системний аналіз і прийняття інноваційних рішень : навч. посібник / Т.К. Гречко, Л.С. Чернова. Миколаїв: видавець Торубара В.В., 2015. 244 с.

2. Сидорчук О.В., Ратушний Р.Т., Сидорчук О.О., Демедюк М.А. Системний підхід до управління проєктами та програмами: означення засад. *Східно-Європейський журнал передових технологій*. Харків, 2011. № 1/5. С. 30-32. URL: http://nbuv.gov.ua/UJRN/Vejpte_2011_1%285%29__10.

3. Чимшир В.И., Тесленко П.А. Проект как система [Монография]. Одесса : Институт креативных технологий, 2011. 159 с.

4. Литюга Ю.В., Позняк С.В. Процесне управління ризиками розвитку підприємства як джерело його конкурентоспроможності. *Ефективна економіка*.

2015. № 9. Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=4612 (дата звернення: 30.08.2022).

5. Маматова Т.В. Системная модель методологии управления на основе качества в условиях новой экономики. *Управління проєктами та розвиток виробництва: зб. наук. пр.* Луганськ: Східноукр. держ. ун-т, 2003. № 2 (10). С. 48-55. Режим доступу: http://www.pmdp.org.ua/index.php/ua/component/content/article/72-2004/10/924-mamatova.

6. Маматова Т.В. Управління на основі якості в органах державного контролю: методологічні аспекти. *Актуальні проблеми державного управління : зб. наук. пр.* Дніпропетровськ : ДРІДУ НАДУ, 2004. Вип. 1 (15). С. 97-110.

7. Маматова Т., Гладка О. Організаційно-правові засади функціонування академічних бізнес-інкубаторів як інструмент місцевого розвитку. *Публічне адміністрування: теорія та практика*. 2013. Вип. 2. Режим доступу: http://nbuv.gov.ua/UJRN/Patp_2013_2_19.

8. Нетепчук В.В. Процесний підхід у побудові корпоративних систем управління проєктами. *Вісник НУВГП. Економічні науки : зб. наук. праць*. Рівне : НУВГП, 2020. Вип. 2(90). С. 112-121. DOI: https://doi.org/10.31713/ve22022012.

9. Каражия Е.А. Процесно-орієнтоване управління інноваційною діяльністю підприємств України. *Агросвіт*. 2021. № 16. С. 69-76. DOI: https://doi.org/10.32702/2306-6792.2021.16.69.

10. Борисова Л.Є. Процесно-функціональний підхід у системі управління сучасного телекомунікаційного підприємства. *Науковий вісник Херсонського державного університету*. Херсон : ХДУ, 2015. № 11. С. 55-58. Режим доступу: http://nbuv.gov.ua/UJRN/Nvkhdu_en_2015_11%282%29__14.

11. Миронюк М.О. Процесний підхід в управлінні інноваційними проектами. *Сучасні підходи до управління підприємством*: зб. тез доп. VII всеукр.наук.-практ. конф. з міжн. участю (м. Київ, 28 квіт. 2016 р.). Київ, 2016. С. 36. Режим доступу: https://kafedra.management.fmm.kpi.ua/main/wp-content/uploads/2022/07/konf2016.pdf.

12. Солосіч О.С., Хринюк О.С. Інтеграція процесного та функціонального підходів в сучасних бізнесмоделях у складі систем управління економічною безпекою підприємств. *Бізнес, інновації, менеджмент: проблеми та перспективи*: зб. тез доп. ІІ міжнар. наук.-практ. конф. (м. Київ, 22 квіт. 2021 р.). Київ, 2021. С. 108-109.

13. Данченко О.Б. Методологія інтегрованого управління відхиленнями в проєктах : автореф. дис. … д-ра техн. наук : 05.13.22. Київ, КНУБА, 2015. 45 с. Режим доступу: http://irbis-nbuv.gov.ua/publ/REF-0000595672.

14. Рач В.А., Міхальова О.В. Побудова базових (пріоритетних) процесів податкової інспекції. *Управління проектами та розвиток виробництва: Зб. наук. пр.* Луганськ: Східноукр. держ. ун-т, 2002. № 2 (5). С. 81-84. Режим доступу: http://www.pmdp.org.ua/index.php/ua/component/content/article/84-2002/5/1141-rach-mikhaleva.

15. Рач В.А., Солоп О.Г., Михалкова О.В. Особливості проведення функціонально-структурного дослідження процесів державної податкової інспекції районного рівня за допомогою функціонального моделювання. *Сучасні інформаційні та енергозберігаючі технології життєзабезпечення людини*: зб. наук. пр. Київ: КНУТД, 2003. Вип. 13. С. 276-280.

16. Маматова Т.В. Особливості визначення та моніторингу базових процесів в органах державного контролю (на прикладі територіального органу Держспоживстандарту України). *Якість та довкілля. 2003* : тези доп. міжнар. Симпозіуму, 18 трав. 2003 р. Київ : Бюро Верітас Україна, 2003. С. 98-99.

17. Управління проєктами: навч. посіб. / Ю.І. Буріменко, Л.В. Галан, І.Ю. Лебедєва, А.Ю. Щуровська; за ред. Ю.І. Буріменко. Одеса: ОНАЗ ім. О.С. Попова, 2017. 208 с.

18. Бурименко Ю.И. Основы теории систем и системного анализа: учебн. пособ. [для вузов], реком. МОНУ / Ю.И. Бурименко. Одесса: Optimum, 2005. 135 с.

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

20. Литвиненко Г., Клясен Н. Управління проєктами: сутність та особливості застосування в освіті. *Рідна школа*. 2017. № 11-12 (листопад-грудень). С. 39-43.

21. Бабаєв В.М. Управління проєктами: навч. посіб. Харків: Харків. нац. ун-т міськ. госп-ва ім. О.М. Бекетова, 2006. 244 с.

22. Боровик М.В. Ризик-менеджмент : конспект лекцій для студентів магістратури усіх форм навчання спеціальності 073 – Менеджмент. М.В. Боровик ; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. Харків : ХНУМГ ім. О. М. Бекетова, 2018. 65 с.

23. Рач В.А., Борулько Н.А. Управление рисками проекта: общее и различия PMBOK 4 и PMBOK 5. *Управління проєктами та розвиток виробництва: Зб.наук.пр.* Луганськ: вид-во СНУ ім. В.Даля, 2014. №1(49). С. 5-16. Режим доступу: http://pmdp.org.ua.

24. Бедрій Д.І., Семко І.Б. Аналіз підходів до управління кадровими ризиками наукового проєкту. *Управління проєктами у розвитку суспільства*. Тези доповідей XV міжнародної науково-практичної конференції 18-19 травня 2018 року. Київ: КНУБА, 2018. С. 32-33.

25. Данченко О.Б. Огляд сучасних методологій управління ризиками в проєктах. *Управління проєктами та розвиток виробництва: Зб.наук.пр*. Луганськ: вид-во СНУ ім. В.Даля, 2014. № 1(49). С. 16-25. Режим доступу: http://pmdp.org.ua.

26. Рач Д.В. Управління невизначеністю та ризиками в проєкті: термінологічна основа. *Управління проєктами та розвиток виробництва: Зб.наук.пр.* Луганськ: вид-во СНУ ім. В.Даля, 2013. № 3(47). С. 146-164. Режим доступу: http://www.pmdp.org.ua/.

27. Возный А.М., Кошкин К.В., Казарезов А.Я. и др. Модели, методы и алгоритмическое обеспечение проектов и программ развития наукоемких производств: монография. Николаев: НУК, 2009. 194 с.

28. Денчик О.Р. Моделі та методи інтегрованого управління ризиками проєктів в агропромисловому комплексі. : дис. … д-ра філос. : 073. Київ, 2020. 229 с.

29. Гогунський В.Д., Чернега Ю.С. Управління ризиками в проектах з охорони праці як метод усунення шкідливих і небезпечних умов праці. *Східно-Європейський журнал передових технологій*. Харків, 2013. № 1/10 (61). С. 83-85.

30. Інтелектуальний аналіз даних (data mining): Інтелектуальні Інтегровані Системи. URL: https://sites.google.com/a/kubg.edu.ua/integrovani-sistemi/intelektualnij-analiz-danih-data-mining.

31. Knowledge Discovery Through Data Mining: What Is Knowledge Discovery? Tandem Computers Inc., 1996. 253 p.

32. Колодчак О.М. Інтелектуальний аналіз даних. *Вісник Національного університету "Львівська політехніка". Комп'ютерні системи та мережі*. Львів, 2013. № 773. С. 49-58. URL: http://nbuv.gov.ua/UJRN/VNULPKSM_2013_773_11.

33. Grant R. Contemporary strategy analysis. Cambridge, M A : Blackwell Publishers, 1995.

34. Шляхта О.М. SWOT-аналіз як інструмент стратегічного менеджменту підприємства. *Економічний простір*. 2012. № 68. С. 301-309. URL: http://nbuv.gov.ua/UJRN/ecpros_2012_68_35.

35. Weihrich H. The TOWS matrix – A tool for situational analysis. *Long Range Planning*. 1982. Vol. 15(2). P. 54-66.

36. Danchenko O., Shendryk V., Hrabina K. Opportunity Management overview in terms of the Risk Management in the software development industry standards. *Управління проєктами: стан та перспективи*. Матеріали XV міжнародної науково-практичної конференції (м. Миколаїв, 10-13 вересня 2019 року). Миколаїв: НУК, 2019. С. 88-89.

37. Грабіна К.В., Шендрик В.В., Данченко О.Б. Складові управління ризиками ІТ-проєктів. *Інформатика. Культура. Технології, ІКТ-2021*. Матеріали VIII Міжнародної науково-практичної конференції (м. Одеса, 13-14 травня 2021 р.). Одеса: Одеська політехніка, 2021. С. 124-126.

38. Данченко О.Б., Занора В.О. Проєктний менеджмент: управління ризиками та змінами в процесах прийняття управлінських рішень : монографія – Черкаси, 2019. – 278 с.

39. Грабіна К.В., Шендрик В.В. Ризик менеджмент як інструмент планування успішних ІТ-проєктів. *Інформатика, математика, автоматика, IMA-2021*. Міжнародна науково-технічна конференція студентів та молодих учених (Суми-Нур-Султан, 19-23 квітня 2021 року). Суми, СумДУ: 2021. С. 76-77. URL: https://drive.google.com/file/d/1c4OYoy7HoYGPrliSb851gXYv_wRwUk3o/view.

40. Batra D. Conceptual Data Modeling Patterns. Journal of Database Management. 2005. Vol. 16. pp. 84-106. URL: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=00201ae925e3ba18002d34e82f64f4ce22c97be1.

41. Бушуєв С.Д., Бушуєв Д.А., Бушуєва В.Б., Бушуєва Н.С. Концептуальна модель цифрового сліду проєктів в умовах цифровізації суспільства. *Управління розвитком складних систем*. 2021. Вип. 46. С. 12-18. DOI: 10.32347/2412-9933.2021.46.12-18. URL: http://nbuv.gov.ua/UJRN/Urss_2021_46_4.

42. Білощицький А.О., Кучанський О.Ю., Андрашко Ю.В., Білощицька С.В., Кузка О.І. Концептуальна модель інформаційної технології оцінювання результатів науково-дослідної діяльності. *Управління розвитком складних систем*. 2017. Вип. 30. С. 163-168. URL: http://urss.knuba.edu.ua/files/zbirnyk-30/24.pdf.

43. Проскурін М.В., Морозов В.В., Шелест Т.М. Модель системи управління ІТ-проєктами на основі машинного навчання. *Вісник Національного технічного університету "ХПІ". Серія : Стратегічне управління, управління портфелями, програмами та проектами*. 2019. № 1. С. 42-50. DOI: 10.20998/2413-3000. 2019.1326.7. URL: http://nbuv.gov.ua/UJRN/vntux_ctr_2019_1_9.

44. Бушуєв С.Д., Дорош М.С., Шакун Н.В. Інноваційне мислення при формуванні нових методологій управління проєктами. *Управління розвитком*

складних систем. 2016. Вип. 26. С. 49-57. URL: http://nbuv.gov.ua/UJRN/Urss_2016_26_9.

45. Тесля Ю.М., Хлевна Ю.Л., Єгорченкова Н.Ю., Кошелєва Д.І. Впливи на формування конкретизованої методології управління проєктами. *Вісник Черкаського державного технологічного університету. Серія : Технічні науки*. 2017. № 2. С. 45-54. URL: http://nbuv.gov.ua/UJRN/Vchdtu_2017_2_8.

46. Грабіна К.В., Шендрик В.В., Данченко О.Б., Мазуркевич А.Г. Застосування SWOT-аналізу для ідентифікації ризиків проекту. Управління проектами у розвитку суспільства. Тези доповідей XVIII Міжнародної науково-практичної конференції (м. Київ, 15 травня 2021 року). Київ: КНУБА, 2021. С. 133-137.

47. Дідух Т.М. Глобальні ризики використання ІТ-аутсорсингу. *Світове господарство і міжнародні економічні відносини*. 2017. № 20. С. 28-32. URL: http://global-national.in.ua/issue-20-2017/28-vipusk-20-gruden-2017-r/3501-didukh-t-m-globalni-riziki-vikoristannya-it-autsorsingu.

48. Грабіна К.В., Шендрик В.В. Огляд процесів управління ризиками в ІТ-проєктах в контексті стандартів проєктного менеджменту. *Управління розвитком складних систем*. Київ: КНУБА, 2020. Вип. 43. С. 26-32. DOI: https://www.doi.org/10.32347/2412-9933.2020.43.26-32. URL: http://mdcs.knuba.edu.ua/article/view/219812/219536.

49. Targeted therapy in the American Cancer Society. URL: https://www.cancer.org/treatment/treatments-and-side-effects/treatment-types/targeted-therapy.html.

50. Данченко О.Б., Лепський В.В. Загальна класифікація «хвороб» проєктів. *Управління проектами: стан та перспективи*: матеріали X Міжнар. наук.-практ. конф. (м. Миколаїв, 16-19 верес. 2014 р.). Миколаїв: НУК, 2014. С. 75-78.

51. Тесля Ю.М., Данченко О.Б. Синергетична модель «хвороб» проєктів. *Управління розвитком складних систем*. Київ: вид-во Київський національний

університет будівництва і архітектури, 2014. Вип. 20. С. 87-90. URL: http://urss.knuba.edu.ua/files/zbirnyk-20/18.pdf.

52. Тесля Ю.М., Данченко О.Б. Управління «хворобами» проєкту. *Управління проектами у розвитку суспільства*. Тези доп. XI міжнар. наук.-практ. конф. (м. Київ, 23-24 трав. 2014 р.). Київ: Київ. нац. ун-т буд. і архіт., 2014. С. 60-61.

53. Грабіна К.В., Шендрик В.В., Данченко О.Б. Синергетичний ефект від управління загрозами та можливостями в IT-проєктах. *Project, Program, Portfolio Management*. Матеріали П'ятої Міжнародної науково-практичної конференції (м. Одеса, 04-05 грудня 2020 року). Одеса: ОНПУ, 2020. С. 26-30.

54. Hrabina K., Danchenko O., Shendryk V. Target models of integrated risk management for IT-projects. *The scientific heritage*. Budapest, 2021. Vol. 1, № 71 (71). p. 55-61. DOI: https://www.doi.org/10.24412/9215-0365-2021-71-1-55-61. URL: http://www.scientific-heritage.com/wp-content/uploads/2021/08/The-scientific-heritage-No-71-71-2021-Vol-1.pdf.

55. Practice Standard for Project Risk Management. USA: PMI, 2019. 116 p.

56. A Guidebook of Project & Program Management for Enterprise Innovation: PMAJ. URL: http://www.pmaj.or.jp/ENG/p2m/p2m_guide/p2m_guide.html.

57. Hrabina K., Shendryk V. Intelligent model of choosing the optimal risk events management strategy: threats and opportunities. *Artificial Intelligence*. Київ, 2022. № 2. P. 84-90. DOI: https://doi.org/10.15407/jai2022.02. URL: http://jai.in.ua/index.php/ua/issues?paper_num=1558.

