

УДК 005.8:004.056.52

Крамський Сергій Олександрович

Кандидат технічних наук, старший викладач кафедри "Судноремонт"
Одеський національний морський університет, Одеса

**ЗАСТОСУВАННЯ КОМПЛЕКСНОЇ ОЦІНКИ РИЗИК-ОРІЄНТОВАНИХ ЗАСОБІВ
В УПРАВЛІННІ ІННОВАЦІЙНИМИ ІТ-ПРОЕКТАМИ**

***Анотація.** Розкрито особливості імплементації ризик-інструментів інноваційних проектів, загальні закономірності їх функціонування у технічній, соціальній сферах. Таким чином, аналіз ризику і безпеки може слугувати для формалізованої оцінки безпеки і методів ризик-менеджменту. У основі управління ризиком лежить методика порівняння витрат і отримуваних вигод від зниження ризиків. Проведено аналіз наявних проблем підбору персоналу, людських (трудова) ресурсів в компаніях, діяльність яких пов'язана з розробкою програмного забезпечення різного спрямування. Обґрунтовано доцільність синтезу ризик-орієнтованих засобів та виявлення інноваційних сфер ІТ-проектів, які можна отримати лише за умов гнучкого середовища ІТ-проектів. Набули розвитку комплексний підхід та обґрунтування імплементації ризик-орієнтованого підходу управління ІТ-проектами, а також методи інноваційних неоднорідних проектів.*

***Ключові слова:** ризик-менеджмент; ризик-орієнтовані засоби; контролінг; інноваційні ІТ-проекти*

Вступ

Контекстний формат управління проектами – галузь менеджменту, яка з кожним роком привертає все більше уваги, як бізнес-структур, так і органів публічного управління, які запроваджують принципи проектного менеджменту у роботу підприємств. Ефективне управління проектами дозволяє ІТ-організаціям правильно планувати, оптимізувати витрати часових, фінансових і людських ресурсів, але при цьому не відхилятися від запланованої якості кінцевого продукту проекту. Особливе місце відводиться інноваційним підходам, ідеям, методам, що з'явилися у динамічному оточенні, і можуть застосовуватися у сфері управління ризиками проектів.

Нині активно розвивається підхід до управління інноваційними проектами, що заснований на методології контролінгу ризиків для розробки інновацій у системних і комерційних компаніях. Отже, постала необхідність у системній інтеграції різних аспектів управління інноваційними ІТ-проектами у стартапах, аерокосмічній, військовій, морській та інших галузях. Проектний підхід, як основа управління ризиками, девіаціями, змінами, орієнтує будь-яку діяльність на проактивні, тобто з упередженням подій, засади управління системою "проект – проектна команда – технології – турбулентне оточення". Проектам у галузі ІТ властиві специфічні характеристики, в силу яких ефективне управління ризиками стає життєво важливим для їхнього успіху.

**Аналіз публікацій
та досліджень**

Еволюція технічних стандартів, так само як і інші чинники, може змусити, працюючи над ІТ-проектом групи, модифікувати прийняті рішення в середині проекту. З ними працюють люди, поведінка яких визначена правилами і вимогами. Зазвичай виокремлюють чотири підходи до аналізу і оцінки ризиків.

1. *Інженерний* – такий, що спирається на статистику, розрахунок частот, імовірнісний аналіз безпеки, побудову дерев небезпеки.

2. *Модельний* – заснований на побудові моделей дії шкідливих чинників на окрему людину, соціальні, професійні ІТ-групи і т.ін. Ці методи засновані на розрахунках, для яких не завжди є дані.

3. *Експертний* – коли вірогідність різних подій визначається на основі досвіду дослідних фахівців, тобто експертів.

4. *Соціологічний* – заснований на досвіді населення. Наведені методи відображають різні аспекти ризиків, тому за можливості застосовувати їх необхідно в комплексі.

