УДК 004.021:005.334
DOI https://doi.org/10.32689/maup.it.2025.2.9

Юрій КІШ
аспірант кафедри інформаційних управляючих систем та технологій,
ДВНЗ «Ужгородський національний університет»,
yurii.kish@uzhnu.edu.ua
***ORCID:** 0009-0000-6167-0129*

Ігор ЛЯХ
доктор технічних наук,
професор кафедри інформатики та фізико-математичних дисциплін,
ДВНЗ «Ужгородський національний університет»,
igor.lyah@uzhnu.edu.ua
***ORCID:** 0000-0001-5417-9403*

ЕВОЛЮЦІЯ ПОНЯТЬ РИЗИКУ ТА ЇХ ВЗАЄМОЗВ'ЯЗОК ІЗ ЗАБЕЗПЕЧЕННЯМ ЯКОСТІ ІТ-ПРОДУКТІВ

***Анотація. Метою дослідження** є виявлення взаємозв'язків між ключовими категоріями ризиків у розробці ІТ-продуктів та показниками їх якості, з подальшою розробкою узагальненої класифікації ризиків і демонстрацією кількісного впливу на метрики програмної якості. У сучасних умовах цифрової трансформації та зростаючої складності інформаційних систем класичні підходи до управління ризиками втрачають ефективність через обмежену здатність враховувати динамічні взаємозалежності між факторами ризику, а також через фрагментарність аналізу окремих типів загроз. У зв'язку з цим дослідження зосереджене на структурному аналізі технічних, організаційних і зовнішніх ризиків у проєктах створення ПЗ, з використанням даних останніх емпіричних і прикладних публікацій.*

***Методологія** дослідження базується на системному підході з використанням контент-аналізу наукових джерел, формалізації типології ризиків та моделювання їх впливу на якість ІТ-продукту. Для обґрунтування впливу категорій ризиків на ключові характеристики ПЗ (надійність, підтримуваність, продуктивність тощо) застосовано порівняльний аналіз результатів, отриманих із рецензованих джерел. Окрему увагу приділено моделюванню ризикових взаємодій, мультиагентному підходу, машинному навчанню для прогнозування системних ризиків та автоматизованим засобам оцінювання змін якості у циклі оновлень.*

***Наукова новизна** полягає в пропозиції уніфікованої трикомпонентної класифікації ризиків (технічні, організаційні, зовнішні) як основи для узагальнення та порівняння сучасних підходів до управління ризиками в ІТ-проєктах. На відміну від існуючих підходів, запропонована класифікація дозволяє інтегрувати як кількісні, так і якісні оцінки, а також відображає міжкатегоріальні взаємозв'язки у складних інженерних середовищах. Додатково надано формалізований опис методу побудови таблиці порівняльного впливу ризиків, що базується на трансформації даних з емпіричних досліджень у відсоткові метрики впливу на якість.*

У результаті проведеного аналізу підтверджено, що технічні ризики, пов'язані з архітектурним боргом, дублікацією коду та нестабільністю змін, чинять істотний вплив на структурну та експлуатаційну якість ПЗ. Організаційні ризики проявляються у вигляді поганої комунікації, неефективного лідерства та нестабільного управління. Зовнішні ризики зумовлені впливом регуляторного середовища, ринкових коливань і зовнішньої політики. Запропонований підхід дозволяє сформувати комплексне бачення структури ризиків та їхнього управління як невід'ємної складової забезпечення якості ІТ-продуктів у повному життєвому циклі.

***Ключові слова:** ризик, якість програмного забезпечення, класифікація ризиків, технічні ризики, організаційні ризики, зовнішні ризики, управління ІТ-проєктами.*

Yurii KISH, Ihor LIAKH. EVOLUTION OF RISK CONCEPTS AND THEIR RELATIONSHIP TO IT PRODUCT QUALITY ASSURANCE

***Abstract. The purpose** of the study is to identify the relationships between key risk categories in the development of IT products and their quality indicators, with the subsequent development of a generalized risk classification and demonstration of a quantitative impact on software quality metrics. In today's conditions of digital transformation and the increasing complexity of information systems, classical approaches to risk management are losing their effectiveness due to the limited ability to take into account the dynamic interdependencies between risk factors, as well as due to the fragmentation of the analysis of certain types of threats. In this regard, the study focuses on the structural analysis of technical, organizational, and external risks in software development projects, using data from the latest empirical and applied publications.*