58. Грабіна К.В., Шендрик В.В. Формування інтелектуальної моделі для вибору оптимальної стратегії управління ризиками. *Управління проєктами у розвитку суспільства*. Тези доповідей XX Міжнародної науково-практичної конференції (м. Київ, 12 травня 2023 року). Київ: КНУБА, 2023. С. 78-81.

59. Piterska V., Kolesnikov O., Lukianov D., Kolesnikova K., Gogunskii V., Olekh T., Shakhov A., Rudenko S. Development of the Markovian model for the life cycle of a project's benefits. *Eastern-European journal of enterprise technologies*.

2018. № 5(4). P. 30-39. DOI: 10.15587/1729-4061.2018.145252. URL: http://nbuv.gov.ua/UJRN/Vejpte_2018_5(4)__5.

60. Бушуєв С.Д., Бушуєв Д.А., Козир Б.Ю. Зміна парадигм в управлінні інфрастуктурними проєктами і програмами. *Управління розвитком складних систем*. 2019. Вип. 37. С. 6-12. DOI: 10.6084/m9.figshare.9783149. URL: http://nbuv.gov.ua/UJRN/Urss_2019_37_3.

61. Kuchansky A., Biloshchytskyi A., Andrashko Y., Wang Y. Devising a competence method to build information spaces for executors of educational projects in a dynamic environment. *Eastern-European journal of enterprise technologies*. 2022. № 1(3). P. 66-73. DOI: 10.15587/1729-4061.2022.253043. URL: http://nbuv.gov.ua/UJRN/Vejpte_2022_1(3)__9. (Scopus).

62. Butler S.A. Security attribute evaluation method: a cost-benefit approach. *Proceedings of the 24th international conference on Software engineering*. 2002. P. 232-240.

63. Lei C., Ma D.H., Zhang H.Q. Optimal strategy selection for moving target defense based on Markov game. *IEEE Access*. 2017. Vol. 5. P. 156-169.

64. Butler S.A., Fischbeck P. Multi-attribute risk assessment. *Proceedings of the Symposium on Requirements Engineering for Information Security*. 2002. Vol. 2.

65. Тесленко П.А. Эволюционная теория и синергетика в управлении проектами. *Управління проектами та розвиток виробництва: зб.наук.праць*. Луганськ: вид-во Східноукраїнський національний університет ім. В.Даля, 2010. № 4(36). С. 38-43. URL: http://www.pmdp.org.ua/images/Journal/36/10tpasup.pdf.

66. Сьомкіна Т.В., Литвинова О.В., Лобань О.О. Особливості моделей функціонування ІТ-компаній в Україні. *Науковий вісник Ужгородського національного університету. Серія : Міжнародні економічні відносини та світове господарство*. 2018. Вип. 19(3). С. 84-87. URL: http://nbuv.gov.ua/UJRN/Nvuumevcg_2018_19%283%29__19.

67. Семко І.Б. Моделі та методи управління ризиками портфелів проектів в енергетичній галузі: дис. … канд. техн. наук : 05.13.22. Черкаси, 2012. 165 с.

68. Biloshchytskyi A., Tsiutsiura S., Kuchansky A., Serbin O., Tsiutsiura M., Biloshchytska S., Faizullin A. Development of mathematical models of the project-vector space of educational environments. *Eastern-European journal of enterprise technologies*. 2022. № 5(4). P. 50-61. DOI: 10.15587/1729-4061.2022.266262. URL: http://nbuv.gov.ua/UJRN/Vejpte_2022_5(4)__8. (Scopus).

69. Лисак В.М., Ноздріна Л.В. Методи і моделі бізнес-аналізу в ІТ-галузі. *Вісник Університету банківської справи*. 2020. № 3. С. 94-103. URL: http://nbuv.gov.ua/UJRN/VUbsNbU_2020_3_16.

70. Палій С. Сучасні тенденції розвитку інформаційно-аналітичного забезпечення у контексті прийняття ефективних управлінських рішень (на прикладі органів державної влади України). *Український журнал з бібліотекознавства та інформаційних наук*. 2022. Вип. 10. С. 166-174. DOI: 10.31866/2616-7654.10.2022.269493. URL: http://nbuv.gov.ua/UJRN/ujlis_2022_10_16.

71. Грабіна К.В., Шендрик В. В. Метод управління ризиками ІТ-проєктів з врахуванням загроз та можливостей. *Управління розвитком складних систем.* Київ: КНУБА, 2023. Вип. 55. С. 18-28. DOI: https://doi.org/10.32347/2412-9933.2023.55.18-28. URL: http://mdcs.knuba.edu.ua/article/view/291119.

РОЗДІЛ 3.
МЕТОДИ ІНТЕГРОВАНОГО УПРАВЛІННЯ ЗАГРОЗАМИ ТА МОЖЛИВОСТЯМИ В ІТ-ПРОЄКТАХ

3.1. Метод інтегрованого управління загрозами та можливостями в ІТ-проєктах

Враховуючи розроблені моделі інтегрованого управління загрозами та можливостями в ІТ-проєктах, що наведені у підрозділі 2 цього дослідження, автором пропонується їхня реалізація за допомогою відповідних методів.

В умовах сьогодення впровадження новітніх та сучасних інформаційних технологій стає запорукою комфортного існування людини в суспільстві [1, 2]. Одним з головних результатів їхнього використання є збільшення та підвищення якості послуг, які можна надавати через Інтернет. Що, у свою чергу, призводить до необхідності швидкого перетворення та забезпечення умов цифрової трансформації в різних сферах діяльності людини. ІТ-індустрія, як і більшість інших сфер діяльності людини, активно та ефективно використовує моделі, методи та інструменти методології управління проєктами [1, 2, 3]. Зважаючи на те, що планування та реалізація будь-яких проєктів, зокрема й ІТ-проєктів, відбувається в умовах мінливості та невизначеності, які в свою чергу характеризуються великою кількістю ризиків, тому актуальним є розроблення та вдосконалення інструментів проектного керівника для управління ризиками з врахуванням загроз та можливостей.

Усі проєкти можуть наражатися на ризики, оскільки вони є унікальними підприємствами з різним ступенем складності, які здійснюються з метою отримання вигоди для стейкхолдерів. Вони реалізуються в умовах обмежень та припущень, а також очікувань стейкхолдерів, які можуть суперечити один одному та змінюватись. Команда проєкту повинна брати на себе усвідомлений та контрольований ризик щодо виконання проєкту з метою створення цінності з урахуванням ризиків та вигод [1, 3, 4, 5].

Із цього видно, що проєкти існують у середовищах із різним ступенем невизначеності. За невизначеністю приховані як можливості, так і загрози, які команди проєктів досліджують, оцінюють та вирішують, що з ними робити [1].

Метою управління ризиками проєкту є ідентифікація ризиків та управління ними, які не є предметом інших процесів управління проєктом. Якщо не керувати ризиками, вони можуть спричинити відхилення проєкту від плану та призводити до того, що проєкт може не досягти встановлених цілей. Зрештою, від результативності управління ризиками проєкту прямо залежить його успішне завершення [1].

Невизначеність у широкому сенсі – це стан незнання чи непередбачуваності. У невизначеності є багато нюансів, зокрема:

- ризик, пов'язаний із незнанням майбутніх подій;
- неоднозначність, пов’язана із незнанням поточних або майбутніх умов;
- складність, пов’язана із динамічними системами, які мають неочікувані кінцеві результати [1].

Успішне подолання невизначеності починається із розуміння середовища, в якому функціонує проєкт. До аспектів середовища, які характеризують невизначеність проєкту відносяться:

- економічні фактори – доступність ресурсів, можливість запозичення коштів, інфляційні процеси тощо;
- технічні особливості – нові або перспективні технології, складність, що пов’язана із системами, інтерфейси;
- юридичні або законодавчі обмеження та вимоги;
- фізичне середовище – безпека та умови праці, кліматичні умови;
- неоднозначність, що пов’язана із поточними або майбутніми умовами;
- соціальні впливи, які пов’язані із громадською думкою;
- політичні впливи, як зовнішні, так і внутрішні.

Невизначеність притаманна усім проєктам. Виходячи із цього, наслідки будь-якої діяльності неможливо точно передбачити та може виникнути низка кінцевих результатів – можливостей та загроз. Можливість – це результат, який

приносить вигоди цілям проєкту, а загроза – це результат, який негативно впливає на цілі проєкту. Разом можливості та загрози становлять сукупність ризиків проєкту. Існує кілька варіантів реагування на невизначеність (табл. 3.1) [1].

Таблиця 3.1. Стратегії реагування на невизначеність

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

Отже, ризики є аспектом невизначеності. Ризик – це невизначена подія або умова, що у разі настання матиме позитивний чи негативний вплив на одну чи більше цілей проєкту.

Члени команди проєкту повинні активно виявляти ризики протягом життєвого циклу проєкту, щоб уникнути або мінімізувати вплив загроз та ініціювати або максимізувати вплив можливостей. Як загрози, так і можливості мають набір можливих стратегій реагування, які можна запланувати для виконання у разі виникнення ризику.

Для ефективного управління ризиками команді проєкту необхідно знати, який рівень впливу ризику є прийнятним для досягнення цілей проєкту [1, 3, 6]. Це визначається вимірюваними порогами ризику, які відображають схильність

до ризику та ставлення компанії й стейкхолдерів проєкту. Поріг ризику виражає прийнятне відхилення від цілі, що відображає схильність компанії та стейкхолдерів проєкту до ризику. Поріг зазвичай вказують та доводять до відома команди проєкту, а також відображають у визначеннях рівнів впливу ризиків для проєкту [1].

Загальний ризик проєкту – це вплив невизначеності на проєкт в цілому, який виникає з усіх джерел невизначеності. Сюди входять індивідуальні ризики та вплив наслідків змін у кінцевих результатах проєкту, як позитивних, так і негативних. Загальний ризик часто залежить від складності, неоднозначності ....Реакція на загальний ризик проєкту така ж, як і для окремих загроз та можливостей, хоча реакцію застосовують до проєкту в цілому, а не до конкретної події. Якщо загальний ризик проєкту великий, то компанія може вирішити скасувати проєкт [1].

Як тільки набір заходів реагування на ризики буде розроблено, його необхідно переглянути з метою виявлення будь-яких вторинних ризиків у запланованих заходах реагування. Перегляд ризиків також має на меті оцінку залишкового ризику після виконання заходів реагування. Тому планування відповідних заходів необхідно повторювати до тих пір, поки залишковий ризик не буде сумісний зі схильністю компанії до ризику [1].

Інтегроване управління загрозами та можливостями в ІТ-проєктах (рис. 3.1.) ґрунтується на концептуальній моделі управління ризиками в ІТ-проєктах з урахуванням загроз та можливостей (рис. 2.2.), та відповідних моделях [6, 7, 8, 9], включає у себе наступні етапи:

1. Формування реєстру ІТ-проєктів.
2. Ідентифікація ризиків ІТ-проєктів з урахуванням загроз та можливостей.
3. Побудова матриці RIO-RIT-REO-RET для ІТ-проєктів (п. 2.3.1.).
4. Проведення оцінки ризиків ІТ-проєктів з урахуванням загроз та можливостей за допомогою таргетних моделей (п. 2.3.2.).

5. Оцінка синергетичного ефекту від управління загрозами та можливостями в ІТ-проєктах (п. 2.4.).

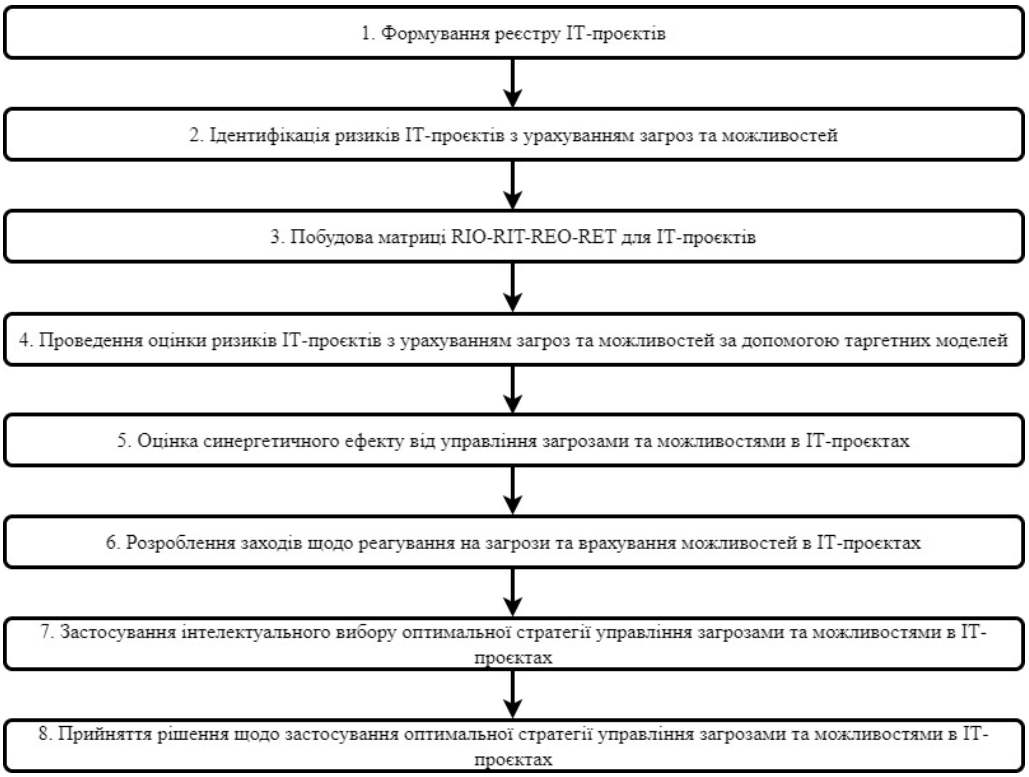


Рисунок 3.1. - Етапи інтегрованого управління загрозами та можливостями в ІТ-проєктах

6. Розроблення заходів щодо реагування на загрози та врахування можливостей в ІТ-проєктах.

7. Застосування інтелектуального вибору оптимальної стратегії управління загрозами та можливостями в ІТ-проєктах (п. 2.3.3.).

8. Прийняття рішення щодо застосування оптимальної стратегії управління загрозами та можливостями в ІТ-проєктах.

Зважаючи на наведене вище, у цьому дослідженні автором пропонується розробка методу управління ризиками ІТ-проєктів з врахуванням загроз та можливостей, який включає у себе наступні етапи (рис. 3.2.) [1]:

1. Ідентифікація загроз та можливостей за допомогою матриці RIO-RIT-REO-RET, яка наведена у підрозділі 2.3.1. цього дослідження.

На цьому етапі пропонується застосування SWOT-аналізу, який дозволяє провести аналіз проєкту з точку зору кожного з аспектів: сильних чи слабких сторін, сприятливих можливостей та загроз (рис. 2.3.).

