



Отримано: 08 вересня 2023 р.

Прорецензовано: 15 вересня 2023 р.

Прийнято до друку: 19 вересня 2023 р.

e-mail: Gubarevairyna@gmail.com

ORCID-ідентифікатор: <https://orcid.org/0000-0002-9002-5564>

e-mail: nata_tru@ukr.net

ORCID-ідентифікатор: <https://orcid.org/0000-0002-6741-7738>

DOI: 10.25264/2311-5149-2023-30(58)-84-88

Губарєва І. О., Трушкіна Н. В. Процес управління ризиками в ІТ-проектах. *Наукові записки Національного університету «Острозька академія». Серія «Економіка»* : науковий журнал. Острог : Вид-во НаУОА, вересень 2023. № 30(58). С. 84–88.

УДК: 005.334:658

JEL- класифікація: L86, O22

Губарєва Ірина Олегівна,

доктор економічних наук, професор,
заступник директора з наукової роботи,

Науково-дослідний центр індустріальних проблем розвитку НАН України

Трушкіна Наталія Валеріївна,

кандидат економічних наук, старший дослідник, старший науковий співробітник
Науково-дослідний центр індустріальних проблем розвитку НАН України

ПРОЦЕС УПРАВЛІННЯ РИЗИКАМИ В ІТ-ПРОЕКТАХ

Метою статті є дослідження процесу управління проєктними ризиками та розробка рекомендацій щодо його адаптації для ІТ-проєктів. У статті представлено огляд процесу управління проєктними ризиками згідно стандартів: Project Management Body of Knowledge (PMBOK), International Organization for Standardization (ISO); Projects in Controlled Environments (PRINCE2). Зроблено висновок, що представлені стандарти достатньо структуровані і можуть бути застосовані для управління ризиками в різноманітних проєктах, в тому числі і в сфері інформаційних технологій. Розкрито особливості процесу управління ризиками в ІТ-проєктах відповідно до методології Microsoft Solutions Framework. Зосереджено увагу на формуванні процесу управління ризиками в проєктах відповідно до моделей Risk Management Maturity Model (RM Maturity Model); Capability Maturity Model Integration (CMMI); Maturity Level of Risk Management in IT Projects. При формуванні процесу управління ризиками в ІТ-проєктах, особливо в проєктах ІТ стартапів, вибір стандарту, методології чи їх комбінації (окремих розділів) повинен враховувати специфіку проєкту, характеристику проєктної команди, менеджменту, корпоративної культури, сегменту та кон'юнктури ринку, стейкхолдерів, кваліфікацію спеціалістів, які займаються управлінням ризиками.

Ключові слова: ризики, проєктні ризики, менеджмент, ІТ-проєкт, стартап, модель, процес управління.

Iryna Hubariewa,

Doctor of Economics, Professor, Deputy Director of the Research Centre of Industrial Problems
of Development of NAS of Ukraine

Nataliia Trushkina,

Ph.D. (in Economics), Senior Researcher,
Research Centre for Industrial Problems of Development of NAS of Ukraine

PROCESS OF RISK MANAGEMENT IN IT-PROJECTS

The purpose of the article is to study the process of project risk management and develop recommendations for its adaptation for IT projects. In the sphere of project management in the formation of project risk management process most often relies on international standards. The article presents an overview of the process of project risk management according to the standards: Project Management Body of Knowledge (PMBOK), International Organisation for Standardisation (ISO); Projects in Controlled Environments (PRINCE2). It is determined that the presented standards are sufficiently structured and can be applied to risk management in various projects, including those in the field of information technologies. The peculiarities of the risk management process in IT projects in accordance with the Microsoft Solutions Framework methodology are disclosed. It focuses on the formation of risk management process in projects in accordance with the Risk Management Maturity Model; Capability Maturity Model Integration (CMI); Maturity Level of Risk Management in IT Projects. IT projects have specific characteristics, and market competition, customer requirements, rapid development of technologies, team qualification – all this requires adaptability to the formation of the risk management process. When forming a risk management process in IT projects, especially in IT startup projects, the choice of a standard, methodology, or a combination of them (individual sections) should take into account the specifics of the project, project team, management, corporate culture, segment and market conditions, stakeholders, qualification of specialists engaged in risk management. In order to improve the effectiveness of risk management in IT projects, it is recommended that IT companies create structural and infra-red elements of risk management, namely: to attract risk management specialists; to develop job descriptions that define their functional duties and responsibilities; to develop corporate standards for risk management.

