https://doi.org/10.31891/2307-5732-2025-359-97
УДК 004.94:004.85:004.415.2

**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

# ГІБРИДНА МОДЕЛЬ ПРОГНОЗУВАННЯ ТА МОНІТОРИНГУ РИЗИКІВ З ВИКОРИСТАННЯМ ML ТА ЕКСПЕРТНИХ ПРАВИЛ

*Стрімке поширення DevOps- і MLOps-практик, інтенсивне використання генеративного ШІ та зростаюча складність програмних екосистем радикально змінюють характер ризиків у процесі життєвого циклу програмного забезпечення. Традиційні методи управління ризиками, що ґрунтуються на статичних оцінках або ручному аналізі, виявляються недостатніми для роботи в умовах динамічного середовища, де ризики виникають одночасно на рівні коду, архітектури, процесів CI/CD, даних і людських факторів. У цій роботі запропоновано гібридну модель прогнозування та моніторингу ризиків, яка поєднує алгоритми машинного навчання, історичні дані проєктів, сигнали з конвеєрів CI/CD та експертні правила для формування адаптивного ризик-профілю. Модель функціонує як безперервний цикл, що охоплює ідентифікацію, оцінювання, прогнозування, реагування та моніторинг ризиків, забезпечуючи постійне оновлення профілю загроз у режимі, близькому до реального часу. Запропоноване рішення реалізовано у вигляді тримодульної архітектури, яка включає збір і підготовку даних, ансамблеве прогнозування ризиків за допомогою моделей градієнтного бустингу та випадкових лісів, а також систему нечіткої логіки для контекстного коригування прогнозів. Експериментальна перевірка, проведена на основі понад 50 реальних проєктів, продемонструвала високу точність прогнозування та здатність моделі своєчасно виявляти пікові точки ризику. Теплова карта динаміки ризиків підтвердила її ефективність у відстеженні змін у ключових категоріях, зокрема стабільності збірок, вразливостей, дефектності коду та продуктивності сервісів. Результати дослідження засвідчили, що поєднання машинного навчання з експертними знаннями значно підвищує точність, адаптивність і пояснюваність рішень, створюючи підґрунтя для впровадження інтелектуальних систем управління ризиками у складних середовищах розробки. Отримані результати можуть бути використані для автоматизації управління якістю IT-продуктів, підвищення стійкості DevSecOps-процесів та підтримки прийняття стратегічних рішень на рівні організації.*

***Ключові слова:*** *управління ризиками, машинне навчання, DevOps, CI/CD, експертні системи, прогнозування ризиків.*

**YURII KISH**
**LIAKH IHOR**
Uzhhorod National University

## HYBRID MODEL OF RISK FORECASTING AND MONITORING USING ML AND EXPERT RULES

*The rapid spread of DevOps and MLOps practices, the intensive use of generative AI, and the growing complexity of software ecosystems are radically changing the nature of risks in the software lifecycle. Traditional methods of risk management, based on static assessments or manual analysis, turn out to be insufficient to work in a dynamic environment, where risks arise simultaneously at the level of code, architecture, CI/CD processes, data and human factors. This paper proposes a hybrid model of risk forecasting and monitoring, which combines machine learning algorithms, historical project data, signals from CI/CD pipelines, and expert rules for the formation of an adaptive risk profile. The model functions as a continuous loop encompassing risk identification, assessment, forecasting, response, and monitoring, providing a continuous update of the threat profile in near real-time. The proposed solution is implemented in the form of a three-module architecture, which includes data collection and preparation, ensemble risk forecasting using gradient boosting and random forest models, as well as a fuzzy logic system for contextual forecast adjustment. Experimental verification based on more than 50 real-world projects demonstrated high forecasting accuracy and the model's ability to identify peak risk points in a timely manner. The Risk Dynamics Heatmap confirmed its effectiveness in tracking changes in key categories, including build stability, vulnerabilities, code defects, and service performance. The results of the study showed that the combination of machine learning with expert knowledge significantly increases the accuracy, adaptability and explainability of solutions, creating the basis for the implementation of intelligent risk management systems in complex development environments. The results obtained can be used to automate the quality management of IT products, increase the resilience of DevSecOps processes, and support strategic decision-making at the organizational level.*

