УДК 004.052.3:005.8 https://doi.org/10.35546/kntu2078-4481.2023.3.15

О. Г. ТРОФИМЕНКО
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій
Національний університет «Одеська юридична академія»
ORCID: 0000-0001-7626-0886

Н. І. ЛОГІНОВА
кандидат педагогічних наук, доцент,
завідувачка кафедри інформаційних технологій
Національний університет «Одеська юридична академія»
ORCID: 0000-0002-9475-6188

П. О. ТЕСЛЕНКО
кандидат технічних наук, доцент,
завідувач кафедри штучного інтелекту та аналізу даних
Національний університет «Одеська політехніка»
ORCID: 0000-0001-6564-6185

О. С. САВЄЛЬЄВА
доктор технічних наук, професор,
професор кафедри інтегрованих технологій управління
Національний університет «Одеська політехніка»
ORCID: 0000-0002-0453-4777

В. М. ПОЛЯКОВ
Senior Front End Lead, Krusche & Company
ORCID: 0009-0008-0135-0973

КЛАСИФІКАЦІЯ РИЗИКІВ У ПРОЄКТАХ ІЗ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Сучасна розробка програмного забезпечення стикається з численними ризиками. Щоб залишатися конкурентними, ІТ-компанії мають швидко реагувати та мінімізувати можливі ризики провалу. Проєкти з розробки програмного забезпечення мають свою специфіку, пов'язану зі швидкими темпами розробки і з численними змінами під час неї. Природа цих змін є дуже різноплановою. Задля пом'якшення ризиків потрібне визначення можливих ризиків, їх оцінка та план управління ризиками. Класифікація ризиків, тобто групування пов'язаних типів ризиків, сприяє більш ефективному загальному управлінню ними. Вона допомагає виявити загальні джерела ризику, об'єднати ресурси ризику, точніше застосувати стратегії пом'якшення ризику та управляти взаємозв'язком конкретних ризиків. Якщо ризики не класифіковані, може відбуватися ненавмисне збігання або суперечливість роботи з пом'якшення ризиків, що спричинить проблеми, тобто додаткові негативні ризики. Аналіз літератури виявив відсутність єдиного підходу до класифікації ризиків управління проєктами з розробки програмного забезпечення. У більшості наявних класифікацій ризиків не враховується специфіка проєктів із розробки програмного забезпечення, нехтуються ризики кібербезпеки. Автори статті проаналізували наявні підходи до ідентифікації та класифікації ризиків управління проєктами і запропонували багатофакторну класифікацію ризиків у програмних проєктах, в якій враховано специфіку сфери розробки програмного забезпечення. Застосування такої класифікації сприятиме ясності та прозорості у розумінні можливих наслідків, якісній оцінці ризиків, створенню ефективної стратегії реагування на ризики та ефективному пом'якшенню їх. Саме тому керівники програмних проєктів мають знати категорії ризиків та їх роль в управлінні ризиками. Корисно розвивати культуру стійкості до ризиків, яка дозволить компанії адаптуватися та швидко реагувати у разі настання цих ризиків. Систематичне застосування методології управління ризиками та її поширення на всю організацію може забезпечити суттєву конкурентну перевагу в умовах дедалі більшої невизначеності.

Ключові слова: *управління ризиками, оцінка ризиків, план управління ризиками, розробка програмного забезпечення, ризики програмного проєкту.*

O. G. TROFYMENKO
Candidate of Technical Science, Associate Professor,
Associate Professor at the Department of Information Technologies
National University “Odesa Law Academy”
ORCID: 0000-0001-7626-0886

N. I. LOGINOVA
Candidate of Pedagogical Sciences, Associate Professor,
Head of the Department of Information Technologies
National University “Odesa Law Academy”
ORCID: 0000-0002-9475-6188

P. O. TESLENKO
Candidate of Technical Science, Associate Professor,
Head of the Department of Artificial Intelligence and Data Analysis
Odesa Polytechnic National University
ORCID: 0000-0001-6564-6185

O. S. SAVIELIEVA
Doctor of Technical Sciences, Professor,
Professor at the Department of Integrated Management Technologies
Odesa Polytechnic National University
ORCID: 0000-0002-0453-4777

V. M. POLIAKOV
Senior Front End Lead, Krusche & Company
ORCID: 0009-0008-0135-0973

CLASSIFICATION OF SOFTWARE PROJECT RISKS

Modern software development faces numerous risks. IT companies must respond quickly and minimize the risk of failure to remain competitive. Software development projects have their own specifics associated with the rapid pace of development and numerous changes during it. The nature of these changes is very diverse. Risk mitigation requires identifying potential risks, assessing them, and developing a risk management plan. Risk classification, that is, the grouping of related types of risks, facilitates more effective overall risk management. It helps identify common sources of risk, combine risk resources, more accurately apply risk mitigation strategies, and manage the interrelationship of specific risks. If risks are not classified, there may be an unintentional overlap or conflict of risk mitigation work, causing problems, i.e. additional negative risks. The analysis of the literature revealed the lack of a unified approach to the classification of software development project management risks. Most existing risk classifications do not consider the specifics of software development projects, cybersecurity risks are neglected. The authors of the article analyzed the available approaches to the identification and classification of project management risks and proposed a multifactor classification of risks in software projects, which considers the specifics of the software development area. The use of such a classification will contribute to clarity and transparency in the understanding of possible consequences, a qualitative assessment of risks, creation of an effective strategy for responding to risks and their effective mitigation. Therefore, project managers need to be aware of risk categories and their role in risk management. It is useful to develop a risk-resilient culture that allows the company to adapt and respond quickly when these risks occur. The systematic application of risk management methodology and its distribution throughout the organization can provide a significant competitive advantage in conditions of increasing uncertainty.

Key words: *risk management, risk assessment, risk management plan, software development, software project risks.*

Постановка проблеми

На сьогодні програмне забезпечення стало невіддільною частиною нашого життя через повсюдне використання цифрових продуктів та послуг. Сучасні програмні технології стрімко розвиваються й сприяють появі та безпрецедентному поширенню різноманітних цифрових продуктів. Ця тенденція спостерігається в більшості сфер життєдіяльності людей. При цьому проєкти, орієнтовані на використання програмного забезпечення, ніколи не стають завершеними, оскільки вебсайти та мобільні застосунки продовжують розвиватися й оновлюватись відповідно до появи новітніх технологій і вимог клієнтів. Ринок програмного забезпечення стрімко розвивається, а сучасна розробка програмного забезпечення стикається з численними ризиками через гіперконкурентне середовище, яке зосереджується на досвіді клієнтів і скороченні часу виходу на ринок. Щоб залишатися конкурентними, ІТ-компанії мають швидко реагувати на вимоги клієнтів, впроваджувати новітні технології і при цьому враховувати та мінімізувати можливі ризики провалу.