Key worlds: risks, project risks, management, IT project, start-up, model, management process.



Постановка проблеми. Сьогодні одним з перспективних напрямів менеджменту є управління ризиками проєктів, особливо в сфері інформаційних технологій. Про ризикованість ІТ-проєктів свідчать данні Standish Group International: більшість 70% реалізованих проєктів в США та європейських країнах були визнані проблемними або незавершеними, а матеріальні збитки від реалізації одного негативного ризику оцінюються в середньому в 1000\$ [1]. Під ризиком в ІТ-проєктах [2; 3] зазвичай розуміють ймовірну подію, яка походить з певних джерел і може призвести до певних наслідків та мати негативний та/або позитивний вплив на заплановані цілі проєкту. Найбільш ризиковими вважаються проєкти ІТ стартапів. V. Nikolaenko, A. Sidorov [4] зазначили, що незалежно від розміру, складності, тривалості, типу та методів управління ІТ-проєкт наражається на 105 ризиків.

Аналіз досліджень та постановка завдання. Дослідженням теорій та методів управління ризиками ІТ-проєктів, розробкою практичних рекомендацій щодо оцінки ризиків присвячено багато праць науковців світу. Так, Jenes Schmidt [5] визначив фактори та причини, що призводять до провалу ІТ-проєктів, проаналізував послідовність у часі виявлених факторів та причин, а також запропонував рекомендації щодо оцінки ризиків ІТ-проєктів. V. Nikolaenko, A. Sidorov [4] з метою підвищення вірогідності успішної реалізації ІТ-проєкту виявили джерела 105 універсальних ризиків і встановили причинно-наслідкові зв'язки між ними. О. Сметанюк, А. Бондарчук [5] надали характеристику стану розвитку ІТ-галузі в Україні, розкрили особливості системи управління ІТ-проєктами, місце проєкт-менеджера у ній. К. Грабіна, В. Шендрік [6] здійснили огляд процесів управління ризиками в ІТ-проєктах у контексті стандартів проєктного менеджмента.

Метою статті є дослідження процесу управління проєктними ризиками та розробка рекомендацій щодо його адаптації для ІТ-проєктів.

Виклад основного матеріалу дослідження. У сфері проєктного менеджменту при формуванні процесу управління проєктними ризиками частіше всього спираються на міжнародні стандарти. До найбільш відомих світових стандартів необхідно віднести: Project Management Body of Knowledge (PMBOK), International Organization for Standardization (ISO); Projects in Controlled Environments (PRINCE2).

Project Management Body of Knowledge (PMBOK) [8] – найбільш популярне зібрання знань з управління проєктами, який було розроблено Project Management Institute. У зв'язку із воєнною агресією росії проти України, Project Management Institute затвердив ряд ініціатив з підтримки проєктного менеджменту в Україні, одним з яких є – безкоштовне оприлюднення PMBOK 7 видання українською мовою на сайті PMI Ukraine [9].

Project Management Institute приділив окрему увагу управлінню ризиками проєктів, розробивши окремий Стандарт з управління ризиками у портфелях, програмах та проєктах, який включає ключові поняття ризик-менеджменту, систему управління ризиками в управлінні портфелями, програмами та проєктами, життєвий цикл управління ризиками в управлінні портфелями, програмами та проєктами, управління ризиками в контексті управління проєктами [8].

Згідно зі стандартом PMBOK управління ризиками містить процеси, пов'язані з ідентифікацією, оцінюванням, аналізом ризиків та прийняттям рішень, які спрямовані на максимізацію позитивних і мінімізацію негативних наслідків настання ризиків [10].