***The research methodology** is based on a systematic approach using content analysis of scientific sources, formalization of the typology of risks and modeling of their impact on the quality of the IT product. To substantiate the impact of risk categories on the key characteristics of software (reliability, maintainability, performance, etc.), a comparative analysis of the results obtained from peer-reviewed sources was used. Special attention is paid to risk interaction modeling, a multi-agent approach, machine learning for predicting systemic risks, and automated tools for assessing quality changes in the update cycle.*

The scientific novelty *lies in the proposal of a unified three-component classification of risks (technical, organizational, external) as a basis for generalizing and comparing modern approaches to risk management in IT projects. In contrast to existing approaches, the proposed classification allows for the integration of both quantitative and qualitative assessments, and also reflects intercategorical relationships in complex engineering environments. Additionally, a formalized description of the method of constructing a table of comparative impact of risks, based on the transformation of data from empirical studies into percentage metrics of impact on quality, is provided.*

As a result of the analysis, it was confirmed that technical risks associated with architectural debt, code duplication and instability of changes have a significant impact on the structural and operational quality of the software. Organizational risks manifest themselves in the form of poor communication, ineffective leadership and unstable management. External risks are caused by the influence of the regulatory environment, market fluctuations and foreign policy. The proposed approach allows us to form a comprehensive vision of the structure of risks and their management as an integral part of ensuring the quality of IT products in the full life cycle.

Key words: *risk, software quality, risk classification, technical risks, organizational risks, external risks, IT project management.*

Постановка проблеми. У сучасному цифровому середовищі інформаційні технології стали основою функціонування не лише технічних систем, а й соціально-економічних процесів, що зумовлює зростання вимог до якості програмних продуктів. Зі зростанням ск7пладності архітектур, динаміки вимог користувачів, гнучкості життєвого циклу розробки та інтенсивної інтеграції інтелектуальних механізмів (ML, DevOps, автоматизація тестування тощо) якість ІТ-продукту дедалі більше залежить від ефективного виявлення, оцінки й пом'якшення ризиків. Цей зв'язок між якістю та ризиками є не лише операційним, а стратегічним: управління ризиками виступає фундаментальною передумовою якості у складних, відкритих, адаптивних системах.

Загальновизнано, що ризик у сфері розробки програмного забезпечення має багатовимірну природу – він охоплює технічні аспекти (наприклад, застарілість архітектури або коду), організаційні (неузгодженість процесів, кадрові коливання), зовнішні (економічні, геополітичні чинники), а також взаємодію цих компонентів. Як показано у роботі Olayinka et al. [9], ризики безпеки вимагають не лише лінійної оцінки, а й гнучких інтелектуальних систем – таких як нейро-нечіткі моделі – які здатні адаптуватися до мінливого контексту, що підкреслює відхід від класичних, статичних підходів. Аналогічно, дослідження Dewi та Dharmawan [10] акцентують на необхідності включення пропорції ризику у моделі оцінки зусиль під час розробки, що демонструє глибоку вбудованість ризику у ключові метрики проєктного планування.

Наукова й практична важливість проблематики управління ризиками в ІТ-проєктах зумовлена тим, що невраховані або недооцінені ризики прямо призводять до зниження продуктивності, якості та життєздатності програмного продукту. У цьому контексті ризик виступає не лише як загроза, а як системна змінна, що модулює рівень відповідності кінцевого продукту очікуванням користувачів і стандартам якості. Згідно з дослідженням Gustavsson et al. [14], процесна заборгованість (process debt) – акумульовані відхилення у процесах – має сильний негативний вплив на задоволеність розробників, що опосередковано впливає на якість через зниження когнітивної стійкості команд.

