УДК 004.65:005.334:005.8 DOI https://doi.org/10.35546/kntu2078-4481.2026.2.47

Д. С. ТРОЦЕНКО
аспірант кафедри інформаційних технологій
Сумський державний університет
ORCID: 0009-0006-1159-6550

Ю. В. ПАРФЕНЕНКО
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій
Сумський державний університет
ORCID: 0000-0003-4377-5132

ІНФОРМАЦІЙНА СИСТЕМА ОЦІНЮВАННЯ РИЗИКІВ ІТ-ПРОЄКТІВ

Дослідження присвячене розробленню веборієнтованої інформаційної системи оцінювання ризиків ІТ-проєктів, яка забезпечує комплексну підтримку процесів ідентифікації, аналізу та реагування на загрози. Система автоматизує процедури експертного оцінювання, трансформуючи нечіткі лінгвістичні судження у строгі кількісні показники за допомогою візуальних інтерактивних шкал. Розроблений функціонал (ведення реєстру проєктів, класифікатор загроз, аналітична звітність) підвищує ефективність ризик-менеджменту та дозволяє здійснювати проактивне управління факторами, що критично впливають на бюджет, строки та якість проєкту. Вебсистема побудована за клієнт-серверною архітектурою на основі патерну MVC. Серверна частина реалізована мовою PHP з використанням фреймворку Laravel, а динамічна взаємодія та реактивне оновлення інтерфейсу забезпечуються інтеграцією технології Livewire і шаблонізатора Blade. Таке рішення оптимізує процес оцінювання завдяки асинхронному збереженню метрик у фоновому режимі, мінімізуючи когнітивне навантаження на експертів. В основу системи покладено адаптовану математичну модель, яка агрегує показники ймовірності та деструктивного впливу загроз за допомогою спеціалізованих теплових матриць. Фокусування виключно на негативних ризиках та розрахунок їх інтегральних показників формують об'єктивне підґрунтя для пріоритетизації завдань. Поєднання експертного підходу з математичним аналізом дозволяє компенсувати брак історичних даних та врахувати неформалізовані фактори організаційного середовища ІТ-галузі. Функціональне тестування підтвердило абсолютну алгоритмічну точність вебсистеми: зіставлення автоматизованих та еталонних мануальних розрахунків не виявило жодних відхилень. Це засвідчує повне нівелювання людського фактора на етапі математичної обробки даних. Крім того, вбудований інструментарій візуалізації (матриця ризиків та цільові фасетні діаграми) довів високу ефективність у наочній ідентифікації найбільш проблемних аспектів проєкту.

Ключові слова: *ІТ-проєкт, ризик, експертний підхід, математичне моделювання, управління проєктами, управління ризиками, інформаційна система.*

D. S. TROTSENKO
Postgraduate Student at the Department of Information Technologies
Sumy State University
ORCID: 0009-0006-1159-6550

YU. V. PARFENENKO
Candidate of Technical Sciences, Associate Professor,
Associate Professor at the Department of Information Technologies
Sumy State University
ORCID: 0000-0003-4377-5132

WEB-BASED INFORMATION SYSTEM FOR IT PROJECT RISK ASSESSMENT BASED ON EXPERT METHODS

The study is devoted to the development of a web-based information system for IT project risk assessment, which provides comprehensive support for the processes of identification, analysis, and response to threats. The system automates expert assessment procedures by transforming fuzzy linguistic judgments into strict quantitative indicators using visual interactive scales. The developed functionality (project registry management, threat classifier, and analytical reporting) increases the efficiency of risk management and enables proactive management of factors that critically affect the project's budget, schedule, and quality.

 ISSN 2078-4481

The web system is built on a client-server architecture based on the MVC pattern. The server part is implemented in PHP using the Laravel framework, while dynamic interaction and reactive interface updates are provided by integrating Livewire technology and the Blade templating engine. This solution optimizes the assessment process through the asynchronous saving of metrics in the background, minimizing the cognitive load on experts.

The system is based on an adapted mathematical model that aggregates indicators of the probability and destructive impact of threats using specialized heat matrices. Focusing exclusively on negative risks and calculating their integral indicators form an objective basis for task prioritization. The combination of an expert approach with mathematical analysis makes it possible to compensate for the lack of historical data and take into account the non-formalized factors of the IT industry's organizational environment.