Project Management Institute розділяє процес управління ризиками на такі процеси [8]:

- планування управління ризиками – вибір підходів і планування діяльності з управління ризиками проєкту;
- ідентифікація ризиків – визначення ризиків, здатних вплинути на проєкт, та їх характеристика;
- якісна оцінка ризиків – якісний аналіз ризиків і умов їх виникнення з метою визначення їх впливу на ефективність проєкту;
- кількісна оцінка – кількісний аналіз ймовірності виникнення та впливу наслідків ризиків на проєкт;
- планування реагування на ризики – визначення процедур і методів мінімізації негативних наслідків ризикових подій та використання можливих переваг;
- реагування на ризики та моніторинг ризиків.

Міжнародною організацією зі стандартизації розроблено ISO 31000 – міжнародний стандарт, що містить принципи, структуру, та процес управління ризиками [11]. Згідно ISO 31000 процес управління ризиками має бути невід'ємною частиною управління та прийняття рішень інтегрований в структуру, операції та процеси організації. Його можна застосовувати на стратегічному, операційному, програмному або проєктному рівні. Процес управління ризиками включає:

- спілкування та комунікації з метою допомоги відповідним зацікавленим сторонам зрозуміти природи ризику, що є основою для прийняття певних рішень;



– визначення сфери застосування, зовнішнє та внутрішнє середовище, критерії (прийнятний рівень ризику);

– оцінка ризику. Оцінка ризику – це процес ідентифікації ризику, його аналізу та оцінки. Аналіз ризику повинен враховувати такі фактори, як: ймовірність подій і наслідків; характер і масштаби наслідків; складність і зв'язність; фактори, пов'язані з часом, і волатильність; ефективність існуючих засобів контролю; рівні чутливості та довіри. Оцінка ризику передбачає порівняння результатів аналізу ризику зі встановленими критеріями ризику, щоб визначити, де потрібні додаткові дії. Це може призвести до рішення: далі нічого не робити; розглянути варіанти лікування ризику; провести подальший аналіз, щоб краще зрозуміти ризик; підтримувати існуючі засоби контролю; переглянути цілі.

– вибір та реалізація варіантів з нейтралізації ризиків, що передбачає послідовність: формулювання та вибір варіантів нейтралізації ризиків; планування та впровадження заходів; оцінка ефективності; прийняття рішення про прийнятність залишкового ризику; якщо рівень ризику неприйнятний, повернення на перший етап;

– моніторинг;

– звітність. Процес управління ризиками та його результати повинні бути задокументовані та звітовані.

Project in Controlled Environments (PRINCE2) було розроблено Центральним телекомунікаційним та комп'ютерним агентством (CCTA), як державний стандарт Великобританії з управління проектами у сфері ІТ. PRINCE2 базується на процесно-орієнтованому підході і включає 7 принципів, 7 тем та 7 процесів. Принципи, теми та процеси пов'язані та взаємодіють один з одним, а ризики, а також час, гроші, вигоди, якість та зміст проекту є встановленими обмеженнями [12]. У PRINCE2 ризики розглядаються в рамках стадій проєктів, наприклад, ініціації та планування, а також як окрема компонента ризик-менеджменту [13].

Представлені стандарти достатньо структуровані, можуть бути застосовані для управління ризиками в різноманітних проєктах, в тому числі і в сфері інформаційних технологій, але в деяких випадках вони не дозволяють адаптувати процес управління ризиками під специфіку ІТ-проєкту.

Значний внесок в розвиток методології управління ризиками в ІТ-проєктах зробила корпорація Microsoft. Так, Microsoft Solutions Framework (MSF) – методологія розробки програмного забезпечення, спирається на практичний досвід Microsoft і описує управління людьми і робочими процесами в процесі розробки рішення. Процес управління ризиками MSF, визначає шість логічних етапів, за допомогою яких, проєктна група керує поточними ризиками, розробляє і виконує стратегії управління ризиками та вчить уроки зі свого досвіду для використання на рівні компанії: виявлення; аналіз і пріоритизація; планування; моніторинг; управління; коригування; набуті уроки [14].

Розвиток моделей зрілості управління проєктами стимулює створення моделей зрілості з точки зору управління ризиками, яка по мірі підвищення зрілості дозволяє усунути найбільш загрозливі ризики [15].