***Keywords:*** *risk management, machine learning, DevOps, CI/CD, expert systems, risk forecasting.*

Стаття надійшла до редакції / Received 30.10.2025
Прийнята до друку / Accepted 15.11.2025

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

Цифровізація життєвого циклу ПЗ, поширення DevOps/MLOps-практик (підходів до безперервної розробки та експлуатації програмного забезпечення й моделей машинного навчання) та інтенсивне використання генеративних моделей створюють нову конфігурацію ризиків, що виникають одночасно на рівні процесів, архітектури, даних і людських факторів. Емпіричні дослідження демонструють, що борги процесів в agile-командах знижують задоволеність роботою та опосередковано погіршують якість, що підвищує ймовірність відмов і дефектів [1].

В умовах розподіленої та хмарної розробки зростає значущість автоматизованого розподілу задач, безперервного моніторингу, а також інтегрованої безпеки (DevSecOps), які мають вплив на ризик-профіль проєкту вже на рівні CI/CD-конвеєрів [3].

Паралельно швидке впровадження генеративного ШІ у виробничі процеси породжує специфічні кіберризики — отруєння даних, витоки конфіденційної інформації, упередженість — які потребують даних з

телеметрії та артефактів CI/CD (набір практик автоматизації, що включає безперервну інтеграцію коду та його автоматичне постачання або розгортання) для своєчасного виявлення і реагування [13].

Попри прогрес у точкових напрямах — дефектопрогнозуванні, автоматизації забезпечення якості, методах пояснюваного ШІ для ризик-оцінювання — все ще відсутні практики, які б системно поєднували історичні дані проєктів, сигнали з CI/CD і експертні правила у єдину гібридну модель, що безперервно оновлює ризик-профіль. Отже, наукова проблема полягає у створенні відтворюваної гібридної моделі прогнозування та моніторингу ризиків, яка інтегрує машинне навчання з доменними правилами та забезпечує операційне вбудовування у CI/CD-процеси, зберігаючи інтерпретованість результатів для менеджерів і команд.

**Аналіз досліджень та публікацій**

У сучасних дослідженнях управління ризиками програмних проєктів спостерігається зміщення акценту від реактивних методів до проактивних, які поєднують автоматизовану аналітику, машинне навчання та експертні знання. Ця еволюція зумовлена зростаючою складністю IT-середовищ, високими вимогами до надійності та швидким темпом змін у DevOps/DevSecOps-практиках. Наукова література демонструє різні підходи до вирішення цих завдань, які утворюють методологічне підґрунтя для побудови гібридних моделей прогнозування ризиків.

Одним із ключових напрямів стала оцінка організаційних факторів як джерела ризику. Gustavsson із колегами показали, що накопичення «процесного боргу» — сукупності неефективних процесів, неформалізованих практик та невирішених технічних питань — суттєво впливало на задоволеність команд і якість кінцевого продукту [1]. Такий підхід дав підстави розглядати не лише технічні, а й соціотехнічні показники як критично важливі для прогнозування ризиків. У подібному контексті Lesum та співавтори довели, що чітко структуроване управління, посилене лідерською роллю керівництва, знижувало негативний вплив ризикових факторів і сприяло стабільності проєктного виконання [2].

Операційні ризики, пов'язані з розподілом навантаження, були предметом дослідження Al-Fraihat із колегами. Вони продемонстрували, що застосування алгоритмів машинного навчання для автоматичного розподілу завдань підвищувало ефективність роботи команд і зменшувало кількість критичних збоїв [3]. Цей висновок підтвердив потенціал використання поведінкових даних проєктів як предикторів ризику. У свою чергу, Odu та його команда розробили метод автоматичного формування «assurance cases» за допомогою великих мовних моделей, що дозволило значно скоротити кількість помилок і підвищити якість процесів верифікації [4].

Значний внесок у розуміння процесів оцінювання безпеки зробили Rosado зі співавторами, які представили фреймворк MARISMA-BP, що інтегрував ризик-менеджмент у бізнес-процеси й забезпечував повторне використання ризикових моделей у різних проєктах [5]. Подальші дослідження Zhao та колег деталізували ключові виміри DevSecOps, окресливши такі аспекти, як процеси, команди, інструментарій і спостережуваність, як базові для побудови безперервних моделей оцінювання ризиків [6]. Систематичний огляд Saeed із колегами узагальнив техніки інтеграції безпеки на різних стадіях життєвого циклу ПЗ, довівши ефективність раннього впровадження контролів і стандартів для зменшення ризиків [7].