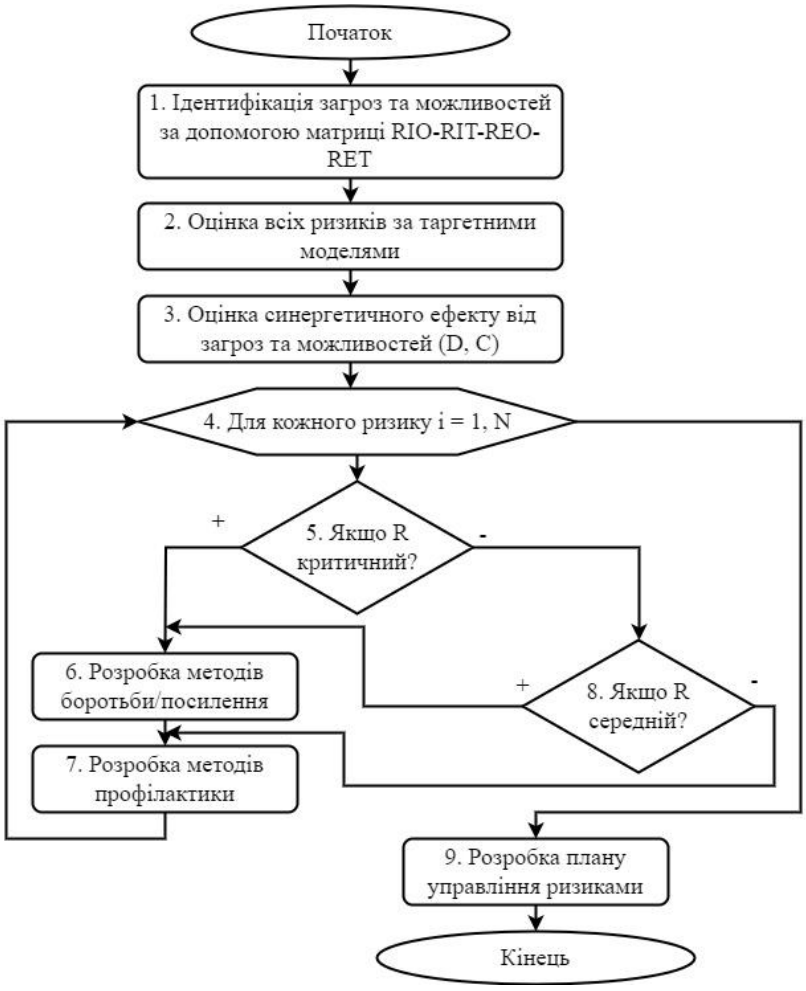


Рисунок 3.2. - Схема методу управління ризиками IT-проєктів з врахуванням загроз та можливостей

Згідно [1, 3, 7] цей метод використовується при ідентифікації ризиків, щоб розширити ідентифікацію ризиків за рахунок ризиків, які виникають в середині самого проєкту. Розглядаючи ризики для типового IT-проєкту, можна відзначити рівень їх виникнення: проектний, організаційний (рівень компанії) чи галузевий з класифікованими ризиками. Будемо вважати ризики проєктного рівня – внутрішніми (Internal), а ризики рівня компанії, організації чи галузі –

зовнішніми (External). Тому введено класифікацію за джерелом виникнення – внутрішні ризики (I) та зовнішні ризики (E).

Аналізуючи необхідність та типову класифікацію ризиків для IT-проєктів, можна константувати, що є потреба у адаптації класичного SWOT-аналізу, з урахуванням того, що ризики можуть представляти собою як загрозу, так і можливість, а також подальшого цільового використання цих даних.

Для кожного проєкту можна розділяти ризики на внутрішні можливості – Risks Internal Opportunities (RIO) та внутрішні загрози – Risks Internal Treats (RIT), а також зовнішні можливості – Risks External Opportunities (REO) та зовнішні загрози – Risks External Treats (RET).

Отже, результатом цього етапу є матриця RIO-RIT-REO-RET, яка містить у собі ідентифіковані внутрішні та зовнішні можливості й загрози.

2. Оцінка всіх ризиків за таргетними моделями [1, 8], які наведені у підрозділі 2.3.2 цього дослідження.

На цьому етапі, виходячи із рівняння (2.6) проводиться оцінка ідентифікованих ризиків, зокрема загроз та можливостей, за допомогою формул (2.7) та (2.8).

Результатом цього етапу є кількісна оцінка загроз та можливостей для IT-проєкту.

3. Оцінка синергетичного ефекту від загроз та можливостей (D, C) [1, 9], яка наведена у підрозділі 2.4. цього дисертаційного дослідження.

На цьому етапі проводиться оцінка синергетичного ефекту від загроз та можливостей шляхом розрахунку сукупного ефекту у певні інтервали часу, який визначається формулами (2.27), (2.28) та (2.29).

Результатом цього етапу є розрахунок відносного синергетичного ефекту від управління загрозами та можливостями, який відбувається за допомогою формули (2.30).

4. Для кожного ризику $i = 1, N$ (N – кількість ризиків IT-проєкту) проводиться ранжування за допомогою матриці ймовірності та впливу ризиків

або інших інструментів управління ризиками на критичні (1-0,7), середні(0,6-0,4), низькі (0,3-0).

До уваги беруться тільки критичні та середні ризики, низькі приймаються, як такі, що мають не значний рівень впливу.

5. Якщо *R* критичний? Якщо умова виконується, то відбувається перехід до п. 6, якщо ні, то до п. 8.

6. Розробка методів боротьби/посилення [3, 10, 11].

Загроза – це подія або умова, яка у випадку настання негативно впливає на одну або кілька цілей. Для боротьби із загрозами можна використовувати будь-яку із п’яти альтернативних стратегій (табл. 3.2).

Таблиця 3.2. Стратегії реагування на загрози

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

Можливість – це подія або умова, яка у випадку настання позитивно впливає на одну або декілька цілей проєкту. Для роботи із можливостями можна розглянути п’ять альтернативних стратегій (табл. 3.3).

7. Розробка методів профілактики [10, 11].

Для того, щоб під час виконання проєкту уникнути виникнення загроз та посилити вплив можливостей в проєкті, пропонується застосування методів профілактики.

Таблиця 3.3. Стратегії реагування на можливості

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

1) Індивідуальні – профілактичні заходи, що проводяться на окремих задачах проєкту чи з окремими членами команди/учасниками проєкту.

2) Групові – профілактичні заходи, що проводяться з групами членів команди/учасниками проєкту, з групами задач проєкту, якщо ці групи мають схожі причини виникнення загроз та можливостей в проєкті.

3) Масові – профілактичні заходи, спрямовані на весь проєкт – всіх учасників та всі задачі.

Після розробки заходів профілактики відбувається перехід до наступного ризику (п. 4). Якщо ризики закінчились, то перехід до п. 9.

8. Якщо *R* середній? То відбувається перехід до п. 6, якщо ні, то до п. 7.

9. Розробка плану управління ризиками.

На цьому етапі формується план управління ризиками – це складова частина плану управління проєктом, в якому описуються яким чином усі дії щодо управління ризиками будуть структуровані та виконані, зокрема: стратегії управління ризиками; ролі та сфери відповідальності; фінансування заходів;

визначення строків; категорії ризиків; ймовірності та впливи; матриця впливу та ймовірності, тощо.

З метою підвищення якості управління ІТ-проєктами доцільно покращити виконання процесів управління ризиками означених проєктів з урахуванням ризиків та можливостей та запровадити ще й ті процеси, які не виконуються. Це також може бути зроблено за допомогою розробки та впровадження інформаційної технології управління ризиками ІТ-проєктів з урахуванням ризиків та можливостей.

Підвищення якості надання послуг з розробки інформаційних технологій споживачам, необхідність розробки та удосконалення програмного забезпечення, необхідність підвищення конкурентоспроможності та ефективності системи управління ІТ-компаніями вимагає ґрунтованого вивчення та аналізу саме застосування проєктного підходу до управління ризиками ІТ-проєктів. У цьому дослідженні розглянуто метод управління ризиками ІТ-проєктів з урахуванням загроз та можливостей для подальшого розроблення інформаційної технології управління ризиками ІТ-проєктів. З метою забезпечення ефективності управління пропонується застосування управління ризиками ІТ-проєктів з урахуванням загроз та можливостей.

3.2. Метод інтелектуального вибору оптимальної стратегії управління ризиковими подіями: загрозами та можливостями

Відповідно до концептуальної моделі управління ризиками в ІТ-проєктах з урахуванням загроз та можливостей (рис. 2.2.) [6] та інтелектуальної моделі вибору оптимальної стратегії управління ризиковими подіями: загрозами та можливостями (рис. 2.13.) [12, 13, 14] з урахуванням методу інтегрованого управління загрозами та можливостями в ІТ-проєктах (рис. 3.2.) [1] пропонується метод інтелектуального вибору, який наведено на рис. 3.3.

Метод інтелектуального вибору оптимальної стратегії управління ризиковими подіями: загрозами та можливостями включає у себе наступні етапи:

Рисунок 3.3. - Схема методу інтелектуального вибору оптимальної стратегії управління ризиковими подіями: загрозами та можливостями

1. Дослідження ІТ-проєкту. На цьому етапі застосовується запропонований автором метод інтегрованого управління загрозами та можливостями в ІТ-проєкті, який був детально описаний у підрозділі 3.1. цього дисертаційного дослідження.

1.1.Сканування ІТ-проєкту. Проводиться попередня оцінка ІТ-проєкту за такими критеріями, як: час, якість, вартість, обсяг робіт. Також проводиться попередня ідентифікація загроз та можливостей відповідно до п. 1 схеми методу, наведеного на рис. 3.2.

1.2.Вибір ІТ-проєкту. За результатами попередньої оцінки ІТ-проєкту проводиться його вибір за трикутником управління проєктами з обмеженням (рис. 2.8.).

1.3.Проведення якісної оцінки за допомогою таргетної моделі інтегрованого управління ризиками в ІТ-проєкті. Цей етап відбувається відповідно до п. 2 схеми методу, що наведений на рис. 3.2.

1.4.Здійснення класифікації ризикових подій, зокрема загроз та можливостей. За результатами п. 1.2. та п. 1.3. цього методу проводиться класифікація ризикованих подій з урахуванням загроз та можливостей.

1.5.Визначення кількісних показників впливу ризикованих подій з урахуванням загроз та можливостей. Відповідно до п. 2 схеми методу, що наведений на рис. 3.2., проводиться кількісна оцінка загроз та можливостей.

1.6.Визначення синергетичного впливу загроз та можливостей. На цьому етапі проводиться визначення синергетичного впливу з урахуванням п. 3 схеми методу, що наведений на рис. 3.2.

2. Побудова цільової функції та можливих сценаріїв розвитку подій. В основі цього етапу лежить розроблена автором інтелектуальна модель вибору оптимальної стратегії управління ризиковими подіями: загрозами та можливостями, наведена у підрозділі 2.3.3. цього дисертаційного дослідження.

2.1. Генерування графу ризиків з урахуванням загроз та можливостей. За результатами застосування методу інтегрованого управління загрозами та можливостями в ІТ-проєкті, який був застосований на першому етапі цього методу, пропонується згенерувати граф ризиків з урахуванням загроз та можливостей.

2.2. Створення множини альтернативних стратегій. На цьому етапі відбувається визначення можливих стратегій розвитку ризикових подій відповідно до формули (2.18).

2.3. Розрахунок ймовірності успішного використання ризиків з урахуванням загроз та можливостей. Цей етап полягає у розрахунку ймовірності настання ризикової події з урахуванням індикаторів та реалізується за допомогою формули (2.19).

3. Вибір оптимальної стратегії управління ризиковою подією. В основі цього етапу також лежить розроблена автором інтелектуальна модель, що наведена у підрозділі 2.3.3. цього дисертаційного дослідження.

3.1.Кількісний аналіз вартості стратегій. На цьому етапі пропонується провести кількісний аналіз оцінки вартості стратегій, результатом якого є отримання множини вартостей (2.20). Для отримання множини вартості автором пропонується користуватися формулами (2.21) – (2.25).

3.2.Формування цільової функції. Завершальним етапом методу є формування цільової функції (2.26), яка ґрунтується на даних, що отримані у п. 3.1.

Отже, запропонований автором метод інтелектуального вибору оптимальної стратегії управління ризиковими подіями: загрозами та можливостями, дозволяє за допомогою інтелектуального аналізу даних обирати оптимальну стратегію управління загрозами та можливостями з метою підвищення ефективності управління ІТ-проєктом.

3.3. Висновки за третім розділом

За результатами проведених досліджень у третьому розділі можна дійти таких висновків:

1. Розроблені етапи інтегрованого управління загрозами та можливостями в ІТ-проєктах, які включають у себе процеси ідентифікації та оцінки ризиків з урахуванням загроз та можливостей, проведення оцінки синергетичного ефекту

від управління ними, а також застосування інтелектуального вибору оптимальної стратегії управління загрозами та можливостями.

2. Розроблений метод інтегрованого управління загрозами та можливостями в ІТ-проєктах, який на відміну від існуючих, враховує ідентифікацію, оцінку та реагування на ризики, як для загроз, так і для можливостей. Це, у свою чергу, дозволяє підвищити ефективність управління ризиками з метою зниження впливу загроз та врахування впливу можливостей.

3. Запропонований метод інтелектуального вибору оптимальної стратегії управління ризиковими подіями: загрозами та можливостями дозволяє за допомогою інтелектуального аналізу даних обирати оптимальну стратегію управління загрозами та можливостями з метою підвищення ефективності управління ІТ-проєктом.

Результати досліджень третього розділу опубліковані у таких роботах [1, 6, 7, 8, 9, 12, 13].

Список використаних джерел за третім розділом

1. Грабіна К.В., Шендрик В. В. Метод управління ризиками ІТ-проєктів з врахуванням загроз та можливостей. *Управління розвитком складних систем.* Київ: КНУБА, 2023. Вип. 55. С. 18-28. DOI: https://doi.org/10.32347/2412-9933.2023.55.18-28. URL: http://mdcs.knuba.edu.ua/article/view/291119.

2. Кухар А.В., Свірська В.О. Впровадження сучасних інформаційно-комунікаційних технологій як фактор розвитку підприємства. *Вісник студентського наукового товариства ДонНУ імені Василя Стуса*. Вінниця : ДонНУ імені Василя Стуса, 2021. Вип. 13. Том 1. С. 267-271.

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

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

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

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

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

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

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

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

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

12. Hrabina K., Shendryk V. Intelligent model of choosing the optimal risk events management strategy: threats and opportunities. *Artificial Intelligence*. Київ, 2022. № 2. P. 84-90. DOI: https://doi.org/10.15407/jai2022.02. URL: http://jai.in.ua/index.php/ua/issues?paper_num=1558.

13. Грабіна К.В., Шендрик В.В. Формування інтелектуальної моделі для вибору оптимальної стратегії управління ризиками. *Управління проєктами у розвитку суспільства*. Тези доповідей XX Міжнародної науково-практичної конференції (м. Київ, 12 травня 2023 року). Київ: КНУБА, 2023. С. 78-81.

14. Грабіна К. В., Шендрик В. В., Івашова Н. В. Алгоритм методу управління ризиками та можливостями в ІТ проєктах. *Теоретичні та практичні аспекти розвитку науки та освіти.* Тези доповідей X міжнародної науково-практичної конференції (м. Львів, 9-10 січня 2024 року). Львів: 2024, С. 77-80.

РОЗДІЛ 4. ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ІНТЕГРОВАНОГО УПРАВЛІННЯ ЗАГРОЗАМИ ТА МОЖЛИВОСТЯМИ В ІТ-ПРОЄКТАХ

4.1. Структура та схема інформаційної технології інтегрованого управління загрозами та можливостями в ІТ-проєкті

4.1.1 Розробка структури інформаційної бази інтегрованого управління загрозами та можливостями в ІТ-проєкті

В процесі досліджень, що були проведені у розділах 2 та 3 цієї дисертаційної роботи, були розроблені моделі та методи інтегрованого управління загрозами та можливостями в ІТ-проєктах. Метою цих моделей та методів є забезпечення інтегрованого управління ризиками в ІТ-проєктах з урахуванням впливу загроз та можливостей [1, 2, 3, 4, 5, 6, 7].

У підрозділі 1.4. цього дисертаційного дослідження були проаналізовані інформаційні технології, які можуть бути застосовані для управління ризиками в ІТ-проєктах, але автором визначено, що вони не дають змоги інтегровано управляти ризиками з урахуванням загроз та можливостей.

Інформаційна технологія інтегрованого управління загрозами та можливостями в ІТ-проєкті буде побудована на основі розробленої структури відповідної інформаційної бази (рис. 4.1.), яка включає у себе [8]:

0 – довідникова база інтегрованого управління загрозами та можливостями в ІТ-проєкті;

1 – інформаційна база загроз та можливостей в ІТ-проєкті;

2 – інформаційна база оцінки загроз та можливостей в ІТ-проєкті;

3 – інформаційна база управління загрозами та можливостями в ІТ-проєкті.