Саме контролінг проектів забезпечує методичну та інструментальну базу для підтримки основних функцій менеджменту: планування, обліку, контролю та аналізу, а також оцінки ситуацій для прийняття правильних управлінських рішень. Останніми роками у зв'язку з безперервними конфліктами і протистоянням у багатьох "гарячих" точках, активізацією терористичних дій, війн, у тому числі гібридних, проблема визначення ризику загроз

для людей і природного середовища та їх мінімізації стала вельми актуальною [1; 2].

Різним аспектам ризику, методам його аналізу і оцінки, його застосування до природних явищ, технічних систем, діяльності людей присвячена величезна кількість публікацій С.Д. Бушуєва, С.В. Руденко, А.В. Шахова, І.О. Гордевої та інших наукових розробок, проектів, матеріалів семінарів і конференцій. Таким чином, створюються основи для формування загальної теорії ризиків у проектах, яка повинна охоплювати соціальні, політичні, економічні й інші аспекти цього поняття, питання методології визначення і оцінки ризиків. Аналізуються поняття "ризик", "управління ризиком", "ризик-менеджмент". Існує також значна кількість класифікацій ризиків і проектних у тому числі [3; 5; 7].

Проектні ризики розглядаються як можливість негативних наслідків для ІТ-проекту, при цьому не уточнюється ступінь негативного впливу на складну систему "проект". Для такої теорії може бути використана формалізована оцінка безпеки, стандарти ризик-менеджменту та комп'ютерне моделювання. При забезпеченні безпеки технічних систем ні теорія абсолютної надійності, ні імовірнісний підхід до аналізу ризиків не дозволяють отримати задовільні відповіді відносно можливих аварій і відмов, оскільки частенько "слабкою" ланкою системи є людина.

Мета статті

Мета статті – обґрунтування застосування комплексного підходу до аналізу ризиків ІТ-проектів на етапах створення проектних команд в управлінні інноваційними ІТ-проектами.

Виклад основного матеріалу дослідження

Виникає проблема комплексної оцінки ризику у соціальних системах управління ризиком. Як правило, підвищення рівня безпеки здійснюють в трьох напрямках: а) вдосконалення технічних систем і об'єктів; б) підготовка персоналу; в) попередження надзвичайних ситуацій. Для їх визначення необхідний спеціальний аналіз конкретних даних і умов. Знайти керівника ІТ-проекту, планувальника та інженера з управління ризиками, які мають достатню кваліфікацію і готові працювати на проекті, незважаючи на загальне скорочення кількості проектів, в сучасній економічній ситуації все ще досить складно. Шкода від ризику втрати ІТ-команди значна. Формування нової професійної команди ІТ-проекту у таких умовах вкрай важко.

Невизначеність, непередбачуваність і нестабільність зовнішнього середовища обумовлюють об'єктивний характер виникнення ризик-факторів, які ускладнюють процес адаптації

бізнес-структур до змін, що відбуваються. На першому етапі контролінгу інновацій необхідно вирішити завдання вибору варіанта реалізації проекту. Вибір між варіаціями очевидний, якщо один з варіантів кращий за інший за всіма показниками. У реальних ситуаціях вибору варіанти зазвичай непорівнянні – перший краще за одними показниками, другий – за іншими. Етапи контролінгу інновацій ІТ-проекту такі:

- оцінка можливості бути реалізованим проектом;
- інформаційна підтримка планування розробки інноваційного проекту;
- інформаційна підтримка контролю над здійсненням інноваційного проекту;
- інформаційна підтримка функції аналізу проекту.

На цій стадії контролеру проекту необхідно відповісти на питання: чи досягне комерційне підприємство поставлених перед ним цілей, якщо приступить до реалізації ІТ-проекту.

Таким чином, на першому етапі виникає завдання вибору варіанта реалізації проекту, що дозволяє досягти загальнофірмові, офісній цілі. Для вирішення цього завдання можна скористатися економетричними методами. Він може характеризуватися кількісними економічними показниками, такими, як витрати, надходження та інше; технічними показниками, що описують характеристики якості продукту, що розробляється; та якісними показниками, вираженими у вигляді термінів, наприклад, малий, середній, великий.