Подальші розробки у сфері автоматизації управління ризиками включали архітектуру «resilient cloud cluster», запропоновану Alghawli та співавторами, яка забезпечувала безперервний аналіз даних, виявлення вразливостей і розрахунок ризиків у хмарних середовищах [8]. Паралельно Scommegna із колегами створили систему OREO, яка локалізувала ланцюги fault–error–failure у програмних системах і забезпечувала раннє виявлення критичних станів [9]. В аспекті аналітичної оптимізації Qiu та співавтори розробили метод відбору ознак для прогнозування дефектів, який підвищував точність моделей та знижував обсяг необхідних даних [10].

Окрему увагу дослідники приділили питанням пояснюваності рішень. Badhon та його команда створили пояснюваний AI-фреймворк IRAF-BRB, який не лише підвищував точність прогнозів, але й забезпечував прозорість прийняття рішень [11]. Boamah із колегами продемонстрували ефективність використання історичних даних для побудови моделей автоматизованого виявлення ризиків у великих інфраструктурних проєктах [12], тоді як Mohawesh зі співавторами дослідили виклики, пов'язані з ризиками від генеративного ШІ, і запропонували підходи для їх раннього виявлення та пом'якшення [13].

Ширший огляд стану галузі представили Tian із колегами, які провели бібліометричний аналіз застосування ШІ в управлінні ризиками будівельних проєктів і виявили зростаючу тенденцію до міждисциплінарних підходів та стандартизації даних [14]. Нарешті, Warnett та його команда запропонували модель-керований підхід до оцінювання нефункціональних характеристик архітектур MLOps, який забезпечував інтегроване управління ризиками на рівні CI/CD-конвеєра [15].

Сукупно проаналізовані дослідження продемонстрували логічну еволюцію від ізольованих моделей до комплексних систем, які використовують історичні дані, експертні правила, машинне навчання та автоматизовану аналітику для побудови динамічних ризик-профілів. Результати вказують на необхідність гібридних підходів, здатних не лише виявляти загрози, а й адаптуватися до мінливого середовища розробки програмного забезпечення.

**Формулювання цілей статті**

**Метою роботи є:** розробка гібридної моделі прогнозування та моніторингу ризиків, що поєднує алгоритми машинного навчання, історичні дані проєктів, сигнали з конвеєрів CI/CD та експертні правила для формування адаптивного ризик-профілю у процесі життєвого циклу програмного забезпечення. Модель має забезпечити безперервне оновлення ризиків у режимі, близькому до реального часу, підвищити точність,

інтерпретованість і гнучкість оцінювання, а також створити основу для інтелектуалізації управління якістю IT-продуктів у DevOps/MLOps-середовищах.

**Виклад основного матеріалу**

Розроблена гібридна модель прогнозування та моніторингу ризиків базується на інтеграції алгоритмів машинного навчання з експертними правилами для забезпечення динамічного оновлення ризик-профілю впродовж життєвого циклу програмного продукту. Концепція моделі ґрунтується на припущенні, що точність оцінки ризиків істотно підвищується за умов комбінування кількісних характеристик із процесів CI/CD, історичних даних про завершені проєкти та якісних експертних оцінок, що враховують контекстні фактори середовища розробки.

Логіка роботи запропонованої системи наведена на рис. 1.