Модель зрілості управління ризиками Risk Management Maturity Model (RM Maturity Model) була розроблена португальськими вченими D. Proenca, J. Estevens, R. Viera, J. Borbinha в 2017 р. [16]. Модель базується на міжнародному стандарті управління ризиками ISO 31000. Вчені запропонували розкласти класичні процеси управління ризиками на 39 підпроцесів, розподілив їх по 5 рівням:

Рівень 1 Ініціація. На цьому рівні визначають джерела ризиків та можливі наслідки, вдосконалення процесу управління ризиками та інструментів.

Рівень 2. Управління. В організації виділяють співробітників для управління ризиками і визначають ресурси.

Рівень 3. Фактичне управління. Цей рівень найбільш трудомісткий, він потребує від керівництва організації ініціювання одночасного запуску 26 підпроцесів, серед яких: інтеграція управління ризиками у всі організаційні процеси; визначення критеріїв ризиків; виявлення, реєстрація та опис ризиків; розподілення повноважень та відповідальності між посадовими особами за управління ризиками тощо.

Рівень 4. Кількісний. Кожний процес управління ризиками має кількісне вираження. На цьому етапі використовуються спеціальні методи для оцінки ризиків, формування звітів про результати управління ризиками.

Рівень 5. Оптимізація. Пошук потенційних областей для покращення, вдосконалення існуючих процесів управління ризиками та інструментів. Інформація, яка накопичена в організації може бути використана для моделювання майбутніх станів. Цей рівень спрямовано на самовдосконалення.

Таким чином, RM Maturity Model – це дорожня карта, яку можна використовувати для планування послідовного впровадження процесів управління ризиками в організації.

Capability Maturity Model Integration (CMMI) – набір стандартизованих підходів для вдосконалення процесів від окремих проєктів до всієї організації. CMMI визначає 22 процесні області, для кожної із них



існує ряд цілей, які повинні бути досягнуті. Risk Management – є однією з процесних областей СММІ, де розглядається визначення потенційних проблем до їх виникнення. Специфіку ризик-менеджменту по СММІ можна розглянути, але модель являє собою набір обов'язкових елементів, які можуть бути виконані у будь-якій формі та використовуючи будь-які інструменти [17]. СММІ регламентує, що входить до процесу управління ризиками, але не дає чітких інструкцій, як це зробити.

Заслуговує на увагу модель Maturity Level of Risk Management in IT Projects [18]. Модель включає 4 рівня:

Рівень 0. Відсутній. Відсутнє управління проектами та ризиками.

Рівень 1. Початковий. Фахівці намагаються управляти ризиками, зосереджуючи увагу на проектних ризиках, але управління носить не системний характер.

Рівень 2. Рандомний. Фахівці, відповідальні за управління ризиками усувають комерційні та комплаєнс-ризиками. Процес управління ризиками є нестабільним, неповторюваним і випадковим. Найкращі практики управління ризиками не формалізовані та не закріплені в стандартах, що створює ризик втрати цих практик зі звільненням спеціалістів, відповідальних за управління ризиками.

Рівень 3. Стандартизація. Найкращі практики управління ризиками, напрацьовані попередниками, закріплені у внутрішніх стандартах організації. Фахівці, відповідальні за управління ризиками, керуються цими нормативними документами. Управління ризиками постійно вдосконалюється шляхом виявлення нових кращих практик.

Висновки. IT-проекти, особливо проекти IT старапів, мають специфічні характеристики, а ринкова конкуренція, вимоги замовника, стрімкий розвиток технологій, кваліфікація команди – все це вимагає адаптивності до формування процесу управління ризиками. При формуванні процесу управління ризиками в IT-проектах вибір стандарту, методології чи їх комбінації (окремих розділів) повинен враховувати специфіку проекту, проектною команди, менеджменту, корпоративної культури, сегменту та кон'юнктури ринку, стейкхолдерів, кваліфікацію спеціалістів, які займаються управлінням ризиками. З метою підвищення ефективності управління ризиками в IT-проектах рекомендується створити структурні та інфраструктурні елементи з управління ризиками в IT-компанії, а саме: залучити фахівців з управління ризиками; розробити посадові інструкції, в яких визначити їх функціональні обов'язки та відповідальність; розробити корпоративні стандарти з управління ризиками тощо.