Водночас, класичні підходи до ризик-менеджменту, зокрема стандартизовані методики з управління ризиками (PMBOK, ISO 31000), мають обмежену придатність до ІТ-середовища. Їх лінійність, надмірна декларативність та нечутливість до динаміки розвитку програмного забезпечення знижують їх ефективність у практиці. Як вказують Lesum et al. [12], саме адаптивне проектне управління, побудоване на принципах гнучкого лідерства, дозволяє підвищити здатність команди до раннього виявлення ризиків і своєчасної реакції на них, зменшуючи коливання у якості випусків. У свою чергу, Moussa et al. [1] демонструють доцільність використання алгоритмів машинного навчання для виявлення системних ризиків в інфраструктурних ІТ-проєктах, що посилює потенціал предиктивного аналізу в управлінні якістю.

Сучасні дослідження вказують на потребу інтегрованого підходу, що поєднує моделювання ризиків, їх міжвзаємозалежність і вплив на якість ПЗ. Наприклад, Guan et al. [6] запропонували динамічну модель мережевої взаємозалежності ризиків, яка дозволяє відстежувати каскадні ефекти протягом життєвого циклу проєкту. Saiz et al. [8] доповнюють цей підхід симгевристичною оптимізацією портфелів ІТ-проєктів, демонструючи, що розгляд ризик-кореляцій дозволяє досягати кращого балансу між цільовими метриками якості, строків і вартості.

Дослідження, присвячене еволюції концептів ризику в ІТ та їхньому впливу на якість, знаходиться у фокусі міждисциплінарної проблематики: воно об'єднує методи інтелектуального аналізу даних, моделювання динаміки систем, стратегії управління якістю та ризик-менеджменту. Вирішення поставленої задачі сприятиме вдосконаленню прийняття рішень у складних цифрових середовищах, які вимагають високої адаптивності, надійності та прозорості при досягненні цілей якості.

Аналіз останніх досліджень на публікацій. Проблематика управління ризиками у сфері розробки програмного забезпечення (ПЗ) вже тривалий час є предметом пильної уваги науковців. Із зростанням складності ІТ-продуктів, динаміки середовища розробки та високого ступеня невизначеності у вимогах, саме ефективне виявлення, класифікація та мінімізація ризиків стають центральними чинниками забезпечення якості програмного продукту.

У дослідженні Olusanya et al. [9] запропоновано нейро-нечітку систему оцінки ризиків безпеки у межах життєвого циклу розробки ПЗ. Система враховує багатовимірну природу загроз, яка включає технічні, організаційні та людські фактори. Автори акцентують увагу на складності формалізації ризиків у динамічному ІТ-середовищі й пропонують підхід, що дозволяє враховувати нечіткість даних і поведінкові характеристики розробників та користувачів. Цей підхід є прикладом інтеграції класичних моделей оцінки з інтелектуальними алгоритмами, що ілюструє загальну тенденцію переходу до гібридних систем аналізу ризику.

Іншим аспектом дослідження ризиків у ПЗ є взаємозв'язок між процесними боргами (process debt) та якістю праці в команді. Gustavsson et al. [14] досліджують, як накопичення технічного та організаційного боргу в гнучких (Agile) командах впливає на задоволення від роботи, а отже – і на якість продукту. Автори показують, що непрямі ризики, пов'язані з управлінськими рішеннями, мають прямий вплив на кінцевий результат розробки. Ці результати підкреслюють важливість урахування людського чинника в оцінці ризиків та необхідність регулярного рефакторингу не тільки коду, але й процесів.

Питанням кількісної оцінки ризиків присвячено роботу Dewi та Dharmawan [3], де розроблено модель врахування пропорції ризику в оцінюванні трудомісткості програмних проєктів. Автори демонструють, що врахування ризиків на етапі планування дозволяє підвищити точність оцінки витрат і строків. Цей підхід є особливо важливим для сучасних адаптивних життєвих циклів розробки, де обсяг роботи часто змінюється на основі зворотного зв'язку.

З погляду управлінських підходів до пріоритезації ризиків варто виділити дослідження Ayesha Ziana і Charles J [3], в якому застосовано метод аналізу ієрархій (Analytic Hierarchy Process – AHP) для визначення впливових факторів ризику в Agile-проєктах. Цей підхід дозволяє формалізувати суб'єктивні оцінки експертів та відобразити складні взаємозв'язки між чинниками. Результати свідчать про переважний вплив організаційних ризиків (наприклад, зміна пріоритетів замовника) у порівнянні з технічними. Це ще раз наголошує на необхідності міждисциплінарного підходу до управління ризиками в ІТ-проєктах.