Як приклад таких показників можна назвати інноваційність проекту, відповідність ІТ-проекту стратегічним цілям компанії, вплив на репутацію офісу і т.ін. Доцільно виділити еталонний варіант реалізації інноваційного проекту і його характеристики. Характеристики підбираються саме таким чином, щоб проект був оптимальним з точки зору вимог, що висувуються до нього. Щоб порівняти варіації реалізації проекту з еталонним варіантом і вибрати з них кращий, можна застосувати методи, засновані на якісних і кількісних даних [6].

На другому етапі здійснюється розробка планово-організаційних заходів. Підготовлений план перевіряється на реалізованість, потім вирішуються питання, пов'язані з координацією учасників проекту, з організацією інформаційного потоку, з організацією робіт і призначенням відповідальних членів команди проекту.

На третьому етапі встановлюється час проведення контрольних заходів, пов'язаних з виконанням певних блоків робіт. Вибираються підконтрольні показники, що характеризують фінансовий і організаційний стан проекту. Встановлюються допустимі відхилення обраних

показників, перевищення яких може призвести до негативних наслідків. Проводиться облік показників, фіксація відхилень. Виявляються причини і винуватці цих відхилень.

На заключному четвертому етапі підрозділ контролінгу оцінює вплив виявлених відхилень на подальші кроки реалізації проекту. З'ясовує, як виявлені відхилення вплинули на основні керовані параметри проекту. По закінченні циклу контролер проекту готує звіт з пропозицією варіантів вирішення виниклих проблем та зміною планових величин на наступний період.

Потрібна сучасна якісна інноваційна підготовка компетентних ІТ-фахівців, менеджерів обізнаних у питаннях ефективного застосування до визначення рівня ІТ-ризиків, їхньої кількісної оцінки для подальшої мінімізації та усунення на базі ризик-орієнтованого підходу. Проектну ІТ-команду слід починати формувати до етапів планування і виконання проекту. Незалежно від детального змісту ІТ-проекту пошуком людей, на основні ролі в проектній команді, необхідно займатися якомога раніше. На етапі формування ІТ-команди важливо усвідомлювати, що існує стандартний ризик просто не знайти персонал, який володіє професійними знаннями і досвідом. Але, навіть зумівши на початкових етапах проекту залучити досвідчених людей в ІТ-команду, пізніше можна їх втратити. Підхід до оцінки ризиків, пов'язаних з персоналом, повинен бути таким же, як і підхід до оцінки інших (виробничих, фінансових) ризиків проекту. У цьому комплементарному процесі, керівнику ІТ-проекту повинні допомагати інженер з управління ризиками і фахівець з управління персоналом.

Методи для роботи з HR-ризиками практично повністю повторюють стандартні антиризикові заходи з управління ризиками проектів. Розглянемо найбільш імовірні й значні ризики, пов'язані з персоналом проектної команди. Якщо після початку ІТ-проекту виникло ще кілька подібних проектів у конкурентів, вони цілком можуть зайнятися цілеспрямованим переманюванням ключових гравців проектної команди. Для мінімізації збитку від такої події необхідно заздалегідь продумати, яким чином можна компенсувати 100% втрату ІТ-команди, і заздалегідь визначити джерела її поповнення персоналом: кого, на які ролі і на яких умовах можна оперативно залучити. Якщо є можливість – підготувати ІТ-команду дублерів, нехай навіть не з кращих гравців, а учнів [7].

Основні ризик-фактори в управлінні ІТ-проектами пов'язані з необхідністю підвищення кваліфікації і розвитком членів проектної ІТ-команди під час виконання проекту, як правило, не враховуються на етапі планування. Наприклад, якщо відомо, що команда ІТ-проекту молода і не володіє