Файли довідникової бази інтегрованого управління загрозами та можливостями в ІТ-проєкті:

D1 – реєстр ІТ-проєктів;

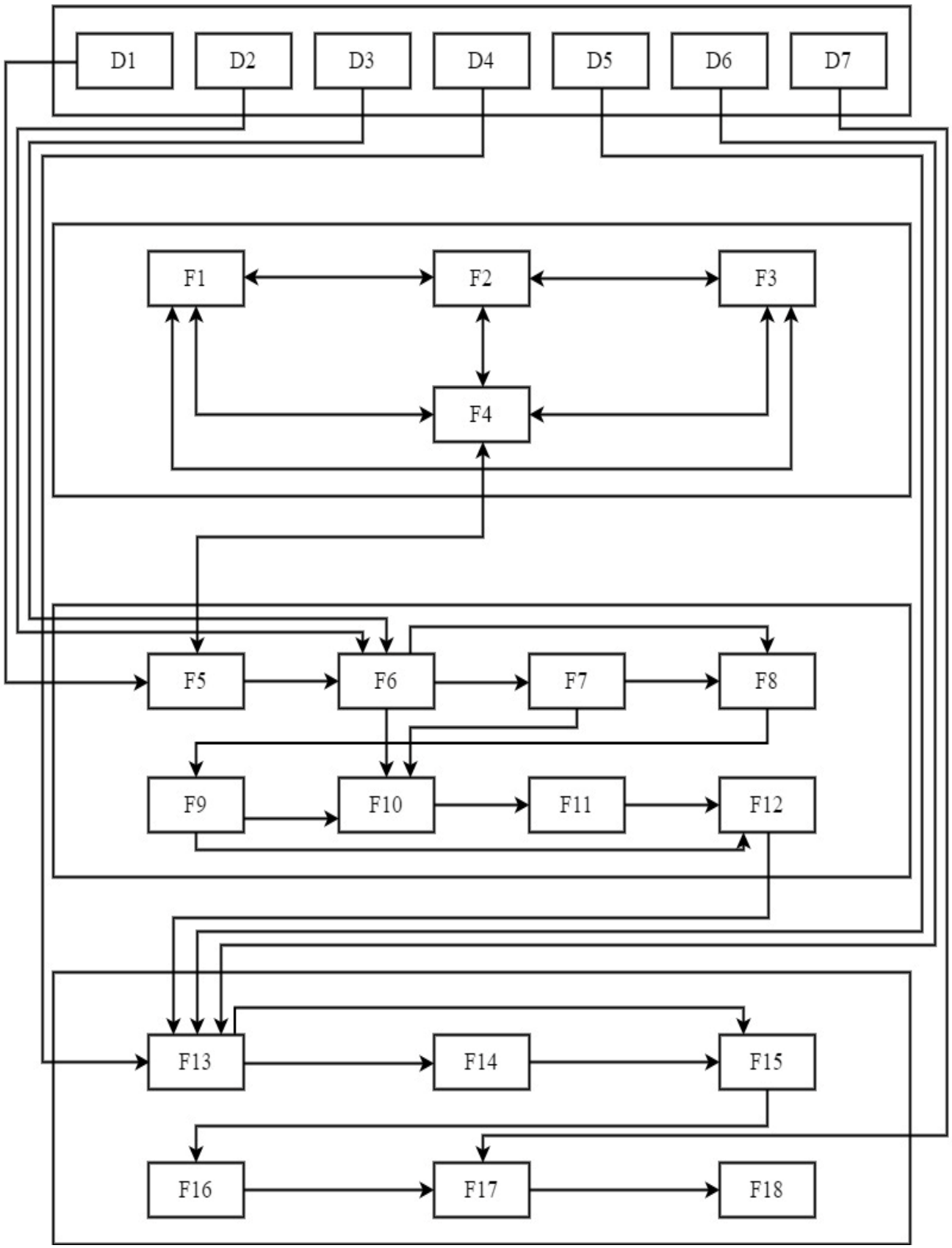


Рисунок 4.1. - Структура інформаційної бази інтегрованого управління загрозами та можливості в IT-проєкті

D2 – таблиця загроз IT- проєкту;

D3 – таблиця можливостей IT-проєкту;

D4 – стратегії реагування на невизначеність;

D5 – стратегії реагування на загрози;

D6 – стратегії реагування на можливості;

D7 – методи профілактики інтегрованого управління загрозами та можливостями в IT-проєкті.

Файли інформаційної бази інтегрованого управління загрозами та можливостями в IT-проєкті:

F1 – модель RIO-RIT-REO-RET аналізу в IT-проєкті;

F2 – таргетні моделі інтегрованого управління загрозами та можливостями в IT-проєкті;

F3 – інтелектуальна модель інтегрованого управління загрозами та можливостями в IT-проєкті;

F4 – вихідні дані для розрахунку математичної моделі інтегрованого управління загрозами та можливостями в IT-проєкті.

Файли інформаційної бази оцінки загроз та можливостей в IT-проєкті:

F5 – інформація про IT-проєкт;

F6 – попередній реєстр загроз та можливостей IT-проєкту;

F7 – результати RIO-RIT-REO-RET аналізу IT-проєкту, зокрема формування остаточного реєстру загроз та можливостей;

F8 – результати якісної оцінки загроз та можливостей IT-проєкту;

F9 – результати класифікації ризикованих подій IT-проєкту;

F10 – результати визначення кількісних показників впливу ризикованих подій IT-проєкту;

F11 – результати визначення синергетичного впливу загроз та можливостей в IT-проєкті;

F12 – граф ризиків IT-проєкту з урахуванням загроз та можливостей;

Файли інформаційної бази управління загрозами та можливостями в IT-проєкті:

F13 – множина альтернативних стратегій реагування на вплив невизначеності, загроз та можливостей в ІТ-проєкті;

F14 – результати розрахунку ймовірності успішного використання ризиків з урахуванням загроз та можливостей в ІТ-проєкті;

F15 – результати кількісного аналізу вартості стратегій реагування на вплив невизначеності, загроз та можливостей в ІТ-проєкті;

F16 – фактичні параметри загроз та можливостей ІТ-проєкту після застосування стратегій реагування;

F17 – методи профілактики для невизначеності, загроз та можливостей в ІТ-проєкті;

F18 – цільова функція управління загроз та можливостей в ІТ-проєкті після застосування методів профілактики.

Розроблена структура інформаційної бази інтегрованого управління загрозами та можливостями в ІТ-проєкті дасть можливість реалізувати моделі та методи управління ризиками в ІТ-проєкті з метою забезпечення накопичення статистичної та експертної інформації щодо управління загрозами та можливостями.

4.1.2. Розробка інформаційної технології інтегрованого управління загрозами та можливостями в ІТ-проєкті

На основі розроблених моделей та методів інтегрованого управління загрозами та можливостями в ІТ-проєктах (розділи 2 та 3 цього дисертаційного дослідження), а також відповідної структури інформаційної бази, що наведена у п. 4.1.1. цього дисертаційного дослідження, можна розробити відповідну інформаційну технологію [2, 3, 4, 5, 7].

В процесі розробки інформаційної технології стануть наукові праці, які були досліджені у п. 1.4. цього дослідження, та зокрема й такі: [9, 10, 11, 12, 13].

Структура інформаційної технології інтегрованого управління загрозами та можливостями в ІТ-проєкті наведена на рис. 4.2. та складається з наступних елементів [8]:

Рисунок 4.2. - Структура інформаційної технології інтегрованого управління загрозами та можливостями в ІТ-проєктах

1. Технологія наповнення інформаційної бази невизначеностей з урахуванням загроз та можливостей в ІТ-проєкті, що реалізується за допомогою моніторингу фактичних параметрів ІТ-проєкту із проєктної документації в процесі регулярного контролю його виконання.

При цьому використовуються розроблені моделі – модель RIO-RIT-REO-RET аналізу в ІТ-проєкті; таргетні моделі інтегрованого управління загрозами та можливостями в ІТ-проєкті; інтелектуальна модель інтегрованого управління загрозами та можливостями в ІТ-проєкті; математична модель інтегрованого управління загрозами та можливостями в ІТ-проєкті.

2. Технологія наповнення інформаційної бази оцінки загроз та можливостей в ІТ-проєкті, яка реалізується за допомогою розроблених моделей та методів інтегрованого управління загрозами та можливостями в ІТ-проєкті, зокрема:

– ідентифікації невизначеностей з урахуванням загроз та можливостей та класифікація ризикованих подій, що реалізується за допомогою RIO-RIT-REO-RET аналізу;

– визначення якісної та кількісної оцінки ризикових подій ІТ-проєкту за допомогою експертних методів та запропонованих автором таргетних моделей управління загрозами та можливостями ІТ-проєкту;

– визначення синергетичного впливу ризикованих подій ІТ-проєкту за допомогою математичної моделі управління загрозами та можливостями ІТ-проєкту та методу інтегрованого управління загрозами та можливостями в ІТ-проєкті.

3. Технологія наповнення інформаційної бази управління загрозами та можливостями в ІТ-проєкту, що складається з підбору та оцінки ефективності стратегій реагування на невизначеність, загрозим та можливості ІТ-проєкту, методів профілактики інтегрованого управління ризиками та можливостями ІТ-проєкту та зберігання здобутих уроків.

Означена технологія реалізується за допомогою розроблених методів зокрема: стратегій реагування на невизначеність, загрози та можливості, методів профілактики інтегрованого управління загрозами та можливостями в ІТ-проєкті, методу інтелектуального вибору оптимальної стратегії управління ризиковими подіями: загрозами та можливостями.

Схема інформаційної технології інтегрованого управління загрозами та можливостями в ІТ-проєкті наведена на рис. 4.3 [8].

Таким чином, розроблені структура інформаційної технології інтегрованого управління загрозами та можливостями в ІТ-проєкті, а також схема її реалізації, які у свою чергу дадуть змогу керівнику ІТ-проєкту та його команді реалізувати розроблені автором відповідні моделі та методи з метою забезпечення успішного та своєчасного виконання ІТ-проєкту для задоволення потреб його учасників.

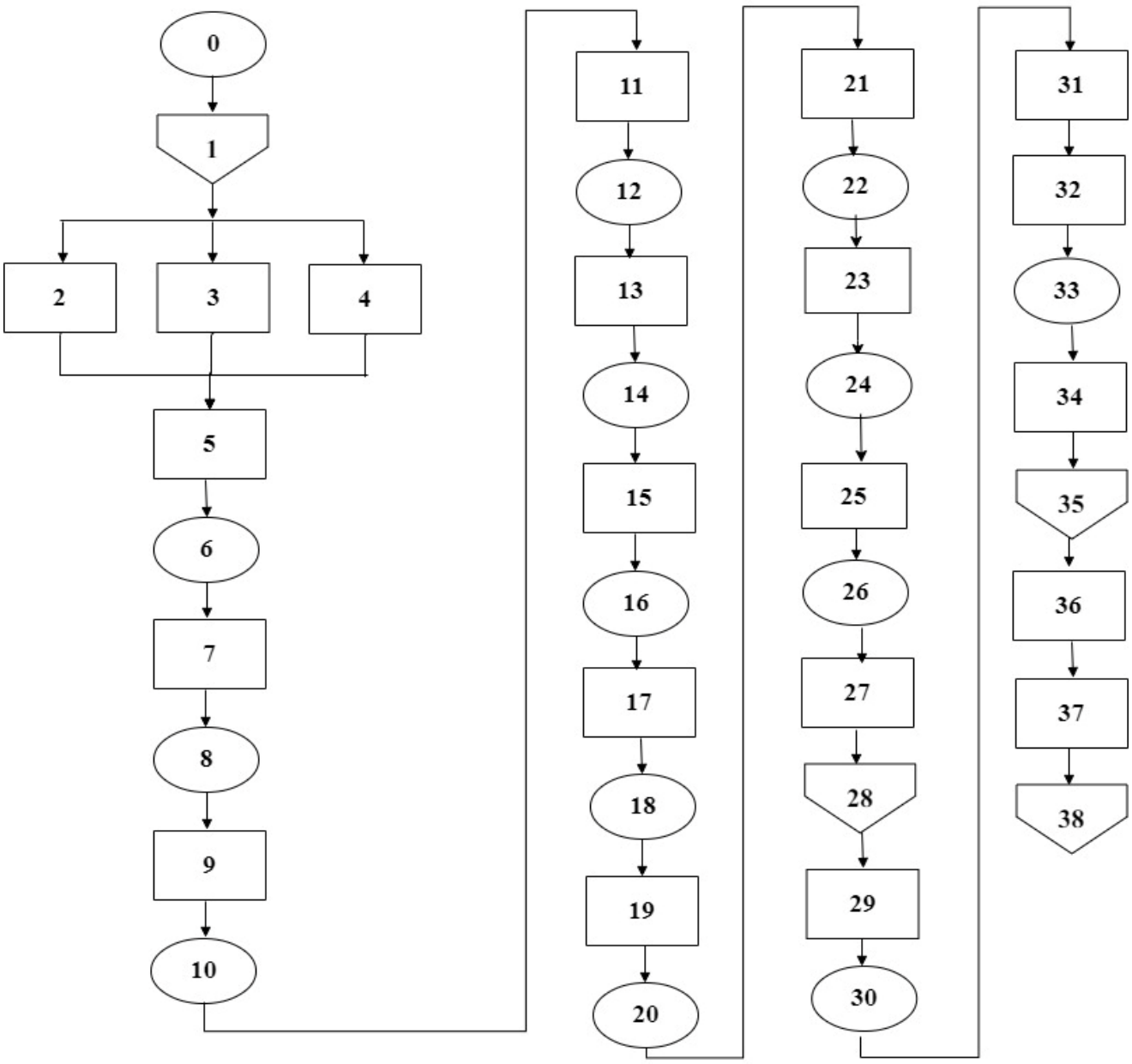


Рисунок 4.3. - Схема інформаційної технології інтегрованого управління загрозами та можливостями ІТ-проєкту

4.1.3. Алгоритм інформаційної технології інтегрованого управління загрозами та можливостями в ІТ-проєкті

Відповідно до проведених досліджень, що наведені у п. 4.1.1. та 4.1.2. цього дисертаційного дослідження, була розроблена інформаційна технологія інтегрованого управління загрозами та можливостями в ІТ-проєктах.

Враховуючи дослідження, що запропоновані науковцями у своїх роботах [9, 10, 12, 13, 14, 15, 16, 18], автором пропонується алгоритм інформаційної технології інтегрованого управління загрозами та можливостями в ІТ-проєкті [8]:

0. Формування довідникової бази інтегрованого управління загрозами та можливостями в ІТ-проєкті – наповнення даними файлів [1, 2, 3, 4, 5, 6, 7]:

– D1 – реєстр ІТ-проєктів (визначені у п. 1.1. цього дисертаційного дослідження);

– D2 – таблиця загроз ІТ-проєкту (приклад, яких наведено у табл. 2.1.);

– D3 – таблиця можливостей ІТ-проєкту (приклад, яких наведено у табл. 2.1.);

– D4 – стратегії реагування на невизначеність (див. табл. 3.1.);

– D5 – стратегії реагування на загрози (див. табл. 3.2.);

– D6 – стратегії реагування на можливості (див. табл. 3.3.);

– D7 – методи профілактики інтегрованого управління загрозами та можливостями в ІТ-проєкті (запропоновані у п. 3.1. цього дисертаційного дослідження).

1. У результаті регулярного контролю ІТ-проєкту надходять тижневі звіти з виконання робіт ІТ-проєкту, в яких наведені заплановані та фактичні показники робіт ІТ-проєкту (обсягів, часу та вартості), а також розраховані відхилення.

2. Відповідно до даних, що наведені у щотижневих звітах, будуються модель RIO-RIT-REO-RET аналізу в ІТ-проєкті (запропонована у п. 2.3.1. цього дисертаційного дослідження) [2].

3. Відповідно до даних, що наведені у щотижневих звітах, будуються таргетні моделі інтегрованого управління загрозами та можливостями в ІТ-проєкті (запропоновані у п. 2.3.2. цього дисертаційного дослідження) [3].

4. Відповідно до даних, що наведені у щотижневих звітах, будується інтелектуальна модель інтегрованого управління загрозами та можливостями в ІТ-проєкті (запропонована у п. 2.3.3. цього дисертаційного дослідження) [5, 6].

5. Відповідно до пунктів 2-4 розробляється математична модель інтегрованого управління загрозами та можливостями в ІТ-проєкті (запропонована у п. 2.4. цього дисертаційного дослідження) [4].

6. На підставі отриманих даних у пунктах 2-5, заповнюється інформаційна база інтегрованого управління загрозами та можливостями в ІТ-проєкті, зокрема: файли F1 – F4.

7. Відповідно до даних, що наведені в інформаційній базі інтегрованого управління загрозами та можливостями в ІТ-проєкті (файл D1), будується попередній реєстр ІТ-проєктів, як це було наведено у п. 1.1. цього дисертаційного дослідження.