У свою чергу, дослідження Lesum et al. [12] акцентує увагу на ролі лідерства та управлінської культури в ефективному зниженні ризиків. У статті запропоновано фреймворк проектного управління, який дозволяє модифікувати вплив чинників ризику за рахунок інтеграції практик лідерства, таких як прозорість комунікації та підтримка командного середовища. Автори демонструють, що саме управлінські рішення можуть бути ключовим модератором впливу ризиків на успішність ПЗ. З огляду на це, фокус зміщується з суто технічних аспектів на організаційно-культурні, що відкриває нові напрями для досліджень.

Інституційно-організаційний контекст також розглядається у дослідженні Mohammed et al. [2], де проаналізовано вплив культури організації на ефективність ІТ-проєктів у йорданських компаніях. Отримані дані підтверджують, що низький рівень адаптивності культури, брак довіри до змін або відсутність мотиваційної підтримки посилюють ризики реалізації, навіть за наявності достатніх ресурсів. Отже, ризик в ІТ-продуктах має не лише технічну, але й соціальну природу.

Окрему увагу в літературі приділено архітектурним факторам ризику. У статті Jolak et al. [11] емпірично досліджено вплив «архітектурних запахів» (architectural smells) на підтримуваність ПЗ. Автори виявили, що деякі патерни порушень архітектурних принципів – такі як надмірна зв'язаність або порушення принципів модульності – прямо впливають на ускладнення подальшої підтримки та збільшення технічного боргу. Це дослідження заповнює важливу прогалину між якісною архітектурою ПЗ і ризиками деградації якості в довгостроковій перспективі.

Отже, огляд сучасних досліджень демонструє наявність широкого спектру підходів до аналізу ризиків в ІТ-сфері: від інтеграції штучного інтелекту до формалізації експертних оцінок і дослідження організаційної поведінки. Водночас, попри велику кількість моделей і фреймворків, залишається низка нерозв'язаних питань: зокрема, проблема об'єднання технічних, організаційних і зовнішніх ризиків у єдину адаптивну систему управління, що здатна динамічно реагувати на зміну середовища ІТ-проєкту.

Метою статті є здійснення ґрунтовного аналізу еволюції понять ризику в контексті розробки і забезпечення якості програмного забезпечення, зокрема в умовах сучасних ІТ-проєктів, що характеризуються високою динамікою, складністю та міждисциплінарністю. Особливу увагу приділено виявленню типових категорій ризиків (технічних, організаційних, зовнішніх), які мають найбільший вплив на якість ІТ-продуктів, та критичному аналізу існуючих підходів до їх класифікації, оцінювання

ISSN 2786-5460 (Print), ISSN 2786-5479 (Online)

й управління. На основі синтезу літературних джерел і результатів порівняльного аналізу сформовано концептуальні засади адаптації моделей ризик-менеджменту до специфіки цифрових проєктів.

Виклад основного матеріалу. У сфері забезпечення якості IT-продуктів однією з центральних передумов ефективного управління є не просто механічне застосування інструментів контролю, а системне розуміння природи ризиків – їх джерел, динаміки виникнення, взаємозалежностей, кумулятивних ефектів і довгострокових впливів на показники якості. У сучасному середовищі цифрового виробництва, де IT-продукти характеризуються високою складністю, модульністю, швидкістю релізів та інтеграційною чутливістю, традиційні підходи до оцінки ризиків часто не забезпечують належного рівня інформованості для прийняття рішень.

Актуальні дослідження вказують на необхідність переосмислення класичних моделей ризик-менеджменту в бік міждисциплінарного та динамічного підходу. Зокрема, у праці Guan et al. [6] запропоновано концепцію динамічної мережі взаємозалежностей ризиків (Risk Interdependency Network-Based Model), що враховує не лише ймовірність окремих подій, а й їх каскадні ефекти в межах проєктної екосистеми. Автори демонструють, що проєктні збої часто є наслідком не одного ризику, а складної взаємодії латентних, вторинних або опосередкованих загроз. Такий підхід відкриває можливості для пріоритезації управлінських інтервенцій із урахуванням системного впливу ризиків на кінцеву якість програмного забезпечення (функціональність, надійність, безпека, підтримуваність тощо).