Проєкти з розробки програмного забезпечення (ПЗ) мають свою специфіку, пов'язану зі швидкими темпами розробки і з численними змінами під час неї. Природа цих змін є дуже різноплановою: від втілення новітніх ідей у реальність задля просування своїх компаній та суспільства в цілому і до збоїв у кібербезпеці, геополітичних криз, екстремальних погодних умов та пандемій. Оскільки зараз зміни відбуваються дуже стрімко, управління ризиками у проєктах із розробки ПЗ є вкрай важливим. Задля пом'якшення ризиків потрібне визначення можливих ризиків, їх оцінка та план управління ризиками. Вчасне реагування, виявлення та врахування тих чи інших ризиків дозволить заощадити значні кошти та запобігти репутаційним втратам для бізнесу. Але для цього потрібен постійний всебічний моніторинг для виявлення, оцінки та пом'якшення ризиків протягом усього життєвого циклу програмного проєкту.

Аналіз останніх досліджень і публікацій

Проблеми та аспекти ідентифікації ризиків під час управління проєктами в різний час були розглянуті в численних наукових публікаціях вітчизняними і закордонними вченими. Автори статті [1] дійшли висновку, що використання категорій ризиків для їх ідентифікації та документування створює всебічне розуміння того, як в управлінні проєктом реагувати на ризик для зменшення його впливу. У дослідженні [2] пропонується оцінювати ризики управління проєктом за п'ятьма критеріями: 1) ризикована подія, що може статися і вплинути на проєкт; 2) часові рамки ризику; 3) ймовірність настання; 4) очікуваний вплив; 5) фактори, які можуть попередити або спровокувати ризиковану подію. Дослідження [3] класифікує ризики у розробці ПЗ за п'ятьма видами: бюджетні, операційні, технічні, програмні та розкладу. Автори статті [4] стверджують, що групування ризиків зі схожими характеристиками є фундаментальним для діяльності будь-якої інженерної системи, і класифікувати ризики у середовищі програмної інженерії слід за такими категоріями: стратегічні, фінансові, програмні, операційні, технологічні, технічні, зовнішні, екологічні, організаційні, проєктні, регуляторні, будівельні та проїзду. У роботі [5] запропоновано використовувати дві загальні категорії ризиків, у кожній з яких згруповано декілька типів ризиків: 1) ризики на основі джерела (внутрішні, зовнішні, технічні, нетехнічні, галузеві, загальні) та 2) ризики на основі впливу на проєкт (графіку, вартості, якості, сфери застосування, ресурсів). У статті [6] ризики класифіковано за такими основними категоріями: вимог, персоналу, технологічні, політичні. Дослідження [7] пропонує класифікувати ризики в IT-проєктах за чотирма типами: 1) обсягу; 2) планування; 3) ресурсні; 4) технологічні. Автори статті [8] пропонують класифікувати ризики за шістьма факторами: унікальність, складність, припущення та обмеження, люди, стейкголдери, зміни. Дослідження [9] пропонує ризики циклу розробки ПЗ класифікувати через зв'язок з одним із трьох компонентів (дані, людина, система) і при цьому враховувати ступінь впливу і відповідальності результатів оцінки ризиків для різних методологій розробки ПЗ. Автори роботи [10], намагаючись звузити класифікацію ризиків, поділивши їх на два типи: явні та неявні проблеми ризику.

Проведений аналіз наявних досліджень свідчить про відсутність єдиного підходу до класифікації ризиків управління проєктами, формування реєстру ризиків та створення ієрархічної структури ризиків. Через часті зміни, з одного боку, та широке розмаїття сфер застосування і засобів розробки програмного забезпечення, з іншого, наразі використовуються різні підходи до класифікації ризиків у сфері розробки програмних проєктів. Численні публікації з цього приводу свідчать про важливість вирішення завдання управління ризиками при розробці ПЗ, а повсюдне впровадження інформаційних технологій потребує підвищеної уваги до цього напрямку, і відповідно, більш глибокого висвітлення питань ризик-менеджменту IT-індустрії. Проте наразі спостерігається відсутність комплексного і системного підходу до проблеми критерізації й ідентифікації ризиків при розробці ПЗ.

Мета роботи

Порівняльний аналіз підходів щодо ідентифікації ризиків управління проєктами та формування класифікації ризиків в програмних проєктах з урахуванням специфіки сфери розробки ПЗ.

Викладення основного матеріалу дослідження

Провідна професійна асоціація з управління проєктами (Project Management Institute, PMI), яка є найбільшою професійною організацією у сфері управління проєктами, визначила управління ризиками та управління якістю двома основними напрямками Зводу знань про управління проєктами (Project Management Body of Knowledge, PMBOK) [11, 12]. З іншого боку, для допомоги організаціям в інтеграції ефективної структури прийняття рішень в управлінні ризиками 2018 року розроблено міжнародний стандарт ISO 31000 [13], на якій організації можуть орієнтуватись у своїй практиці управління ризиками задля надійного забезпечення принципів ефективного менеджменту та корпоративного управління.

Відповідно до термінології управління проєктами, рекомендованої PMI, ризик – це невизначена подія або умова, яка, якщо вона трапиться, матиме позитивний або негативний вплив на одну або більше цілей проєкту, а управління ризиками – це процес мінімізації будь-яких потенційних проблем, які можуть негативно вплинути на графік проєкту [14]. Ризиком може бути будь-яка несподівана подія, яка може вплинути на людей, процеси, технології та ресурси, залучені до проєкту. На відміну від проблем, які обов'язково виникнуть, ризики – це події, які можуть відбутися, і неможливо сказати, коли саме. Через цю невизначеність ризики проєкту вимагають певної

підготовки для ефективного управління ними. Отже, управління ризиками в управлінні проєктами – це певна підготовка до перешкод і проблем, які можуть завадити успіху проєкту, та їх вирішення.

Діяльність з управління ризиками охоплює такі основні етапи: виявлення ризиків, їх оцінювання, вибір методів та засобів управління, запобігання, контролювання, фінансування, оцінювання результатів. Ризики можуть бути позитивними (можливості) або негативними (загрози). Оптимізоване реагування на ризики полягає в постійному оцінюванні ризиків, щоб максимізувати позитивний вплив та мінімізувати негативний вплив на проєкт та його результати. Отже, по-перше, треба визначити ризики, по-друге, провести комплексну оцінку ризиків, а, по-третє, варто підготувати відповідний план управління ризиками, який можна буде активувати у разі настання проблеми.