8. Результати виконання пункту 7 заносяться у файл F5.

9. Для ІТ-проєктів, які ідентифіковані у пункті 8 (файл F6), проводиться формування попереднього реєстру загроз та можливостей ІТ-проєкту, із інформаційної бази інтегрованого управління загрозами та можливостями в ІТ-проєкті (файли D2 – D3), як це було представлено у п. 2.3.2. цього дисертаційного дослідження [2].

10. Результати виконання пункту 9 заносяться у файл F7.

11. Відповідно до даних, що наведені у файлах F6 та F7 (пункти 8 та 10), проводиться експертна якісна оцінка загроз та можливостей, як було наведено у п. 2.3.2. цього дисертаційного дослідження [3].

12. Результати, що отримані у пункті 11, заносяться у файл F8.

13. На підставі даних, що отримані у пункті 12, проводиться класифікації ризикованих подій ІТ-проєкту.

14. Результати, які отримані у пункті 13, вносяться до файлу F9 [5, 6, 7].

15. На основі даних, що наведені у файлі F9, визначаються кількісні показники впливу ризикованих подій ІТ-проєкту відповідно до таргетних моделей інтегрованого управління загрозами та можливостями в ІТ-проєкті, що була розроблена у п. 2.3.2. цього дисертаційного дослідження [3].

16. Результати пункту 15 заносяться у відповідний файл інформаційної бази інтегрованого управління загрозами та можливостями в ІТ-проєкті – F10.

17. Відповідно до даних, що отримані у пункті 16, та математичної моделі управління загрозами та можливостями в ІТ-проєктах (п. 2.4. цього дисертаційного дослідження), визначається синергетичний вплив загроз та можливостей в ІТ-проєкті [4].

18. Результати виконання пункту 17 заносяться у файл F11.

19. На підставі даних, що наведені у файлі F11, а також за допомогою застосування методу інтегрованого управління загрозами та можливостями в ІТ-проєктах (п. 3.1. цього дисертаційного дослідження), будується граф ризиків ІТ-проєкту з урахуванням загроз та можливостей [7].

20. Результати виконання пункту 19 заносяться у файл F12.

21. На підставі даних, що наведені у файлі F12, а також довідкових файлів D5 – D7, менеджер ІТ-проєкту формує множину альтернативних стратегій реагування на вплив невизначеності, загроз та можливостей в ІТ-проєкті [5, 6].

22. Результати пункту 21 заносяться у файл F13.

23. Відповідно до даних, що наведені у файлі F13, а також з урахуванням методу інтелектуального вибору оптимальної стратегії управління ризиковими подіями: загрозами та можливостями (п. 3.2. цього дисертаційного дослідження), проводиться розрахунок ймовірності успішного використання ризиків з урахуванням загроз та можливостей в ІТ-проєкті [5, 6].

24. Результати пункту 23 вносяться до файлу F14.

25. Відповідно до даних, що наведені у файлах F13 та F14, а також за допомогою методу інтелектуального вибору оптимальної стратегії управління ризиковими подіями: загрозами та можливостями (п. 3.2. цього дисертаційного дослідження), проводиться кількісний аналіз вартості стратегій реагування на вплив невизначеності, загроз та можливостей в ІТ-проєкті [5, 6].

26. Результати пункту 25 вносяться до файлу F15.

27. Реалізація стратегій реагування на невизначеність, загрози та можливості ІТ-проєкту, відповідно до обраних стратегій [7].

28. Надходять щотижневі звіти з виконання робіт ІТ-проєкту, а також з застосованих стратегій інтегрованого управління загрозами та можливостями в ІТ-проєкті.

29. На підставі даних, що отримані у пунктах 22, 24 та 26, а також відповідно до методу інтелектуального вибору оптимальної стратегії управління ризиковими подіями: загрозами та можливостями (п. 3.2. цього дисертаційного дослідження), визначаються фактичні параметри загроз та можливостей ІТ-проєкту після застосування стратегій реагування [5, 6].

30. Результати виконання пункту 29 заносяться у файл F16.

31. Контроль результатів реалізації зменшення впливу загроз та врахування впливу можливостей – якщо застосування обраних стратегій не допомогло зменшити негативні наслідки в ІТ-проєкті, перехід до пункту 2 або до пункту 23 інформаційної технології інтегрованого управління загрозами та можливостями в ІТ-проєкті, залежно від прийнятого рішення керівником ІТ-проєкту.

32. У разі успішної реалізації інтегрованого управління загрозами та можливостями ІТ-проєкту керівником ІТ-проєкту проводиться вибір методів профілактики для невизначеності, загроз та можливостей в ІТ-проєкті із довідникового файлу D7.

33. Інформація щодо виконання пункту 32 вноситься до файлу F17.

34. Застосування обраних методів профілактики для невизначеностей, загроз та можливостей ІТ-проєкту.

35. Надходження щотижневих звітів в ІТ-проєкті щодо виконаних робіт та реалізованих заходів профілактики для невизначеностей, загроз та можливостей.

36. Фактичні параметри невизначеностей, загроз та можливостей ІТ-проєкту після застосування відповідних методів профілактики вносяться до файлу F18 інформаційної бази інтегрованого управління загрозами та можливостями в ІТ-проєкті шляхом формування цільової функції управління загроз та можливостей в ІТ-проєкті [5, 6, 7].

37. Контроль впливів невизначеностей, загроз та можливостей на ІТ-проєкт на підставі даних, що наведені у файлі F18. У разі не зменшення впливу після

застосування методів профілактики можливий повтор вибору методів профілактики – перехід до пункту 32.

38. У разі успішного застосування методів профілактики реалізація інформаційної технології завершується й проводиться формування та роздрукування звітів з інтегрованого управління загрозами та можливостями в ІТ-проєкті.

Наведений алгоритм наповнення інформаційної технології інтегрованого управління загрозами та можливостями в ІТ-проєкті дозволить управляти ризиками з урахуванням загроз та можливостей відповідно до розроблених моделей та методів інтегрованого управління загрозами та можливостями в ІТ-проєкті, яка відрізняється від сучасних підходів до управління ризиками в методології управління проєктами та програмами й дозволить зменшити негативні впливи та врахувати позитивні впливи в ІТ-проєкті.

4.2. Приклад реалізації ІТ-проєкту

З метою реалізації розроблених моделей та методів інтегрованого управління загрозами та можливостями в ІТ-проєкті пропонується розглянути проєкти відповідної предметної галузі [1, 2].

Спочатку автором цієї роботи пропонується проаналізувати ІТ-проєкт, який реалізовувався до застосування розроблених моделей та методів, що були висвітлені у цьому дослідженні, а також ІТ-проєкт, де досліджувані нами у роботі моделі і методи були застосовані. Після цього розглянемо різницю у результатах, які показало таке підприємство порівняно з підприємством, де досліджувані нами у роботі моделі і методи не були застосовані, а також які переваги при реалізації другого проєкту було отримано [3, 4, 5, 6, 7, 8].

Найменування ІТ-проєкту: Інтерв’ю з клієнтом, версія №6.

Метою ІТ-проєкту є внесення змін до автоматизованого процесу підготовки співробітників та кандидатів компанії до співбесід із замовниками, зокрема:

− додавання завдання менеджеру проєкту (PM) для затвердження оновленого резюме заощаджує час та зусилля на додаткові комунікації з помічниками щодо операцій й вимагає затвердження PM резюме кандидата;

− усунення обов’язку директора затверджувати оновлене резюме економить час та зусилля директора від проблем нижчого рівня;

− оновлення причин відмови на співбесіді допомагає зробити їх більш універсальними та вибрати правильну причину;

− додавання нових полів до списку кандидатів запобігає помилкам у звіті про управління ресурсами та окупиться через ~ 4 місяці;

− оновлення правил виконання та опису сповіщення про початок робочого процесу надає своєчасну інформацію про нових кандидатів;

− об’єднання завдань РЗ-9 «Домовитися про зустріч з кандидатом» та РЗ-11/РЗ-12 «Проінструктувати кандидата» запобігає частому переходу між завданнями, скорочує час і зусилля на виконання завдання та окупається через 19 місяців;

− об’єднання завдань РЗ-14 «Надіслати резюме замовнику» та РЗ-15 «Отримати відповідь клієнта» запобігає частому переходу між завданнями, скорочує час і зусилля на виконання завдання та окупається через ~ 10 місяців;

− об’єднання завдань РЗ-16 «Провести пробну співбесіду» та РЗ-17 «Провести пробну співбесіду» запобігає частому переходу між завданнями, скорочує час і зусилля на виконання завдання та окупається через ~ 10 місяців.

− додавання проєктного менеджера та назви проєкту до завдань РЗ-1 «Підготуйте та завантажте коротку оповідь про себе» та РЗ-13 «Ознайомтеся з резюме» заощаджує час та зусилля на додаткові комунікації кандидата, команди управління ресурсами, команди HR.

Продукт ІТ-проєкту: Автоматизований процес з підготовки до інтерв'ю співробітника компанії з замовником на основі технологій Microsoft, SharePoint 2013. Робочі процеси SharePoint – це попередньо запрограмовані міні-додатки, які спрощують та автоматизують різноманітні бізнес-процеси. Робочі процеси можуть варіюватися від збору підписів, відгуків або схвалень плану чи

документа до відстеження поточного статусу рутинної процедури. Робочі цикли SharePoint створені, щоб заощадити час і зусилля, а також забезпечити послідовність і ефективність завдань, які ви виконуєте регулярно.

Тип ІТ-проєкту: внутрішній проєкт для обслуговування інфраструктури компанії.

Тип фінансування ІТ-проєкту: фіксована ціна.

ІТ-проєкт був запланований та реалізований за допомогою водоспадної моделі (Waterfall).

Період реалізації ІТ-проєкту: 01.03.2022 – 31.07.2022.

Отримані уроки за результатами реалізації ІТ-проєкту:

− для перевірки цього складного робочого процесу було призначено 4 QAEs. Деякі з них були тимчасово призначені для робочих процесів SP, щоб допомогти команді та перейти до оплачуваних проєктів. Загальновідомо, що ресурси, призначені на поточний базис, є більш ефективними. Крім того, близько 50 годин було витрачено на повне ознайомлення з різними частинами функціональності всіма членами команди;

− огляд експерта SDE (TL) був вирішальним для версії №6;

− у разі ускладнення робочих процесів або його змін експертний огляд SDE (TL) специфікації повинен бути проведений якнайшвидше;

− стабілізаційні пакети робіт були досить недооцінені;

− команда повинна проаналізувати причину заниженої оцінки. На стабілізацію зі сторони розробки потрібно приділити більше часу, що залежить від процедури розгортання;

− у вечірній час обов'язково мають бути додаткові перевірки, оскільки виникло багато проблем;

− робочий процес слід перевіряти у вечірній час для такого складного робочого процесу (він має паралельні процеси);

− одне завдання вимагало зміни, яке не потрібно;

− потрібні додаткові повідомлення щодо переліку питань. Для важливого моменту між TL, BA, SDE та QAE має бути проведена щоденна зустріч проєкту або додаткове спілкування;

− робочі процеси SharePoint працювали нестабільно через роботу з обслуговування SharePoint, яку виконувала Microsoft, що потенційно могло призвести до затримки доставки робочого процесу. У разі браку часу під час доставки PM і TL повинні допомогти команді визначити пріоритетність робочих дій у виробництві, щоб досягти обмежень доставки;

− новий BA був призначен на проєкт через те, що попередній залишив компанію. Бажано призначити одного бізнес-аналітика до версії, щоб досягти єдиного розуміння функціональності та виконання завдань;

− після стабілізації продукту сталося, що для доставки версії робочого процесу необхідно дочекатися завершення всіх процесів на виробництві. Тому необхідно реалізувати можливість включення режиму тестування. Режим тестування має бути реалізований для всіх робочих процесів з V6 і пізнішою версією;

− специфікація була готова і відправлена в реалізацію ~ за 1,5 місяці до необхідної дати початку діяльності. Кожного релізу стикалися з ситуацією, що бракує часу на впровадження версії. Тому краще не планувати відпустку для виділених ресурсів протягом 2-3 місяців підготовки версії, особливо дизайну.

Основні показники реалізації IT-проєкту наведені у табл. 4.1.

Таблиця 4.1. Основні показники реалізації IT-проєкту

Показники	Значення		Відхилення	
	план	факт	+/-	%
Тривалість IT-проєкту, міс.	1	5	+ 4	+ 400,0
Витрати часу співробітників, год.	113,5	324	+ 210,5	+ 185,5
Бюджет проєкту, тис. дол.	5,7	6,2	+ 0,5	+ 8,7

З аналізу даних, що наведені у табл. 4.1. видно, що IT-проєкт був завершений із затримкою на 4 місяці, перевитрати часу співробітників склали

210,5 год. та перевищення бюджету ІТ-проєкту склало 530 дол., можна дійти висновку, що реалізація ІТ-проєкту не є успішною.

4.3. Практична реалізація розроблених моделей та методів інтегрованого управління загрозами та можливостями в ІТ-проєкті

Найменування ІТ-проєкту: Розробка програмного забезпечення, фаза №2.

Метою ІТ-проєкту є скорочення часу обробки пропозицій клієнта та підвищення відсотку виграшу від використання веб-додатку, дозволивши своїм клієнтам легко розробляти індивідуальні додатки із готових металевих металевих виробів та компонентів і миттєво отримувати пропозиції.

Продукт ІТ-проєкту: веб-платформа для простого та інтуїтивно зрозумілого конструювання конструкцій у 3D на основі каталогу деталей компанії X та замовлення їх онлайн. У каталозі представлений широкий асортимент деталей від металевих профілів до фурнітури, кронштейнів і кріплень різних серій. Клієнти можуть розмістити потрібні їм частини в потрібних розмірах на 3D-сцені, з’єднати їх одна з одною за допомогою широкого спектру кріплень, отримати остаточний вигляд свого дизайну в засобі 3D-перегляду, отримати специфікацію матеріалів, прораховані ціни та отримати своє замовлення онлайн. Програмне забезпечення також підтримує експорт проєктів клієнтів у STEP файл, щоб клієнти могли продовжувати працювати зі створеними проєктами в будь-якому програмному забезпеченні САПР, яке вони використовують.

Тип ІТ-проєкту: клієнт є провідним виробником виготовлених на замовлення та готових металевих кріплень та елементів. Металеві профілі цієї компанії були визначними компонентами для багатьох інноваційних продуктів і застосувань у будівництві та промисловості.

Тип фінансування ІТ-проєкту: Time and Material with Cap.

ІТ-проєкт був запланований та реалізований за допомогою гнучкої методології управління проєктами (Scrum).

Період реалізації ІТ-проєкту: 2022 –2023.

Для означеного ІТ-проєкту пропонується застосування розроблених автором моделей та методів інтегрованого управління загрозами та можливостями в ІТ-проєкті, який наведено у розділі 3. цього дисертаційного дослідження. Відповідно до методу інтегрованого управління загрозами та можливостями в ІТ-проєкті, який наведено у п. 3.1. цього дослідження, розглянемо його етапи:

1. Ідентифікація загроз та можливостей за допомогою матриці RIO-RIT-REO-RET. Результати якої наведемо у вигляді табл. 4.2 [1, 2, 8]. У табл. 4.2. наведені результати ідентифікації та якісного аналізу загроз та можливостей ІТ-проєкту.

Таблиця 4.2. Ідентифікація загроз та можливостей ІТ-проєкту

Код	Ризики	Джерело виникнення	Ступінь впливу
1	2	3	4
d1	Каталог не містить повної інформації про необхідні послуги обробки, умови розміщення елементів тощо. Таким чином, обсяг проєкту може збільшитися, якщо під час розробки з’являться нові випадки використання або умови та необхідні послуги обробки.	E	Високий
d2	Висока ймовірність потреби у створенні окремого підходу для замикання деталей з унікальною геометрією, що може збільшити час впровадження.	I	Високий
d3	Затримки в наданні необхідних ресурсів (заповнених шаблонів для імпорту даних у базу даних програмного забезпечення, зображень і файлів STEP елементів каталогу, хмарних сховищ тощо) від команди замовника.	E	Високий

Продовження табл. 4.2.