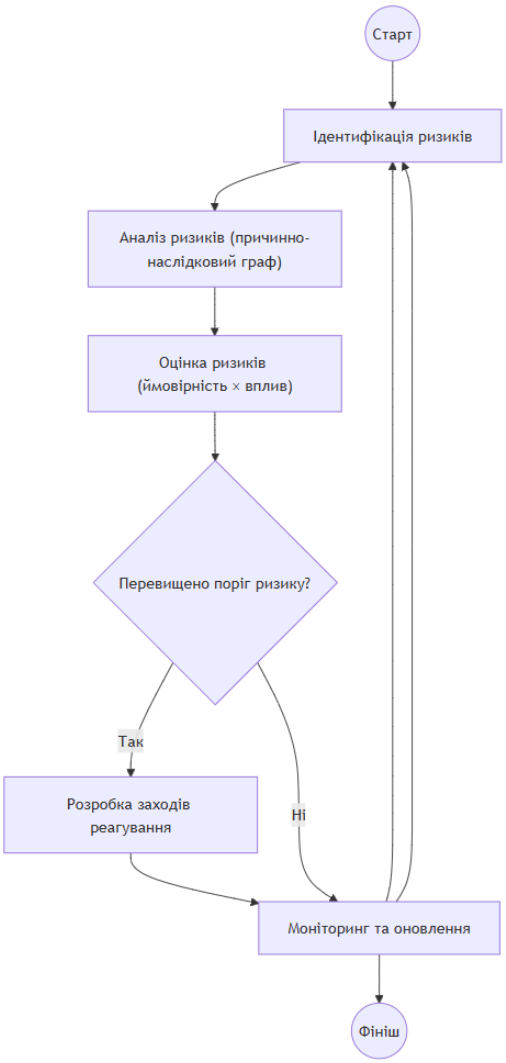


**Рис. 1. Логічна схема гібридної моделі прогнозування та моніторингу ризиків у процесі життєвого циклу IT-проєкту (розроблено автором)**

Модель функціонує як циклічний процес, що починається з етапу ідентифікації ризиків, на якому здійснюється збір первинної інформації з історичних даних проєктів, метрик CI/CD та експертних оцінок. Далі відбувається їх аналітична обробка у вигляді побудови причинно-наслідкових зв'язків, що дозволяє виявити не лише окремі фактори ризику, а й системні залежності між ними. На основі сформованої моделі виконується оцінка ризиків за критерієм добутку ймовірності на очікуваний вплив, що забезпечує кількісну основу для подальшого прийняття рішень.

Після розрахунку інтегрального показника відбувається перевірка на відповідність встановленому пороговому значенню ризику. Якщо воно перевищене, система ініціює етап розробки заходів реагування, який може включати технічні, організаційні або процесні дії для зменшення потенційного впливу. Якщо поріг не досягнуто, процес переходить безпосередньо до стадії моніторингу та оновлення. На цьому етапі реалізується адаптивний механізм спостереження за змінами в середовищі проєкту, який постійно оновлює ризик-профіль і, за необхідності, повертає систему до етапу ідентифікації для повторного циклу аналізу. Такий підхід забезпечує безперервність управління ризиками та дозволяє оперативно реагувати на нові загрози, що з'являються у процесі життєвого циклу ПЗ.

Архітектура експериментальної системи передбачає три взаємопов'язані модулі. Перший відповідає за збір і попередню обробку даних з різних джерел: історичних звітів про проєкти, репозиторіїв контролю версій, систем безперервної інтеграції (CI/CD) та експертних матриць ризиків. На цьому етапі застосовуються методи нормалізації та фільтрації для усунення аномалій, а також процедури синхронізації часових рядів.

Другий модуль реалізує модель машинного навчання для прогнозування рівня ризиків. Навчальна вибірка формується з векторів ознак, до складу яких входять: показники стабільності збірок, частота дефектів, тривалість циклів тестування, коефіцієнти виконання вимог, історичні прецеденти критичних інцидентів та суб'єктивні оцінки впливу з боку експертів. Для підвищення точності прогнозування використовується ансамбль моделей, що поєднує алгоритми градієнтного бустингу та випадкових лісів, тоді як узгодження результатів здійснюється через механізм голосування з вагами, які оптимізуються за допомогою крос-валідації.

Формально задачу прогнозування можна подати як оцінювання ризику R для проєкту p у момент часу t:

$$R_{p,t} = \sum_{i=1}^{n} w_i \cdot f_i(x_{p,t}), \quad (1)$$

де $f_i(x_{p,t})$ — нормалізовані предиктори ризику, отримані з різних джерел даних, $w_i$ — вагові коефіцієнти, визначені під час навчання моделі, $n$— кількість предикторів.

Третій модуль реалізує механізм експертних правил, які дозволяють скоригувати прогнозовані значення ризику відповідно до контекстних факторів, що не можуть бути формалізовані у вигляді вхідних ознак. Для цього застосовується система нечіткої логіки.

Ці правила не лише підвищують інтерпретованість моделі, але й забезпечують адаптивність оцінки у випадках появи нових факторів або змін у середовищі розробки.