Functional testing confirmed the absolute algorithmic accuracy of the web system: a comparison of automated and reference manual calculations revealed no deviations. This confirms the complete elimination of the human factor at the stage of mathematical data processing. In addition, the built-in visualization toolkit (risk matrix and target faceted diagrams) has proven its high efficiency in the visual identification of the most problematic aspects of the project.

Key words: *IT project, risk, expert approach, evaluation, mathematical modeling, project management, risk management, information system.*

Постановка проблеми

Управління ризиками є одним із визначальних факторів забезпечення успішної реалізації ІТ-проєктів. Попередні дослідження процесів ризик-менеджменту в ІТ-компаніях підтвердили, що ключовим етапом є своєчасна ідентифікація ризиків, оскільки коректне виявлення потенційних загроз на ранніх стадіях суттєво підвищує загальну ефективність розробки. Доведено, що формування плану реагування має позитивний вплив на результативність проєкту, проте надмірна деталізація процедур аналізу здатна призвести до необґрунтованого збільшення витрат і затримок у виконанні [1]. Крім того, результати аналізу ризиків створюють підґрунтя для формування обґрунтованих часових та бюджетних резервів, що дозволяє мінімізувати негативні наслідки в разі настання кризових ситуацій [2].

Існуючі системи управління ІТ-проєктами здебільшого пропонують базовий інструментарій для відстеження завдань, тоді як механізми глибокого аналізу та оцінювання ризиків часто залишаються поза межами єдиного робочого середовища розробників. Це призводить до ускладнення процесів моніторингу загроз і знижує швидкість реакції команди на потенційні проблеми. У зв’язку з цим актуальною є задача розроблення інформаційної системи, у межах якої функції трекінгу доповнюються інтегрованими методами ідентифікації та оцінювання проєктних ризиків.

Формулювання мети дослідження

Метою роботи є розроблення веборієнтованої інформаційної системи оцінювання ризиків ІТ-проєктів для підтримки прийняття управлінських рішень під час ідентифікації, аналізу та моніторингу потенційних загроз методами експертного оцінювання.

Аналіз останніх досліджень і публікацій

Аналіз існуючих підходів до оцінювання ризиків продемонстрував наявність широкого спектру методів [4]. Зокрема, дерева рішень вирізняються наочністю та простотою візуальної інтерпретації, тоді як штучні нейронні мережі демонструють вищу ефективність під час обробки значних масивів нелінійних факторів [5, 6], що робить їх перспективними для застосування в ІТ-галузі [7]. Для побудови моделей імовірнісного розподілу ризиків традиційно застосовуються статистичні підходи, такі як метод Монте-Карло та екстремальна теорія значень [8], а також методологія ймовірнісної оцінки ризику (Probabilistic Risk Assessment, PRA), яка дозволяє визначити частоту виникнення загроз та їхні можливі наслідки [9]. Однак, незважаючи на високу обчислювальну потужність, застосування винятково статистичних та машинних методів часто ускладнюється через вимогу наявності великих обсягів валідованих історичних даних. В умовах високої динаміки ІТ-сфери та унікальності багатьох розробок такі дані можуть бути відсутніми або не релевантними. Водночас доведено, що критично важливою складовою комплексного аналізу проєктних ризиків є використання експертного підходу. Його застосування дозволяє ефективно компенсувати об'єктивні обмеження суто математичних моделей під час роботи з новими, слабоструктурованими або безпрецедентними загрозами. Цей підхід ґрунтується на залученні евристичних знань, практичного досвіду та інтуїції фахівців предметної області, що забезпечує глибоке розуміння прихованих взаємозв'язків та якісних аспектів ризикових подій. Встановлено, що експертні оцінки є практично безальтернативним інструментом для аналізу «м'яких» (неформалізованих) факторів організаційного середовища. До таких факторів належать особливості корпоративної культури, специфіка внутрішніх комунікацій, соціальна взаємодія та поведінкові характеристики команд розробників. Оскільки зазначені критерії характеризуються високим рівнем нечіткості та нелінійності, вони складно піддаються прямій кількісній формалізації, проте здійснюють системний вплив на загальний профіль ризику проєкту. Застосування методології експертних систем дозволяє формалізувати та структурувати емпіричні знання фахівців, перетворивши їх на чіткі правила прийняття рішень та багатокритеріальні сценарії управління ризиками. Завдяки такому перетворенню стало можливим не лише точне ідентифікування неочевидних загроз на ранніх етапах життєвого циклу розробки, але й автоматизована генерація обґрунтованих рекомендацій щодо їх превентивної мінімізації. Формування таких стратегій базується

на ретроспективному аналізі успішних практик та досвіді реалізації аналогічних проєктів [10]. Таким чином, з огляду на специфіку поставленої задачі, експертний підхід до оцінювання ризиків визначено як найбільш гнучкий та адаптивний інструмент, що органічно доповнює кількісні методи оцінювання.

