https://doi.org/10.31891/2307-5732-2026-365-30
УДК 004.056:004.415.2

КІШ ЮРІЙ
Ужгородський національний університет
https://orcid.org/0009-0000-6167-0129
e-mail: yurii.kish@uzhnu.edu.ua
ЛЯХ ІГОР
Ужгородський національний університет
https://orcid.org/ 0000-0001-5417-9403
e-mail: igor.lyah@uzhnu.edu.ua

АЛГОРИТМ ІДЕНТИФІКАЦІЇ, ПРІОРИТЕЗАЦІЇ ТА ІЄРАРХІЧНОЇ КЛАСИФІКАЦІЇ РИЗИКІВ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ З УРАХУВАННЯМ ТИПУ ІТ-ПРОДУКТУ

У статті розглянуто проблему формалізованого управління ризиками забезпечення якості програмного забезпечення в умовах зростання складності сучасних ІТ-продуктів, що поєднують хмарні сервіси, компоненти штучного інтелекту, data-centric підсистеми та DevSecOps-процеси. Запропоновано математичну модель алгоритму ідентифікації, багатокритеріальної пріоритезації та ієрархічної класифікації ризиків якості з урахуванням типу ІТ-продукту та фази життєвого циклу розробки. Модель ґрунтується на представленні ризиків у вигляді багатовимірних векторів ознак, що включають імовірність дефектності, агрегований вплив на характеристики якості, контекстні коефіцієнти критичності та параметри продуктового середовища. Для кількісного ранжування ризиків введено інтегральний індекс пріоритету, який дозволяє порівнювати ризики різної природи в єдиному метричному просторі. Ієрархічна класифікація реалізована методом агломеративної кластеризації, що забезпечує формування адаптивної таксономії ризиків на основі фактичних метричних даних. З метою експериментальної апробації моделі розроблено програмний прототип системи підтримки прийняття рішень мовою Python, який реалізує повний цикл обчислювальних процедур: прогнозування дефектності програмних модулів, обчислення векторів ризику, багатокритеріальну пріоритезацію та побудову ієрархії ризиків. Емпіричну основу дослідження становлять дані NASA Metrics Data Program, що містять статичні метрики коду та бінарні ознаки дефектності. Отримані результати підтвердили можливість формування відтворюваної ієрархічної структури ризиків і кількісного ранжування модулів за рівнем критичності. Показано, що навіть за помірної точності прогнозування дефектності використання багатокритеріального підходу забезпечує превентивно орієнтовану оцінку ризиків і підвищує інформативність управлінських рішень порівняно з експертними методами. Наукова новизна полягає в інтеграції ідентифікації, пріоритезації та класифікації ризиків у єдину формалізовану процедуру з урахуванням типу ІТ-продукту та використанні метричних даних як основи для побудови адаптивної ієрархії ризиків. Практичне значення результатів полягає у можливості застосування запропонованого алгоритму в системах управління якістю та ризиками для підтримки стратегічного планування тестування, управління технічним боргом і оптимізації ресурсів забезпечення якості в умовах багатокритеріальних обмежень.

Ключові слова: *ризик якості програмного забезпечення, пріоритезація ризиків, ієрархічна класифікація, метрики якості, система підтримки прийняття рішень, дефектність ПЗ, управління ризиками.*

KISH YURII, LIAKH IHOR
Uzhhorod National University

ALGORITHM FOR IDENTIFICATION, PRIORITIZATION AND HIERARCHICAL CLASSIFICATION OF SOFTWARE QUALITY ASSURANCE RISKS, TAKING INTO ACCOUNT THE TYPE OF IT PRODUCT

The paper addresses the problem of formalized risk management in software quality assurance under the increasing complexity of modern IT products that integrate cloud services, artificial intelligence components, data-centric subsystems, and DevSecOps processes. A mathematical model of an algorithm for risk identification, multi-criteria prioritization, and hierarchical classification is proposed, taking into account the type of IT product and the software development lifecycle phase. The model represents risks as multidimensional feature vectors including defect probability, aggregated impact on quality attributes, contextual criticality coefficients, and product-specific parameters. An integral priority index is introduced to enable quantitative comparison of heterogeneous risks within a unified metric space. Hierarchical classification is implemented using agglomerative clustering, allowing the construction of an adaptive risk taxonomy based on empirical metric data. To validate the proposed model, a decision support system prototype was developed in Python, implementing the full computational workflow: defect risk prediction, risk vector construction, multi-criteria prioritization, and hierarchical risk structuring. The empirical basis of the study is the NASA Metrics Data Program dataset containing static code metrics and binary defect labels. The results demonstrate the feasibility of constructing a reproducible hierarchical risk structure and quantitatively ranking software modules by criticality. It is shown that even with moderate defect prediction performance, the multi-criteria approach provides a preventive risk assessment and improves the informativeness of decision-making compared to expert-based methods. The scientific novelty lies in the integration of risk identification, prioritization, and classification into a single formalized procedure sensitive to IT product type and grounded in metric-driven adaptive hierarchies. The practical significance of the results is associated with the applicability of the proposed algorithm in software quality and risk management systems for strategic test planning, technical debt management, and resource optimization under multi-criteria constraints.

Keywords: *software quality risk, risk prioritization, hierarchical classification, quality metrics, decision support system, software defects, risk management.*

Стаття надійшла до редакції / Received 11.02.2026
Прийнята до друку / Accepted 11.03.2026
Опубліковано / Published 28.05.2026

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Сучасні ІТ-продукти дедалі частіше поєднують хмарні сервіси, DevSecOps-практики, компоненти з генеративним ШІ та кіберфізичні або IoT-підсистеми, через що ризики забезпечення якості ПЗ набувають багатовимірного характеру: одна й та сама загроза проявляється по-різному залежно від типу продукту, його життєвого циклу та контексту експлуатації. Окремі напрями досліджень детально висвітлюють ризики безпеки

та їхню оцінку, однак підкреслюють статичність і слабку масштабованість традиційних підходів, а також нестачу безперервного забезпечення впевненості у властивостях систем у мережевих та динамічних середовищах [7].

Додатково, у хмарних екосистемах ризики якості прямо пов'язані з контрактними цілями та конфліктними метриками (наприклад, порушення SLA проти енергоефективності або безпеки проти накладних витрат), що ускладнює одночасну ідентифікацію, пріоритезацію та узгоджену класифікацію ризиків для різних класів продуктів [6].

У результаті виникає потреба в алгоритмічному підході, який здатний формалізовано поєднати виявлення ризиків, їхню пріоритезацію та ієрархічну класифікацію з урахуванням типу IT-продукту та вимірюваних проявів ризику на рівні метрик якості, процесних індикаторів і контекстних обмежень.

Аналіз досліджень та публікацій

Minani та співавтори виконали систематизацію тестування IoT-систем через таксономію та емпіричний аналіз практик, де методологічно поєднано огляд літератури з узагальненням рекомендацій і верифікаційними елементами, а вимірювані результати подані як частотні характеристики застосування підходів і прогалин у покритті (зокрема, акцент на фрагментованості тестових стратегій для різних класів IoT та залежності від контексту розгортання) [1]. У контексті ризик-орієнтованого забезпечення якості цінність цього дослідження полягає в тому, що ризики якості тут природно класифікуються за рівнями системи та видами тестової діяльності, однак невирішеним залишається питання узгодження такої класифікації з пріоритетами ризиків, які змінюються залежно від типу продукту та критичності його функцій; об'єктивною причиною є гетерогенність IoT-архітектур і різні експлуатаційні умови, а суб'єктивною – відмінності в інженерних традиціях тестування в різних доменах.

