УДК 381:006.1

# АЛГОРИТМ ОЦІНКИ ТИПОВИХ ТЕХНІЧНИХ РИЗИКІВ ЗА ВИМОГАМИ МІЖНАРОДНОГО СТАНДАРТУ ISO 31000:2009

Г.І. Хімічева, д.т.н, проф.
*Київський національний університет технологій та дизайну*
К.С. Безпалий, магістр
*Київський національний університет технологій та дизайну*

Ключові слова: алгоритм, ризики, технічні рішення, міжнародний стандарт ISO 31000:2009.

Сьогодні найбільш ризикованою та такою, що стрімко розвивається в сучасних умовах, є галузь будівництва. Проектно-архітектурні установи реалізують складні проекти, для яких характерною є поява ризиків, спричинених зовнішніми та внутрішніми факторами. Застосування міжнародних стандартів при оцінці ризиків надає можливість керівникам проектів зробити управління ризиками ефективним та коректним [1].

Одним із шляхів подолання ризиків є впровадження міжнародного стандарту ISO 31000:2009 «Ризик-менеджмент. Принципи та рекомендації» [2]. Цей документ рекомендує підприємствам розвивати, впроваджувати та постійно поліпшувати систему, метою якої є інтеграція процесу з управління ризиками з керівництвом, стратегією і плануванням, управлінням, процесами звітності, політикою, цінностями і культурою.
Незважаючи на існуючі теоретичні та практичні напрацювання у сфері управління ризиком, його ефективному використанню на українських підприємствах заважає ряд обставин. По-перше, стандарти, розроблені закордонними організаціями, призначені для застосування, в основному у великих компаніях, досвідчені фахівці яких пройшли відповідну підготовку та володіють сучасними методами ризик-менеджменту. По-друге, розробники стандартів, у більшості випадків, прямо вказують на те, що «ідентифікація ризиків організації, як правило, проводиться незалежними консультантами». Тому вітчизняні підприємства потребують певної адаптації змісту цих документів до їх діяльності. При цьому успішна реалізація проектів потребує наукових розробок щодо вдосконалення методів, прийомів, стандартів управління ризиками, які б опиралися на міжнародний досвід та враховували специфіку цієї галузі в Україні.

Для вирішення даної задачі авторами в ході досліджень був запропонований спеціальний алгоритм, який включає в себе 7 етапів.

На першому етапі відбуваються комунікації та консультації з усіма зацікавленими сторонами. Цей процес є важливим, оскільки керівники і менеджери висловлюють судження, які засновані на їх власному сприйнятті ризику. Погляди сторін ідентифікуються, документуються і приймаються до уваги при прийнятті рішень.

На другому етапі визначають зовнішні та внутрішні параметри, які впливають на виникнення і управління ризиками проекту. Процедура визначення складається із обґрунтування ресурсів та впорядкування діяльності керівників і менеджерів проекту.

Третій етап алгоритму полягає в ідентифікації, тобто визначенні джерел та сфер впливу ризиків. Результатом даного етапу є перелік факторів, які можуть перешкоджати досягненню поставлених цілей.

На четвертому етапі керівники і менеджери проекту повинні зрозуміти кожний ризик, його наслідки та ймовірність їх виникнення. Даний етап передбачає визначення типу ризику, доступної інформації і мети результату його обробки.

П'ятий етап передбачає визначення ступеню ризику, тобто дозволяє виявити найбільш загрозливі для досягнення цілей проекту ризики. Результатом є прийняття рішення щодо розробки організаційно-технічних заходів стосовно їх подолання.

Шостий етап включає обробку однієї або декількох позицій модифікації ризиків і порядок їх застосування. Обробка ризику являється циклічним процесом, який починається з оцінки обробки ризику і закінчується оцінкою ефективності цієї обробки.

Сьомий етап являє собою моніторинг та аналіз всіх аспектів процесу ризик-менеджменту з метою гарантії того, що методи управління ефективні і достатні як при розробці, так і при їх застосуванні. Дані процеси супроводжуються виявленням змін у внутрішньому та зовнішньому контекстах, включаючи зміни в критеріях ризику. Результати моніторингу і аналізу мають бути представлені зацікавленим сторонам і використані для аналізу концепції ризик-менеджменту. При цьому особливу увагу слід приділяти інформаційним ризикам, які загрожують забезпеченню конфіденційності, цілісності та доступності інформації. Для їх зменшення доцільно застосовувати міжнародний стандарт ISO/IEC 27001:2005 «Системи менеджменту інформаційної безпеки» [3].

Таким чином, застосування вищенаведеного алгоритму оцінки типових технічних ризиків за вимогами міжнародного стандарту ISO 31000:2009 дозволяє підприємствам своєчасно передбачати і виявляти потенційні ризики та розробляти організаційно-технічні заходи по їх попередженню і запобіганню.

Список використаних джерел

1. Хімічева Г. І. Застосування стандартів ISO серії 31000 при оцінці ризиків архітектурних робіт / Г.І. Хімічева, М. В. Шкура // Східно-Європейський журнал передових технологій. – 2012. – № 3/3 (57).

2. Risk management – Principles and guidelines: IEC/ISO 31000:2009. — [Електронний ресурс]. – Режим доступу: https://www.iso.org/iso-31000-risk-management.html

3. Системи менеджменту інформаційної безпеки. Вимоги: ISO/IEC 27001:2005 [Електронний ресурс]. – Режим доступу: http://rutracker.org/forum/viewtopic.php?t=1404852