УДК 004.02:519.85

МЕТОДИ ОЦІНЮВАННЯ ТА УПРАВЛІННЯ РИЗИКАМИ

Ященко С.С.
stanislav.iashchenko@nure.ua
Науковий керівник – канд. техн. наук, ст. викл. Путятіна О.Є.
Харківський національний університет радіоелектроніки, каф. ІНФ
м. Харків, Україна

This paper explores modern methods of risk assessment and management within the lifecycle of IT projects. Given the high degree of uncertainty, technological complexity, and dynamic changes in the software development environment, effective risk management is crucial for preventing budget overruns and missed deadlines. The study analyzes the transition from reactive problem-solving to proactive forecasting by integrating both qualitative (e.g., Risk Matrix) and quantitative assessment techniques. Furthermore, it outlines classical risk response strategies — avoidance, transfer, mitigation, and acceptance — and highlights the role of iterative methodologies in continuous risk monitoring. Ultimately, the research emphasizes that a systematic approach to risk management is an essential component for the successful and timely delivery of complex IT systems.

Сучасна індустрія інформаційних технологій характеризується надзвичайно високим рівнем динамічності, технологічної складності та невизначеності. Розробка та впровадження програмних систем або масштабованих апаратних комплексів завжди супроводжується значною кількістю внутрішніх та зовнішніх ризиків. Згідно з галузевими дослідженнями, значна частка ІТ-проєктів стикається з перевитратою затвердженого бюджету, зривом встановлених термінів (дедлайнів) або частковою невідповідністю кінцевого продукту початковим вимогам замовника [1].

Традиційний підхід, за якого команди розробників реагують на інциденти та проблеми лише після їх фактичного виникнення (так зване «реактивне управління»), демонструє свою неефективність у складних проєктах. Натомість критичною стає необхідність переходу до проактивного управління — системного та безперервного процесу прогнозування, ідентифікації та нейтралізації потенційних загроз ще на ранніх етапах планування та проєктування архітектури.

З огляду на це, метою даної роботи є комплексний аналіз сучасних методів оцінювання ІТ-ризиків, класифікація ключових загроз, а також визначення найбільш ефективних стратегій управління та реагування на них у межах життєвого циклу розробки програмного забезпечення для забезпечення його успішної та безпечної реалізації.

Ідентифікація та класифікація ризиків. Першим та фундаментальним етапом у системі управління ризиками є їх своєчасна ідентифікація. У контексті розробки програмного забезпечення ризик визначається як непевна

подія або умова, настання якої має прямий вплив на ключові обмеження проєкту: обсяг робіт, бюджет, терміни реалізації або якість кінцевого продукту.

Для ефективного системного аналізу виявлені загрози підлягають обов'язковій класифікації за джерелом їх виникнення [2]. Технічні ризики безпосередньо пов'язані з архітектурними недоліками, інтеграцією нових або неперевірених технологій, а також проблемами масштабованості системи. Організаційні (або управлінські) ризики охоплюють проблеми неадекватної оцінки часових витрат (естімації), плинності кадрів та порушення комунікації всередині команди розробників. Натомість зовнішні ризики включають загрози інформаційній безпеці (наприклад, цілеспрямовані кібератаки), раптову зміну законодавчих регулювань або збої на стороні сторонніх постачальників хмарних послуг та API.

Якісні та кількісні методи оцінювання. Після ідентифікації та класифікації загроз виникає необхідність їх пріоритезації. Сучасна методологія управління ІТ-проєктами вимагає комплексного застосування якісних та кількісних методів оцінювання [3].

Якісний аналіз є інструментом первинного та швидкого скринінгу, що базується на експертних судженнях. Основу цього підходу становить побудова «Матриці ризиків» (Risk Matrix), де кожній ідентифікованій загрозі присвоюються значення за двома ключовими параметрами: *ймовірність настання* та *ступінь впливу* на проєкт (від незначного до критичного). Для підвищення об'єктивності таких оцінок часто застосовується метод Дельфі (Delphi), що дозволяє шляхом анонімного опитування досягти консенсусу серед незалежних фахівців щодо найскладніших технічних загроз [4].

Кількісний аналіз, натомість, оперує об'єктивними математичними та статистичними моделями для вимірювання ризику у конкретних числових показниках (грошовому еквіваленті або людино-годинах). До класичних інструментів кількісного оцінювання належить аналіз очікуваної грошової вартості та метод побудови дерев рішень, які допомагають керівнику обрати оптимальний шлях розвитку системи з урахуванням фінансової вартості потенційних наслідків.

Для складних ІТ-проєктів із надвисоким ступенем невизначеності активно застосовується імітаційне моделювання за методом Монте-Карло (Monte Carlo simulation) [5]. Цей алгоритм використовує комп'ютерні потужності для багаторазового перерахунку моделі проєкту з випадковими значеннями вхідних змінних, що дозволяє з високою статистичною точністю визначити реальну ймовірність завершення розробки в межах затвердженого бюджету та дедлайнів.

Стратегії управління та реагування. Після проведення детального якісного та кількісного оцінювання розробляється план реагування на ризики. Згідно з міжнародними стандартами управління проєктами, виділяють чотири базові стратегії роботи з негативними ризиками (загрозами) [3]:

Уникнення (Avoidance): зміна архітектури або плану проєкту з метою повного усунення джерела загрози (наприклад, відмова від використання бета-версії нестабільного фреймворку на користь перевіреного рішення). *Передача (Transfer)*: перенесення відповідальності та фінансових наслідків ризику на третю сторону. В IT-галузі це найчастіше реалізується через аутсорсинг складних модулів спеціалізованим компаніям або використання хмарних SLA-контрактів. *Пом'якшення (Mitigation)*: превентивні дії, спрямовані на зниження ймовірності настання або сили впливу ризику до прийнятного рівня (наприклад, впровадження автоматизованого тестування коду, резервне копіювання баз даних). *Прийняття (Acceptance)*: свідома згода команди з імовірністю настання події, коли витрати на уникнення ризику перевищують потенційні збитки. У такому разі формується управлінський резерв (бюджетний або часовий буфер) для покриття можливих втрат.

Окремо варто відзначити роль гнучких методологій розробки (Agile/Scrum). В умовах високої невизначеності ітеративний підхід виступає потужним інструментом безперервного пом'якшення ризиків [5].

Підсумовуючи, можна стверджувати, що ефективне управління ризиками в IT-галузі є не одноразовою процедурою, а безперервним, циклічним процесом, який пронизує всі стадії розробки програмного забезпечення. Перехід від реактивної моделі гасіння "пожеж" до системного проактивного прогнозування вимагає чіткої класифікації загроз та розуміння їхньої природи [2].

Список використаних джерел:

1. Bent Flyvbjerg, Alexander Budzier Why your IT project may be riskier than you think // Harvard Business Review. – 2011. – Vol. 89, No. 9. – P. 23–25.

2. Barry W. Boehm Software risk management: principles and practices // IEEE Software. – 1991. – Vol. 8, No. 1. – P. 32–41.

3. Project Management Institute A Guide to the Project Management Body of Knowledge (PMBOK Guide). – 7th ed. – Newtown Square : Project Management Institute, 2021. – 370 p.

4. Gary J. Skulmoski, Francis T. Hartman, Jennifer Krahn The Delphi method for graduate research // Journal of Information Technology Education. – 2007. – Vol. 6. – P. 1–21.

5. Alan Moran Agile Risk Management. – Cham : Springer, 2014. – 186 p.