Журан О.А., *к.е.н., доцент*
Кафедра економічної кібернетики та інформаційних технологій
Глава М.Г.
Кафедра інформаційних систем
Одеський національний політехнічний університет

УПРАВЛІННЯ РИЗИКАМИ В ІТ-ПРОЕКТАХ

В рамках дослідження розглянуто особливості управління проектами в ІТ-сфері. Висвітлені основні методи розрахунку ризиків та підходи до їх подолання.
Ключові слова: *ІТ-проект, прогнозування ризиків, управління ризиками, управління проектами.*

Постановка проблеми та ціль дослідження. Управління проектами являє собою вміле поєднання та використання досвіду, сучасних інструментів, технологій, знань та технік, які необхідні для досягнення мети проекту. Загальновизнаним є той факт, що значна доля проектів у галузі ІТ не відповідає поставленим цілям, бюджету або термінам – в середньому в світі цей показник перевищує 50%, а у державному секторі майже 70% [1]. Найчастіше ці проблеми пов’язані з нестачею або взагалі відсутністю повного та якісного управління ризиками.

Мета дослідження. Аналіз методів та механізмів управління ризиками проектів ІТ-галузі.

Результати дослідження. Розробка програмного забезпечення достатньо ризикований бізнес тому, що ІТ-проектам властива велика кількість факторів, які дуже швидко змінюються та впливають на кінцевий результат проекту [2]: вимоги користувачів; новітні технології; ринкова конкуренція; удосконалення стандартів; підвищення вимог до інформаційної безпеки.

PMBOK рекомендує керувати ризиками у 4 етапи:

1. Ідентифікація. Виявити ризики, які можуть перешкодити цілям проекту.

На практиці, як правило, технічні ризики в ІТ-проекті трапляються дуже часто, але їх простіше вирішити. Набагато складніше вирішувати таки ризики, як

«політичні ігри», «відсутність підтримки керівництва», «небажання, опір користувачів, підрядників», «недостатнє фінансування».

2. Аналіз. Завдання цього етапу полягає у визначенні найбільш небезпечних з ідентифікованих ризиків, тому що боротьба з усіма ризиками водночас неефективна та дорога.

3. Планування. Фактично, на цьому етапі саме відбувається управління проектом. Для кожного ризику зі списку критичних необхідно розробити стратегію боротьби з ним. Всього використовують три стратегії:

Transfer. Переносимо відповідальність за наслідки ризику на третю сторону (замовника, партнера, страхову компанію та ін.). Застосовувати цю стратегію є сенс, якщо самі ми не можемо вплинути на ризик і є на кого цю відповідальність перекласти.

Accept. Приймаємо відповідальність за наслідки ризику на себе, але нічого не робимо, залишаємо все як є. Застосовувати цей підхід є сенс тільки коли з ризиком ми вдіяти нічого не можемо, а робити трансфер на третю сторону невиправдано дорого.

Mitigate. Боремося з ризиком, беручи відповідальність за нього на себе. Для боротьби з ризиком добре мати кілька планів: основний, для того, щоб ризик подавити, і відхідний, на випадок якщо ризик все ж таки трапився і впливає на проект.

4. Моніторинг та контроль. Підтримувати план проекту й перелік ризиків в актуальному стані.

На практиці використовують декілька статистичних методів прогнозування ризиків:

1. Метод Buffer time у 30%. Просто додають 30% до загальної тривалості планових задач. Цей резерв використовують на покриття ризиків.

2. Метод Load Factor (або на скільки перемножити слова відповідального за визначення терміну). Величина коефіцієнту визначається на основі статистичних даних та залежить від складності й унікальності проекту.

3. Схема PERT розрахунок реального терміну:

$$Реальний\ термін = \frac{Оптимістичний\ термін + 4 \cdot Очікуваний\ термін + Песимістичний\ термін}{6}$$

Коефіцієнти в наведеній формулі (4 та 6) отримані ляхом аналізу статистики великої кількості проектів. Даний метод підходить тільки для дуже грубої прикидки можливого впливу ризиків.

4. Найчастіше в світовій практиці використовують метод Монте-Карло. Системи моделювання ризиків на базі Монте Карло більш точні, а також дозволяють задавати рівень ризику у проекті.

IT-компанії найчастіше страхують свої ризики і відповідальність в окремих договорах із замовником або через фінансові гарантії. Так звана «Угода про рівень послуг» (Service Level Agreement, SLA) використовується в проектах з підтримки і супроводу програмного забезпечення, а також у роботах, пов'язаних з аутсорсингом бізнес-процесів. SLA підхід для IT-послуг включає управління нестандартними ситуаціями, проблемами, змінами, релізами, рівнем сервісу [3].

У світовій практиці IT-компанії також користуються послугами страхових компаній та роблять ставки на страхування ризиків професійної відповідальності, щоб захистити себе від помилок і упущень при розробці та впровадженні IT-системи. Але в Україні такі страхові послуги не надаються.

Висновки. Управління ризиками та використання різноманітних механізмів не гарантує 100% успіху. Але зневажання моніторингу та технологій управління ризиками скоріш всього призведе до не виконання поставлених перед ним цілей.

Література

1. Слюсаренко А. Управление рисками в проектах внедрения информационных систем управления предприятием [Электронный ресурс] / А. Слюсаренко // CIO.– 2008.– № 7. – Режим доступа: http://www.topsbi.ru/default.asp?artID=1489

2. Березин В. Управление проектами в мире и Украине. Современные тенденции [Электронный ресурс] / В. Березин // Режим доступа: http://beleader.com.ua/stati/upravlenie-proektami/upravlenie-proektami-v-mire-i-ukraine-sovremennye-tendencii.html

3. Лебедовський В. Як IT-компанії в Україні страхують свої проекти [Електронний ресурс] / В. Лебедовський // Режим доступу: http://brit-mark.com/ua/press-centre/brit-mark-media/2013/kak-it-kompanii-v-ukraine-strahuyut-svoi-proektyi