УДК 005.334

Кочерга В. І.
магістрант кафедри економіки і підприємництва
ORCID: 0009-0000-7130-3226;
Дергалюк Б. В.
д-р екон. наук, проф.,
професор кафедри економіки і підприємництва
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря
Сікорського», Київ, Україна
ORCID: 0000-0001-8791-9121

ОЦІНЮВАННЯ ЕКОНОМІЧНИХ НАСЛІДКІВ РИЗИКІВ В ІТ-ПРОЄКТАХ ПІДПРИЄМСТВА

У сучасних умовах швидкого цифрового розвитку наявність ІТ-проєктів у межах діяльності підприємства та успішна їх реалізація може значно підвищити конкурентоспроможність та рівень інноваційності. Водночас процес впровадження таких проєктів, як і низки інших, супроводжується високим рівнем невизначеності, особливо через сильний економічний вплив. Це призводить до необхідності ефективного управління ризиками та до моніторингу оцінки їх економічних наслідків для компанії.

Проаналізувавши результати наукових досліджень, можна зробити висновок, що ІТ-проєкти мають кілька основних характеристик, а саме: підвищену складність структури, інноваційність та динамічність змін, що значно ускладнює можливість точного прогнозування результатів їх реалізації (mdcs.knuba.edu.ua). У той же час, наявність ризиків є невід'ємною складовою ІТ-проєктів і виникають вони беззастережно на всіх етапах життєвого циклу проєкту – від опису ідеї до завершення та супроводу отриманого продукту. Також, судячи в проведених досліджень, ризики можуть мати різну природу: технічну, організаційну, фінансову чи зовнішню, а їх вплив може мати накопичувальний ефект упродовж реалізації проєкту [1, с. 129]. До прикладу, вони можуть проявлятися у вигляді раптових помилок у програмному забезпеченні, недостатньої координації та комунікації в межах команди, перевищенні бюджету або швидкоплинних змін ринкових умов.

Якщо розглянути економічні наслідки ризиків в ІТ-проєктах більш поглиблено, то можна розділити їх на дві категорії, із прямим та непрямим характером. До прямих наслідків можна віднести перевищення запланованого бюджету на витрати, затримки дедлайнів або зниження рівня рентабельності самого проєкту. Натомість непрямі можуть проявлятися у втраті конкурентної позиції на ринку, погіршенні репутації підприємства або ж у недосягненні стратегічних цілей.

Важливим етапом в управлінні ІТ-проєктами є правильний вибір методів оцінювання ризиків, оскільки саме це великою частиною впливає на точність визначення їх економічних наслідків для діяльності компанії та ефективність прийняття управлінських рішень.

Наразі на практиці використовують широкий спектр методів оцінки ризиків, які відрізняються за рівнем формалізації, точністю та складністю у застосуванні. Розглянемо перелік основних методів, які компанії використовують у своїй діяльності для проведення аналізу рівня ризику (див. рис. 1).

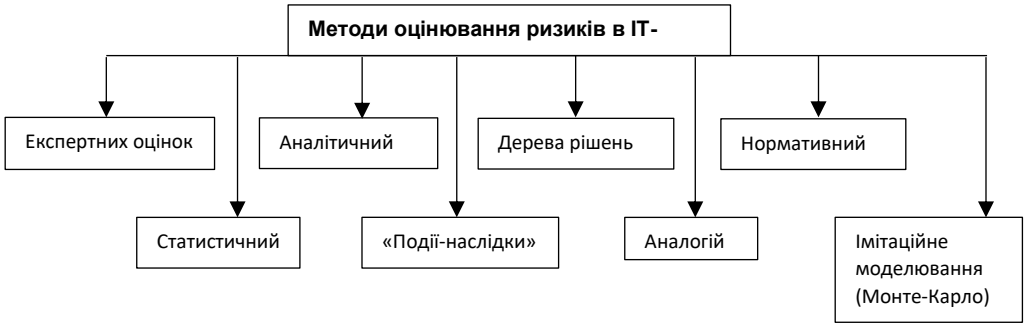

Рисунок 1 – Основні методи оцінки ризиків в ІТ-проєктах
Джерело: створено авторами на основі [2, с. 5]

Розглянемо методи більш детально, а отже статистичні – базуються на використанні кількісних даних і дозволяють отримати найбільш обґрунтовані результати, однак їх застосування обмежується потребою наявного значного обсягу достовірної інформації. Натомість методи експертних оцінок доцільні в умовах, коли статистичних даних недостатньо, що характерно для інноваційних ІТ-проєктів, проте отримані результати мають певний рівень суб'єктивності та залежать від кваліфікації залучених фахівців. Аналітичні методи забезпечують відносну простоту розрахунків і доступність застосування, однак не завжди дозволяють врахувати повний спектр факторів ризику, особливо у складних проєктах.