1	2	3	4
d4	Розширення сфери застосування в процесі розробки. У випадку зміни правил для послуг обробки, додавання нових послуг обробки або з’явлення правил для окремих компонентів тощо, це збільшить обсяг роботи проєкту.	E	Високий
d5	У разі розширення списку ролей для облікових записів адміністраторів або дистриб’юторів замовника можуть знадобитися додаткові	I	Високий
	зусилля щодо розробки (наприклад, зміна бази даних).		
d6	Зміни в ієрархії клієнтів та дистриб’юторів можуть викликати зміни в облікових записах компаній та клієнтів, що призведе до зміни у базі даних.	I	Високий
d7	Залежність від версії пристрою, програмних модулів, встановлених на пристрої, окремих налаштувань пристрою може не гарантувати стабільну роботу програмного забезпечення.	E	Високий
d8	Обмеження, несумісність та помилки в сторонніх бібліотеках і API компонентів.	E	Середній
d9	Початково визначені треті сторони для моделювання CAD та інші бібліотеки з відкритим кодом можуть не відповідати всім вимогам після детального уточнення.	E	Середній
d10	Розширена обробка сітки може не виконуватися повністю за допомогою бібліотек WGL і PD, можуть знадобитися додаткові компоненти.	E	Середній
d11	Складність і потреба в додатковому досвіді для виконання тестування безпеки та продуктивності/навантаження/інтеграції.	I	Середній
d12	Попередньо налаштовані кадри будуть представлені як окремі частини на 3D-сцені, якщо буде відбуватися з’єднання один з одним, то вони не будуть розглядатися як група.	I	Високий
d13	Точки прив’язки можуть бути неправильно визначені технічною командою, інакше програмне забезпечення не працюватиме належним чином щодо замикання частин і створення з’єднань.	I	Високий

Продовження табл. 4.2.

1	2	3	4
d14	Кріплення для типів з'єднання «компонент» і «панель – сторона екструзії» буде показано лише як комбінації. Технічна команда підготує комбінації, які будуть показані для кожного типу підключення. У раз необхідності іншого підходу, потрібно буде змінювати комбінації.	I	Низький
d15	У Америці, Канаді та Австралії немає спеціальних політик щодо доступу до персональних даних (наприклад, GDPR у Європі), є ризик публічного доступу до даних.	E	Високий
d16	У разі розширення на європейський ринок, програма потребує додаткових налаштувань, оскільки необхідно підтримувати GDPR.	I	Низький
d17	Якщо цековки будуть представлені у вигляді складних фігур з фасками, то буде потреба у спрощенні фігур за допомогою додаткових алгоритмів.	I	Середній
d18	Похибка від відсутності різьби у геометрії отворів може вплинути на деякі конструкції.	I	Високий
d19	Час для створення точок прив'язки для вимірювань в системі У може значно перевищувати заплановану величину.	I	Високий
d20	Усі необхідні параметри для додавання модифікацій геометрії для експорту геометрії в STEP можуть бути недоступні у властивостях відповідної служби обробки (наприклад, діаметр розточування, глибина розточування, діаметр отвору, глибина отвору, відстань до центру розточування від кінця екструзії тощо).	I	Високий
d21	Адміністратори матимуть лише 1 роль із однаковими дозволами, що може спричинити розповсюдження інформації та викликає конфлікт інтересів між ними.	I	Високий
d22	Сумісність з'єднувальних панелей з екструзійними пазами буде залежати не тільки від серії та товщини, ця невизначеність може спричинити колліжени у панелях.	I	Низький

Продовження табл. 4.2.

1	2	3	4
c1	Остаточна назва програмного забезпечення та остаточний маркетинговий вміст (наприклад, текст сповіщень електронною поштою) при старті проєкту не вирішені та не входить в загальний зміст проєкту, необхідно додатково запропонувати ці послуги замовнику.	E	Середній
c2	Пошукова система не потрібна, програмне забезпечення не буде окремо індексуватися на момент старту проєкту, така необхідність може виникнути, необхідно додатково запропонувати ці послуги замовнику.	E	Високий
c3	Програмне забезпечення буде інтегровано в головний веб-сайт. Підхід до інтеграції буде обговорено пізніше та узгоджено з командою замовника. Інтеграція виходить за рамки проєкту, необхідно додатково запропонувати ці послуги замовнику.	E	Високий
c4	Автоматизована пропозиція компонентів, таких як з'єднувальні пластини, кронштейни для з'єднань «екструзія до екструзії», їх автоматичне розміщення на 3D-сцені та візуалізація виходить за рамки проєкту. Необхідно додатково запропонувати ці послуги замовнику під кінець проєкту.	E	Високий
c5	Перфоменс, безпека та локалізація виходять за межі проєкту та можуть бути додані за запитом замовника, необхідно запропонувати ці роботи з часом.	E	Високий
c6	Команда замовника хоче сама забезпечити необхідне віддалене виробниче середовище, хмарні можливості та процеси налаштування та розгортання, але є можливість продати ці послуги, запропонувавши конкурентні ціни на послуги у порівнянні з американським ринком праці.	E	Високий
c7	BPCS наразі використовується як програмне забезпечення ERP, але в майбутньому планується перехід на Oracle Cloud ERP. Oracle Cloud ERP буде встановлено до моменту роботи над інтеграцією ERP, що дає змогу запропонувати замовнику інтеграційний пакет.	E	Високий

2. Оцінка всіх ризиків, зокрема, загроз та можливостей, за таргетними моделями [3, 7].

Результати цього етапу наведені у вигляді табл. 4.3. та табл. 4.4.

Таблиця 4.3. Кількісний аналіз виявлених загроз ІТ-проєктів

Код	P_{jd}	V_{jdb}	V_{jdt}	V_{jds}	V_{jdq}	D_b	D_t	D_s	D_q
d1	0.8	-9	-10	-4	0	-7.2	-8.0	-3.2	0.0
d2	0.9	-9	-10	-5	-5	-8.1	-9.0	-4.5	-4.5
d3	0.8	-3	-7	-6	-3	-2.4	-5.6	-4.8	-2.4
d4	0.7	-8	-10	-4	-7	-5.6	-7.0	-2.8	-4.9
d5	0.8	-10	-10	-10	-5	-8.0	-8.0	-8.0	-4.0
d6	0.9	-9	-7	-7	-9	-8.1	-6.3	-6.3	-8.1
d7	0.7	-5	-1	-1	-9	-3.5	-0.7	-0.7	-6.3
d8	0.5	-10	-1	-1	0	-5.0	-0.5	-0.5	0.0
d9	0.6	0	-10	-1	0	0.0	-6.0	-0.6	0.0
d10	0.4	-10	-5	0	0	-4.0	-2.0	0.0	0.0
d11	0.6	-10	-9	0	-7	-6.0	-5.4	0.0	-4.2
d12	0.8	-10	-9	0	0	-8.0	-7.2	0.0	0.0
d13	0.9	-10	-10	0	-9	-9.0	-9.0	0.0	-8.1
d14	0.2	-3	-10	0	-10	-0.6	-2.0	0.0	-2.0
d15	0.7	-3	-8	-1	-10	-2.1	-5.6	-0.7	-7.0
d16	0.1	-8	-10	-1	-3	-0.8	-1.0	-0.1	-0.3
d17	0.6	-9	-8	-7	-10	-5.4	-4.8	-4.2	-6.0
d18	0.9	-10	-10	-10	-7	-9.0	-9.0	-9.0	-6.3
d19	0.8	-6	-8	-1	-4	-4.8	-6.4	-0.8	-3.2
d20	0.9	-2	-10	0	-6	-1.8	-9.0	0.0	-5.4
d21	0.7	-6	-8	-1	-4	-4.2	-5.6	-0.7	-2.8
d22	0.3	-2	-10	0	-6	-0.6	-3.0	0.0	-1.8
Разом:						-104.2	-121.1	-46.9	-77.3

Таблиця 4.4. Кількісний аналіз виявлених можливостей ІТ-проєктів

Код	P_{ic}	V_{icb}	V_{ict}	V_{ics}	V_{icq}	C_b	C_t	C_s	C_q
c1	0.6	8	7	3	1	4.8	4.2	1.8	0.6
c2	0.9	1	8	2	2	0.9	7.2	1.8	1.8
c3	0.8	1	9	1	9	0.8	7.2	0.8	7.2
c4	0.7	8	7	10	4	5.6	4.9	7.0	2.8
c5	0.7	5	9	10	1	3.5	6.3	7.0	0.7
c6	0.8	6	8	7	5	4.8	6.4	5.6	4.0
c7	0.7	5	2	4	1	3.5	1.4	2.8	0.7
Разом:						23.9	37.6	26.8	17.8

За результатами оцінки ризиків, зокрема загроз та можливостей, ІТ-проєкту будуються таргетні моделі їхнім впливом на бюджет, час, обсяг та якість, як наведено на рис. 2.4. – 2.7. та 2.9. – 2.12.

3. Оцінка синергетичного ефекту від загроз та можливостей (*D*, *C*), за допомогою формули (2.30) [4, 7, 19].

$$E = \frac{1250.0 - 492.0 - \left((23.9 + 37.6 + 26.8 + 17.8) - (-104.2 + (-121.1) + (-46.9) + (-77.3))\right)}{1250.0 - 492.0 + (23.9 + 37.6 + 26.8 + 17.8) - (-104.2 + (-121.1) + (-46.9) + (-77.3))} = 0.25.$$

Виходячи із отриманих результатів, можна дійти висновку, що ІТ-проєкт, який розглядається, має негативний синергетичний ефект від управління загрозами та можливостями, що, у свою чергу, вимагає застосування заходів управління ризиками з урахуванням загроз та можливостей.

4. Для кожного ризику $i = 1, N$ (N – кількість ризиків ІТ-проєкту) проводиться ранжування за допомогою матриці ймовірності та впливу ризиків або інших інструментів управління ризиками на критичні, середні та низькі [19]. Результати цього пункту наведені у вигляді табл. 4.5.

Таблиця 4.5. Матриця ймовірностей та впливу виявлених загроз та можливостей ІТ-проєкту

Вплив / Ймовір-ність	Загрози					Можливості				
	-4	-12	-20	-28	-36	36	28	20	12	4
0.8-1.0			d1, d3, d12, d19, d20	d2, d13	d5, d6, d18		c6	c3	c2	
0.6-0.8			d7, d15, d21	d4			c4, c5	c1	c7	
0.4-0.6		d8, d9, d10		d11	d17					
0.2-0.4			d22							
0.0-0.2			d14, d16							

З табл. 4.5. видно результати ранжування загроз та можливостей ІТ-проєкту, що розглядається, зокрема:

- критичні – d2, d4, d5, d6, d13, d17, d18, c4, c5 та c6;
- середні – d1, d3, d7, d11, d12, d15, d19, d20, d21, c1, c2 та c3;
- низькі – d8, d9, d10, d14, d16, d22 та c7.

5. Якщо *R* критичний? Якщо умова виконується, то відбувається перехід до п. 6, якщо ні, то до п. 8. Як видно із пункту 4, то до критичних відносяться наступні загрози (d2, d4, d5, d6, d13, d17 та d18) та можливості (c4, c5 та c6). Для них необхідно у першу чергу розробити методи боротьби та посилення [12, 13, 17, 19].

6. Розробка методів боротьби/посилення [12, 13, 17, 19]. На цьому етапі відбувається вибір оптимальної стратегії управління ризиковою подією. Результати виконання цього етапу наведені у табл. 4.6.

Таблиця 4.6. Пропоновані методи боротьби із критичними загрозами та посилення впливу критичних можливостей в ІТ-проєкті

Код	Ризики	Методи боротьби/посилення
1	2	3
d2	Висока ймовірність потреби у створенні окремого підходу для замикання деталей з унікальною геометрією, що може збільшити час впровадження.	Передача
d4	Розширення сфери застосування в процесі розробки. У випадку зміни правил для послуг обробки, додавання нових послуг обробки або з’явлення правил для окремих компонентів тощо, це збільшить обсяг роботи проєкту.	Передача
d5	У разі розширення списку ролей для облікових записів адміністраторів або дистриб’юторів замовника можуть знадобитися додаткові зусилля щодо розробки (наприклад, зміна бази даних).	Прийняття
d6	Зміни в ієрархії клієнтів та дистриб’юторів можуть викликати зміни в облікових записах компаній та клієнтів, що призведе до зміни у базі даних.	Прийняття
d13	Точки прив’язки можуть бути неправильно визначені технічною командою, інакше програмне забезпечення не працюватиме належним чином щодо замикання частин і створення з’єднань.	Пом’якшення

Продовження табл. 4.6.

1	2	3
d17	Якщо цековки будуть представлені у вигляді складних фігур з фасками, то буде потреба у спрощенні фігур за допомогою додаткових алгоритмів.	Прийняття
d18	Похибка від відсутності різьби у геометрії отворів може вплинути на деякі конструкції.	Прийняття
c4	Автоматизована пропозиція компонентів, таких як з'єднувальні пластини, кронштейни для з'єднань «екструзія до екструзії», їх автоматичне розміщення на 3D-сцені та візуалізація виходить за рамки проєкту. Необхідно додатково запропонувати ці послуги замовнику під кінець проєкту.	Розподіл
c5	Перфоменс, безпека та локалізація виходять за межі проєкту та можуть бути додані за запитом замовника, необхідно запропонувати ці роботи з часом.	Використання
c6	Команда замовника хоче сама забезпечити необхідне віддалене виробниче середовище, хмарні можливості та процеси налаштування та розгортання, але є можливість продати ці послуги, запропонувавши конкурентні ціни на послуги у порівнянні з американським ринком праці.	Використання

З табл. 4.6. видно, що команда IT-проєкту в більшості випадків бере на себе боротьбу із критичними ризиками та використання критичних можливостей.

7. Розробка методів профілактики [12, 13].

Зважаючи на наведені у табл. 4.6. загрози та можливості IT-проєкту, то можна дійти висновку, що для кожної критичної загрози та можливості необхідно застосовувати індивідуальні методи профілактики.

8. Якщо *R* середній? То відбувається перехід до п. 6, якщо ні, то до п. 7.

Як було виявлено у п. 4 (див. табл. 4.5.) цього підрозділу, то до середніх можна віднести загрози: d1, d3, d7, d11, d12, d15, d19, d20 та d21, а також можливості – c1, c2 та c3.

Запропонований автором метод передбачає управління ще й середніми загрозами та можливостями, то зважаючи на це, у табл. 4.7. наведено методи боротьби/посилення для них.

Таблиця 4.7. Пропоновані методи боротьби із середніми загрозами та посилення впливу середніх можливостей в IT-проєкті

Код	Ризики	Методи боротьби/посилення
1	2	3
d1	Каталог не містить повної інформації про необхідні послуги обробки, умови розміщення елементів тощо. Таким чином, обсяг проєкту може збільшитися, якщо під час розробки з'являться нові випадки використання або умови та необхідні послуги обробки.	Передача
d3	Затримки в наданні необхідних ресурсів (заповнених шаблонів для імпорту даних у базу даних програмного забезпечення, зображень і STEP файлів каталогу, хмарних сховищ тощо) від команди замовника.	Прийняття
d7	Залежність від версії пристрою, програмних модулів, встановлених на пристрої, окремих налаштувань пристрою може не гарантувати стабільну роботу програмного забезпечення.	Прийняття
d11	Складність і потреба в додатковому досвіді для виконання тестування безпеки та продуктивності/навантаження/інтеграції.	Ескалація
d12	Попередньо налаштовані кадри будуть представлені як окремі частини на 3D-сцені, якщо буде відбуватися з'єднання один з одним, то вони не будуть розглядатися як група.	Прийняття
d15	У Америці, Канаді та Австралії немає спеціальних політик щодо доступу до персональних даних (наприклад, GDPR у Європі), є ризик публічного доступу до даних.	Уникнення
d19	Час для створення точок прив'язки для вимірювань в системі У може значно перевищувати заплановану величину.	Ескалація

Продовження табл. 4.7.