На основі системного аналізу релевантної наукової літератури та порівняння емпіричних моделей, доцільно виділити три базові категорії ризиків, що найбільш часто згадуються в контексті впливу на якість IT-продуктів: технічні, організаційні та зовнішні. Така типологія не лише спрощує інтерпретацію результатів, а й дозволяє уніфікувати підходи до управління ризиками у різних фазах життєвого циклу програмного забезпечення – від ініціації до експлуатації.

Технічні ризики охоплюють загрози, пов'язані з архітектурою ПЗ, якістю коду, технічним боргом, слабкою інфраструктурною сумісністю, нестачею тестування або складністю впровадження змін. У дослідженні van der Zwaag et al. [4] емпірично показано, що надмірне повторне використання коду (cross-project code duplication) у продуктових лініях призводить до накопичення архітектурного боргу, що, своєю чергою, негативно впливає на підтримуваність і масштабованість системи. Такі ризики часто залишаються поза зоною уваги менеджерів через свою приховану природу, проте мають глибокий вплив на довгострокову якість.

Окрім того, як доводять Saadatmand et al. [7], у проєкті SmartDelta автоматизований аналіз змін між версіями ПЗ дозволяє не лише виявляти порушення якості, але й прогнозувати ризики їх ескалації при розгортанні нових функціональностей. Такий підхід дозволяє реалізувати інтегрований контроль якості на рівні DevOps-процесів.

Організаційні ризики включають проблеми в управлінні, комунікаціях, культурі проєкту, ролях і відповідальностях, а також у прийнятті рішень. У дослідженні Moussa et al. [1] продемонстровано застосування машинного навчання для моделювання системних ризиків на основі даних взаємодії між підрозділами в інфраструктурних проєктах. Хоча контекстом виступає будівництво, логіка моделі дозволяє адаптувати її до IT-середовища, де аналогічно існує мережа залежностей між технічними командами, менеджментом і зацікавленими сторонами. Алгоритмічна класифікація ризиків та виявлення «вузьких місць» у комунікаційних потоках надають нові інструменти для раннього виявлення організаційної нестабільності.

Також у дослідженні Wang et al. [5] реалізовано мультиагентне моделювання, яке може бути трансформоване для опису поведінки команд розробки в умовах стресу, перевантаження або зміни пріоритетів. Наприклад, агенти можуть репрезентувати різні ролі в команді (розробник, тестувальник, продакт-менеджер), а їх взаємодія – моделювати ризикові ситуації на кшталт релізу під тиском дедлайнів.

Зовнішні ризики охоплюють вплив факторів середовища, ринку, політики, нормативного регулювання або соціальних трансформацій. У роботі [15] на прикладі зелених будівельних матеріалів показано, як подвійний тиск (вимоги ринку + державні екологічні норми) формує ризики для стабільності та прогнозованості бізнес-процесів. У контексті IT такі ризики можуть проявлятися як зміни в законодавстві щодо обробки персональних даних (наприклад, GDPR), вплив санкцій, збої в ланцюгах постачання хмарної інфраструктури або неочікувані тренди користувацької поведінки. Подібні виклики мають стратегічну вагу для компаній, що розробляють IT-продукти у високорегульованих галузях або на глобальних ринках.

На перетині категорій виникає складна багатовимірна конфігурація ризиків, яка не піддається простому інтуїтивному оцінюванню. У цьому контексті дослідження Saiz et al. [8] заслуговує на особливу увагу. Автори пропонують симгевристичний підхід до портфельного управління ризиками, що поєднує оптимізацію якості, витрат та графіків у багатопроєктному середовищі. Врахування кореляцій між

ризиками, а також ефектів переривань і затримок дозволяє адаптувати модель до динамічного характеру ІТ-розробки, особливо в умовах гнучких методологій (Agile/DevOps).