Оновлення ризик-профілю здійснюється в режимі реального часу шляхом періодичного перерахунку функції ризику з урахуванням нових даних та результатів експертного аналізу. Для врахування часової динаміки вводиться коефіцієнт згладжування $\alpha$, який забезпечує баланс між історичними даними та актуальними значеннями:

$$R_{p,t}^{new} = \alpha R_{p,t}^{pred} + (1-\alpha) R_{p,t-1} \quad (2)$$

де $R_{p,t}^{pred}$— прогнозована оцінка ризику, $R_{p,t-1}$— значення ризику з попереднього циклу моніторингу.

Експеримент проводився на основі даних з понад 50 завершених проєктів середнього та великого масштабу, включаючи інформацію про понад 10 000 збірок, 250 000 комітів та понад 1 000 експертних оцінок ризиків. Навчання моделі виконувалося за принципом стратифікованої крос-валідації з використанням метрик точності (Precision), повноти (Recall), F1-міри та середньоквадратичної помилки (RMSE) для прогнозів рівня ризику.

На рис. 2 подано візуалізацію результатів роботи гібридної моделі прогнозування та моніторингу ризиків у форматі теплової карти, яка відображає зміну рівня ризику для восьми ключових категорій упродовж дванадцяти ітерацій проєкту.

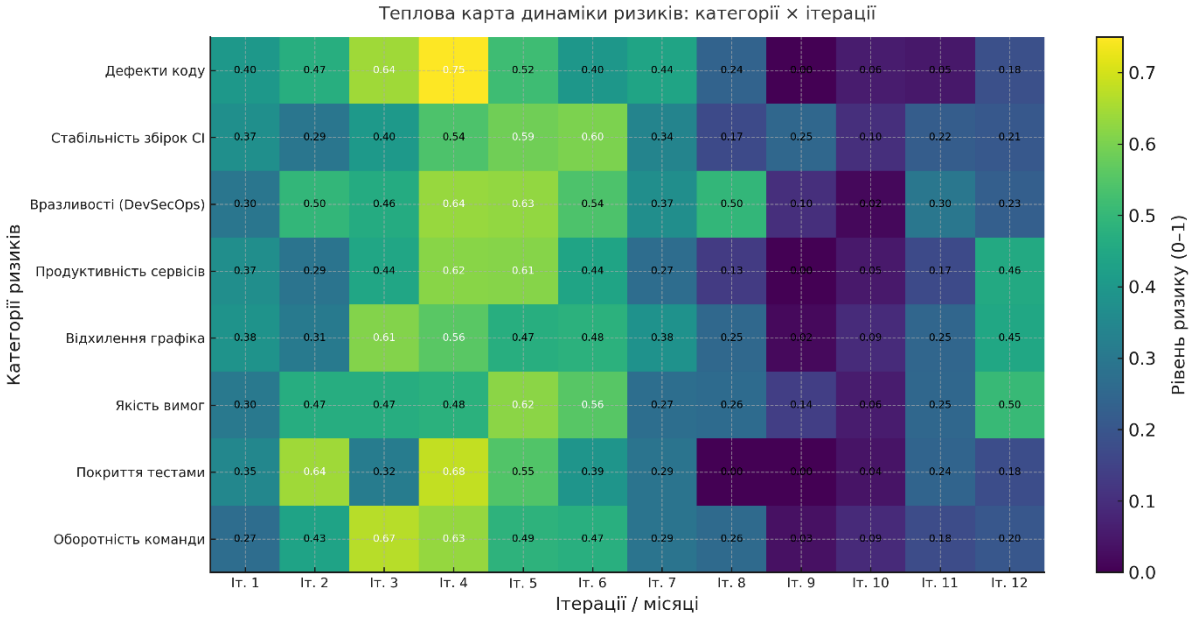


**Рис. 2. Теплова карта динаміки ризиків у процесі життєвого циклу проєкту (побудовано програмним забезпеченням, розробленим автором)**

Вісь ординат ілюструє групи ризиків, що мають критичний вплив на якість IT-продукту: дефекти коду, стабільність збірок CI, вразливості в контексті DevSecOps, продуктивність сервісів, відхилення графіка, якість вимог, покриття тестами та оборотність команди. Вісь абсцис відповідає часовій шкалі виконання проєкту, розбитій на окремі ітерації (місяці або спринти).