Викладення основного матеріалу дослідження

Оцінювання ризиків в ІТ-проєктах з використанням методології інтегрованого управління ризиками. Для аналізу ймовірності виникнення та потенційних наслідків ідентифікованих ризиків у дослідженні застосовано метод експертних оцінок. Початковим етапом процесу є агрегація даних щодо можливих загроз для ІТ-проєктів, зокрема затримок у часі, зниження якості продукту та перевитрат бюджету. Оцінювання кожної загрози здійснюється з урахуванням ретроспективних даних, експертних суджень та специфічних характеристик поточного проєкту. Такий підхід забезпечує адаптацію метрик ризику до конкретних проєктних обмежень, що максимізує точність і достовірність результатів.

Для кількісного визначення впливу ідентифікованих загроз на ключові обмеження проєкту (бюджет, строки, якість) застосовано математичні моделі, які описуються рівняннями (1)–(3):

$$D_b = \sum_{j=1}^{m} P_{jd} \cdot V_{jdb} \tag{1}$$

$$D_t = \sum_{j=1}^{m} P_{jd} \cdot V_{jdt} \tag{2}$$

$$D_q = \sum_{j=1}^{m} P_{jd} \cdot V_{jdq} \tag{3}$$

де:

– j – набуває значення від 1 до m;
– m – загальна кількість ідентифікованих загроз у проєкті;
– Db, Dt, Dq – інтегральні показники впливу j-ї загрози на бюджет, строки та якість відповідно;
– Pjd – ймовірність настання j-ї загрози (набуває значень у діапазоні від 0 до 1);
– Vjdb, Vjdt, Vjdq – значення впливу j-ї загрози на бюджет, графік та якість відповідно (набувають значень у діапазоні від -10 до 0).

Для розрахунку сукупного впливу окремого ризику на проєкт за всіма категоріями обмежень, використано формулу (4):

$$D_c = P_{jd} \cdot \left(V_{jdb} + V_{jdt} + V_{jdq} \right) \tag{4}$$

де:

– Dc – сукупний вплив окремого ризику на проєкт.

Відповідно, інтегральний показник ризику всього проєкту визначається за формулою (5) як агрегована величина ймовірностей та наслідків:

$$D_{total} = \sum_{j=1}^{m} P_{jd} \cdot \left(V_{jdb} + V_{jdt} + V_{jdq} \right) \tag{5}$$

де:

– Dtotal – інтегральний показник ризику проєкту.

Слід зазначити, що математичні моделі (1)–(5) були адаптовані на основі досліджень, наведених у роботі [11]. Ключова відмінність запропонованого апарату полягає у виключенні параметра впливу загрози на загальний обсяг робіт, що дозволило сфокусувати модель на найбільш критичних для ІТ-сфери обмеженнях.

Введення експертних оцінок у розробленій системі реалізовано через зручний користувацький інтерфейс із використанням повзунків та вибору якісних дескрипторів. Це позбавляє експерта необхідності вводити точні числові значення вручну, дозволяючи оперувати лінгвістичними оцінками. Конвертація лінгвістичних оцінок ймовірності у числові еквіваленти здійснюється відповідно до шкали (табл. 1), адаптованої з дослідження [2].

Таблиця 1

Оцінювання ймовірності настання загрози

Шкала оцінювання експертом	Значення, що підставляється у формулу
Слабо-ймовірна	0.1
Малоймовірна	0.3
Ймовірна	0.5
Вельми ймовірна	0.7
Майже гарантована	0.9

Розподіл шкали впливу на проєктні обмеження базується на градації, запропонованій у роботі [11], та поданий у вигляді теплової матриці (табл. 2).