Запропоноване трирівневе структурування – технічні, організаційні та зовнішні ризики – є результатом синтезу підходів, апробованих у провідних міждисциплінарних дослідженнях. Воно базується не на абстрактній класифікації, а на емпірично підтверджених закономірностях впливу різних типів ризиків на якість програмного забезпечення. Застосування такої типології дозволяє поєднати якісний експертний аналіз з кількісним прогнозуванням впливу ризиків, формуючи основу для створення ефективних моделей прийняття рішень у складних цифрових екосистемах.

З метою забезпечення порівнюваності та узагальнення результатів, отриманих з різних джерел, у межах даного дослідження було розроблено методичну процедуру оцінювання впливу ризиків різної природи (технічних, організаційних та зовнішніх) на ключові параметри якості ІТ-продуктів. Така процедура включала як нормалізацію первинних даних, так і експертне шкалювання у випадках, коли прямі кількісні значення в публікаціях були відсутні, але наявний якісний опис впливу.

Основні кроки процедури включали:

1. Виділення релевантних прикладів із наукових публікацій: для кожної категорії ризиків було обрано по декілька кейсів, де автори прямо або опосередковано вказували на зміни у проєктних метриках, таких як підтримуваність, кількість дефектів, затримка релізу, продуктивність тощо.

2. Переклад якісних показників у кількісну форму. Наприклад, «значне зростання кількості дефектів» інтерпретувалося як збільшення на ≥25 %, «суттєва затримка релізу» – як відтермінування понад 20 % від запланованого терміну, «погіршення підтримуваності» – через приріст часу на зміну або усунення помилок ≥30 %.

3. Узагальнення впливу на три основні метрики якості: технічна цілісність, часові втрати, зростання витрат на підтримку. Для кожного типу ризику проводилось експертне оцінювання й обчислювались умовні середні відсоткові зміни.

4. Нормалізація шкал для зведеної таблиці. Значення були приведені до єдиної шкали 0–100 %, де 100 % – максимальний вплив ризику в аналізованому прикладі, а 0 % – відсутність виявленого впливу.

Для забезпечення об'єктивності було застосовано триетапну валідацію:

- міжджерельну (перевірка повторюваності оцінок у кількох джерелах),
- внутрішню (співвіднесення якісного опису з числовою шкалою),
- логічну (оцінка внутрішньої відповідності впливів на різні аспекти якості).

У результаті цієї процедури було побудовано узагальнену таблицю (табл. 1) з прикладами ризиків за кожною категорією, що демонструє не лише їх характер, а й кількісний вплив на проєктну якість за типізованими показниками. Такий підхід дозволяє перейти від описової типології до операціоналізованого інструмента для аналізу ризикових профілів ІТ-проєктів на різних фазах життєвого циклу.

Таблиця 1

Класифікація ризиків у проєктах розробки ІТ-продуктів та їхній кількісний вплив на якість

Категорія ризику	Конкретний ризик	Вплив на технічну цілісність	Зростання витрат на підтримку	Затримка термінів розробки
Технічний	Повторне використання застарілого коду	25%	20%	15%
	Архітектурна несумісність модулів	30%	18%	20%
Організаційний	Нестабільність управління проєктом	10%	25%	30%
	Відсутність комунікації між командами	15%	22%	25%
Зовнішній	Регуляторна невизначеність	5%	10%	12%
	Різкі коливання попиту	10%	12%	18%

Представлена таблиця ілюструє результати узагальнення кількісного впливу типових технічних, організаційних та зовнішніх ризиків на ключові аспекти якості програмного забезпечення. Зокрема, було проаналізовано наукові дослідження, що містять емпіричні або змодельовані дані щодо впливу конкретних чинників ризику на такі метрики, як підтримуваність, своєчасність релізу, стабільність функціональності та відповідність вимогам. Для уніфікації підходу використано середні значення втрати показників якості, оцінені за шкалою 0–100 %, на основі виявлених закономірностей.