100% компетенцією або достатнім досвідом, то з самого початку потрібно розрахувати фінансові та часові витрати і ризики на навчання і розвиток персоналу, а також обговорити їх разом із замовником і спонсором проекту. Зрозуміло, кваліфікаційні ризики багаторазово зростають при реалізації інноваційних проектів. Даний фактор призводить до збільшення ризиків демотивації персоналу, зниження його лояльності по відношенню до проекту або до розвалу ІТ-команди. Незважаючи на те, що ІТ-проект суттєво змінюється у часі, важливо закріпити ключові домовленості: те, що повинно залишитися непорушним і незмінним, наприклад, принципи прийняття управлінських рішень, фінансові та організаційні ролі, ієрархічна модель проекту, його фінансові та часові рамки. В результаті можуть змінюватися вимоги користувачів, новий інструментарій та ноу-хау. При цьому зростають загрози для інформаційної безпеки, плінність кадрів – все це додаткові фактори, здатні спричинити за собою зміни в ІТ-проект і змусити проектну групу приймати рішення в умовах невизначеності ризику.

Оцінка ризиків у сфері ІТ-обслуговування передбачає виділення факторів, що являють загрозу конкурентоспроможності підприємства, її фінансового стану і результатів діяльності підприємства. Деякі фахівці навіть виділяють їх в окремий вид ризику – ІТ-ризики. Однак, оскільки ми розглядаємо джерела виникнення ризиків на підприємстві, чия основна виробнича діяльність і є створення ІТ-продуктів, тому вважається недоцільним виокремлення ІТ як окремого виду ризику в даному дослідженні, а специфіка діяльності підприємства, на погляд автора, є джерелом виникнення ряду ризик-утворюючих факторів, відмінних для кожної окремо взятої галузі і сфери діяльності та пов'язаних з успішністю вирішення бізнес-завдань [8]. У таблиці вказані шкали для оцінювання імовірності виникнення ризиків ІТ-проекту та оцінювання їх наслідків.

Таблиця – Шкала для оцінювання імовірності виникнення ризиків

Оцінка (бал)	Імовірність ІТ ризиків
0,01 – 0,24	Дуже низька (ризик без різких змін не виявиться)
0,25 – 0,49	Низька (ризик, скоріше, не виявиться)
0,5	Імовірності появи та не появи однакові
0,51- 0,75	Висока (ризик, скоріше, виявиться)
0,76 – 0,99	Дуже висока (ризик без різких змін виявиться)

В останні роки в діяльності Міжнародної морської організації, у класифікаційних товариствах і великих судноплавних компаній почав впроваджуватись методичний підхід – формалізована оцінка безпеки (Formal Safety Assessment – FSA) [4]. Формалізована оцінка безпеки створює основу для цілеспрямованого управління ризиками. Даний підхід, автором пропонується застосовувати до конкретних проєктів, а також в методології проєктно-орієнтованого управління. Оскільки формалізована оцінка безпеки охоплює проєктні, ремонтні, експлуатаційні параметри конкретних проєктів і дозволяє отримувати інформацію про ризики, а також варіанти управління ними і пов'язаними з цим витратами у проєкті. Таким чином, формалізована оцінка безпеки – це підхід, який заснований на оцінці ризику виникнення небажаної ситуації і спрямований на виявлення небезпек до того, як вони викличуть аварійну ситуацію. За відсутності дослідних даних, єдиним шляхом вирішення проблеми прийняття оптимальних рішень є вживання імовірнісного аналізу, який дозволяє логічно визначити ризики і розробити шляхи їх зменшення.

Саме концепція та методологія ризик-орієнтованого підходу є тим підґрунтям менеджменту, на підставі якого можуть і мають здійснюватися адекватні кількісні оцінки небезпек, що дозволяє:

- зіставляти альтернативні ІТ-проєкти, побудови об'єктів і систем;

- виявляти фактори, що відіграють істотну роль у дотриманні безпеки конкретного ІТ-проєкту, чи будь-якого джерела загрози;

- визначати оптимальну кількість витрат для управління величиною ризику і зменшенням існуючого рівня небезпеки соціально-технічних систем до прийнятного рівня інноваційного менеджменту із соціальної та економічної точок зору;

- створювати базу даних експертних систем для підтримки осіб, які ухвалюють рішення, відпрацьовують нормативи та експортують конкретні ІТ-проєкти;

- впливати на суспільну думку, орієнтуючи її на об'єктивні, а не на емоційні чи популістські оцінки експертів [9].