Yu та колеги запропонували мапування метрик якості генеративних AI-систем до характеристик якості, застосувавши snowballing-огляд як основний метод добору та синтезу джерел; вимірювані результати сформовано як структуровану відповідність між класами метрик і характеристиками якості, що дає змогу інтерпретувати, які саме аспекти якості вимірюються, а які залишаються поза увагою [2]. Це важливо з огляду на те, що генеративний компонент у різних типах IT-продуктів породжує специфічні ризики якості (наприклад, неконтрольована варіативність результатів або деградація якості під час дрейфу даних), але в роботі відкритим залишається питання алгоритмічної пріоритезації таких ризиків у поєднанні з класичними ризиками ПЗ; об'єктивно це зумовлено відсутністю єдиних стандартів вимірювання та швидкою еволюцією моделей, а суб'єктивно – домінуванням метрик, зручних для експериментів, над метриками, релевантними для життєвого циклу продукту.

Gentili зі співавторами дослідили сприйняття практиками так званих requirements smells, використавши емпіричні методи збору думок і узгодження інтерпретацій (інтерв'ювання/опитування та аналіз узгодженості оцінок), а вимірювані результати відображають, які типи "запахів" вимог найчастіше пов'язують із ризиками помилкового трактування та подальших дефектів [3]. Значення роботи полягає в демонстрації того, що ризики якості можуть зароджуватися на рівні вимог як ранні сигнали майбутніх проблем, однак не вирішено проблему формального віднесення цих сигналів до ієрархії ризиків та їхнього порівняння між різними типами продуктів; об'єктивною причиною є контекстність вимог і доменна специфіка, а суб'єктивною – різна культура роботи з вимогами та неоднакові пороги "серйозності" в командах.

Graetsch та колеги здійснили спостережний кейс-стаді щодо управління технічним боргом у мультидисциплінарній data-intensive команді, використавши якісні методи польового дослідження та інтерпретативний аналіз практик; вимірювані результати подані як виявлені типи технічного боргу, їхні причини та наслідки для темпів змін і стабільності якості [4]. Для ризик-менеджменту якості цінним є те, що технічний борг тут виступає як агрегований ризик, що ієрархічно "накриває" низку локальних дефектів процесу та архітектури, але невирішеним залишається питання кількісної пріоритезації технічного боргу між продуктами різних типів (наприклад, платформа даних проти мобільного клієнта); об'єктивно це спричинено різними бізнес-цілями та моделями експлуатації, а суб'єктивно – різною толерантністю стейкхолдерів до відкладених виправлень.

Akbar та співавтори запропонували decision-making framework для успішного DevSecOps, поєднавши узагальнення бар'єрів/чинників із процедурою підтримки ухвалення рішень; вимірювані результати полягають у структурованій системі критеріїв і чинників, що впливають на результативність DevSecOps-переходу, та у впорядкуванні пріоритетів управлінських дій [5]. У контексті ризиків якості це демонструє, що ризики безпеки та якості можуть бути "вбудовані" в процес доставки, але залишається невирішеним питання трансляції процесних пріоритетів DevSecOps у єдину ієрархію ризиків для різних типів продуктів; об'єктивна причина – багатоваріантність DevSecOps-практик і різні рівні зрілості організацій, суб'єктивна – різне трактування балансу швидкості релізів і глибини контролів.

Qazi та колеги надали таксономію SLA-підходів у хмарних обчисленнях, застосувавши оглядову методологію з категоризацією робіт за проблемами та метриками; вимірювані результати відображено через класифікацію технік, параметри оцінювання та типові платформи, а також через підкреслення того, що значна частина підходів оптимізує лише одну-дві метрики.

Це важливо для ризик-орієнтованого забезпечення якості, адже SLA-порушення є вимірюваним проявом ризику якості для сервісних продуктів, однак невирішеним лишається питання одночасної пріоритезації конфліктних метрик у межах єдиної ієрархії ризиків; об'єктивно це пов'язано з багатокритеріальністю QoS/QoE та динамікою навантажень, а суб'єктивно – з фокусом досліджень на окремих оптимізаційних цілях, а не на узгодженні ризиків між різними рівнями продукту [6].

Shukla та співавтори виконали систематичний огляд system security assurance, формалізувавши процеси, вимоги та метрики безпеки, а також типові методи забезпечення впевненості; вимірювані результати подані як узагальнені категорії діяльностей, обмеження наявних підходів і перелік прогалин, зокрема наголошено на статичності методів і проблемах масштабування до розподілених IT-систем [7].

Значення цього огляду для управління ризиками якості полягає в тому, що безпекові ризики формують окрему гілку ієрархії ризиків і потребують узгодження з іншими атрибутами якості, однак невирішено питання, як об'єднати assurance-активності в адаптивну, безперервну та продукт-специфічну модель пріоритезації; об'єктивна причина – залежність assurance від доменних стандартів і фаз життєвого циклу, суб'єктивна – інерція сертифікаційних практик і різний рівень доступності даних для вимірювання.

Bernardo та співавтори розглянули інновації в data governance та управлінні якістю даних, синтезувавши підходи з різних галузей і окресливши напрями для інтеграції стандартів та інструментів моніторингу; вимірювані результати в роботі відображені як виявлені прогалини інтеграції принципів, відсутність порівнянної емпірики ефективності та потреба в критичних показниках ризику й продуктивності, які можна відстежувати у часі [8].

У площині ризиків якості це особливо релевантно для data-centric продуктів, де якість даних є джерелом системних ризиків якості ПЗ, але невирішеним залишається питання формальної ієрархізації ризиків на стику "дані–модель–сервіс" та узгодження цієї ієрархії між типами продуктів; об'єктивно це зумовлено різною зрілістю практик data governance, суб'єктивно – відсутністю уніфікованих індикаторів ризику, прийнятних одночасно для інженерних і управлінських рішень.

Tran-Truong зі співавторами провели систематичний огляд багатофакторної автентифікації в цифрових платіжних системах з фокусом на відповідність NIST і практики впровадження; методологія включає відбір і класифікацію досліджень, а вимірювані результати виражаються як узагальнені тенденції використання факторів, типові архітектурні рішення та ступінь узгодження з рекомендаціями стандартів [9]. Значення роботи полягає в тому, що для певних типів продуктів (фінтех, платежі) ризики якості тісно зчеплені з ризиками безпеки та відповідності, однак не вирішено питання, як уніфіковано ранжувати такі ризики відносно, наприклад, ризиків продуктивності чи надійності, коли метрики різнорідні; об'єктивно це спричинено нормативною специфікою домену та різними моделями загроз, суб'єктивно – розривом між стандарт-орієнтованими критеріями і продуктовими метриками якості, що використовуються командами [9].

Benmalek здійснив огляд ransomware для кіберфізичних систем, запропонувавши таксономізації, узагальнення кейсів та аналіз прогалин безпеки; методично робота спирається на класифікацію інцидентів і систематизацію векторів атак, а вимірювані результати представлені як типові класи загроз, уразливі ланки та відкриті виклики захисту [10]. Для ризик-орієнтованої якості це демонструє, що для CPS/IoT-продуктів ризики якості не можуть бути відокремлені від стійкості до атак, але лишається невирішеним питання узгодженої ієрархії ризиків, яка одночасно враховує безпеку, доступність і вплив на фізичні процеси; об'єктивна причина – складність моделювання наслідків у фізичному середовищі, суб'єктивна – дефіцит репрезентативних даних про інциденти та різна готовність організацій публікувати результати розслідувань.

Suomalainen та колеги проаналізували кібербезпеку тактичних 6G-мереж, застосувавши комплекс методів threat/risk analysis, зокрема STRIDE, MITRE, DREAD, CVSS, Delphi та X.805, і подали результати спільного дослідження пріоритезації ризиків; вимірювані результати описані як ідентифікація, класифікація та кількісне представлення найбільш значущих загроз, а також як висновки про застосовність метрик і методів у новому домені [11].

Цінність цього підходу полягає в демонстрації механізму переходу від ідентифікації загроз до їхньої пріоритезації, однак невирішеним залишається питання перенесення подібних процедур на задачі якості ПЗ поза безпекою та на різні типи продуктів, де ризики проявляються через інші метрики; об'єктивно це зумовлено тим, що в нових доменах бракує історичних кількісних даних ризику, а суб'єктивно – залежністю Delphi-процедур від складу експертної панелі та неоднакової інтерпретації шкал.