Більш гнучким інструментом оцінки порівняно з іншими є застосування дерева рішень, який передбачає побудову альтернативних сценаріїв розвитку подій і дозволяє обрати оптимальний варіант реалізації проєкту, проте його використання супроводжується з підвищеними витратами часу та складністю моделювання.

Важливе місце займають нормативні методи, що базуються на використанні встановлених стандартів і забезпечують чіткість та простоту оцінювання, однак вони не враховують індивідуальні особливості конкретного ІТ-проєкту. Метод «подій–наслідків» дозволяє детально проаналізувати причинно-наслідкові зв'язки між ризиками та їх впливом, проте є достатньо трудомістким і потребує значних ресурсів.

Також на практиці доволі часто застосовується метод аналогій, який ґрунтується на використанні досвіду реалізації подібних проєктів. Для нього більш характерна простота та швидкість застосування, однак є обмеженість точності через складність підбору релевантних аналогів. Одним із найбільш сучасних підходів є використання імітаційного моделювання, зокрема методу Монте-Карло, який дозволяє враховувати невизначеність і оцінювати вплив великої кількості факторів ризику одночасно, при цьому забезпечує високу точність прогнозування.

Таким чином, кожен із методів оцінювання ризиків має свої переваги та обмеження, що зумовлює доцільність їх комплексного застосування. Поєднання якісних і кількісних підходів дозволяє скомпонувати більш об'єктивну оцінку ризиків та їх економічних наслідків, підвищити точність прогнозування результатів проєкту і забезпечити ефективність управлінських рішень в умовах невизначеності.

Варто підкреслити, що ризики ІТ-проєктів впливають не лише на строки та бюджет їх реалізації, а й безпосередньо на якість кінцевого продукту. Недостатній рівень управління ризиками може призводити до виникнення дефектів програмного забезпечення, зниження функціональності систем, порушення вимог до безпеки та, як наслідок, до зниження загальної цінності продукту для користувачів.

Таблиця 1 – Перелік міжнародних стандартів управління ризиками в ІТ-проєктах

№	Назва стандарту	Основна характеристика стандарту
1	Стандарт ISO 31000 та ISO 31010	Дані стандарти формують концептуальну основу управління ризиками на рівні підприємства. Орієнтовані не лише на ідентифікацію ризиків, а й на інтеграцію ризик-менеджменту у всі управлінські процеси [3, с. 68].
2	Стандарт ISO 27001	Зосереджений на забезпеченні інформаційної безпеки як критичного елементу ІТ-проєктів. Його особливістю є орієнтація на запобігання ризикам, пов'язаним із витоком, втратою або несанкціонованим доступом до даних [3, с. 68].
3	Стандарт NIST 800-53	Цей стандарт має більш прикладний і технічно орієнтований характер, оскільки містить детальний перелік контрольних заходів для забезпечення кібербезпеки. Його перевага полягає у глибокій деталізації механізмів захисту [3, с. 68].
4	Стандарт PMBOK	Виступає як універсальна методологічна база управління проєктами, в якій ризик-менеджмент є невід'ємною складовою. Його особливістю є чітка структуризація процесів управління ризиками – від їх ідентифікації до моніторингу та реагування [3, с. 68].

Отже, дотримання міжнародних стандартів дозволяє забезпечити комплексний підхід до управління ризиками, підвищити якість кінцевого продукту та мінімізувати негативний вплив невизначеності. Найбільш ефективним є поєднання елементів різних стандартів, що дає змогу адаптувати систему управління ризиками до специфіки конкретного ІТ-проєкту. У свою чергу, дозволяє підвищити економічну ефективність ІТ-проєктів та забезпечити стабільний розвиток підприємства в умовах цифрової трансформації.

Список використаних джерел

1. НАЗАРОВА К., ПАРАСІЙ-ВЕРГУНЕНКО І., ОСТАПЕЦЬ А. Класифікація ризиків компаній ІТ-індустрії. SCIENTIA FRUCTUOSA. 2023. Т. 150, № 4. С. 120–137. URL: https://doi.org/10.31617/1.2023(150)08 (дата звернення: 21.03.2026)
2. Прохорова В. Методи оцінки проєктних ризиків ІТ-компаній. Adaptive Management Theory and Practice Economics. 2023. Т. 16, № 32. URL: https://doi.org/10.33296/2707-0654-16(32)-16 (дата звернення: 21.03.2026).
3. Maksymov A. Analysis of risk management standards and their application in IT projects. Management of Development of Complex Systems. 2025. № 61. С. 66–75. URL: https://doi.org/10.32347/2412-9933.2025.61.66-75 (the date of application: 21.03.2026)