Література:

1. The CHAOS Manifesto; The Standish Group: Boston, MA, USA, 2014; 16p.
2. Brandas, Claudiu, Otniel Didraga, and Nicolae Aurelian Bibu (2012) Study on risk approaches in software development project. *Informatica Economica*. 16. 148–57.
3. Mishra, Anant, Sidhartha Das, and James Murray (2014) Managing Risk in Government Information Technology Projects: Does Process Maturity Matter? *Production and Operations Management*. 24. 365–68.
4. Nikolaenko, V.; Sidorov, A. (2023) Analysis of 105 IT Project Risks. *Journal of Risk Financial Management*. 16. 33. <https://doi.org/10.3390/jrfm16010033>
5. Jens Schmidt (2023) Mitigating risk of failure Causes and mechanisms. *Project Leadership and Society*. 4. 100097. <https://doi.org/10.1016/j.plas.2023.100097>.
6. Сметанюк О.А., Бондарчук А.В. (2020) Особливості системи управління проектами в IT-компаніях. *Агросвіт*. 10. 105-111 DOI: 10.32702/2306-6792.2020.10.105
7. Smetaniuk, O.A., Bondarchuk, A.V (2020). Features of the project management system in IT companies. *Agrosvit*. 10. 105-111 DOI: 10.32702/2306-6792.2020.10.105 [in Ukrainian]
8. Грабіна К., Шендрік В. (2020) Огляд процесів управління ризиками в IT-проектах у контексті стандартів проектного менеджменту. *Управління розвитком складних систем*. 43. 26-32 DOI: 10.32347/2412-9933.2020.43.26-32
9. Hrabina, K., Shendryk, V. (2020) Overview of risk management processes in IT projects in the context of project management standards. *Managing the development of complex systems*. 43. 26-32. DOI: 10.32347/2412-9933.2020.43.26-32 [in Ukrainian]
10. The Standard for Risk Management in Portfolios, Programs, and Projects (2019). URL: <https://www.pmi.org/pmbok-guide-standards/foundational/risk-management>
11. Стандарт з управління проектами та настанова до зводу знань з управління проектами (Настанова РМВОК) 7 видання https://pmiukraine.org/wp-content/uploads/2022/08/PMBOK7_Ukr_ForPersonalUseOnly.pdf
12. PMBOK 7 URL: https://pmiukraine.org/wp-content/uploads/2022/08/PMBOK7_Ukr_ForPersonalUseOnly.pdf
13. A Guide to the Project Management Body of Knowledge (PMBOK Guide) Seventh Edition and The Standard for Project Management. 2021.
14. Risk Management Guidelines – Second Edition, ISO 31000: 2018
15. Managing Successful Projects with PRINCE 2. London: TSO, 2005. 457 p.
16. Bentley C. PRINCE2: A Practical Handbook. Third Edition / London UK: Routledge, 2010 p. 322.



14. Microsoft Solutions Framework. Basic principles. URL: <https://newline.tech/microsoft-solutions-framework-basic-principles/>
15. Anderson, E.S.; Jessen, S.A. (2003) Project maturity in organizations. *International Journal of Project Management*. 21. 457–461. [https://doi.org/10.1016/S0263-7863\(02\)00088-1](https://doi.org/10.1016/S0263-7863(02)00088-1)
16. Proenca, D.; Estevens, J.; Vieira, R.; Borbinha, J. (2019) Risk Management a Maturity Model based on ISO 31000. In Proceedings of the 2019 IEEE 19th Conference on Business Informatics, Thessaloniki, Greece, 24–27 July 2019; pp. 99–108.
17. CMMI for Development, version 1.3 – CMMI, 2010. 482.
18. Nikolaenko V., Sidorov A. (2023) Assessing the Maturity Level of Risk Management in IT Projects. *Sustainability*. 15. 12752. <https://doi.org/10.3390/su151712752>