1	2	3
d20	Усі необхідні параметри для додавання модифікацій геометрії для експорту геометрії в STEP можуть бути недоступні у властивостях відповідної служби обробки (наприклад, діаметр розточування, глибина розточування, діаметр отвору, глибина отвору, відстань до центру розточування від кінця екструзії тощо).	Пом’якшення
d21	Адміністратори матимуть лише 1 роль із однаковими дозволами, що може спричинити розповсюдження інформації та викликає конфлікт інтересів між ними.	Прийняття
c1	Остаточна назва програмного забезпечення та остаточний маркетинговий вміст (наприклад, текст сповіщень електронною поштою) при старті проєкту не вирішені та не входить в загальний зміст проєкту, необхідно додатково запропонувати ці послуги замовнику.	Ескалація
c2	Пошукова система не потрібна, програмне забезпечення не буде окремо індексуватися на момент старту проєкту, така необхідність може виникнути, необхідно додатково запропонувати ці послуги замовнику.	Прийняття
c3	Програмне забезпечення буде інтегровано в головний веб-сайт. Підхід до інтеграції буде обговорено пізніше та узгоджено з командою замовника. Інтеграція виходить за рамки проєкту, необхідно додатково запропонувати ці послуги замовнику.	Прийняття

З табл. 4.7. видно, що команда ІТ-проєкту в більшості випадків бере на себе боротьбу із середніми ризиками та використання середніх можливостей.

Крім того, зважаючи на наведені у табл. 4.7. загрози та можливості ІТ-проєкту, то можна дійти висновку, що для кожної середньої загрози та можливості необхідно застосовувати індивідуальні методи профілактики.

Основні показники реалізації ІТ-проєкту наведені у табл. 4.8.

Таблиця 4.8. Основні показники реалізації ІТ-проєкту

Показники	Значення		Відхилення	
	план	факт	+/-	%
Тривалість ІТ-проєкту, міс.	12	9	- 3	- 25
Витрати часу співробітників, год.	6 253,75	13 476,95	+ 7 223,2	+ 115,5
Бюджет проєкту, тис. дол.	492,0	499,0	+ 7,0	+ 1,4

З аналізу даних, що наведені у табл. 4.8. видно, що ІТ-проєкт був завершений раніше на 3 місяці, незважаючи на те, що перевитрати часу співробітників склали 7 223,2 год. та перевищення бюджету ІТ-проєкту склало 7,0 тис. дол., можна дійти висновку, що реалізація цього ІТ-проєкту є успішною.

Застосування моделей, методів та інформаційної технології інтегрованого управління загрозами та можливостями в ІТ-проєктах показали свою дієвість та дозволили завершити ІТ-проєкт раніше на три місяці, але з перевищенням бюджету.

Унаслідок проведеного аналізу стає зрозумілим, що наявними у ІТ-проєкті загрозами необхідно управляти та застосовувати стратегії щодо управління ними з метою зниження їхнього впливу на проєкт.

Отже, загрози ІТ-проєктів потребують більшої уваги, оскільки саме від якості інтегрованого управління ними залежить успіх реалізації ІТ-проєкту.

Моделі, методи та інформаційна технологія інтегрованого управління загрозами та можливостями в ІТ-проєктах, що запропоновані автором у цьому дисертаційному досліджені, полягають в інтегрованому управлінні ризиками з урахуванням загроз та можливостей шляхом застосування стратегій управління ними з метою зниження негативного впливу загроз та посилення впливу можливостей на реалізацію ІТ-проєкту.

Відповідно до даних, що були отримані у підрозділах 4.2. та 4.3. цього дослідження, зокрема табл. 4.1 та 4.8, можна провести аналіз отриманих результатів. Результати наведемо у вигляді табл. 4.9.

Таблиця 4.9. Порівняльний аналіз основних показників реалізації ІТ-проєктів

Показники	До				Після			
	Значення		Відхилення		Значення		Відхилення	
	план	факт	+/-	%	план	факт	+/-	%
Тривалість ІТ-проєкту, міс.	1	5	+ 4	+ 400,0	12	9	- 3	- 25
Витрати часу співробітників, год.	113,5	324	+ 210,5	+ 185,5	6 253,75	13 476,95	+ 7 223,2	+ 115,5
Бюджет проєкту, тис. дол.	5,7	6,2	+ 0,5	+ 8,7	492,0	499,0	+ 7,0	+ 1,4

Виходячи із даних, що наведені у табл. 4.9 можна дійти висновку, що застосування моделей, методів та інформаційної технології інтегрованого управління загрозами та можливостями в ІТ-проєктах дозволило зменшити непередбачувані витрати на ІТ-проєкт на 7,3%.

Таким чином, можна вважати, що застосування моделей, методів та інформаційної технології інтегрованого управління загрозами та можливостями в ІТ-проєктах є дієвим інструментом, які дозволили знизити вплив загроз та посилити вплив можливостей на ІТ-проєкт, а розроблені стратегії управління ними дозволили знизити вплив критичних та середніх загроз.

4.4. Висновки за четвертим розділом

За результатами практичної реалізації розроблених моделей, методів та інформаційної технології інтегрованого управління загрозами та можливостями в ІТ-проєктах можна зробити наступні висновки:

1. Науково-практичні інструменти, розроблені та удосконалені в роботі, дають змогу ефективно управляти ризиками ІТ-проєктів, зокрема дозволяють ефективніше управляти загрозами та збільшувати вплив можливостей.

2. Результати дисертаційного дослідження впроваджені в процес управління ІТ-проєктами в ІТ компанії AMC Bridge та ТОВ “БРОКОДЕРС” (акти впровадження додані в Додаток Б).

3. Розроблена структура інформаційної бази інтегрованого управління загрозами та можливостями в ІТ-проєкті дасть можливість реалізувати моделі та методи управління ризиками в ІТ-проєкті з метою забезпечення накопичення статистичної та експертної інформації щодо управління загрозами та можливостями.

4. Розроблені структура інформаційної технології інтегрованого управління загрозами та можливостями в ІТ-проєкті, а також схема її реалізації, які у свою чергу дадуть змогу керівнику ІТ-проєкту та його команді реалізувати розроблені автором відповідні моделі та методи з метою забезпечення успішної та своєчасної реалізації ІТ-проєкту для задоволення потреб його стейкхолдерів [19].

5. Наведений алгоритм інформаційної технології інтегрованого управління загрозами та можливостями в ІТ-проєкті дозволить управляти ризиками з урахуванням загроз та можливостей відповідно до розроблених моделей та методів інтегрованого управління загрозами та можливостями в ІТ-проєкті, яка відрізняється від сучасних підходів до управління ризиками в методології управління проєктами та програмами й дозволить зменшити негативні впливи та врахувати позитивні впливи в ІТ-проєкті.

6. На прикладі ІТ-проєкту: Інтерв'ю з клієнтом, версія №6, який реалізовувала AMC Bridge компанія, що займається розробкою, впровадженням та підтримкою програмного забезпечення для замовників зі всього світу. Автором були проаналізовані проблеми, які призвели до невдачі виконання ІТ-проєкту, що дозволило врахувати їх при впровадженні інтегрованого управління загрозами та можливостями.

7. На прикладі Розробка програмного забезпечення, фаза №2, що був реалізований AMC Bridge компанією, що займається розробкою, впровадженням та підтримкою програмного забезпечення для замовників зі всього світу. У цьому проєкті було показано застосування моделей, методів та інформаційної технології інтегрованого управління загрозами та можливостями в ІТ-проєкті. За допомогою методу інтегрованого управління загрозами та можливостями в ІТ-

проєктах був проведений аналіз загроз та можливостей, з урахуванням застосування моделі RIO-RIT-REO-RET-аналізу, яка дозволила провести їхню ідентифікацію. У результаті було проведено ранжування загроз та можливостей на критичні, середні та низькі. В результаті застосування методу інтелектуального вибору оптимальної стратегії управління ризиковими подіями: загрозами та можливостями були запропоновані методи боротьби/посилення критичних та середніх загроз й можливостей, а також запропоновані заходи профілактики для усіх загроз та можливостей. Означені результати дали змогу підвищити ефективність прийняття рішень керівником ІТ-проєкту щодо стратегій реагування на загрози та врахування можливостей ІТ-проєкту.

8. За результатами застосування розроблених автором моделей, методів та інформаційної технології інтегрованого управління загрозами та можливостями в ІТ-проєктах дозволило знизити рівень непередбачених витрат на 7,3% порівняно з іншими подібними проєктами.

Результати досліджень четвертого розділу опубліковані у таких роботах [1, 2, 3, 4, 5, 6, 7, 8].

Список використаних джерел за четвертим розділом

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

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

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

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

5. Hrabina K., Shendryk V. Intelligent model of choosing the optimal risk events management strategy: threats and opportunities. *Artificial Intelligence*. Київ, 2022. № 2. P. 84-90. DOI: https://doi.org/10.15407/jai2022.02. URL: http://jai.in.ua/index.php/ua/issues?paper_num=1558.

6. Грабіна К.В., Шендрик В.В. Формування інтелектуальної моделі для вибору оптимальної стратегії управління ризиками. *Управління проєктами у розвитку суспільства*. Тези доповідей XX Міжнародної науково-практичної конференції (м. Київ, 12 травня 2023 року). Київ: КНУБА, 2023. С. 78-81.

7. Грабіна К.В. Метод управління ризиками ІТ-проєктів з врахуванням загроз та можливостей. *Управління розвитком складних систем*. Київ: КНУБА, 2023. Вип. 55. С. 18-28. DOI: https://doi.org/10.32347/2412-9933.2023.55.18-28. URL: http://mdcs.knuba.edu.ua/article/view/291119.

8. Hrabina Kateryna, Shendryk Vira. Information technology of integrated management of threats and opportunities in IT-projects. *Herald of Advanced Information Technology*. Odessa: 2023. №6(4). P. 363-374. DOI: https://doi.org/10.15276/hait.06.2023.24. URL:https://hait.od.ua/index.php/journal/article/view/194.

9. Тесля Ю.М., Данченко О.Б. Інформаційна технологія формування бази ризиків будівництва складних енергетичних об’єктів. *Вісник ЧІТІ*. Черкаси: "Графія України", 1998. № 3. С. 158-161.

10. Данченко О.Б. Інформаційна технологія формування протиризикових розкладів робіт при будівництві складних енергетичних об’єктів: дис. ... канд. техн. наук : 05.13.06. Черкаси: Черк. держ. технолог. ун-т, 2000. 201 с.

11. Бас Д.В., Данченко О.Б., Тесленко П.О. Інформаційна технологія ціннісно-орієнтованого управління арт-проектами. *Project, Program, Portfolio*

Management. PЗМ: матеріали IV міжнародної науково-практичної конференції. Одеса : ОНПУ, 2019. С. 153-156.

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

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

14. Єгорченков О.В., Єгорченкова Н.Ю., Лисицін О.Б. Модель декомпозиції інформаційної дії. Управління розвитком складних систем. Київ: КНУБА, 2013. Вип. 15. С. 51-55.

15. Єгорченков О.В., Єгорченкова Н.Ю., Чорна Н.О. Вплив інструментів візуалізації інформації на хід реалізації проектів. Управління розвитком складних систем. Київ: КНУБА, 2014. Вип. 19. С. 27-33.

16. Єгорченков О.В., Єгорченкова Н.Ю. Моделі управління інформаційними ресурсами 4П-середовища. Управління розвитком складних систем. Київ: КНУБА, 2019. Вип. 37. С. 26-32.

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

18. Грабіна К. В., Шендрик В. В., Івашова Н. В. Алгоритм методу управління ризиками та можливостями в ІТ проєктах. *Теоретичні та практичні аспекти розвитку науки та освіти.* Тези доповідей X міжнародної науково-практичної конференції (м. Львів, 9-10 січня 2024 року). Львів: 2024, С. 77-80.

19. Грабіна К.В., Шендрик В. В. Метод управління ризиками ІТ-проєктів з врахуванням загроз та можливостей. *Управління розвитком складних систем.* Київ: КНУБА, 2023. Вип. 55. С. 18-28. DOI: https://doi.org/10.32347/2412-9933.2023.55.18-28. URL: http://mdcs.knuba.edu.ua/article/view/291119.

ВИСНОВКИ

У дисертаційній роботі вирішена **актуальна науково-прикладна задача** розробки моделей та методів інформаційної технології інтегрованого управління ризиками в ІТ-проєктах з урахуванням впливу загроз та можливостей. За результатами проведеного дослідження було зроблено наступні висновки:

1. Проаналізовано предметну галузь, зокрема: особливості управління ІТ-проєктами, сучасні моделі, методи та інформаційні технології управління ризиками (загрозами та можливостями) в ІТ-проєктах.

2. Вперше розроблено **концептуальну модель управління ризиками в ІТ-проєктах з урахуванням загроз та можливостей**, яка ґрунтується на тому, що будь-який проєкт може бути описаний в просторі найголовніших метрик – час, гроші, обсяг та якість. Цей результат дозволяє заздалегідь врахувати вплив можливих ризиків з урахуванням загроз та можливостей в момент планування проєкту, завдяки чому проєктний менеджер є більш підготовленим до швидкоплинних реалій проєктної діяльності, які в свою чергу містять велику кількість незапланованих явищ, робіт, або іншими словами – змін.

3. Вперше запропонована **модель RIO-RIT-REO-RET-аналізу** дозволяє на етапі ідентифікації ризиків провести аналіз проєкту з точку зору кожного з аспектів: сильних чи слабких сторін, сприятливих можливостей та загроз. Зовнішні загрози та можливості (REO-RET) в цілому потенційно представляють цінність не лише для управління кожним проєктом компанії, але й для управління компанією чи організацією загалом. Внутрішні загрози та можливості (RIO-RIT) є цінними в більшій мірі у ході перебігу проєкту та представляють собою історичні дані після закриття проєкту та можуть бути використані при ініціалізації наступного проєкту схожого типу у подальшому.

4. Вперше розроблена **таргетна модель інтегрованого управління ризиками в ІТ-проєктах** ґрунтується на аналогії медицини та управління проєктами, яка дозволяє створити новий альтернативний підхід до управління ризиками проєкту, як загрозами, так і можливостями. На основі таргетної моделі

інтегрованого управління ризиками в ІТ-проєктах, будуються графіки, за допомогою яких формуються обмеження проєкту, які є найбільш чутливими та вимагають належного управління. Вони водночас найбільш ризиковані та сповнені можливостей, які можуть призвести до запланованого результату проєкту та принести певні переваги проєкту.

5. Вперше запропонована **математична модель управління загрозами та можливостями в ІТ-проєктах** ґрунтується на розрахунку синергетичного ефекту ІТ-проєкту з урахуванням таких показників як бюджет, тривалість, його сумарний ризик та можливість, та дозволяє оцінити ефективність управління ІТ-проєктом й порівняти її з ефективністю управління проєктом з урахуванням окремих груп ризиків та можливостей. Таке порівняння дозволить обрати найбільш оптимальну та успішну модель управління ризиками з урахуванням загроз та можливостей, що дозволить менеджеру успішно керувати проєктом, а компанії розумно оптимізувати витрати.

6. Удосконалено **інтелектуальну модель вибору оптимальної стратегії управління ризиковими подіями: загрозами та можливостями**, яка забезпечує декомпозицію процесу на три підпроцеси, які враховують графи розвитку подій, синергію можливих загроз та можливостей. Вибір оптимального рішення забезпечується оптимізацією витрат, для яких запропоновано критерії, цільову функцію. Застосовується розподіл загроз та можливостей у вигляді розробленої таргетної моделі за введеними вагами загроз та можливостей на основі експертних оцінок. Враховується як вартість реалізацій стратегій, так і загальні витрати на їх реалізацію, використовується обережний підхід до заощадливого використання ресурсів, що дозволяє балансування вигоди від реалізації можливості та витрат від загрози при обмежених наявних ресурсах;

7. Удосконалено **метод інтелектуального вибору оптимальної стратегії управління ризиковими подіями: загрозами та можливостями** дозволяє за допомогою інтелектуального аналізу даних обирати оптимальну стратегію управління загрозами та можливостями з метою підвищення ефективності управління ІТ-проєктом.

8. Отримав подальший розвиток **метод інтегрованого управління загрозами та можливостями в ІТ-проєктах**, який на відміну від існуючих, враховує ідентифікацію, оцінку та реагування на ризики, як для загроз, так і для можливостей. Це, у свою чергу, дозволяє підвищити ефективність управління ризиками з метою зниження впливу загроз та врахування впливу можливостей.