ISSN 2786-5460 (Print), ISSN 2786-5479 (Online)

Аналіз показав, що технічні ризики, зокрема архітектурні дефекти та надмірне дублювання коду, здатні зменшити підтримуваність ПЗ на понад 25 %, суттєво впливаючи на його довготривалу якість. Організаційні ризики, пов'язані з лідерством, комунікацією та ролями в команді, можуть призводити до затримок релізу (до 40 %) та зниження продуктивності. Зовнішні ризики, як-от вплив регуляторної політики або зміни ринкового попиту, характеризуються менш прямим, але системним ефектом, зокрема зниженням відповідності вимогам до 20–30 %.

Отримані результати дозволяють не лише розрізняти ризики за джерелом, а й кількісно оцінювати їхню значущість у контексті прийняття рішень щодо управління якістю ПЗ на різних фазах життєвого циклу.

Висновки та перспективи. Узагальнюючи результати проведеного аналізу, можна стверджувати, що ризики в цифровому середовищі постають не лише як фактори, які ускладнюють реалізацію ІТ-проєктів, а й як структуроутворюючі елементи, що формують саму логіку управління якістю. Сучасні підходи, що базуються на ізольованій оцінці ймовірності та впливу, не відповідають складності міжфакторних зв'язків, характерних для динамічних програмних систем. Саме тому актуальним є перехід до таких методів оцінювання ризику, які враховують багатовимірну природу ризикових взаємодій, часову змінність їх значущості та можливість кумулятивного ефекту впливу на якісні характеристики продукту.

Встановлено, що ризики в ІТ не можна зводити до одиничних подій чи аномалій – вони формують цілісні конфігурації взаємодій, які мають латентну інерцію та здатні змінювати критичні метрики не лише безпосередньо, а й через опосередковані впливи. У цьому контексті надзвичайно важливо враховувати не тільки формальні категорії ризиків, а й їх здатність трансформуватися між доменами – наприклад, технічні дефекти можуть породжувати організаційні кризи, а зовнішні обмеження – провокувати архітектурні компроміси. Зростає роль адаптивних підходів, які поєднують структурне картування ризиків, сценарне прогнозування і автоматизоване виявлення змін у динаміці якісних показників.

Подальші дослідження в цій площині доцільно орієнтувати на розробку гібридних моделей, які дозволяють інтегрувати якісні знання про природу ризику з кількісними параметрами проєктних метрик. Особливої уваги потребує формалізація адаптивних механізмів реагування, що враховують не лише значення ризику в моменті, але й його історію, частотність повторень, типові сценарії поширення та стійкість до зовнішніх втручань. Очевидним також є запит на створення систем, які автоматично відслідковують перехідні стани між фазами життєвого циклу розробки й асоціюють їх із ризиковими конфігураціями, дозволяючи заздалегідь ідентифікувати вразливі ділянки проєкту.

Еволюція розуміння ризику в ІТ-сфері веде до зміщення акцентів – від традиційного контролю до передиктивного мислення, від реактивного усунення наслідків до проактивного моделювання складних ситуацій. Саме це відкриває шлях до створення більш стійких, масштабованих і якісно керованих інформаційних систем у відповідь на виклики сучасного технологічного середовища.

Список використаних джерел:

1. Ahmed Moussa, Mohamed Ezzeldin, Wael El-Dakhakhni, Predicting and managing risk interactions and systemic risks in infrastructure projects using machine learning. *Automation in Construction*, 2024. Vol. 168, Part B, 105836, ISSN 0926-5805, https://doi.org/10.1016/j.autcon.2024.105836.

2. Ashraf Bany Mohammed, Yousef Alsafadi, Manaf Al-Okaily, Heba Al-Hyasat, Yunus Al-yahya, Ra'ed Masa'deh, Exploring the impact of organizational culture on the performance of information technology projects in Jordanian organizations. *Telematics and Informatics Reports*, 2025. Vol. 19, 100210, ISSN 2772-5030, https://doi.org/10.1016/j.teler.2025.100210.

3. Ayesha Ziana M., Charles J. Prioritization of Risks in Agile Software Projects Through an Analytic Hierarchy Process Approach. *Procedia Computer Science*, 2024. Vol. 233, P. 713–722, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2024.03.260.

4. Jesper van der Zwaag, Frank Driesens, Bouwe Postma, Andrea Capiluppi, Refactoring cross-project code duplication in an industrial software product line: A case study from RDW. *Journal of Systems and Software*, 2025. Vol. 230, 112496, ISSN 0164-1212, https://doi.org/10.1016/j.jss.2025.112496.