Міжнародним суспільством під супроводом Всесвітньої торговельної організації (WTO) висунуто відповідні вимоги до застосування методів імовірнісної оцінки ризиків під час прийняття рішень, спрямованих на зниження потенційної небезпеки для людей, об'єктів, технологій, процесів при виникненні надзвичайних ситуацій. Вони

базуються на конвенціях, стандартах і рекомендаціях, розроблених під керівництвом секретаріатів Міжнародної конвенції захисту рослин (IPPC), Міжнародної морської організації (ІМО), Міжнародної організації праці (ІЛО) тощо за сприяння регіональних організацій, які діють під егідою зазначених структур. Відповідність резолюціям та вимогам WTO, ІМО, ІЛО, IPPC при застосуванні методів ймовірнісної оцінки ризик менеджменту визначається за такими критеріями:

- 1) наявність наукової обґрунтованості, тобто використання найбільш надійних і повних вихідних даних для проведення оцінок ризику. Вказане має здійснюватися через застосування комплексного підходу, що включає детальне вивчення предмета дослідження, оцінку його можливого стану у звичайних умовах і небезпечних ситуаціях, а також своєчасне виявлення невизначеності інформації;

- 2) логічність та доступність оцінки ризиків, які враховують її актуальність, раціональність, обґрунтованість та об'єктивність;

- 3) гнучкість результатів оцінки ризик-менеджменту [10]. Наприклад, відомості про зростання кількості небезпечних подій мусять бути гнучкими за їхньою корисністю для широкого діапазону різноманітних ситуацій, а сам процес оцінки ризику, при його відповідності встановленим вимогам, динамічним і здатним до оперативного врахування нових вихідних даних, технологій і методів оцінки;

- 4) послідовність, яку пропонується сприймати для оцінки ризику, різних ситуацій з метою розповсюдження отриманих результатів на інші аналогічні події. Можливі три варіанти прийнятих рішень: ризик приймається цілком, частково або не приймається [11].

Сутність їх полягає в розвитку проєктно-орієнтованих моделей і методів для підвищення ефективності управління латентними мультиплікативними ризиками в ІТ-проєктах.

Подальшого розвитку набула модель накопичення ІТ-ризикових подій, що відбулися, яка полягає у врахуванні статичних та динамічних параметрів ризикових подій, що дозволило використовувати цю модель для оцінки імовірностей ризиків для ІТ-проєкту.

Комбінована модель прогнозування проєктних ризиків, які істотно впливають на імовірність ризику, дозволила запропонувати систему заходів для управління змішаними ризиками.

Отже, запропонована модель взаємодії проєктних “потенціалів” та “потоків”, наприклад, фінансових, яка заснована на аналогії між проєктними явищами і будується на основі

принципів взаємності, еквівалентності, суперпозиції і симетрії, що дало змогу сформулювати чотири твердження про взаємодії ризикових подій в окремих областях менеджменту та на їх підставі запропонувати шляхи спрощення моделей та зменшення об'єму обчислень під час управління проектами у IT-сфері.

Також запропонована дискретна когнітивна модель 3D-вимірної системи проєктної діяльності та побудований на її основі метод оптимізації фінансових потоків при компенсації ризикових подій за допомогою тензорного аналізу стану проєкту. Це дозволило запропонувати систему підтримки прийняття рішень при управлінні мультиплікативними ризиками в процесах IT-індустрії. Даний елемент має одночасно об'єднувати всі стани управління ризиком, а також стадії його оцінки до єдиного процесу ухвалення рішення, отже до єдиної концепції ризиків [12].

Заключним етапом управління ризиком є моніторинг і коригування результатів реалізації обраної стратегії з урахуванням отриманої інформації.