Таблиця 2

Шкала значень впливу загрози

Теплова шкала оцінювання експерта	Діапазон значень (x), що підставляється у формулу
Зелений	$-1 \le x \le 0$
Світло-зелений	$-3 \le x \le -1$
Жовтий	$-6 \le x \le -3$
Оранжевий	$-9 \le x \le -6$
Червоний	$-10 \le x \le -9$

У межах запропонованого підходу ідентифіковані загрози підлягають обов'язковому ранжуванню з огляду на ступінь їхнього деструктивного впливу на ключові обмеження проєкту: бюджет, графік виконання та якість кінцевого продукту. Кількісне вимірювання ризиків за допомогою наведених математичних моделей забезпечує агрегацію показників імовірності та впливу, формуючи для осіб, які приймають рішення (ОПР), об'єктивне числове підґрунтя для пріоритезації завдань реагування.

Особливістю реалізованої стратегії є свідоме фокусування виключно на загрозах (негативних ризиках), на відміну від класичних методологій управління, що передбачають балансування між ризиками та можливостями. Такий вибір обґрунтовується двома основними чинниками. По-перше, в IT-сфері реалізовані загрози чинять миттєвий і часто незворотний вплив на успішність проєкту. По-друге, розробка програмного забезпечення відбувається у високодинамічному середовищі, де ціна ігнорування небезпек є критично високою. Отже, концентрація функціоналу системи саме на загрозах дозволяє вибудувати методичну систему захисту, що суттєво підвищує загальну стійкість проєкту до кризових ситуацій.

Практичну реалізацію цієї концепції у розробленій інформаційній системі забезпечено через інтеграцію засобів графічної візуалізації даних та комплексних модулів звітності. Впровадження таких аналітичних інструментів створює умови для проактивного управління ризиками, надаючи керівникам проєктів можливість здійснювати моніторинг, ранжування та контроль загроз у режимі реального часу.

Застосована у дослідженні цільова модель інтегрованого управління ризиками формує системний механізм контролю специфічних загроз в IT-секторі. Запропонований підхід дозволяє мінімізувати деструктивний вплив факторів ризику та підвищити результативність проєктів завдяки предиктивному аналізу ймовірностей та оцінці їхньої ваги для критичних параметрів (бюджету, часу, якості).

Реалізація веборієнтованої системи оцінювання ризиків IT проєктів. Програмну реалізацію веборієнтованої інформаційної системи виконано мовою PHP з використанням фреймворку Laravel, архітектура якого базується на шаблоні MVC (Model-View-Controller). На рисунку 1 наведено архітектурну модель системи оцінювання проєктних ризиків.

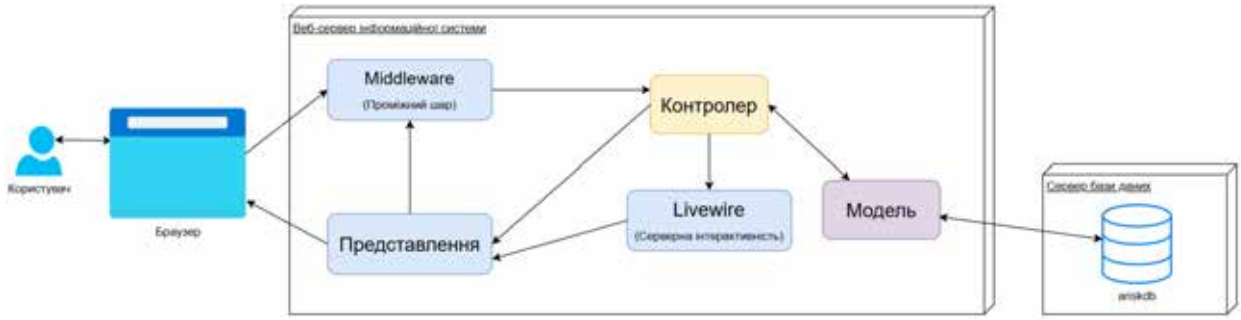

Рис. 1. Архітектура інформаційної системи

Маршрутизація та обробка HTTP-запитів здійснюється через проміжний шар (Middleware), який реалізує механізми аутентифікації та попередньої валідації даних до їх передачі контролеру. Бізнес-логіка, яка охоплює обчислення метрик ризику за наведеними математичними моделями, реалізована на рівні контролерів, тоді як взаємодія з базою даних інкапсульована в об'єктно-реляційних моделях.