Ben Amara та співавтори запропонували онтологічний фреймворк для horizon scanning у забезпеченні безперервності бізнесу критичних сервісів, методологічно поєднавши побудову онтології з оглядом підходів до виявлення загроз і слабких сигналів; вимірювані результати в такій постановці подаються як структурована модель понять, зв'язків і категорій, що підтримує систематичне виявлення ризиків і їх трасування між рівнями системи [12]. Значення цього напряму полягає в можливості формально задавати ієрархії ризиків і забезпечувати семантичну узгодженість між доменами, однак невирішеним лишається питання, як автоматизовано перетворювати онтологічні структури на пріоритети ризику, узгоджені з метриками якості конкретного типу продукту; об'єктивна причина – розрив між семантичними моделями та емпіричними даними про дефекти/інциденти, суб'єктивна – висока трудомісткість підтримки онтологій та неоднорідність термінології в організаціях.

Узагальнення критичного аналізу вказує, що в кожному з розглянутих джерел локальні проблеми повторюються у різних формах: фрагментованість таксономій і практик тестування для гетерогенних систем, неповнота та неоднорідність метрик якості для нових компонентів на кшталт генеративного ШІ, контекстна варіативність ранніх сигналів ризику на рівні вимог, слабка порівнюваність і кількісна пріоритезація процесних і архітектурних ризиків, включно з технічним боргом та DevSecOps-чинниками, а також труднощі узгодження конфліктних метрик у хмарних SLA-постановках. Водночас безпекові огляди і доменно-специфічні аналізи показують обмеження статичних assurance-підходів і дефіцит безперервної адаптації до динамічних середовищ, потребу інтеграції управління якістю даних із ризиковими індикаторами, розрив між стандартами і практичними

продуктовими метриками у високорегульованих доменах, складність пов'язування кіберзагроз із наслідками для якості та надійності кіберфізичних систем, залежність пріоритезації від експертних процедур за відсутності кількісних даних і, нарешті, відсутність стійкого мосту між семантичними (онтологічними) моделями ризику та їхньою метричною пріоритезацією. У підсумку невирішена проблема набуває узагальненого формулювання: відсутній уніфікований алгоритмічний механізм, який би забезпечував відтворювану ідентифікацію ризиків, їх багатокритеріальну пріоритезацію та ієрархічну класифікацію, узгоджену з метриками якості й контекстом експлуатації, причому параметри цього механізму мають бути чутливими до типу ІТ-продукту та доступності емпіричних даних про прояви ризику.

Формулювання цілей статті

Метою роботи є розроблення та експериментальна апробація алгоритму ідентифікації, багатокритеріальної пріоритезації та ієрархічної класифікації ризиків забезпечення якості програмного забезпечення з урахуванням типу ІТ-продукту на основі формалізованої математичної моделі та програмної реалізації, що забезпечує отримання вимірюваних результатів за метриками якості й ефективності ризик-менеджменту в межах життєвого циклу розробки.

Виклад основного матеріалу

У межах дослідження запропоновано формалізовану математичну модель алгоритмічної підтримки ідентифікації, багатокритеріальної пріоритезації та ієрархічної класифікації ризиків забезпечення якості програмного забезпечення, яка орієнтована на інтеграцію у програмний прототип системи підтримки прийняття рішень та експериментально апробована на сценаріях життєвого циклу розробки ІТ-продуктів. Концептуально модель ґрунтується на представленні множини ризиків як багатовимірного простору ознак, у якому кожен ризик описується вектором параметрів, що відображають імовірність виникнення, потенційний вплив на атрибути якості, фазу SDLC, тип ІТ-продукту, джерело походження та рівень виявлення. Формально множину ризиків задано як $R=\{r_i\}_{i=1}^{n}$, де кожному елементу r_i відповідає вектор ознак $x_i=\langle p_i, q_{i1},\ldots,q_{im}, s_i, t_i\rangle$, у якому p_i – оцінка ймовірності, q_{ij} – нормалізований вплив на j-ту характеристику якості, s_i – фаза життєвого циклу, t_i – тип ІТ-продукту.

Ідентифікація ризиків у моделі реалізується як задача відображення множини артефактів процесу розробки $A=\{a_k\}$ у простір ризиків за допомогою функції виявлення $\phi: A \to R$, що базується на правилах відповідності між подіями процесу, метриками якості та типовими патернами дефектів. На відміну від традиційних реєстрів ризиків, таке відображення дозволяє формалізувати появу ризику як функцію спостережуваних показників процесу, що забезпечує його кількісну трасованість у динаміці.

Пріоритезація ризиків здійснюється на основі багатокритеріальної функції корисності, яка враховує вагові коефіцієнти атрибутів якості та контекстні коефіцієнти типу ІТ-продукту. Інтегральний індекс пріоритету визначається як

$$\Pi(r_i)=w_p p_i+\sum_{j=1}^{m} w_j\, q_{ij}\cdot\alpha_{t_i}+\beta_{s_i}, \tag{1}$$

де w_p та w_j – ваги ймовірності та впливу на відповідні характеристики якості, α_{t_i} – коефіцієнт чутливості типу ІТ-продукту до конкретного ризику, β_{s_i} – коефіцієнт критичності фази життєвого циклу. Така форма дозволяє враховувати, що один і той самий ризик має різну вагу для, наприклад, хмарного сервісу та вбудованої системи, що становить методологічне розширення класичних моделей ризик-матриць.

Ієрархічна класифікація ризиків реалізується через побудову дерева кластерів у просторі ознак із використанням метрики подібності між ризиками

$$d(r_i,r_k)=\sqrt{\sum_{j=1}^{m}\gamma_j\,(q_{ij}-q_{kj})^2+\gamma_p(p_i-p_k)^2}, \tag{2}$$

де γ_j – коефіцієнти значущості відповідних вимірів. Отримана ієрархія дозволяє формувати багаторівневу структуру ризиків, у якій верхні рівні відповідають класам джерел загроз, а нижні – конкретним сценаріям їх прояву. На відміну від статичних таксономій, кластеризація виконується на основі фактичних значень метрик, що забезпечує адаптивність структури ризиків до контексту проєкту.

Для кількісної оцінки якості сформованої кластерної структури використано метрику silhouette, яка широко застосовується для аналізу результатів ієрархічної та агломеративної кластеризації. Значення коефіцієнта silhouette визначається як

$$S(i)=\frac{\big(b(i)-a(i)\big)}{max\big(a(i),b(i)\big)}, \tag{3}$$

де a(i) – середня відстань між об'єктом та іншими елементами власного кластера, а b(i) – мінімальна середня відстань між об'єктом та елементами найближчого сусіднього кластера. Значення коефіцієнта S знаходиться у діапазоні від -1 до 1 і відображає ступінь компактності та роздільності кластерів у просторі ознак.

Наукова новизна моделі полягає у поєднанні трьох аспектів, які раніше розглядалися ізольовано: формалізованого відображення артефактів процесу розробки у простір ризиків, багатокритеріальної пріоритезації з урахуванням типу ІТ-продукту та побудови адаптивної ієрархії ризиків на основі метричних даних. Запропонована інтегральна функція пріоритету забезпечує можливість кількісного порівняння ризиків

різної природи, а введення коефіцієнтів контекстної чутливості дозволяє узгодити модель із вимогами масштабування на різні класи програмних систем. Додатково, на відміну від експертно-орієнтованих підходів, модель забезпечує відтворюваність результатів завдяки використанню нормалізованих метрик якості та процесних індикаторів.

Із метою верифікації та експериментальної апробації запропонованої математичної моделі алгоритму ідентифікації, багатокритеріальної пріоритезації та ієрархічної класифікації ризиків забезпечення якості програмного забезпечення було розроблено програмний прототип системи підтримки прийняття рішень, реалізований мовою Python та орієнтований на обробку метричних даних про програмні модулі в контексті життєвого циклу розробки. Прототип реалізує повний цикл обчислювальних процедур, передбачених формалізованою моделлю, починаючи з формування векторного подання ризиків, продовжуючи оцінюванням імовірності дефектності як кількісного прояву ризику, обчисленням впливу ризиків на характеристики якості, визначенням інтегрального індексу пріоритету з урахуванням типу IT-продукту та завершуючи побудовою ієрархічної структури ризиків у просторі ознак. Така реалізація забезпечує відтворюваність результатів і дозволяє здійснювати масштабування моделі для різних класів програмних систем, що відповідає завданням експериментальної апробації в межах четвертого розділу дисертаційного дослідження.