Контролінг полягає в отриманні інформації про збитки, що відбулися, та вжиті заходи щодо їхньої мінімізації. Він може впливати на виявлення нових ризик-орієнтованих обставин, які змінюють рівень ризику, спостереження за ефективністю роботи IT-систем, дотримання регламентів тощо. Для успішного проведення заходів з аналізу ризиків на виробництві кожен кваліфікований робітник має уявляти мету, завдання і етапи ризик-орієнтованого підходу. Тому такий процес при розробці стратегії управління ризиком має містити такі процедури:

- експертизу існуючих ризиків для здоров'я людей, визначення першочергових ризиків, якими необхідно управляти або зменшувати, розробку стратегій управління сумарним ризиком для населення та навколишнього середовища;

- ідентифікацію джерел ризику для здоров'я населення та стану довкілля з узагальненого аналізу витрат та вигід.

Вдосконалення цієї процедури перспективне за умови підсилення значення ризик-орієнтованого підходу як вихідної інстанції, що створює систему оцінок й розподілу ризиків і використовує її в системі “людина – IT – машина”.

Висновки

Управління IT-проєктом розробки програмного забезпечення має бути спрямовано на боротьбу з ризиками (порушення термінів, перевитрачання ресурсів, розробка не того продукту). Головні причини провалу IT-проєктів:

- вимоги замовника відсутні, часто змінюються;

- відсутність необхідних ресурсів і досвіду;
- відсутність робочої взаємодії з замовником;
- неповнота планування ("забуті роботи");
- помилки в оцінках трудовитрат.

Отже, підготовка майбутніх кваліфікованих менеджерів, робітників інноваційних IT-компаній, обізнаних у питаннях повсякденної безпечної експлуатації і стійкого функціонування в умовах надзвичайних подій, є одним із головних завдань IT-системи, з урахуванням шляху України до сталого розвитку.

Список літератури

1. *A Guide to the Project Management Body of Knowledge (PMBOK. Guide), 5th Edition, PMI, Inc., 14 Campus Boulevard, Newton Square, Pennsylvania, USA, 2013. – 587 p. DOI:org/10.1002/pmj.21345.*
2. *PRINCE2 For Beginners, 4th from introduction to passing your foundation exam, Routledge Ltd, 2015. – 294 p. DOI:org/10.1007/1-84628-262-4_11.*
3. Бушуев С.Д., Бушуева Н.С., Бабаев И.А. *Креативные технологии управления проектами и программами: монография.* – К.: Саммит-Книга, 2010. – 768 с.
4. *Guidelines for Formal Safety Assessment (FSA) for use in the IMO Rule-making process. MSC/Circ.1023, MEPC/Circ.392 – London, 2002.- 54 p.*
5. Волошин А.О. *Методологічні основи проектування систем безпеки об'єктів водного транспорту. [Текст] / А.О. Волошин, С.В. Руденко, А.В. Шахов // Науково-виробничий журнал Проблеми техніки. О.: ОНМУ – 2011. – № 3. – С. 96-104.*
6. Крамський С.О. *Концепція контролінга та методу нечітких множин для оцінки інноваційних проєктів на комерційних підприємствах / С.О. Крамський // "Міжнародне співробітництво для локального розвитку"- Ч. 2. – Тези доповідей II міжнар. наук.-практ. конф. – В.: "Нілан-ЛТД", К.: ГО "Слобожанщина", 2016. – С. 7-10 – 146 с.*
7. Гордєєва І.О. *Формування комплементарної команди для управління ризиками інноваційних проєктів. – дис. канд. техн. наук: 05.13.22 / Гордєєва Інна Олександрівна. – КНУБА. – К.: 2010 – 186 с.*
8. Муравецький С.А. *Планування процесів забезпечення якості у великих та географічно розподілених гібридних IT-проєктах [Текст] / С.А. Муравецький, С.О. Крамський // Вісник НТУ «ХПІ». – 2016. – № 1. – С. 106-109. DOI:org/10.20998/2413-3000.2016.1173.21.*

9. *A guide to the Scrum Body of Knowledge (SBOK™ Guide)*, SCRUMstudy™, a brand of VMEdu, Inc., 410 N 44th Street, Phoenix, Arizona 85008 USA, 2013. – 340 p.