Інтенсивність кольору на тепловій карті відображає значення інтегрального ризику в діапазоні від 0 до 1, де темніші тони відповідають нижчому рівню ризику, а світліші — вищому. У першій третині життєвого циклу спостерігається помірний рівень ризику, пов'язаний переважно з нестабільністю збірок та недостатньою деталізацією вимог. У середній фазі проєкту модель фіксує суттєве зростання ризиків у категоріях «Вразливості (DevSecOps)» та «Стабільність збірок CI», що зумовлено підвищенням складності інтеграційних процесів, активізацією процесів релізингу та збільшенням обсягів коду. Водночас у цей період спостерігається короткочасне зростання ризику відхилення графіка через зростання залежностей між підсистемами.

У завершальній частині життєвого циклу ризик поступово знижується в більшості категорій, зокрема для «Дефектів коду» та «Покриття тестами», що свідчить про стабілізацію процесів контролю якості та підвищення ефективності автоматизованого тестування. Помітне зменшення ризику «Оборотності команди» на пізніх етапах пояснюється завершенням фази інтенсивного розширення команди та переходом до стабільної структури проєктної групи. Така динаміка підтверджує ефективність запропонованої гібридної моделі, яка здатна своєчасно виявляти пікові точки ризику та адаптивно оновлювати профіль загроз на основі поєднання машинного навчання з експертними правилами.

## Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

Результати проведеного дослідження засвідчили ефективність гібридного підходу до прогнозування та моніторингу ризиків, який поєднує машинне навчання, експертні правила та багатоджерельну аналітику. Така інтеграція дозволила побудувати модель, здатну адаптивно реагувати на динаміку середовища розробки, виявляти критичні точки ризику на ранніх етапах життєвого циклу та оновлювати ризик-профіль у режимі, близькому до реального часу. На відміну від традиційних підходів, які часто базуються на статичних оцінках і не враховують контекстуальних змін, запропонована система демонструє гнучкість і підвищену точність, що робить її придатною для впровадження у складних DevOps та MLOps середовищах.

Важливим результатом стало підтвердження доцільності використання ансамблевих моделей машинного навчання в поєднанні з експертними правилами нечіткої логіки. Такий підхід забезпечує не лише точність прогнозів, але й їхню інтерпретованість, що є критично важливим для прийняття управлінських рішень. Додатковою перевагою системи є її здатність інтегруватися у процеси CI/CD без істотних змін інфраструктури, що значно знижує бар'єр впровадження у реальні проєкти.

Перспективи подальших досліджень пов'язані з розширенням функціональності моделі у кількох напрямах. По-перше, доцільним є інтеграція методів причинно-наслідкового аналізу для підвищення здатності системи не лише фіксувати ризики, але й виявляти їх джерела та прогнозувати вторинні ефекти. По-друге, важливо дослідити потенціал гібридної моделі у контексті багатопроєктного управління, де ризики можуть мати взаємний вплив і кумулятивний ефект. По-третє, подальша робота може бути спрямована на розроблення пояснюваних інтерфейсів взаємодії зі штучним інтелектом, що забезпечать прозорість і довіру з боку користувачів та підвищать цінність моделі для прийняття стратегічних рішень.

## Література

1. Gustavsson T. Job Satisfaction at Risk: Measuring the Role of Process Debt in Agile Software Development [Електронний ресурс] / Tomas Gustavsson, Muhammad Ovais Ahmad, Hina Saeeda // Journal of Systems and Software. – 2025. – С. 112350. – Режим доступу: https://doi.org/10.1016/j.jss.2025.112350.

2. Project Governance to Improve the Performance of Software Projects by Mitigating the Software Risk Factors: The Moderating Role of Project Leadership [Електронний ресурс] / Samiul Alim Lesum [та ін.] // Procedia Computer Science. – 2024. – Т. 239. – С. 1863–1870. – Режим доступу: https://doi.org/10.1016/j.procs.2024.06.368/.

3. Utilizing Machine Learning Algorithms for Task Allocation in Distributed Agile Software Development [Електронний ресурс] / Dimah Al-Fraihat [та ін.] // Heliyon. – 2024. – С. e39926. – Режим доступу: https://doi.org/10.1016/j.heliyon.2024.e39926.