Архітектурно програмний прототип побудовано за модульним принципом із виокремленням рівня роботи з даними, рівня математичних перетворень та рівня аналітичного узагальнення результатів (рис. 1).

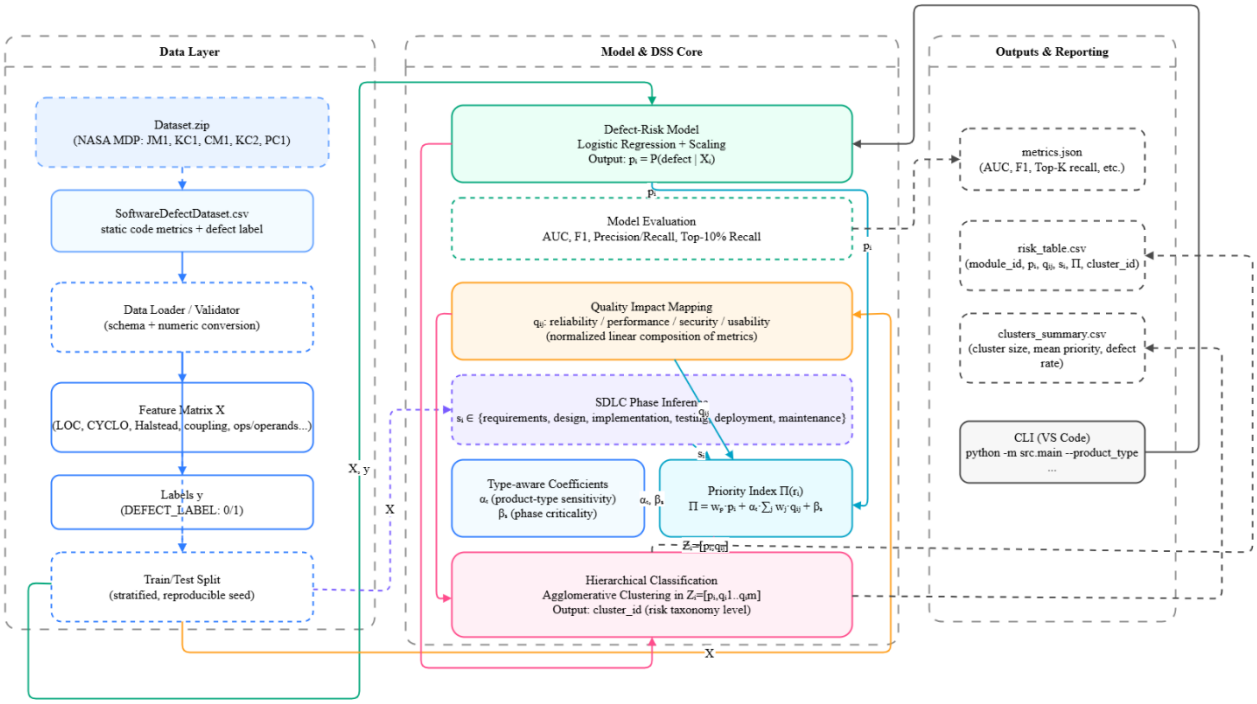

Рис. 1. Архітектура програмного прототипу (побудовано автором)

На першому етапі здійснюється завантаження та попередня обробка набору даних, приведення метричних ознак до числового формату та формування ідентифікаторів програмних модулів. Далі виконується навчання моделі прогнозування дефектності на основі логістичної регресії з балансуванням класів, що дозволяє отримати для кожного модуля оцінку імовірності виникнення дефекту, інтерпретовану як значення p_i у векторі ризику. Паралельно формується вектор впливу на характеристики якості q_{ij} , який обчислюється як нормалізована функція статичних метрик складності, розміру та зв'язності коду, що відображає потенційний вплив ризику на надійність, продуктивність, безпеку та зручність супроводу. Таким чином забезпечується перехід від сирих метричних даних до багатовимірного подання ризику, узгодженого з формалізованою моделлю.

На наступному етапі реалізується контекстно-орієнтована пріоритезація ризиків, у межах якої інтегральний індекс пріоритету обчислюється як зважена функція імовірності дефекту, агрегованого впливу на характеристики якості та коригувальних коефіцієнтів, що враховують тип IT-продукту та критичність фази життєвого циклу. Тип IT-продукту задається параметром запуску та визначає значення коефіцієнта чутливості до ризиків якості, що забезпечує адаптацію моделі до різних класів систем, зокрема хмарних сервісів, вбудованих рішень, фінтех-застосунків або систем із генеративним ШІ. Фаза життєвого циклу визначається на основі евристичного відображення метричних характеристик модулів на етапи SDLC, що дозволяє враховувати зміну критичності ризиків залежно від стадії розробки. Такий підхід забезпечує формалізоване поєднання структурних характеристик коду з процесними параметрами, що є необхідною умовою для кількісного ранжування ризиків у реальних проєктних середовищах.

Ієрархічна класифікація ризиків реалізована шляхом агломеративної кластеризації у просторі ознак, що

включає значення p_iта компоненти вектора q_{ij}. У результаті формується багаторівнева структура ризиків, у якій кожен кластер відповідає групі модулів із подібним профілем ризику та впливу на якість, що дозволяє переходити від аналізу окремих ризиків до узагальнених класів загроз. Додатково виконується агрегування статистик на рівні кластерів, що створює основу для подальшої інтерпретації ризиків як елементів таксономії та підтримує процес прийняття управлінських рішень. Результатом роботи програмного прототипу є таблиці з векторним поданням ризиків, значеннями інтегрального пріоритету та ідентифікаторами кластерів, а також набір метричних показників якості моделі прогнозування, що забезпечує можливість кількісної оцінки ефективності запропонованого підходу.

У дослідженні використано набір даних прогнозування дефектів програмного забезпечення, сформований на основі п’яти широко застосовуваних датасетів JM1, KC1, CM1, KC2 та PC1, отриманих у межах програми NASA Metrics Data Program. Дані містять статичні метричні характеристики реальних програмних модулів разом із бінарною ознакою наявності дефектів, що дозволяє інтерпретувати дефектність як кількісний прояв ризику якості. Кожен модуль описується набором інженерних метрик, зокрема кількістю рядків коду, цикломатичною складністю, показниками Halstead, коефіцієнтами зв’язності та кількістю операторів і операндів, які традиційно використовуються в дослідженнях прогнозування дефектів як індикатори якості програмного забезпечення. Застосування цього набору даних забезпечує емпіричну основу для побудови вектора ризику та дозволяє оцінити поведінку моделі на реальних програмних артефактах, що відповідає сучасним практикам експериментальної валідації в програмній інженерії [13].

У результаті експериментальної апробації програмного прототипу системи підтримки прийняття рішень отримано комплекс кількісних та структурних показників, що відображають ефективність запропонованої математичної моделі алгоритмічної ідентифікації, пріоритезації та ієрархічної класифікації ризиків якості програмного забезпечення. Насамперед проведено оцінювання здатності моделі відображати імовірність дефектності як формалізовану компоненту ризику. Значення площі під ROC-кривою становить 0,474, що свідчить про обмежену дискримінаційну здатність лише за рахунок статичних метрик коду та підтверджує складність задачі прогнозування дефектів у реальних умовах, однак при цьому модель зберігає монотонність ранжування ризиків, що є критично важливим для задач пріоритезації (рис. 2).