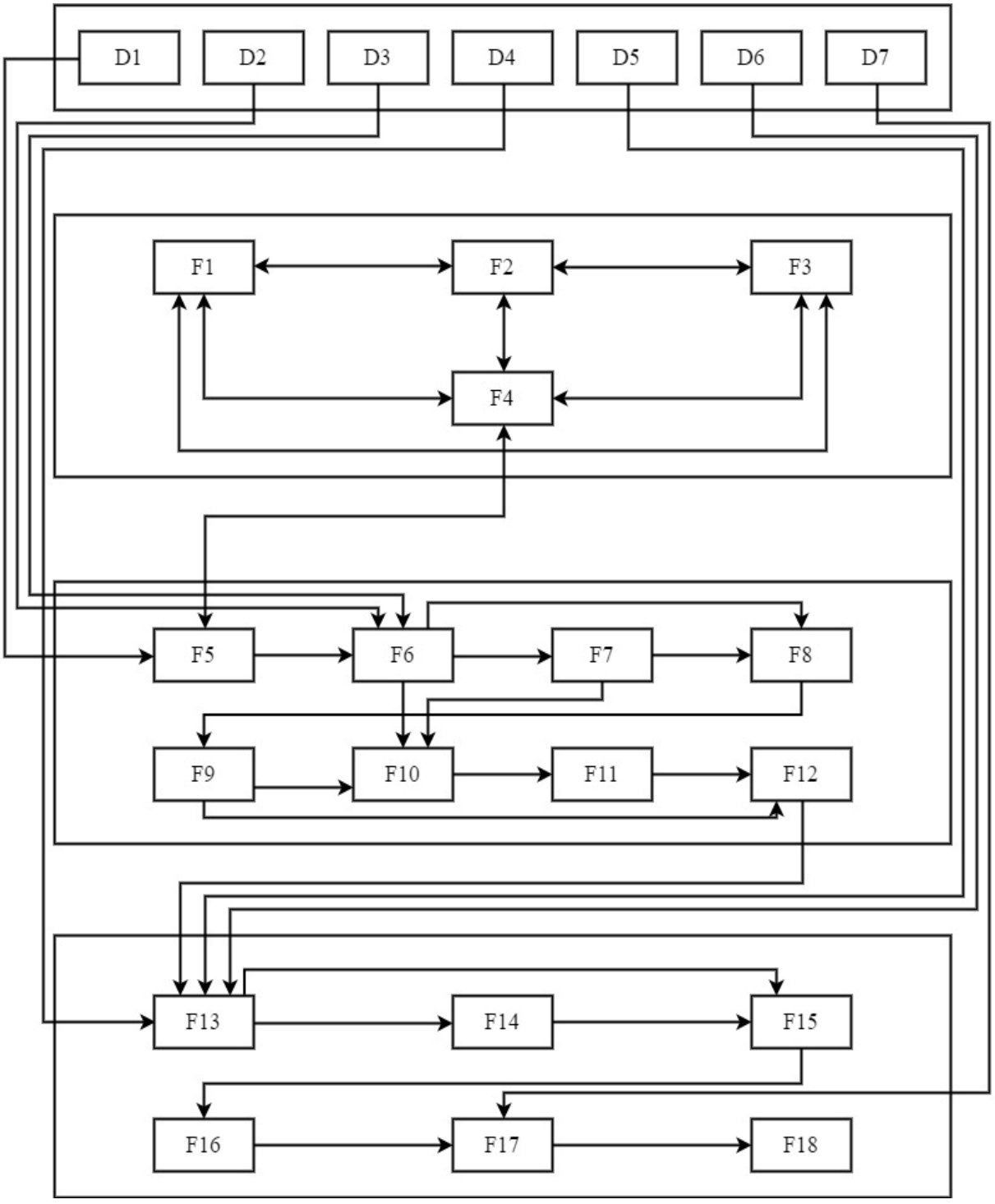
9. Розроблена структура інформаційної бази **інтегрованого управління загрозами та можливостями в ІТ-проєкті** дасть можливість реалізувати моделі та методи управління ризиками в ІТ-проєкті з метою забезпечення накопичення статистичної та експертної інформації щодо управління загрозами та можливостями. Розроблені структура інформаційної технології інтегрованого управління загрозами та можливостями в ІТ-проєкті, а також схема її реалізації, які у свою чергу дадуть змогу керівнику ІТ-проєкту та його команді реалізувати розроблені автором відповідні моделі та методи з метою забезпечення успішної та своєчасної реалізації ІТ-проєкту для задоволення потреб його стейкхолдерів. Наведений алгоритм інформаційної технології інтегрованого управління загрозами та можливостями в ІТ-проєкті дозволить управляти ризиками з урахуванням загроз та можливостей відповідно до розроблених моделей та методів інтегрованого управління загрозами та можливостями в ІТ-проєкті, яка відрізняється від сучасних підходів до управління ризиками в методології управління проєктами та програмами й дозволить зменшити негативні впливи та врахувати позитивні впливи в ІТ-проєкті.

10. За результатами застосування розроблених автором моделей, методів та інформаційної технології інтегрованого управління загрозами та можливостями в ІТ-проєктах дозволило знизити рівень непередбачених витрат на 7,3% порівняно з іншими подібними проєктами.

ДОДАТКИ

Додаток А

Структура інформаційної бази інтегрованого управління загрозами та можливостями в ІТ-проєкті



Додаток Б

Акти впровадження

AMCBRIDGE

Tel: +1 866-575-4791
Fax: +1 973-895-5376
Email: contact@amcbridge.com

АКТ
про впровадження науково-практичних результатів дисертаційної роботи на здобуття наукового ступеня доктора філософії Грабіної Катерини Вікторівни

Комісія у складі консультантів Михайловського Юрія Броніславович, Айсіної Марини Миколаївни, Івашової Надії Василівни даним актом підтверджує, що результати дисертаційної роботи Грабіної Катерини Вікторівни, будуть використовуватися як інструмент управління IT-проєктами в сервісній IT-компанії AMC Bridge, яка надає послуги з розробки програмного забезпечення.

Розроблені моделі та методи інформаційної технології буде інтегровано управління загрозами та можливостями IT-проєктів використовуватиметься для управління проєктами компанії.

У ході аналізу, ретроспективи та рев'ю проєктів компанії підтверджено, що використання запропонованих моделей та методів інформаційної технології при управлінні IT-проєктами дозволяє покращити головні показники проєктів.

Акт складено для надання у спеціалізовану вчену раду.

Голова комісії: _____ / Ю.Б. Михайловський

Члени комісії: _____ / М.М. Айсіна

_____ / Н.В. Івашова

303 Wyman Street, Suite 300 Waltham, MA 02451, USA
www.amcbridge.com

УКРАЇНА
ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ
« БРОКОДЕРС»
код 41207818
40010 м. Суми, вул. Баранівська, буд.203
UA143052990000026000011024681
АТ КБ «ПриватБанк»

+380957917159, bohdana.orel@brocoders.team

Затверджую
Директор Богдана Орел
09 жовтня 2023

АКТ

про впровадження науково-практичних результатів дисертаційної роботи на здобуття наукового ступеня доктора філософії

Грабіної Катерини Вікторівни

Складено комісією у складі:
Голова комісії: Орел Богдана Василівна - директор
Члени комісії:
1. Сагун Валентина Леонідівна – заступник директора
2. Конопленко Віктор Миколайович – головний менеджер

Комісія провела роботу з визначення впровадження результатів дисертаційної роботи Грабіної К. В. в діяльність Brocoders.

Для розгляду комісії передано:

- Інформаційну технологію інтегрованого управління загрозами та можливостями в IT-проектах. Доступ до розробленої моделі надано голові комісії.

- Інструкції щодо користування інформаційною технологією та її головними елементами.

За результатами проведення роботи комісією встановлено:

1. Інформаційна технологія інтегрованого управління ризиками та можливостями в IT-проектах дозволяє на практиці бути використаною проектним менеджером в управлінні IT-проектом, дає змогу працювати як з загрозами, так і з можливостями, враховуючи їх синергетичний ефект, управляти головними показниками проекту.

2. Використання розробленої в дисертаційній роботі інформаційної технології інтегрованого управління ризиками та можливостями в IT-проектах дозволяє підвищити показники ефективності IT-проектів Brocoders

Акт складено без фінансових зобов'язань перед автором дослідження.

Голова комісії Орел Б.В.

Члени комісії Сагун В.Л.
Конопленко В.М.

Додаток В

Список опублікованих праць за темою дисертації

Наукові праці, в яких опубліковані основні наукові результати дисертації:

Статті у наукових фахових виданнях України

1. Грабіна К.В., Шендрик В.В. Огляд процесів управління ризиками в IT-проєктах в контексті стандартів проєктного менеджменту. *Управління розвитком складних систем*. Київ: КНУБА, 2020. Вип. 43. С. 26-32. DOI: https://www.doi.org/10.32347/2412-9933.2020.43.26-32. URL: http://mdcs.knuba.edu.ua/article/view/219812/219536. *Фахове видання України* (включена до Index Copernicus, BASE, Google Scholar, Ulrich's Periodicals Directory).

Автором проведено огляд та порівняння етапів процесу управління ризиками, що включає визначення і види ризиків, поняття загрози та можливостей, їх загальну класифікацію, притаманні стандартні характеристики, їх особливості й відмінності, найвідоміші методи аналізу ризиків та їх сучасні техніки й інструменти в контексті найбільш поширених і відомих стандартів ризик-менеджменту.

2. Hrabina K., Shendryk V. Intelligent model of choosing the optimal risk events management strategy: threats and opportunities. *Artificial Intelligence*. Київ, 2022. № 2. P. 84-90. DOI: https://doi.org/10.15407/jai2022.02. URL: http://jai.in.ua/index.php/ua/issues?paper_num=1558. *Фахове видання України* (включена до Google Scholar, ICI Journals Master List, Ulrich's Periodicals Directory, Journal Factor, World Cat, Academia Edu, Internet Archive, Autor AID, ACM Digital Library, Open Academic Journals Index, Info Base Index, The IAEA'S NUCLEUS).

Автором запропонована інтелектуальна модель для вибору та застосування оптимальної стратегії управління ризиковими подіями, як загрозами, так і можливостями, сучасних невеликих IT-проєктів при обмежених ресурсах та неявних чи невизначених факторах впливу.

3. Грабіна К.В., Шендрик В.В. Метод управління ризиками ІТ-проєктів з врахуванням загроз та можливостей. *Управління розвитком складних систем*. Київ: КНУБА, 2023. Вип. 55. С. 18-28. DOI: TBD. URL: https://doi.org/10.32347/2412-9933.2023.55.18-28. *Фахове видання України* (включена до Index Copernicus, BASE, Google Scholar, Ulrich's Periodicals Directory).

Автором запропоновано розглядати у рамках невизначеності не тільки загрози, а ще й можливості, для забезпечення успішності реалізації управління ризиками.

4. Hrabina Kateryna, Shendryk Vira. Information technology of integrated management of threats and opportunities in IT-projects. *Herald of Advanced Information Technology*. Odessa: 2023. №6(4). P.363-374. DOI: https://doi.org/10.15276/hait.06.2023.24. *Фахове видання України* (включена до Index Copernicus, Research Bible, Academia, Directory of Open Access Scholarly Resources (ROAD), Google Academia, Ulrich's Periodicals Directory).

Автором запропоновано розглядати алгоритм інформаційної технології інтегрованого управління загрозами та можливостями в ІТ-проекті відповідно до розроблених моделей та методів інтегрованого управління загрозами та можливостями в ІТ-проекті.

Статті у виданнях іноземних держав, які включені до міжнародних наукометричних баз

5. Hrabina K., Danchenko O., Shendryk V. Target models of integrated risk management for IT-projects. *The scientific heritage*. Budapest, 2021. Vol. 1, № 71 (71). p. 55-61. DOI: https://www.doi.org/10.24412/9215-0365-2021-71-1-55-61. URL: http://www.scientific-heritage.com/wp-content/uploads/2021/08/The-scientific-heritage-No-71-71-2021-Vol-1.pdf (включена до Index Copernicus; Google Scholar).

Автором запропоновано таргетну модель інтегрованого управління ризиками в ІТ-проєктах та розроблено математичну модель для її розрахунку.

Опубліковані праці апробаційного характеру

6. Danchenko O., Shendryk V., Hrabina K. Opportunity Management overview in terms of the Risk Management in the software development industry standards. *Управління проєктами: стан та перспективи*. Матеріали XV міжнародної науково-практичної конференції (м. Миколаїв, 10-13 вересня 2019 року). Миколаїв: НУК, 2019. С. 88-89.

Автором розглянуто управління можливостями у стандартах управління IT-проєктів.

7. Грабіна К.В., Шендрик В.В. Аналіз та порівняння методів управління ризиками проектів сервісних IT-компаній. *Математичне моделювання процесів в економіці та управлінні проектами і програмами (ММП-2020)*. Міжнародна науково-практична конференція (смт. Коблево, 14-18 вересня 2020 р.). Харків: ХНУРЕ, 2020. С. 49-53. 1

Автором проведено аналіз та порівняння методів управління ризиками проєктів сервісних IT-компаній.

8. Грабіна К.В., Шендрик В.В., Данченко О.Б. Синергетичний ефект від управління загрозами та можливостями в IT-проєктах. *Project, Program, Portfolio Management*. Матеріали п’ятої Міжнародної науково-практичної конференції (м. Одеса, 04-05 грудня 2020 року). Одеса: ОНПУ, 2020. С. 26-30.

Автором запропоновано математичне уявлення визначення синергетичного ефекту від управління загрозами та можливостями в IT-проєктах.

9. Грабіна К.В., Шендрик В.В. Ризик менеджмент як інструмент планування успішних IT-проєктів. *Інформатика, математика, автоматика, IMA-2021*. Міжнародна науково-технічна конференція студентів та молодих учених (Суми-Нур-Султан, 19-23 квітня 2021 року). Суми, СумДУ: 2021. С. 76-77. URL: https://drive.google.com/file/d/1c4OYoy7HoYGPrliSb851gXYv_wRwUk3o/view.

Автором запропоновано враховувати вплив можливих загроз та можливостей в момент планування проєкту, що дозволяє забезпечити успішність реалізації ІТ-проєкту.

10. Грабіна К.В., Шендрик В.В., Данченко О.Б., Мазуркевич А.Г. Застосування SWOT-аналізу для ідентифікації ризиків проекту. *Управління проектами у розвитку суспільства*. Тези доповідей XVIII Міжнародної науково-практичної конференції (м. Київ, 15 травня 2021 року). Київ: КНУБА, 2021. С. 133-137.

Автором запропоновано застосовувати SWOT-аналіз для ідентифікації ризиків проєкту.

11. Грабіна К.В., Шендрик В.В., Данченко О.Б. Складові управління ризиками ІТ-проєктів. *Інформатика. Культура. Технології, ІКТ-2021*. Матеріали VIII Міжнародної науково-практичної конференції (м. Одеса, 13-14 травня 2021 р.). Одеса: Одеська політехніка, 2021. С. 124-126.

Автором проаналізовано термін «ризик» в контексті позитивних можливостей та негативних загроз, що дозволило виділити складові управління ризиками та їхній вплив на успіх проєкту.

12. Грабіна К.В., Шендрик В.В. Формування інтелектуальної моделі для вибору оптимальної стратегії управління ризиками. *Управління проєктами у розвитку суспільства*. Тези доповідей XX Міжнародної науково-практичної конференції (м. Київ, 12 травня 2023 року). Київ: КНУБА, 2023. С. 78-81.

Автором запропонована інтелектуальна модель для вибору оптимальної стратегії управління ризиками, яка забезпечує декомпозицію процесу на три підпроцеси та враховує графи розвитку подій, можливі ризики та можливості.

13. Грабіна К. В., Шендрик В. В., Івашова Н. В. Алгоритм методу управління ризиками та можливостями в ІТ проєктах. *Теоретичні та практичні аспекти розвитку науки та освіти.* Тези доповідей X міжнародної науково-практичної конференції (м. Львів, 9-10 січня 2024 року). Львів: 2024, С. 77-80.

Автором запропоновано алгоритм методу управління ризиками та можливостями в ІТ-проєктах.