10. ISO IEC 31010:2009 Risk management–Risk assessment techniques "ISO IEC 31010:2009 "Risk management". – 176 c. DOI:org/10.3403/30183975.

11. Boyko V. *Concept implementation of decision support software for the risk management of complex technical system [Текст] / Boyko V., Rudnichenko N., Kramskoy S., Hrechukha Y., Shibaeva N. // XI Int. Sci.-Techn. Conf. "Workshop intelligent systems and computing". Springer. Lviv, 2016, 172017. pp. 255-269. DOI:org/10.1007/978-3-319-45991-2_17.*

12. Щедров І.М. Підтримка прийняття рішень в управлінні латентними мультиплікативними ризиками проектів будівництва мегаспоруд. – автореф. дис. канд. техн. наук: 05.13.22 /Щедров Ігор Миколайович. – ОНПУ. – О.: 2015- 20 с.

13. Кулалаєва Н.В. Обґрунтування імплементації ризик-орієнтованого підходу до системи освіти як умови сталого розвитку [Текст] / Н.В. Кулалаєва // Вісник Професійна освіта: проблеми і перспективи. – К.: ІПТО НАПН України, 2015. – №. 8. – С. 30-34.

Стаття надійшла до редколегії 27.12.2016

Рецензент: д-р техн. наук, проф. В.В. Вичужанін, завідувач кафедри інформаційних технологій Одеського національного морського університету, Одеса.

Крамской Сергей Александрович

Кандидат технических наук, старший преподаватель кафедры “Судоремонт”

Одесский национальный морской университет, Одесса

ПРИМЕНЕНИЕ КОМПЛЕКСНОЙ ОЦЕНКИ РИСК-ОРИЕНТИРОВАННЫХ СРЕДСТВ В УПРАВЛЕНИИ ИННОВАЦИОННЫМИ ИТ-ПРОЕКТАМИ

Аннотация. Раскрыты особенности имплементации риск-инструментов инновационных проектов, общице закономерности их функционирования в технической, социальной сферах. Таким образом, анализ риска и безопасности может служить для формализованной оценки безопасности и методов риск-менеджмента. В основе управления риском лежит методика сравнения затрат и получаемых выгод от снижения рисков. Проведен анализ существующих проблем подбора персонала, человеческих (трудовых) ресурсов в компаниях, деятельность которых связана с разработкой программного обеспечения различного направления. Обоснован синтез современных риск-ориентированных средств и выявление инновационных сфер ИТ-проектов, которые можно получить только при условиях гибкой среды ИТ-проектов. Получили развитие комплексный подход и обоснование имплементации риск-ориентированного подхода управления ИТ-проектами, а также методы инновационных неоднородных проектов.

Ключевые слова: *риск-менеджмент; риск-ориентированные средства; контроллинг; инновационные ИТ-проекты*

Kramskiy Sergey

PhD, Senior lecturer at the department ship repair

Odessa national maritime university, Odessa

AN INTEGRATED RISK-ORIENTED ASSESSMENT TOOL IN THE MANAGEMENT OF INNOVATIVE IT-PROJECTS

Abstract. In the article were underlined the features of the implementation of the risk of innovative projects tools, the general laws of their functioning in a technical and social spheres. Thus, risk and safety analysis can be used for formal safety assessment methods and risk management. The risk management is based on the technique of comparing costs and benefit from risk reduction. One of the main causes and implementing the concept of controlling deviations risks for developing innovation in the system and commercial enterprises. Substantiated synthesis of modern risk-oriented funds and the identification of innovation in IT-projects that can only be obtained with a flexible IT-project. Formal safety assessment this method is relatively new to the innovative industry, has long been known and used in many types of manufacturing, in the field industrial risk management – systems for the analysis and selection of priority actions, assess their impact, benefits and costs. The analysis of existing problems of recruitment, human resources in companies whose activities are related to software development in different directions. It covers the design, maintenance, operational parameters specific projects and provides information about the risks and management options. This approach is based on an assessment of the risk of unwanted situations and seeks to identify hazards before they cause an accident. Definition of control steps is the selection of measures that help project team to reduce or eliminate the appropriate level of risk.