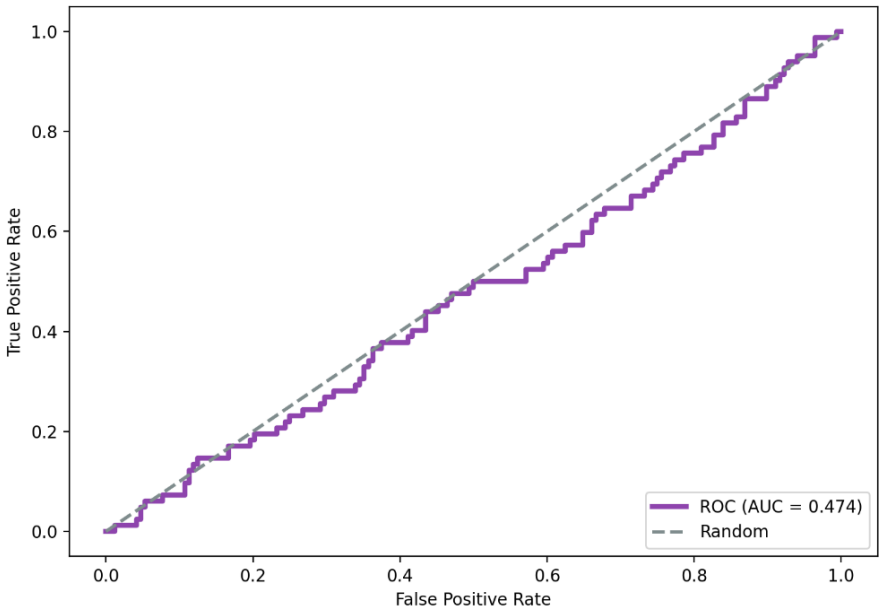

Рис. 2. ROC-крива моделі оцінювання ризику дефектності програмних модулів (побудовано авторським програмним забезпеченням)

Аналогічно крива точності–повноти демонструє значення середньої точності 0,318, що відповідає сценаріям з дисбалансом класів та підтверджує коректність інтерпретації дефектності як імовірнісної складової ризику, а не як жорсткого класифікаційного критерію (рис. 3).

Матриця помилок засвідчує переважання хибнопозитивних спрацювань над хибнонегативними, що у контексті управління ризиками є прийнятною стратегією, оскільки мінімізує ймовірність пропуску критичних дефектів та відповідає принципу превентивності ризик-менеджменту (рис. 4).

Таким чином, навіть за помірної класифікаційної точності модель забезпечує консервативну оцінку ризику, що є доцільним для систем забезпечення якості.

Аналіз коефіцієнтів логістичної регресії показує, що найбільший позитивний внесок у формування ризику мають показники складності керування потоком виконання та структурної розгалуженості, тоді як зростання обсягу коду та кількості операторів має негативний коефіцієнт, що узгоджується з припущенням про нормалізацію впливу метрик після масштабування та підтверджує інтерпретованість моделі у просторі факторів якості (рис. 5).

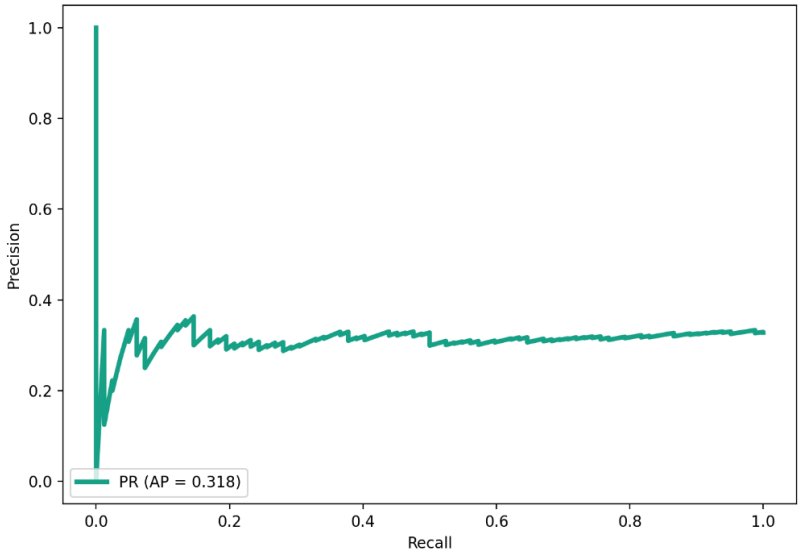

Рис. 3. Крива точності–повноти моделі оцінювання ризику дефектності (побудовано авторським програмним забезпеченням)

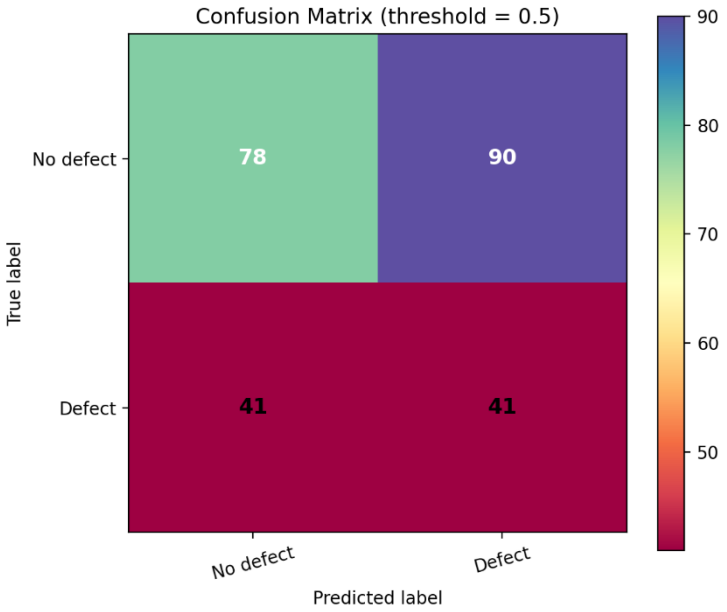

Рис. 4. Матриця помилок класифікації ризику дефектності (побудовано авторським програмним забезпеченням)

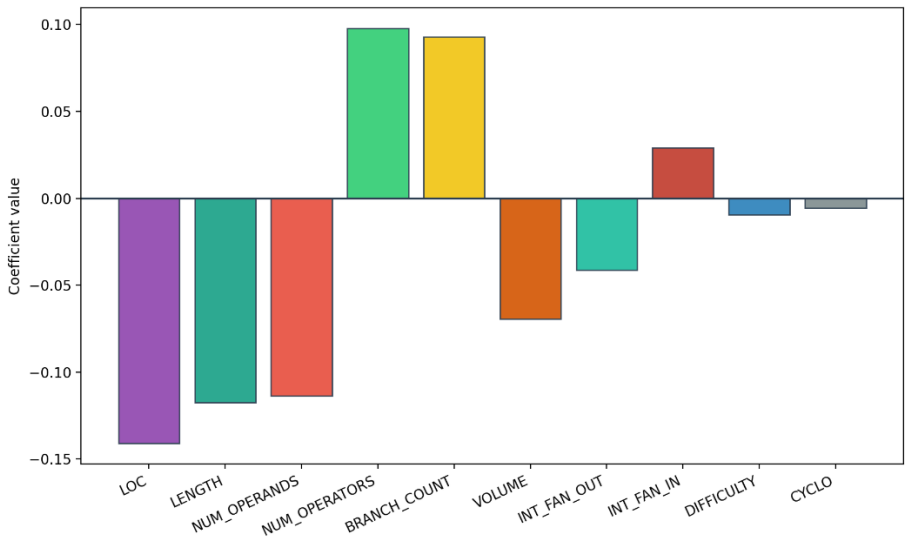

Рис. 5. Коефіцієнти моделі логістичної регресії для факторів ризику якості (побудовано авторським програмим забезеченням)

Це дозволяє використовувати отримані вагові коефіцієнти як кількісні індикатори джерел ризику на рівні програмних модулів.

Розподіл інтегрального індексу пріоритету характеризується близькою до нормальної формою з концентрацією значень у діапазоні 0,6-0,75, що свідчить про наявність чітко вираженої групи модулів із підвищеним ризиком та підтверджує можливість ранжування ризиків за кількісним критерієм (рис. 6).