4. Automatic instantiation of assurance cases from patterns using large language models [Електронний ресурс] / Oluwafemi Odu [та ін.] // Journal of Systems and Software. – 2025. – Т. 222. – С. 112353. – Режим доступу: https://doi.org/10.1016/j.jss.2025.112353.

5. Enabling security risk assessment and management for business process models [Електронний ресурс] / David G. Rosado [та ін.] // Journal of Information Security and Applications. – 2024. – Т. 84. – С. 103829. – Режим доступу: https://doi.org/10.1016/j.jisa.2024.103829.

6. Zhao X. Identifying the primary dimensions of DevSecOps: A multi-vocal literature review [Електронний ресурс] / Xiaofan Zhao, Tony Clear, Ramesh Lal // Journal of Systems and Software. – 2024. – С. 112063. – Режим доступу: https://doi.org/10.1016/j.jss.2024.112063.

7. Review of Techniques for Integrating Security in Software Development Lifecycle [Електронний ресурс] / Hassan Saeed [та ін.] // Computers, Materials & Continua. – 2024. – С. 1–10. – Режим доступу: https://doi.org/10.32604/cmc.2024.057587.

8. Alghawli A. S. A. Resilient cloud cluster with DevSecOps security model, automates a data analysis, vulnerability search and risk calculation [Електронний ресурс] / Abed Saif Ahmed Alghawli, Tamara Radivilova // Alexandria Engineering Journal. – 2024. – Т. 107. – С. 136–149. – Режим доступу: https://doi.org/10.1016/j.aej.2024.07.036.

9. OREO: A tool-supported approach for offline run-time monitoring and fault-error-failure chain localization [Електронний ресурс] / Leonardo Scommegna [та ін.] // Journal of Systems and Software. – 2025. – С. 112518. – Режим доступу: https://doi.org/10.1016/j.jss.2025.112518.

10. A Feature Selection Method for Software Defect Prediction Based on Improved Beluga Whale Optimization Algorithm [Електронний ресурс] / Shaoming Qiu [та ін.] // Computers, Materials & Continua. – 2025. – С. 1–10. – Режим доступу: https://doi.org/10.32604/cmc.2025.061532.

11. IRAF-BRB: An explainable AI framework for enhanced interpretability in project risk assessment [Електронний ресурс] / Bodrunnessa Badhon [та ін.] // Expert Systems with Applications. – 2025. – Т. 285. – С. 127979. – Режим доступу: https://doi.org/10.1016/j.eswa.2025.127979.

12. AI-driven risk identification model for infrastructure project: Utilising past project data [Електронний ресурс] / Fredrick Ahenkora Boamah [та ін.] // Expert Systems with Applications. – 2025. – Т. 283. – С. 127891. – Режим доступу: https://doi.org/10.1016/j.eswa.2025.127891 (дата звернення: 24.10.2025).

13. Mohawesh R. A data-driven risk assessment of cybersecurity challenges posed by generative AI [Електронний ресурс] / Rami Mohawesh, Mohammad Ottom, Haythem Bany Salameh // Decision Analytics Journal. – 2025. – С. 100580. – Режим доступу: https://doi.org/10.1016/j.dajour.2025.100580.

14. Artificial intelligence in risk management within the realm of construction projects: A bibliometric analysis and systematic literature review [Електронний ресурс] / Kun Tian [та ін.] // Journal of Innovation & Knowledge. – 2025. – Т. 10, № 3. – С. 100711. – Режим доступу: https://doi.org/10.1016/j.jik.2025.100711.

15. Warnett S. J. A model-driven, metrics-based approach to assessing support for quality aspects in MLOps system architectures [Електронний ресурс] / Stephen John Warnett, Evangelos Ntentos, Uwe Zdun // Journal of Systems and Software. – 2024. – С. 112257. – Режим доступу: https://doi.org/10.1016/j.jss.2024.112257.

**References**

1. Gustavsson T. Job Satisfaction at Risk: Measuring the Role of Process Debt in Agile Software Development [Electronic resource] / Tomas Gustavsson, Muhammad Ovais Ahmad, Hina Saeeda // Journal of Systems and Software. – 2025. – P. 112350. – Mode of access: https://doi.org/10.1016/j.jss.2025.112350.