Keywords: *risk management; risk-oriented instrument; controlling; innovative IT-projects*

References

1. *A Guide to the Project Management Body of Knowledge "PMBOK. Guide". (2013). 5th Edition, PMI, Inc., 14 Campus Boulevard, Newton Square, Pennsylvania, USA, 587. DOI:org/10.1002/pmj.21345.*
2. *PRINCE2 For Beginners, 4th from introduction to passing your foundation exam. (2015). Routledge Ltd, 294. DOI:org/10.1007/1-84628-262-4_11.*
3. *Bushuev, S.D., Bushueva, N.S., Babayev, I.A. (2010). Creativnye tehnologiyi upravleniya proektami i programami: monografiya. Kiev: Summit-Kniga, 768.*
4. *Guidelines for Formal Safety Assessment (FSA) for use in the IMO Rule-making process. (2002). MSC/Circ.1023, MEPC/Circ.392. London, 54.*
5. *Voloshin, A.O., Rudenko, S.V., Shakhov, A.V. (2011). Methodological design principles of safety of water transport // Scientific Production Journal "Problems of technology":- ONMU.- (3). – 96-104.*
6. *Krams'kiy, S.O. (2016). Controlling concept and method of fuzzy sets to assess innovative projects to commercial enterprises // Theses of a report II Intern. nauk. and practical. Conf. " International cooperation for local development" – Vinnitsya: "Nilan-LTD" Kramators'k: GO "Slobozhanshina" – p2. – 7-10 – 146 p.*
7. *Gordeeva, I.A. (2010). Forming teams for complementary risk management innovation projects: Thesis Ph.D.: 05.13.22 // Gordeeva Inna Oleksandrivna. – Kiev: – KNUBA. – 186 p.*
8. *Muravetskiy, S.A., Krams'kiy, S.O. (2016). Planning quality assurance processes in large and geographically dispersed IT-projects hibrydnyh // Visnyk NTU "KhPI". Kharkov, NTU "KhPI" – (1). – 106–109. DOI:org/10.20998/2413-3000.2016.1173.21.*
9. *A guide to the Scrum Body of Knowledge "SBOK™ Guide" (2013). SCRUMstudy™, a brand of VMEdU, Inc., 410 N 44th Street, Phoenix, Arizona 85008. USA, 340.*
10. *ISO IEC 31010. Risk management-Risk assessment techniques. (2009). ISO IEC 31010: 2009 "Risk management" – 176. DOI:org/10.3403/30183975.*
11. *Boyko, V., Rudnichenko, N., Kramskoy, S., Hrechukha, Y., Shibaeva, N. (2016). Concept implementation of decision support software for the risk management of complex technical system // XI Int. Sci.-Techn. Conf. "Workshop intelligent systems and computing". Lviv, Springer., (17)2017, 255-269. DOI:org/10.1007/978-3-319-45991-2_17.*
12. *Shedrov, I.M. (2015). Support for decision-making in the management of latent multiplicative risk construction projects Big, Bigger, Biggest: Abstract Thesis Ph.D.: 05.13.22 // Shedrov Igor Mykolayovych. – Odessa. – ONPU, 20 p.*
13. *Kulalaeva, N.V. (2015). Justification implementing a risk-based approach to education as a condition for sustainable development. Bulletin of Vocational Education: Problems and Prospects. – Kyiv: IPTO NAPN Ukrainy, (8), 30-34.*

Посилання на публікацію

- APA *Kramskiy, Sergey. (2017). An integrated risk-oriented assessment tool in the management of innovative IT-projects. Management of Development of Complex Systems, 29, 71 – 77.*
- ГОСТ *Крамський, С.О. Застосування комплексної оцінки ризик-орієнтованих засобів в управлінні інноваційними IT-проектами [Текст] / С.О. Крамський // Управління розвитком складних систем. – 2017. – № 29. – С. 71 – 77.*