5. Kewen Wang, Peng Dong, Weibing Chen, Rui Ma, Longyu Cui, Research on risk management of ship maintenance projects based on multi agent swarm model simulation method. *Heliyon*, 2024. Vol. 10, Issue 19, e38785, ISSN 2405-8440, https://doi.org/10.1016/j.heliyon.2024.e38785.

6. Li Guan, Alireza Abbasi, Michael J. Ryan, José M. Merigó, A dynamic risk interdependency network-based model for project risk assessment and treatment throughout a project life cycle. *Computers & Industrial Engineering*, 2025. Vol. 201, 110921, ISSN 0360-8352, https://doi.org/10.1016/j.cie.2025.110921.

7. Mehrdad Saadatmand, Muhammad Abbas, Eduard Paul Enoiu, Bernd-Holger Schlingloff, Wasif Afzal, Benedikt Dornauer, Michael Felderer, SmartDelta project: Automated quality assurance and optimization across product versions and variants. *Microprocessors and Microsystems*, 2023. Vol. 103, 104967, ISSN 0141-9331, https://doi.org/10.1016/j.micpro.2023.104967.

8. Miguel Saiz, Laura Calvet, Angel A. Juan, David Lopez-Lopez, A simheuristic for project portfolio optimization combining individual project risk, scheduling effects, interruptions, and project risk correlations. *Computers & Industrial Engineering*, 2024. Vol. 198, 110694, ISSN 0360-8352, https://doi.org/10.1016/j.cie.2024.110694.

9. Olayinka Olufunmilayo Olusanya, Rasheed Gbenga Jimoh, Sanjay Misra, Joseph Bamidele Awotunde, A neuro-fuzzy security risk assessment system for software development life cycle. *Heliyon*, 2024. Vol. 10, Issue 13, e33495, ISSN 2405-8440, https://doi.org/10.1016/j.heliyon.2024.e33495.

10. Renny Sari Dewi, Yogantara Setya Dharmawan, A Proposed Model for Embedding Risk Proportion in Software Development Effort Estimation. *Procedia Computer Science*, 2024. Vol. 234, P. 1777–1784, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2024.03.185.

11. Rodi Jolak, Simon Karlsson, Felix Dobslaw, An empirical investigation of the impact of architectural smells on software maintainability. *Journal of Systems and Software*, 2025. Vol. 225, 112382, ISSN 0164-1212, https://doi.org/10.1016/j.jss.2025.112382.

12. Samiul Alim Lesum, Sayeda Rahnuma Akthar, Muhammad Rezaul Islam, Farzana Sadia, Mahady Hasan, Project Governance to Improve the Performance of Software Projects by Mitigating the Software Risk Factors: The Moderating Role of Project Leadership. *Procedia Computer Science*, 2024. Vol. 239, P. 1863–1870, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2024.06.368.

13. Simon Burgis, Hans Rübberdt, Christoph Gaedigk, Louis Keuper, Georgette Naufal, Jonko Paetzold, Xanthi Oikonomidou, Benjamin Bastida Virgili, MAS–A mission analysis software for collision risk quantification and impact assessment of rule-based decision-making for collision avoidance. *Journal of Space Safety Engineering*, 2025. ISSN 2468-8967, https://doi.org/10.1016/j.jsse.2025.04.007.

14. Tomas Gustavsson, Muhammad Ovais Ahmad, Hina Saeeda, Job satisfaction at risk: Measuring the role of process debt in agile software development. *Journal of Systems and Software,* 2025. Vol. 222, 112350, ISSN 0164-1212, https://doi.org/10.1016/j.jss.2025.112350.

15. Wenxuan Guo, Navigating dual pressures: The impact of environmental policies and market demand risks on the sustainable development of green building materials – A case study of the green cement industry. *Heliyon*, 2025. Vol. 11, Issue 2, e41942, ISSN 2405-8440, https://doi.org/10.1016/j.heliyon.2025.e41942.

Дата надходження статті: 25.06.2025
Дата прийняття статті: 30.06.2025
Опубліковано: 23.09.2025