Для відображення інформації клієнту застосовано шаблонізатор (Blade), який формує структуру сторінок. Суттєвою архітектурною особливістю є інтеграція технології Livewire, що дозволяє забезпечити реактивне оновлення компонентів інтерфейсу в режимі реального часу без перезавантаження сторінок. Застосування серверного

рендерингу динамічних компонентів виявилося критично необхідним для реалізації зручного інтерфейсу багатофакторного експертного оцінювання ризиків.

Програмна реалізація системи охоплює модулі ідентифікації загроз, автоматизованого формування аналітичної звітності та динамічної взаємодії з користувачем. Інтерфейс та логіка системи спроєктовані з урахуванням специфіки завдань кінцевих користувачів, які розподілені за двома ключовими ролями: «Керівник команди» та «Проєктний менеджер / Експерт». Це гарантує високу ергономічність, швидкість обробки даних і точність у виконанні процедур ризик-менеджменту.

Практична експлуатація вебсистеми ініціюється через етап реєстрації з обов'язковим призначенням рольової моделі керування доступом. Базовий робочий процес розпочинається користувачем із роллю «Керівник команди», який через спеціалізовану вебформу вносить вихідні дані нового ІТ-проєкту.. Після успішної валідації введених даних запис зберігається в базі, а система генерує відповідне візуальне сповіщення про результати операції додавання (рис. 2).

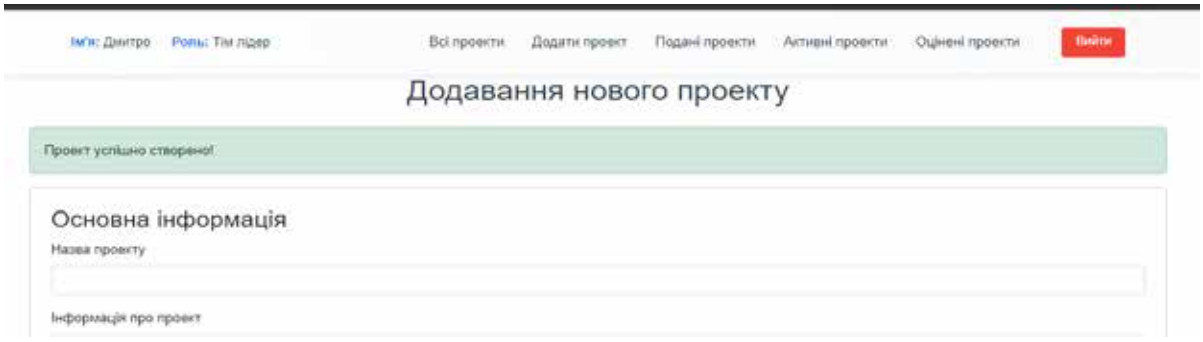

Рис. 2. Візуалізація результату операції з додавання проєкту

Збережені проєкти одразу відображаються у вигляді інтерактивних інформаційних карток, формуючи загальний реєстр поданих на оцінювання проєктів (рис. 3).