Для виявлення потенційних ризиків варто скласти список усіх можливих ризиків. Під час процесу планування проєкту керівнику проєкту (проєктному менеджеру, ПМ) варто попросити допомоги у команди і провести мозковий штурм із досвідченими учасниками проєкту та іншими зацікавленими сторонами. Поширеним для цього є використання метода Кроуфорда – простого, проте ефективного способу збору і порівняння пропозицій та ідей. При цьому важливо тут не нехтувати співпрацею команд із різних відділів.

Початкове виявлення ризиків у проєкті варто провести якомога раніше, а надалі постійно оновлювати протягом усього життєвого циклу проєкту, оскільки ризики впливають на його важливі етапи. Звичайно з часом і з досвідом у компанії накопичується власний каталог можливих ризиків, з якими вона стикалася у завершених проєктах.

При визначенні ризиків корисним для визначення сфер, схильних до ризиків, є класифікація ризиків по категоріях і різновидах. Категорії ризиків – це конкретні елементи в рамках проєкту або його робочого середовища, які можуть піти не так під час планування, реалізації або подальших етапів діяльності [15]. Категорії ризику охоплюють різні сфери: витрати, програмне та апаратне забезпечення, наявний персонал, графік тощо. Вони враховують складові, необхідні для створення успішного проєкту, і можливі наслідки у разі, якщо одна або кілька складових відхиляться від наміченого курсу поведінки. Зібрані по категоріях ризики забезпечують послідовний спосіб відстеження того, що може статися з великими обсягами даних, а також розуміння та бачення того, де і коли потрібно пом'якшити відповідний ризик. Відстеження ризиків на рівні категорії дещо спрощує управління ризиками. За допомогою категорій простіше групувати ризики для відстеження та визначення їх пріоритетів.

Дослідження та аналіз ознак сучасних ризиків у проєктах із розробки ПЗ дозволили згрупувати їх у чотири категорії (рис. 1).

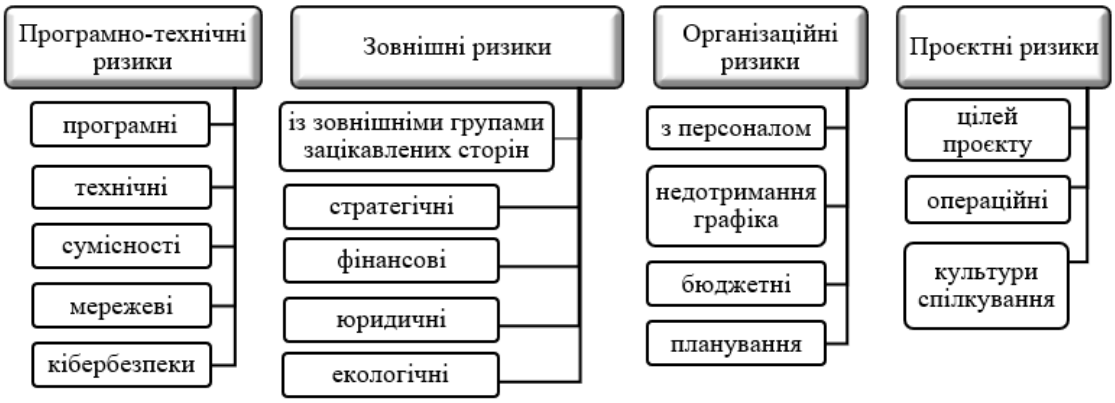

Рис. 1. Категорії ризиків у проєктах із розробки ПЗ

Програмно-технічні ризики пов'язані з функціональністю та продуктивністю програмного продукту чи то його складової, а також з технічною складовою забезпечення його розробки. При визначенні переліку таких ризиків варто відповісти на питання [5]: 1) чи достатньо є апаратного забезпечення для всіх членів команди; 2) чи є фахівці для усунення різного роду програмних, апаратних чи то якихось технічних збоїв, які можуть виникнути; 3) чи є доступ до зовнішніх постачальників, які можуть допомогти; 4) чи створено зручні у користуванні довідкові керівництва для впровадження проєкту тощо. Приклади таких ризиків: проблеми з оновленням ПЗ, зміненням параметрів безпеки мережі, безпекою даних (можливі витоки, пошкодження), зміною вартості ліцензії на ПЗ, апаратна поломка, неузгодженість форматів даних, зміна вимог до аудиту, підключення та доступ до мережі, несумісність платформ тощо. Здебільшого причини програмно-технічних ризиків пов'язані з частими змінами вимог, недостатністю кваліфікованих працівників чи то програмно-апаратного забезпечення, високою складністю в реалізації, неправильною інтеграцією модулів, вразливостями кібербезпеки тощо. Різновидами програмно-технічних ризиків є:

- *програмні ризики* – одні з найважливіших ризиків у проєктах із розробки ПЗ. Вони охоплюють доволі широкий спектр можливих ризиків, оскільки стосуються як розроблюваного програмного продукту, так і узгодженої роботи різноманітного ПЗ, використовуваного під час всього життєвого циклу розробки ПЗ: починаючи від програмних засобів для документування вимог і спілкування з членами команди та іншими стейкголдерами й закінчуючи різними інструментами тестування та розгортання. Це різні програмні фреймворки, бібліотеки, бази даних, системи контролю версій, хмарні сховища, текстові, табличні та графічні редактори, месенджери та ще доволі широкий перелік специфічного ПЗ, набір якого залежить від характеру розроблюваного програмного продукту. До того ж сюди варто додати інструменти для оптимізації процесів ІТ-компанії і безперебійної роботи над проєктами у командах, серед яких найбільш поширеними нині є: Jira, Trello, Airtable, Worksection, Asana тощо. Ці інструменти дозволяють оптимізувати спілкування з клієнтами, а також керувати даними, пов'язаними з клієнтами, наприклад, збирати відгуки клієнтів для кращого реагування на їхні потреби. Що стосується розроблюваного ПЗ, то поширеним є ризик погано продуманого, інтуїтивно незрозумілого або непривабливого UX/UI дизайну продукту. Для усунення цього ризику варто провести глибокий аналіз потреб цільової аудиторії готового продукту, що дозволить врахувати певні особливості при розробці інтерфейсу та зручності використання продукту. Іншим поширеним ризиком, пов'язаним із розробкою ПЗ, є проблеми з кодуванням через низьку якість коду і поганий стиль програмування. На практиці програмний продукт часто розробляється одними програмістами, а вдосконалюється і підтримується іншими. Крім того, технічне обслуговування є найтривалішим етапом життя програмного продукту. Якість оригінального коду сильно впливає на вартість обслуговування. Програми з низькою якістю коду можуть спричинити серйозні проблеми в програмних системах;
- *технічні ризики* стосуються будь-яких аспектів роботи та збоїв у роботі численного апаратного забезпечення, залученого як для розробки програмного забезпечення, так і для нормального функціонування структурних підрозділів ІТ-компанії. Оскільки спектр та кількість використовуваного апаратного забезпечення є доволі масштабним, і здебільшого таке устаткування є тісно взаємопов'язаним із технологічним циклом розробки ПЗ, то нехтувати цією групою ризиків для ІТ-проєктів неприпустимо. До того ж варто зважати на те, що під час тривалого життєвого циклу розробки ПЗ відбувається постійна міграція та оновлення відповідної апаратної складової. На ринок виходять нові технологічні продукти і рішення, з'являються нові гаджети, на яких буде використовуватись створюване ПЗ, що потребує перегляду і врахування усіх параметрів під час розробки оновлень ПЗ та відповідного додаткового тестування [16]. Все зазначене є причиною того, чому ІТ-компанії вважаються організаційними середовищами високого ризику [4];
- *ризики сумісності* роботи численних ІТ-компонентів є специфічною проблемою, з якою стикаються команди розробки ІТ-проєктів, через складні залежності між ІТ-складовими: обладнанням, програмним забезпеченням, мережами, даними. На практиці програмні проєкти неминуче стикаються з помилками та проблемами їх взаємодії, не кажучи вже про численні оновлення, версії та випуски програмного забезпечення [17]. Як приклад, необхідність узгодженої взаємодії різних комп'ютерів, принтерів, планшетів, смартфонів із різними версіями операційних систем, драйверів та утиліт у рамках великої організації, де працюють тисячі різних подібного роду пристроїв;
- *мережеві ризики* зумовлені повсюдним використанням інтернет-технологій. Нині більшість програмно керованих пристроїв налаштовуються і керуються клієнтами через інтернет-мережу. Це потребує постійного доступу до мережі через Wi-Fi, 4G або 5G. Змінення параметрів безпеки мережі зазвичай впливає на всіх кінцевих користувачів або на всі кінцеві сервери, при чому цей вплив значний, адже все, що під'єднано до мережі, з одного боку, зручно оновлювати, змінюючи прошивки, а, з іншого боку, небезпечно з точки зору вразливості;
- *ризики кібербезпеки* розглядають можливі небезпеки через неналежний захист даних від зовнішніх атак. Сучасний цифровий світ побудований на даних – їх зборі, зберіганні, аналізі, розумінні та безпечному обміні. Більшість програмних систем нині потребують та використовують різного роду конфіденційні дані клієнтів. Що стосується спеціального ПЗ для банківської галузі, медичних, освітніх та професійних сфер, то там персональні дані є невіддільною частиною роботи програмних систем [18]. Витоки даних таких систем сильно б'ють по репутації та чинять велику шкоду організаціям [19]. Так, за даними IBM Security, середня загальна вартість витоку даних 2022 року становила 4,35 млн доларів США [20]. Велика складність забезпечення надійної кібербезпеки програмних систем зумовлена різними чинниками, насамперед безліччю загроз від зловмисників, як-от: фішингові шахрайства та шахрайства з видаванням себе за іншу особу, програми-вимагачі, порушення безпеки в хмарі, зловмисне ПЗ для мобільних пристроїв тощо [21]. Дієвим для зміцнення кібербезпеки є розроблення дорожньої карти кіберзахисту для визначення області потенційних уразливостей, пошуку нових можливостей протистояння кіберзагрозам, оцінки безпеки продукту. Також важливим є формування та підтримка культурного рівня обізнаності співробітників і клієнтів про кібербезпеку та дії щодо запобігання кіберзагрозам. Нині в ІТ-компаніях все більше уваги приділяється інвестиціям у проєкти з кібербезпеки. Управління ризиками кібербезпеки має враховувати багато різних речей та вимагає певних зусиль, щоб максимально пом'якшити ризики.

Зовнішні ризики стосуються всього, що може вплинути на проєкт, хоча і є поза прямим контролем компанії. Вони переважно стосуються проблем, які можуть виникнути у субпідрядників або постачальників, наприклад,

у разі їх можливої зміни і того, як це вплине на проєкт. Також вони стосуються можливих законодавчих змін щодо фіскальної політики, міждержавних договорів, війн, світових коливань цін на енергоносії, пандемій тощо. Адже не існує жодного програмного проєкту, який був би на 100% ізольований від впливу зовнішніх змін. Більшість зовнішніх ризиків є непередбачуваними: раптові зміни ринку, поява конкурентного програмного продукту, впровадження нових законодавчих актів, зміни поведінки та пріоритетів споживачів, кліматичні, екологічні чи соціальні катаклізми. Так, російсько-українська війна є прикладом зовнішнього ризику, яка суттєво вплинула на більшість ІТ-проєктів (персонал, ланцюги постачання, клієнти, перебої з енергоносіями, непередбачені витрати). Можна виділити декілька різновидів зовнішніх ризиків:

- *ризики із зовнішніми групами зацікавлених сторін* (постачальниками, клієнтами) переважно стосуються впливу можливих міжорганізаційних проблем у постачальників, затримки консультантів або підрядників, порушення ланцюга постачання. Зовнішні зацікавлені сторони – це особлива група людей, які формують вимоги, очікування та цілі проєкту. Їхні вимоги можуть відрізнятися, збігатися та іноді суперечити одна одній, що призводить до ризиків під час виконання та здачі проєкту. Для цього важлива постійна взаємодія зі стейкголдерами для своєчасного виявлення можливого конфлікту інтересів, прийняття рішень і вирішення проблем;
- *стратегічні ризики* – є зовнішніми оперативними ризиками, які можуть вплинути на стратегічний напрям і виживання компанії. Фактори цього типу зовнішніх ризиків охоплюють ризики через хибні бізнес-рішення і як наслідок злиття та поглинання структурних підрозділів і навіть компаній. За даними дослідження [22] відсоток невдач від злиття і поглинань становить від 70% до 90% угод через неможливість реалізації очікуваної від них вигоди. Прикрим прикладом невдалого злиття з мільярдними збитками є угода між eBay і Skype. Враховуючи кількість грошей, інвестованих у такі підприємства, сам факт більшості невдач свідчить про наявне погане управління ризиками. До того ж, крім спричинених фінансових втрат, невдалі стратегічні бізнес-рішення спричиняють подальші репутаційні ризики. Проте, тут можна навести і декілька вдалих прикладів інтеграції злиття ІТ-компаній, наприклад: Apple і Shazam або IBM і Red Hat. Щодо репутаційних ризиків, то вони можуть стосуватися: проблем управління зацікавленими сторонами, медійних скандалів та негативного висвітлення в ЗМІ, втрати довіри клієнтів та довіри інвесторів через негативний досвід тощо;
- *зовнішні фінансові ризики* можуть вплинути на бізнес з позиції його загальної фінансової життєздатності. Ці зовнішні ризики пов'язані з ринком, на якому працює організація (ринкові ризики), а також здатністю використовувати позики (кредитні ризики) [4]. Прикладами зовнішніх фінансових ризиків можуть бути: неочікувані дії конкурентів, витрати внаслідок відсутності активів і невідомих зобов'язань, невизначена податкова позиція, тиск ринку, непередбачені зміни фінансування тощо. Переважно фінансові ризики є добре зрозумілими для управління ризик-менеджерам, завдяки численним фінансовим інструментам і методам управління ними;
- *юридичні ризики* стосуються різних можливих нормативно-правових, політичних, геополітичних криз, макроекономічних змін, які опосередковано можуть впливати на проєкт. Наприклад: зміни фіскальної політики, загрози судових позовів та процесів, зміни політичних факторів, ризики інтелектуальної власності, розірвання угоди через антимонопольне законодавство тощо;
- *екологічні ризики* для ІТ-проєктів не такі часті, як для інших проєктів, проте зважати на них варто. Так, пандемія COVID-19 є прикладом такого зовнішнього ризику (глобальна криза охорони здоров'я), який суттєво вплинув на більшість ІТ-проєктів (персонал, ланцюги постачання, витрати тощо). Хоча лідери компаній знали про такого роду ризики, проте ніхто не уявляв, які величезні втрати зазнає світ через коронавірус. Це вказує на потребу нового мислення для виявлення, управління та пом'якшення ризиків протягом усього життєвого циклу проєкту. До цього виду ризиків також відносять екстремальні погодні умови, кліматичні катаклізми та катастрофи з екологічних причин: масштабні пожежі, проблеми сукупного впливу на навколишнє середовище, проблеми з якістю води та повітря, і як наслідок очікуваний негативний вплив на людей.

Організаційні ризики стосуються організаційної зрілості керівників проєкту та зацікавлених сторін, навичок, професіоналізму та навчання персоналу, аспектів загальних ресурсів компанії, які можуть вплинути на реалізацію проєкту. Усі проєкти виконуються людьми, включаючи членів проєктної групи та керівництво, клієнтів і замовників, постачальників і субпідрядників, які є певною мірою непередбачувані та вносять невизначеність у проєкти, над якими вони працюють. Організаційні ризики пов'язані з порушеннями внутрішніх процедур і систем в організації, будь-то компанія, департамент, підрозділ, команда чи група друзів у стартапі. До цих ризиків відносять:

- *ризики з персоналом* стосуються: недостатності персоналу, необхідного для вчасного завершення проєкту; помилок через недосвідченість фахівців, призначених на виконання ключових завдань; втрати одразу декількох членів команди на вирішальному етапі проєкту, наприклад, у разі їх хвороби чи то інших життєвих колізій; зміни персоналу протягом проєкту тощо;
- *ризики недотримання графіка* та своєчасної здачі програмного продукту. Наприклад, коли недостатньо часу для планування або коли зацікавлені сторони вимагають пізніх змін з тих чи то інших причин. До цієї групи також відносять можливі проблеми через внутрішню бюрократичну тяганину і, як наслідок, затримки в отриманні погоджених рішень;

- *бюджетні ризики* можуть стосуватися проблем розподілу та достатності фінансування і ресурсів, проблем з постачанням, своєчасної оплати витрат у повсякденній бізнес-діяльності або того, що впливові стейкхолдери вимагатимуть додаткових витрат для власних комерційних цілей;
- *ризики планування* стосуються мінливості процесів всередині організації, її пріоритетів, зміни вимог та залежностей у проєкті, потреби впровадження новітніх технологій і переходу на них під час роботи над проєктом, що може спричинити збої через несумісність інтерфейсів систем, конфлікт версій, необізнаність роботи з ними тощо. До цієї групи можна віднести ризики непередбаченого перенавантаження керівника проєкту, збої управління, появи нового більш пріоритетного проєкту тощо.

Проєктні ризики стосуються того, як працює команда над проєктом і які внутрішні аспекти команди можуть вплинути на успіх проєкту. Тут передусім варто враховувати можливі міжособистісні проблеми членів команди, а також те, як вони можуть вплинути на результати. Ці ризики стосуються проблем сформованої у колективі культури та моралі команди проєкту, наявності чи то відсутності узгодженої роботи та чітких каналів зв'язку між членами команди. Різновидами проєктних ризиків є:

- *ризики цілей проєкту* загалом пов'язані зі складністю або неможливістю досягнення вимог замовника через погане або неповне визначення мети, обсягів, потреб та результатів проєкту, помилки у формуванні графіку та плануванні кошторису, складності одночасної роботи над багатьма програмними проєктами, незаплановану роботу, відсутність контролю над пріоритетами персоналу. Відомо, що понад третину проєктів зазнають невдачі через відсутність чітких цілей [23]. Сюди можна додати проблеми через відсутність підтримки вищого керівництва, його тиск з метою виконання проєкту за прискореним графіком, відсутність координації/комунікації з проєктною командою. Наявність чіткої проєктної документації допомагає ПМ розробити ефективну стратегію для встановлення основних етапів і параметрів якості та кількісної оцінки прогресу проєкту;
- *ризики операційні* стосуються управлінських критеріїв, ділової діяльності керівників проєкту, питань бізнес-процесів, бізнес-інтеграції, організаційних змін, планування та контролю виконання. Важливим тут є визначення пріоритетів завдань і підготовка команди до найімовірніших перешкод задля швидкого подолання проблем та успішного завершення проєкту. Ризики цієї групи можуть бути спричинені недостатнім кваліфікаційним рівнем ПМ, проблемами планування, нечіткістю вимог і поганою комунікацією всередині колективу, а, як наслідок, розповзання обсягів проєкту, перевищення бюджету, порушення графіку проєкту. За даними статистики [24], 32% проєктів зазнають невдачі через погане управління проєктами. Тому до ПМ висуваються високі вимоги. Він має поєднувати в собі риси та навички стратега і тактика, бути глибоко залученим у проєкт, ефективно спілкуватися з командою, створювати міцну організаційну структуру й впроваджувати детальні процеси документування. Немаловажним є наявність у ПМ лідерських та аналітичних здібностей. Залежно від обсягу та складності проєкту, значна частина управління ризиками керівником проєкту полягає в тому, щоб приділити увагу деталям, водночас пам'ятаючи про загальну картину. Корисно мати детальний план пом'якшення таких ризиків, щоб проєкт не закінчився провалом. Спеціальне програмне забезпечення для планування проєкту може допомогти уникнути багатьох ризиків, які можуть виникнути у проєкті;
- *ризики культури спілкування* стосуються формування прозорого робочого середовища, відкритих каналів комунікації та можливостей для членів команди висловлювати своє бачення без страху бути покараним. Команди проєктів складаються з багатьох людей, які мають різні навички, темпераменти, інтереси, знання, досвід. Важливо створити і підтримувати сприятливе для співпраці середовище однодумців. Для формування такого середовища важливим є організаційна і професійна культура, на основі яких формується власна командна культура, яка дає змогу людям працювати разом і забезпечує синергетичний ефект від взаємодії. Одним із наслідків поганого управління проєктами, відсутності комфортного робочого середовища може бути плинність кадрів: ключові розробники проєктів залишають команду, не передаючи нікому важливу інформацію про проєкт, що тягне за собою затримки в розробці, недотримання термінів і бюджету. Тому важливим є індивідуальне та командне навчання для обміну знаннями й досвідом, що, врешті-решт, забезпечує гарні результати проєкту. Запровадження інструментів співпраці має життєво важливе значення для підтримки стейголдерів, створення централізованого центру керування змінами, встановлення чіткої комунікації. Надійність ПМ не в останню чергу означає активне виявлення конфліктів між особистісними інтересами та інтересами організації чи клієнтів. Приблизно 29% проєктів зазнають невдачі [25] через погану комунікацію численних стейкголдерів. Керівникові проєкту для вирішення можливих розбіжностей між стейкголдерами мирним шляхом варто послуговуватись стратегіями керування очікуваннями та звітності [26] перед відповідною групою стейкголдерів:

o *клієнти*: головним тут є знання про потреби клієнта, його культуру та можливі больові точки бізнесу. Такі дані варто зібрати і задокументувати ще до початку виконання проєкту. Це допоможе уникати або швидко вирішувати можливі конфлікти;

o *члени команди проєкту*: ключ до керування очікуваннями команди – постійне спілкування з ними. ПМ варто запланувати неформальні зустрічі віч-на-віч із кожним учасником, щоб розуміти настрої та можливі проблеми

в групі. Для зменшення комунікаційних ризиків варто вибрати зручну для всіх платформу для спілкування і співпраці, спростити комунікаційні потоки проєкту, що дозволить команді бути ефективною;

- *керівники*: тут варто спочатку подати керівництву комплексний план з основними етапами роботи, а надалі постійно інформувати їх про можливі ризики проєкту на основі їхніх інформаційних потреб;
- *менеджери ресурсів*: ключовим тут є встановлення хороших стосунків. Якщо у ПМ хороші стосунки з менеджером ресурсів, то запити на обладнання чи робочу силу не будуть блокуватися.

Слід зазначити, що перелік ризиків розробки ПЗ та методів їх зменшення не є вичерпним і може доповнюватися залежно від складності проєкту, галузі та зовнішніх обставин. Проте високий рівень компетентності ПМ та продумана стратегія управління ризиками значно знижує вплив ризиків на проєкт.

Специфіка ризиків у проєктах із розробки ПЗ зумовлена тим, що кожен проєкт є унікальним, позаяк має принаймні деякі елементи, які раніше не реалізувалися, і, природно, з цими елементами пов'язана невизначеність. Загальною проблемою для всіх програмних проєктів є нерозуміння та/або неврахування нефункціональних вимог, таких як продуктивність, масштабованість, відмовостійкість, моніторинг і перевірка якості. Ці вимоги настільки ж критичні, як і функціональні та бізнес-вимоги, щоб гарантувати, що досвід кінцевого користувача відповідатиме його очікуванням. Сюди варто додати, що сучасні програмні проєкти переважно є складними, оскільки мають інтегруватися з багатьма зовнішніми системами, наприклад, платіжними системами, месенджерами, хмарними сервісами тощо. Командам, які розробляють комерційні програмні продукти, необхідно збалансовувати швидкість розробки, безпеку (включно з конфіденційністю даних) і взаємодію з користувачем. Неможливість успішного виконання одного чи декількох з цих трьох завдань, скоріш за все, призведе до провалу проєкту [27]. До того ж вимоги до програмних проєктів можуть змінюватись. Кожен програмний проєкт є агентом змін, який рухається від відомого теперішнього до невідомого майбутнього з усією невизначеністю, пов'язаною з таким рухом. Знати чи передбачити все, що зміниться за таких умов, неможливо. Аналіз та виявлення ризиків програмного проєкту передбачає створення низки припущень щодо майбутнього. Припущення можуть виявитися хибними, і ймовірно, що деякі з них залишаться прихованими, тобто певним джерелом невизначеності. Усі ці аспекти створюють для програмних проєктів додаткові фактори ризику, до яких треба адаптуватися.

Висновки

Класифікація ризиків, тобто групування пов'язаних типів ризиків, сприяє більш ефективному загальному управлінню ними. Вона допомагає виявити загальні джерела ризику, об'єднати ресурси ризику, точніше застосувати стратегії зменшення (пом'якшення) ризику та управляти взаємозв'язком конкретних ризиків. Якщо ризики не класифіковані, може відбуватися ненавмисний збіг або суперечливість роботи з пом'якшення ризиків, що спричинить проблеми, тобто додаткові негативні ризики. Групування ризиків за категоріями та різновидами допомагає створити ефективніші стратегії реагування на ризики, дозволяючи команді проєкту зосередитися на типах із найвищим ризиком, або напрацювати загальну реакцію для будь-яких ризиків певного типу. Перевагами такого підходу є підвищення ефективності використання часу команди проєкту та точніша робота з управління ризиками в цілому. Саме тому ПМ повинні знати категорії ризиків та їх роль в управлінні ризиками.