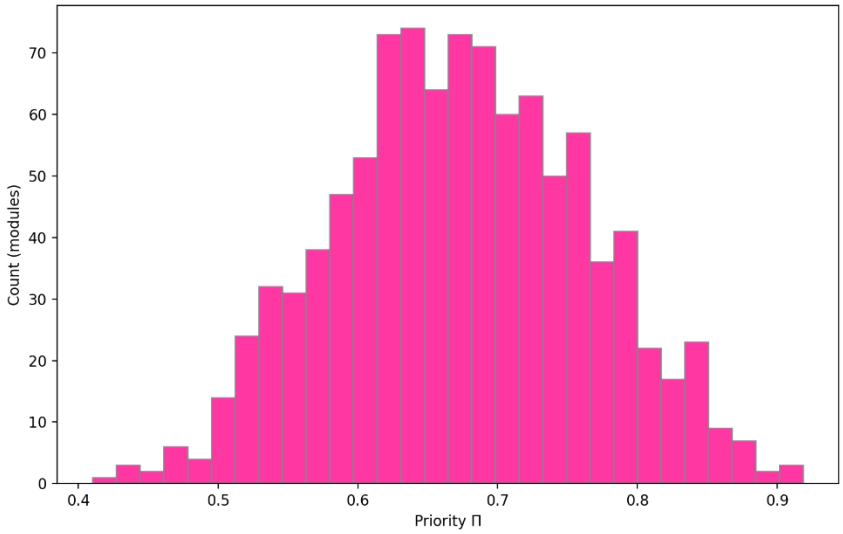

Рис. 6. Розподіл інтегрального індексу пріоритету ризику П (побудовано авторським програмним забезпеченням)

Додатково для оцінювання якості сформованої кластерної структури обчислено середнє значення коефіцієнта silhouette, яке становило 0.41, що свідчить про наявність помірно вираженої кластерної структури у просторі ризикових ознак та підтверджує коректність застосування агломеративної кластеризації для задачі ієрархічної класифікації ризиків.

При цьому діаграма розмаху за кластерами демонструє статистично значущі відмінності між групами ризиків, що підтверджує коректність побудованої ієрархічної таксономії та її здатність відображати різні профілі ризику (рис. 7).

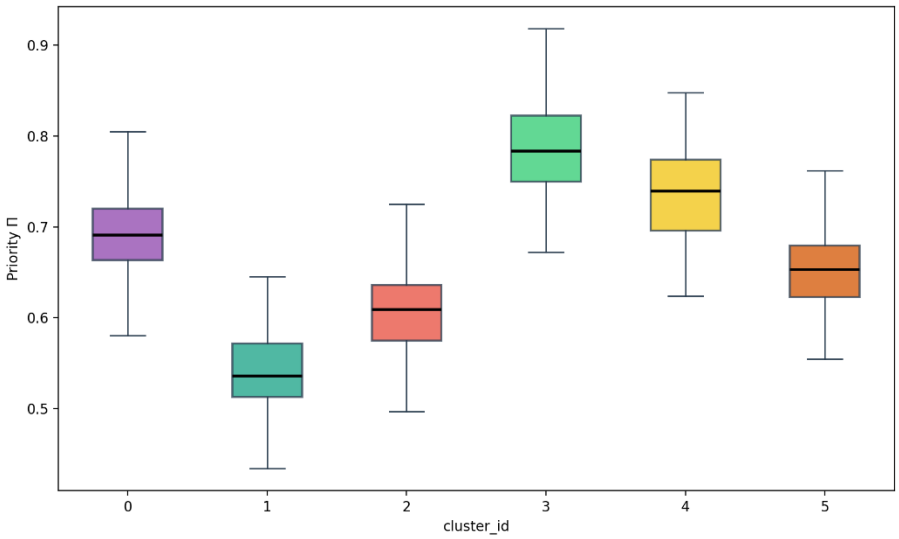

Рис. 7. Порівняльний аналіз індексу пріоритету за кластерами ризиків (побудовано авторським програмним забезпеченням)

У просторі ризику, сформованому осями імовірності дефекту та агрегованого впливу на характеристики якості, спостерігається чітка кластерна структура, що дозволяє виділити групи модулів із високою імовірністю дефектності та високим впливом на якість, які мають пріоритет у процесі управління (рис. 8).

Це підтверджує, що використання багатовимірного векторного подання ризику забезпечує більш інформативну сегментацію порівняно з традиційними матрицями ризику.

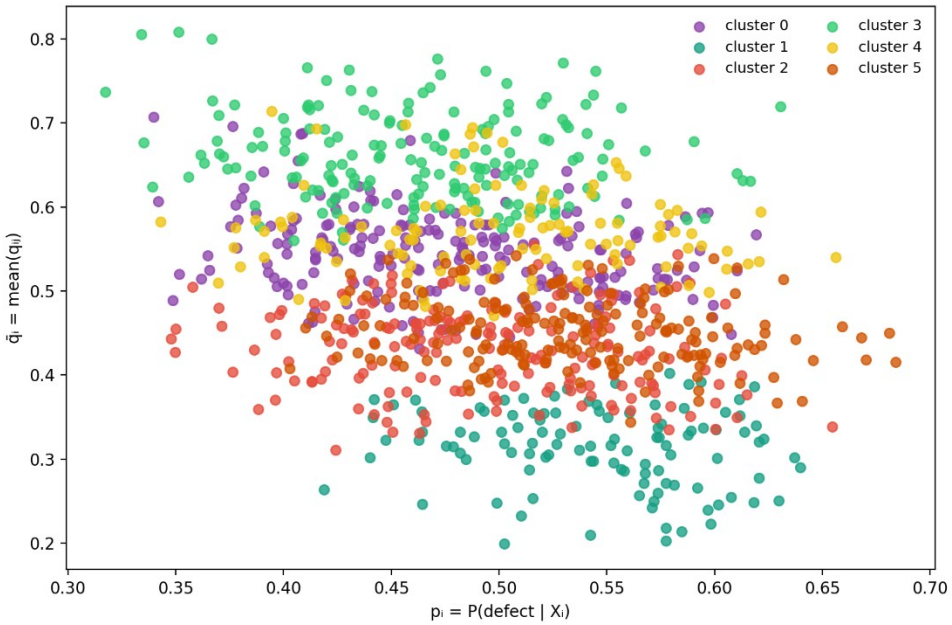

Рис. 8. Простір ризику у координатах імовірності дефекту та агрегованого впливу на якість (побудовано авторським програмним забезпеченням)

Профілі впливу на характеристики якості для кожного кластера демонструють різну конфігурацію домінуючих атрибутів, що дозволяє інтерпретувати кластери як типологічні класи ризиків, орієнтовані на різні аспекти якості, зокрема надійність, продуктивність або безпеку (рис. 9).

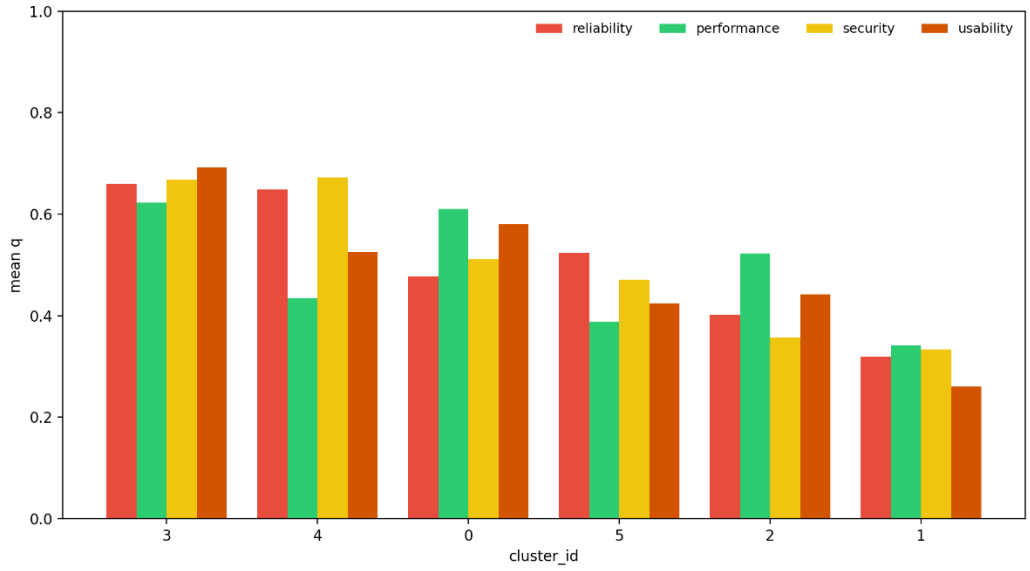

Рис. 9. Профілі впливу кластерів ризиків на характеристики якості програмного забезпечення (побудовано авторським програмним забезпеченням)

Це створює підґрунтя для адаптивного управління ризиками залежно від типу IT-продукту та його пріоритетних характеристик якості.