2. Project Governance to Improve the Performance of Software Projects by Mitigating the Software Risk Factors: The Moderating Role of Project Leadership [Electronic resource] / Samiul Alim Lesum [et al.] // Procedia Computer Science. – 2024. – Vol. 239. – P. 1863–1870. – Mode of access: https://doi.org/10.1016/j.procs.2024.06.368.

3. Utilizing Machine Learning Algorithms for Task Allocation in Distributed Agile Software Development [Electronic resource] / Dimah Al-Fraihat [et al.] // Heliyon. – 2024. – P. e39926. – Mode of access: https://doi.org/10.1016/j.heliyon.2024.e39926.

4. Automatic instantiation of assurance cases from patterns using large language models [Electronic resource] / Oluwafemi Odu [et al.] // Journal of Systems and Software. – 2025. – Vol. 222. – P. 112353. – Mode of access: https://doi.org/10.1016/j.jss.2025.112353.

5. Enabling security risk assessment and management for business process models [Electronic resource] / David G. Rosado [et al.] // Journal of Information Security and Applications. – 2024. – Vol. 84. – P. 103829. – Mode of access: https://doi.org/10.1016/j.jisa.2024.103829.

6. Zhao X. Identifying the primary dimensions of DevSecOps: A multi-vocal literature review [Electronic resource] / Xiaofan Zhao, Tony Clear, Ramesh Lal // Journal of Systems and Software. – 2024. – P. 112063. – Mode of access: https://doi.org/10.1016/j.jss.2024.112063.

7. Review of Techniques for Integrating Security in Software Development Lifecycle [Electronic resource] / Hassan Saeed [et al.] // Computers, Materials & Continua. – 2024. – P. 1–10. – Mode of access: https://doi.org/10.32604/cmc.2024.057587.

8. Alghawli A. S. A. Resilient cloud cluster with DevSecOps security model, automates a data analysis, vulnerability search and risk calculation [Electronic resource] / Abed Saif Ahmed Alghawli, Tamara Radivilova // Alexandria Engineering Journal. – 2024. – Vol. 107. – P. 136–149. – Mode of access: https://doi.org/10.1016/j.aej.2024.07.036.

9. OREO: A tool-supported approach for offline run-time monitoring and fault-error-failure chain localization [Electronic resource] / Leonardo Scommegna [et al.] // Journal of Systems and Software. – 2025. – P. 112518. – Mode of access: https://doi.org/10.1016/j.jss.2025.112518.

10. A Feature Selection Method for Software Defect Prediction Based on Improved Beluga Whale Optimization Algorithm [Electronic resource] / Shaoming Qiu [et al.] // Computers, Materials & Continua. – 2025. – P. 1–10. – Mode of access: https://doi.org/10.32604/cmc.2025.061532.

11. IRAF-BRB: An explainable AI framework for enhanced interpretability in project risk assessment [Electronic resource] / Bodrunnessa Badhon [et al.] // Expert Systems with Applications. – 2025. – Vol. 285. – P. 127979. – Mode of access: https://doi.org/10.1016/j.eswa.2025.127979.

12. AI-driven risk identification model for infrastructure project: Utilising past project data [Electronic resource] / Fredrick Ahenkora Boamah [et al.] // Expert Systems with Applications. – 2025. – Vol. 283. – P. 127891. – Mode of access: https://doi.org/10.1016/j.eswa.2025.127891.

13. Mohawesh R. A data-driven risk assessment of cybersecurity challenges posed by generative AI [Electronic resource] / Rami Mohawesh, Mohammad Ottom, Haythem Bany Salameh // Decision Analytics Journal. – 2025. – P. 100580. – Mode of access: https://doi.org/10.1016/j.dajour.2025.100580.

14. Artificial intelligence in risk management within the realm of construction projects: A bibliometric analysis and systematic literature review [Electronic resource] / Kun Tian [et al.] // Journal of Innovation & Knowledge. – 2025. – Vol. 10, no. 3. – P. 100711. – Mode of access: https://doi.org/10.1016/j.jik.2025.100711.

15. Warnett S. J. A model-driven, metrics-based approach to assessing support for quality aspects in MLOps system architectures [Electronic resource] / Stephen John Warnett, Evangelos Ntentos, Uwe Zdun // Journal of Systems and Software. – 2024. – P. 112257. – Mode of access: https://doi.org/10.1016/j.jss.2024.112257.