Оскільки всі проєкти піддаються ризику, успішними є ті проєкти, в яких цим ризиком управляють правильно. Систематичне застосування методології управління ризиками та її поширення на всю організацію може забезпечити суттєву конкурентну перевагу в умовах дедалі більшої невизначеності. Спеціалісти-практики з управління проєктами шукають нові ефективні та гнучкі інструменти управління ризиками для підтримки своєї повсякденної роботи, але наразі не існує універсального інструмента, який би задовольнив усі їхні потреби. Нині ризики є лише частиною повсякденної роботи щодо управління ними, їх оновлення та пом'якшення. Постійно виникають ризики, про які раніше навіть не чули. Змінюються менталітет і культура, з'являються нові погляди на ризики з позиції адаптації та пошуку в них нових можливостей, щоб забезпечити конкурентоспроможність і зберегти зацікавленість клієнтів у створюваних програмних продуктах. Корисно розвивати культуру стійкості до ризиків, яка дозволить компанії адаптуватися та швидко реагувати у разі настання цих ризиків. Всі члени колективу (менеджери, керівники, розробники, тестувальники та ін.) повинні розуміти ризики, пов'язані зі своїми завданнями, і те, який вплив це може мати не лише на них, а й на всі команди проєкту організацію чи на компанію. Виходячи з притаманних сильних і слабких сторін компаній, варто узгодити стратегії управління ризиками, які дозволять керівникам проєктів робити програмні проєкти успішними. Концепції та навички мають бути вплетені в повсякденне прийняття бізнес-рішень і стати самокоригованими та самодостатніми для постійного вдосконалення програмних продуктів і послуг. Саме тому надалі управління ризиками ставатиме все більш і більш важливим, як і інструменти для визначення ризиків, управління ними, а особливо для визначення дій щодо реагування на них.

Список використаної літератури

1. Crispin G. The Essence of Risk Identification in Project Risk Management: An Overview. *International Journal of Science and Research (IJSR)*, 2020, no. 9, pp. 1553-1557. https://doi.org/10.21275/SR20215023033.

2. Project Risk Assessment (Ultimate Guide to Project Risk, P. 1). URL: https://www.wrike.com/blog/ultimate-guide-to-project-risk-part-1-risk-assessment

3. Different types of risks in Software Project Development. URL: https://geeksforgeeks.org/different-types-of-risks-in-software-project-development

4. Zvonko K., Kafol C. Types of Risk in a System Engineering Environment and Software Tools for Risk Analysis. *Procedia Engineering*, 2014, no. 69, pp. 177-183. https://doi.org/10.1016/j.proeng.2014.02.218.

5. Bell M. Risk Types in Project Management, 2022. URL: https://projectmanagementacademy.net/resources/blog/risk-types-in-project-management

6. Грицюк Ю. І., Далявський В. С. Формалізація процесу управління ризиками розроблення програмного забезпечення. *Науковий вісник НЛТУ України*. 2018. № 28(11). С. 135-154. https://doi.org/10.15421/40281124.

7. Wikarsa L. Risk Management for IT Projects. URL: https://researchgate.net/publication/328653592_Risk_Management_for_IT_Projects

8. Stojcetovic B., Misic M., Živče Š., Lazarević D., Zubac D. Managing of risks and quality in projects. *8th International quality conference*, 2014, pp. 201-207.

9. Коваленко О. В. Методи якісного аналізу та кількісної оцінки ризиків розробки програмного забезпечення. *Збірник наукових праць «Системи управління, навігації та зв'язку*. 2018. № 3. С. 116-125. https://doi.org/10.26906/SUNZ.2018.3.116.

10. Alkhuraiji Sh. L. Incorporating Knowledge Networks to Address Risk associated with Decision-Making in IT Projects. *International Conference on Decision Support System Technology* (ICDSST'2016), Plymouth, UK, 2016, pp. 1-7.

11. PMBOK® Guide. URL: https://www.pmi.org/pmbok-guide-standards/foundational/pmbok.

12. Product Management and Project Management: Alignment and Differences. URL: https://www.pmi.org/learning/thought-leadership/product-and-project-management.

13. ISO 31000 Risk management. URL: https://www.iso.org/iso-31000-risk-management.html.

14. PMI Lexicon of Project Management Terms. URL: https://www.pmi.org/pmbok-guide-standards/lexicon.

15. Bishop K. 4 Types of Risk Categories in Project Risk Management. URL: https://fool.com/the-ascent/small-business/project-management/articles/risk-categories

16. Трофименко О. Г., Пастернак Ю. Ю., Манаков С. Ю., Лобода Ю.Г. Автоматизація тестування вебсайтів електронної комерції. *Сучасна спеціальна техніка.* 2021. № 2(65). С. 46-59. https://doi.org/10.36486/mst2411–3816.2021.2(65).5

17. Ситник В. А., Тесленко П. О., Бедрій Д. І, Шерстюк О. І. Управління прототипуванням та ризиками ІТ-проектів з відкритим кодом. *Управління проектами та розвиток виробництва*. 2018. № 3(67). С. 116-128.

18. Трофименко О. Г., Логінова Н. І., Манаков С. Ю., Дубовой Я. В. Кібеззагрози в освітньому секторі. *Кібербезпека: освіта, наука, техніка*. 2022. № 4(16). С. 76-84. https://doi.org/10.28925/2663-4023.2022.16.7684.

19. Трофименко О. Г., Логінова Н. І., Манаков С. Ю., Янковський О. Г. Кіберризики в освітньому секторі. *Сучасна спеціальна техніка*. 2022. № 2(69). С. 111-117. https://doi.org/10.36486/mst2411–3816.2022.2(69).10.

20. Gordon Y., Jasny M. From Ransomware to Mobile Malware: Emerging Cybersecurity Risks. Project Management Institute (PMI). URL: https://pmi.org/learning/training-development/projectified-podcast/podcasts/from-ransomware-to-mobile-malware-emerging-cybersecurity-risks

21. Трофименко О. Г., Дика А. І., Лобода Ю. Г. Аналіз уразливостей та проблем безпеки вебзастосунків. *Системні технології*. 2023. № 3(146). С. 25-37. https://doi.org/10.34185/1562-9945-3-146-2023-03.