Отримані результати підтверджують досягнення мети дослідження, оскільки реалізовано формалізований алгоритм ідентифікації ризиків на основі метричних даних, забезпечено їх кількісну багатокритеріальну пріоритезацію з урахуванням контексту IT-продукту та побудовано ієрархічну класифікацію, що відображає структуру ризиків у просторі ознак. Запропонована модель є оптимальною у межах поставленої задачі, оскільки забезпечує поєднання інтерпретованості, кількісної відтворюваності та можливості масштабування на різні типи програмних систем, що недосяжно при використанні виключно експертних або однокритеріальних підходів.

З метою позиціонування запропонованого алгоритму в контексті сучасних підходів до управління ризиками програмного забезпечення виконано аналітичне порівняння з класичними експертно-орієнтованими моделями, методами машинного навчання та глибинного навчання. Класичні підходи, зокрема матриці ризику та AHP-моделі, забезпечують ієрархізацію ризиків на основі експертних оцінок, однак характеризуються обмеженою відтворюваністю результатів і відсутністю інтеграції з метричними даними програмних артефактів.

Методи машинного навчання, включаючи логістичну регресію, дерева рішень та ансамблеві моделі, орієнтовані переважно на прогнозування дефектності як бінарної або ймовірнісної змінної та не забезпечують багатокритеріального агрегування впливу ризику на різні характеристики якості. Підходи глибинного навчання, зокрема графові нейронні мережі та трансформерні моделі, демонструють високу точність у задачах класифікації змін або генерації обґрунтувальних схем, проте функціонують на рівні окремих типів ризиків і не формують узагальнену ієрархію ризиків, чутливу до типу ІТ-продукту та фази життєвого циклу.

На відміну від зазначених підходів, запропонований алгоритм реалізує композиційний пайплайн, що поєднує прогнозування дефектності, формування багатовимірного вектора ризику, обчислення інтегрального індексу пріоритету та агломеративну кластеризацію, забезпечуючи перехід від оцінки окремих модулів до побудови адаптивної таксономії ризиків. Використання нормалізованих метричних даних гарантує відтворюваність результатів, а введення контекстних коефіцієнтів типу ІТ-продукту дозволяє узгодити пріоритети ризиків із доменною специфікою систем. Таким чином, запропонований підхід займає проміжне положення між моделями прогнозування та експертними DSS-методами, забезпечуючи одночасно кількісну інтерпретованість, багатокритеріальність і ієрархічну структуру ризиків.

Порівняльну характеристику підходів наведено в табл. 1.

Таблиця 1

Порівняння підходів до ідентифікації та пріоритезації ризиків якості ПЗ

Критерій	**Класичні експертні моделі (матриці, AHP)**	**ML-моделі прогнозування дефектів**	**DL-підходи (GNN, LLM)**	**Запропонований алгоритм**
Джерело даних	Експертні оцінки	Статичні метрики коду	Код, графи залежностей, текстові артефакти	Метричні дані + контекст SDLC
Тип результату	Ранжування ризиків	Ймовірність дефекту	Класифікація змін або генерація знань	Інтегральний індекс пріоритету
Багатокритеріальність	Обмежена	Відсутня	Часткова	Повна
Урахування типу ІТ-продукту	Немає	Немає	Немає	Є
Ієрархічна структура ризиків	Статична	Немає	Немає	Адаптивна кластерна таксономія
Відтворюваність результатів	Низька	Висока	Висока	Висока
Інтерпретованість для DSS	Висока	Середня	Низька–середня	Висока

Примітка: побудовано автором

Отримані результати свідчать, що навіть за помірної точності прогнозування дефектності запропонований алгоритм забезпечує більш інформативну підтримку прийняття рішень порівняно з моделями, орієнтованими лише на класифікацію, оскільки дозволяє узгоджено враховувати імовірність, вплив та контекст ризику й формувати ієрархічну структуру загроз для різних типів ІТ-продуктів.

Висновки з даного дослідження
і перспективи подальших розвідок у даному напрямі

У роботі розроблено та експериментально апробовано формалізований алгоритм ідентифікації, багатокритеріальної пріоритезації та ієрархічної класифікації ризиків забезпечення якості програмного забезпечення з урахуванням типу ІТ-продукту, який реалізовано у вигляді програмного прототипу системи підтримки прийняття рішень і верифіковано на емпіричних метричних даних про програмні модулі. Запропонована математична модель забезпечує відображення артефактів процесу розробки у багатовимірний простір ризику, кількісне оцінювання імовірності дефектності як формалізованої компоненти ризику, агрегування впливу на характеристики якості та обчислення інтегрального індексу пріоритету з урахуванням контекстних коефіцієнтів типу ІТ-продукту та фази життєвого циклу. Отримані результати підтвердили можливість формування відтворюваної ієрархічної структури ризиків на основі метричних даних, що дозволяє переходити від аналізу окремих дефектів до узагальнених класів загроз і забезпечує кількісне ранжування ризиків за критерієм їх управлінської значущості. Встановлено, що навіть за помірної дискримінаційної здатності моделі прогнозування дефектності її використання в контексті багатокритеріальної пріоритезації забезпечує консервативну, превентивно орієнтовану оцінку ризиків, мінімізує ймовірність пропуску критичних дефектів і підвищує інформативність процесу прийняття рішень порівняно з традиційними експертними або однокритеріальними підходами. Кластеризація у просторі ознак підтвердила наявність типологічно різних профілів ризику, орієнтованих на окремі атрибути якості, що створює основу для адаптивного управління ризиками залежно від доменної специфіки та пріоритетів продукту. Кількісна оцінка якості кластеризації за допомогою коефіцієнта silhouette (0.41) підтвердила достатню роздільність сформованих груп ризику у просторі

ознак. Таким чином, досягнуто мету дослідження, оскільки забезпечено інтеграцію ідентифікації, пріоритезації та ієрархічної класифікації ризиків у єдину формалізовану процедуру з кількісно вимірюваними результатами, узгоджену з експериментальною апробацією четвертого розділу дисертації та придатну до масштабування на різні класи програмних систем.

Кількісна апробація моделі показала значення ROC-AUC = 0,474 та середньої точності PR-AUC = 0,318 для оцінювання імовірності дефектності, при цьому інтегральний індекс пріоритету П мав квазинормальний розподіл із концентрацією в інтервалі 0,6–0,75, а кластеризація забезпечила статистично значущу диференціацію профілів ризику за характеристиками якості, що підтверджує можливість кількісного ранжування та ієрархізації ризиків у межах запропонованого підходу.

Перспективи подальших досліджень пов'язані з розширенням моделі за рахунок інтеграції динамічних процесних метрик і часових характеристик, що дозволить реалізувати безперервний моніторинг ризиків у середовищах DevSecOps і MLOps, а також із включенням показників якості даних та поведінкових метрик користувачів для data-centric і генеративних IT-продуктів. Доцільним є застосування ансамблевих та байєсівських підходів для підвищення стійкості оцінювання імовірності дефектності, а також розроблення механізмів автоматичного налаштування вагових коефіцієнтів пріоритету на основі історичних даних про інциденти та ефективність заходів реагування. Подальшого розвитку потребує інтеграція онтологічних моделей ризику з метричною пріоритезацією, що забезпечить семантичну узгодженість таксономій ризиків у міждоменних середовищах, а також апробація моделі на промислових наборах даних із різних типів IT-продуктів для підтвердження її узагальнювальної здатності. Практично перспективним є впровадження розробленого алгоритму у корпоративні системи управління якістю та ризиками як модулю DSS, орієнтованого на підтримку стратегічного планування тестування, управління технічним боргом і оптимізацію ресурсів забезпечення якості в умовах багатокритеріальних обмежень.

Література

1. Minani, J. B., Fellah, Y. E., Sabir, F., Moha, N., Guéhéneuc, Y.-G., Kuradusenge, M., & Masuda, T. (2025). IoT systems testing: Taxonomy, empirical findings, and recommendations. Journal of Systems and Software, 226, 112408. https://doi.org/10.1016/j.jss.2025.112408

2. Yu, L., Alégroth, E., Chatzipetrou, P., & Gorschek, T. (2025). Measuring the quality of generative AI systems: Mapping metrics to quality characteristics – Snowballing literature review. Information and Software Technology, 186, 107802. https://doi.org/10.1016/j.infsof.2025.107802

3. Gentili, E., & Falessi, D. (2025). Practitioners' perceptions on requirements smells. Information and Software Technology, 187, 107823. https://doi.org/10.1016/j.infsof.2025.107823

4. Graetsch, U. M., Hoda, R., Khalajzadeh, H., Shahin, M., & Grundy, J. (2025). Managing technical debt in a multidisciplinary data intensive software team: An observational case study. Journal of Systems and Software, 230, 112546. https://doi.org/10.1016/j.jss.2025.112546

5. Akbar, M. A., Smolander, K., Mahmood, S., & Alsanad, A. (2022). Toward successful DevSecOps in software development organizations: A decision-making framework. Information and Software Technology, 147, 106894. https://doi.org/10.1016/j.infsof.2022.106894

6. Qazi, F., Kwak, D., Khan, F. G., Ali, F., & Khan, S. U. (2024). Service Level Agreement in cloud computing: Taxonomy, prospects, and challenges. Internet of Things, 25, 101126. https://doi.org/10.1016/j.iot.2024.101126

7. Shukla, A., Katt, B., Nweke, L. O., Yeng, P. K., & Weldehawaryat, G. K. (2022). System security assurance: A systematic literature review. Computer Science Review, 45, 100496. https://doi.org/10.1016/j.cosrev.2022.100496

8. Bernardo, B. M. V., Mamede, H. S., Barroso, J. M. P., & dos Santos, V. M. P. D. (2024). Data governance & quality management–Innovation and breakthroughs across different fields. Journal of Innovation & Knowledge, 9(4), 100598. https://doi.org/10.1016/j.jik.2024.100598

9. Tran-Truong, P. T., Pham, M. Q., Son, H. X., Nguyen, D. L. T., Nguyen, M. B., Tran, K. L., Van, L. C. P., Le, K. T., Vo, K. H., Kim, N. N. T., Nguyen, T. M., & Nguyen, A. T. (2025). A systematic review of multi-factor authentication in digital payment systems: NIST standards alignment and industry implementation analysis. Journal of Systems Architecture, 162, 103402. https://doi.org/10.1016/j.sysarc.2025.103402

10. Benmalek, M. (2024). Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges. Internet of Things and Cyber-Physical Systems, 4, 186–202. https://doi.org/10.1016/j.iotcps.2023.12.001

11. Suomalainen, J., Ahmad, I., Shajan, A., & Savunen, T. (2025). Cybersecurity for tactical 6G networks: Threats, architecture, and intelligence. Future Generation Computer Systems, 162, 107500. https://doi.org/10.1016/j.future.2024.107500

12. Ben Amara, O., De Nicola, A., Kamissoko, D., Bénaben, F., & Fijalkow, Y. (2025). Ontological framework for horizon scanning of business continuity of essential services. International Journal of Disaster Risk Reduction, 124, 105526. https://doi.org/10.1016/j.ijdrr.2025.105526

13. Software Defect Prediction Dataset. (б. д.). Kaggle: Your Machine Learning and Data Science Community. https://www.kaggle.com/datasets/ziya07/software-defect-prediction-dataset

References

1. Minani, J. B., Fellah, Y. E., Sabir, F., Moha, N., Guéhéneuc, Y.-G., Kuradusenge, M., & Masuda, T. (2025). IoT systems testing: Taxonomy, empirical findings, and recommendations. Journal of Systems and Software, 226, 112408. https://doi.org/10.1016/j.jss.2025.112408

2. Yu, L., Alégroth, E., Chatzipetrou, P., & Gorschek, T. (2025). Measuring the quality of generative AI systems: Mapping metrics to quality characteristics – Snowballing literature review. Information and Software Technology, 186, 107802. https://doi.org/10.1016/j.infsof.2025.107802

3. Gentili, E., & Falessi, D. (2025). Practitioners' perceptions on requirements smells. Information and Software Technology, 187, 107823. https://doi.org/10.1016/j.infsof.2025.107823

4. Graetsch, U. M., Hoda, R., Khalajzadeh, H., Shahin, M., & Grundy, J. (2025). Managing technical debt in a multidisciplinary data intensive software team: An observational case study. Journal of Systems and Software, 230, 112546. https://doi.org/10.1016/j.jss.2025.112546

5. Akbar, M. A., Smolander, K., Mahmood, S., & Alsanad, A. (2022). Toward successful DevSecOps in software development organizations: A decision-making framework. Information and Software Technology, 147, 106894. https://doi.org/10.1016/j.infsof.2022.106894

6. Qazi, F., Kwak, D., Khan, F. G., Ali, F., & Khan, S. U. (2024). Service Level Agreement in cloud computing: Taxonomy, prospects, and challenges. Internet of Things, 25, 101126. https://doi.org/10.1016/j.iot.2024.101126

7. Shukla, A., Katt, B., Nweke, L. O., Yeng, P. K., & Weldehawaryat, G. K. (2022). System security assurance: A systematic literature review. Computer Science Review, 45, 100496. https://doi.org/10.1016/j.cosrev.2022.100496

8. Bernardo, B. M. V., Mamede, H. S., Barroso, J. M. P., & dos Santos, V. M. P. D. (2024). Data governance & quality management–Innovation and breakthroughs across different fields. Journal of Innovation & Knowledge, 9(4), 100598. https://doi.org/10.1016/j.jik.2024.100598

9. Tran-Truong, P. T., Pham, M. Q., Son, H. X., Nguyen, D. L. T., Nguyen, M. B., Tran, K. L., Van, L. C. P., Le, K. T., Vo, K. H., Kim, N. N. T., Nguyen, T. M., & Nguyen, A. T. (2025). A systematic review of multi-factor authentication in digital payment systems: NIST standards alignment and industry implementation analysis. Journal of Systems Architecture, 162, 103402. https://doi.org/10.1016/j.sysarc.2025.103402

10. Benmalek, M. (2024). Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges. Internet of Things and Cyber-Physical Systems, 4, 186–202. https://doi.org/10.1016/j.iotcps.2023.12.001

11. Suomalainen, J., Ahmad, I., Shajan, A., & Savunen, T. (2025). Cybersecurity for tactical 6G networks: Threats, architecture, and intelligence. Future Generation Computer Systems, 162, 107500. https://doi.org/10.1016/j.future.2024.107500

12. Ben Amara, O., De Nicola, A., Kamissoko, D., Bénaben, F., & Fijalkow, Y. (2025). Ontological framework for horizon scanning of business continuity of essential services. International Journal of Disaster Risk Reduction, 124, 105526. https://doi.org/10.1016/j.ijdrr.2025.105526

13. Software Defect Prediction Dataset. (б. д.). Kaggle: Your Machine Learning and Data Science Community. https://www.kaggle.com/datasets/ziya07/software-defect-prediction-dataset