22. Guide on Mergers and Acquisitions Risks: Lessons Learned from Failed Transactions. URL: https://datarooms.org/vdr-blog/risks-in-merger-and-acquisition

23. 95 Essential Project Management Statistics: 2023 Market Share & Data Analysis. URL: https://financesonline.com/35-essential-project-management-statistics-analysis-of-trends-data-and-market-share/

24. Kononenko V. 7 main types of software development risks, 2022. URL: https://computools.com/software-development-risks

25. Success in Disruptive Times. Expanding the Value Delivery Landscape to Address the High Cost of Low Performance. URL: https://pmi.org//media/pmi/documents/public/pdf/learning/thought-leadership/pulse/pulse-of-the-profession-2018.pdf

26. What Is Project Stakeholder Management? FAQ. Project Management Guide. URL: https://www.wrike.com/project-management-guide/faq/what-is-project-stakeholder-management

27. 16 Obstacles To A Successful Software Project (And How To Avoid Them). URL: https://www.forbes.com/sites/forbestechcouncil/2022/06/21/16-obstacles-to-a-successful-software-project-and-how-to-avoid-them/?sh=76aa87581915

References

1. Crispin G. (2020) The Essence of Risk Identification in Project Risk Management: An Overview. *International Journal of Science and Research (IJSR)*, no. 9, pp. 1553-1557. https://doi.org/10.21275/SR20215023033.

2. Project Risk Assessment (Ultimate Guide to Project Risk, P. 1). Access mode: https://wrike.com/blog/ultimate-guide-to-project-risk-part-1-risk-assessment

3. Different types of risks in Software Project Development. Access mode: https://geeksforgeeks.org/different-types-of-risks-in-software-project-development

4. Zvonko K., Kafol C. (2014) Types of Risk in a System Engineering Environment and Software Tools for Risk Analysis. *Procedia Engineering*, no. 69, pp. 177-183. https://doi.org/10.1016/j.proeng.2014.02.218.

5. Bell M. Risk Types in Project Management, 2022. Access mode: https://projectmanagementacademy.net/resources/blog/risk-types-in-project-management

6. Hrytsiuk Yu. I., Dalyavskyy V. S. (2018) Formalization of the Risk Management Process of Software Development. *Scientific Bulletin of UNFU*, no. 28(11), pp. 135-154. https://doi.org/10.15421/40281124. [in Ukrainian].

7. Wikarsa L. Risk Management for IT Projects. Access mode: https://researchgate.net/publication/328653592_Risk_Management_for_IT_Projects

8. Stojcetovic B., Misic M., Živče Š., Lazarević D., Zubac D. (2014) Managing of risks and quality in projects. *8th International quality conference*, pp. 201-207.

9. Kovalenko O. (2018) Quality analysis and quantitative assessment of risks methods of software development. *Control, Navigation and Communication Systems. Academic Journal*, no. 3, pp. 116-125. https://doi.org/10.26906/SUNZ.2018.3.116. [in Ukrainian].

10. Alkhuraiji Sh. L. (2016) Incorporating Knowledge Networks to Address Risk associated with Decision-Making in IT Projects. *International Conference on Decision Support System Technology* (ICDSST'2016), Plymouth, UK, pp. 1-7.

11. PMBOK® Guide. URL: https://www.pmi.org/pmbok-guide-standards/foundational/pmbok.

12. Product Management and Project Management: Alignment and Differences. Access mode: https://www.pmi.org/learning/thought-leadership/product-and-project-management.

13. ISO 31000 Risk management. Access mode: https://www.iso.org/iso-31000-risk-management.html.

14. PMI Lexicon of Project Management Terms. Access mode: https://www.pmi.org/pmbok-guide-standards/lexicon.

15. Bishop K. 4 Types of Risk Categories in Project Risk Management. Access mode: https://fool.com/the-ascent/small-business/project-management/articles/risk-categories

16. Trofymenko, O., Pasternak, Yu., Manakov, S., Loboda, Yu. (2021). Automation of testing e-commerce websites. *Modern Special Technics*, no. 2(65), pp. 46-59. https://doi.org/10.36486/mst2411–3816.2021.2(65).5 [in Ukrainian].

17. Sytnyk V. A., Teslenko P. O., Bedrii D. I., Sherstyuk O. I. (2018) Management of prototyping and risks of open source IT projects. *Project management and production development*, no. 3(67), pp. 116-128. [in Ukrainian].

18. Trofymenko, O., Loginova, N., Manakov, S., Dubovoi, Y. (2022). Cyberthreats in higher education. *Cybersecurity: Education, Science, Technique*, no. 4(16), pp.76-84. https://doi.org/10.28925/2663-4023.2022.16.7684. [in Ukrainian].

19. Trofymenko, O., Loginova, N., Manakov, S., Iankovskii, O. (2022). Cyber risks in the education sector. *Modern Special Technics*, no. 2(69), pp. 111-117. https://doi.org/10.36486/mst2411–3816.2022.2(69).10. [in Ukrainian].

20. Gordon Y., Jasny M. From Ransomware to Mobile Malware: Emerging Cybersecurity Risks. Project Management Institute (PMI). Access mode: https://pmi.org/learning/training-development/projectified-podcast/podcasts/from-ransomware-to-mobile-malware-emerging-cybersecurity-risks

21. Trofymenko O., Dyka A., Loboda Yu. (2023) Analysis of vulnerabilities and security problems of web applications. *System technologies*, no. 3(146), pp. 25-37. https://doi.org/10.34185/1562-9945-3-146-2023-03. [in Ukrainian].

22. Guide on Mergers and Acquisitions Risks: Lessons Learned from Failed Transactions. Access mode: https://datarooms.org/vdr-blog/risks-in-merger-and-acquisition

23. 95 Essential Project Management Statistics: 2023 Market Share & Data Analysis. Access mode: https://financesonline.com/35-essential-project-management-statistics-analysis-of-trends-data-and-market-share/

24. Kononenko V. 7 main types of software development risks, 2022. Access mode: https://computools.com/software-development-risks

25. Success in Disruptive Times. Expanding the Value Delivery Landscape to Address the High Cost of Low Performance. Access mode: https://pmi.org//media/pmi/documents/public/pdf/learning/thought-leadership/pulse/pulse-of-the-profession-2018.pdf

26. What Is Project Stakeholder Management? FAQ. Project Management Guide. Access mode: https://www.wrike.com/project-management-guide/faq/what-is-project-stakeholder-management

27. 16 Obstacles To A Successful Software Project (And How To Avoid Them). Access mode: https://www.forbes.com/sites/forbestechcouncil/2022/06/21/16-obstacles-to-a-successful-software-project-and-how-to-avoid-them/?sh=76aa87581915.