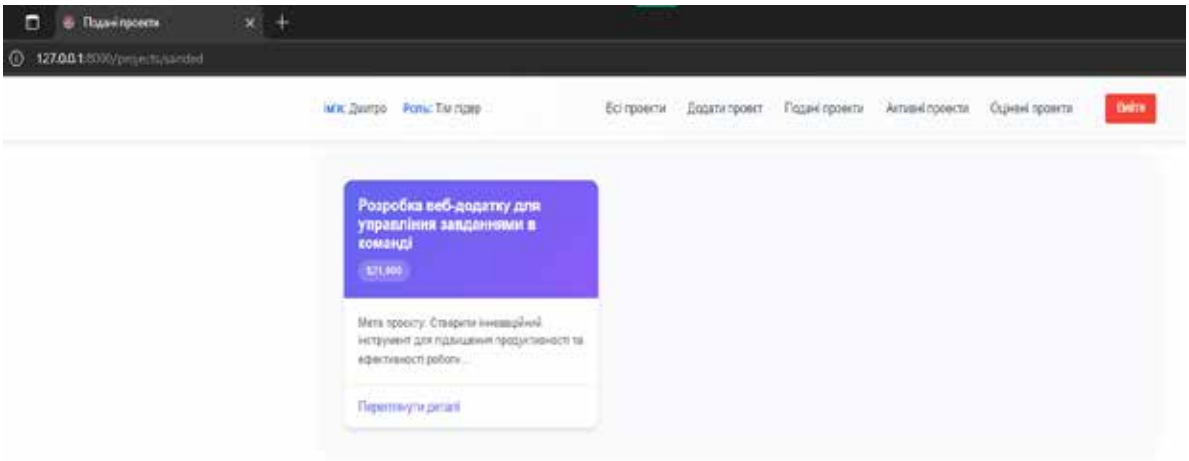

Рис. 3. Інтерфейс відображення списку поданих проєктів

Після того як експерт (Проєктний менеджер) здійснює оцінювання ідентифікованих загроз проєкту, система автоматично оновлює його статус і переміщує запис до відповідної категорії. Як наслідок, ініціатор проєкту отримує доступ до згенерованих аналітичних звітів безпосередньо з картки проєкту. Навігаційна панель вебсистеми забезпечує диференційоване відображення даних: персональні вкладки містять виключно ті проєкти, до яких залучений авторизований користувач, тоді як загальний реєстр надає доступ до консолідованої інформації про всі внесені проєкти відповідно до налаштованих прав доступу.

Візуалізація результатів оцінювання реалізована за допомогою аналітичних діаграм, що базуються на обчислених показниках ризиків і дозволяють наочно ідентифікувати найбільш проблемні аспекти реалізації проєкту. Водночас для формування комплексного розуміння загального рівня загрози успішності проєкту в системі передбачено побудову класичної матриці ризиків (рис. 4).

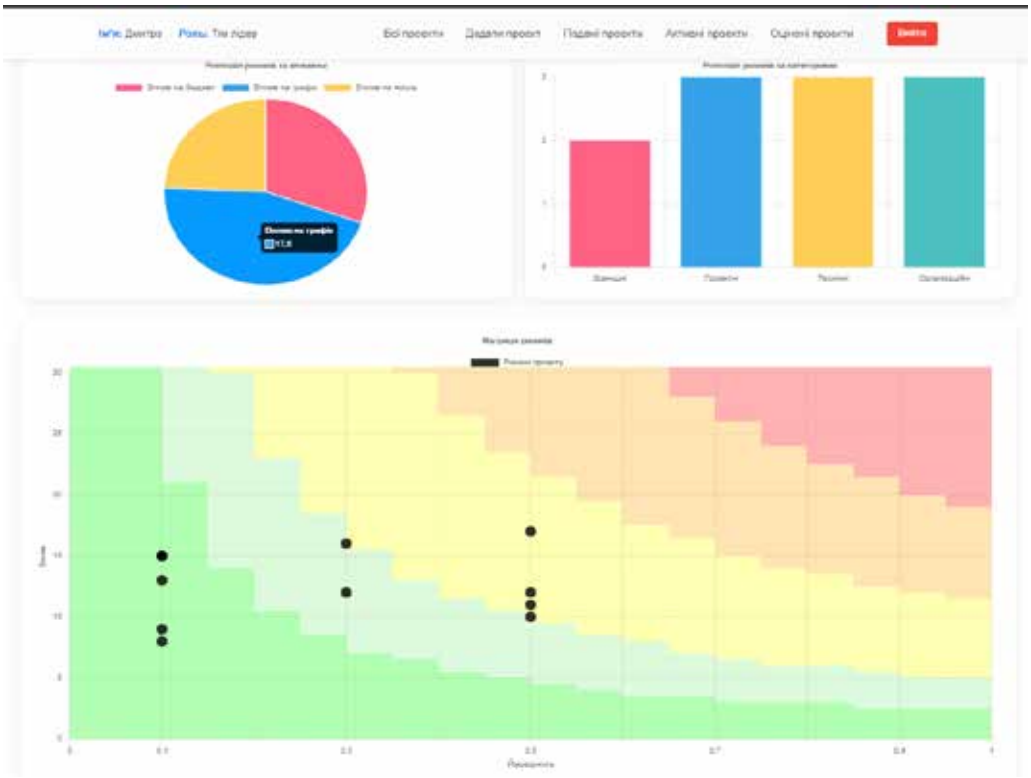

Рис. 4. Візуалізація результатів оцінювання проєктних ризиків

Деталізація аналізу забезпечується через цільові діаграми, які відображають структурний розподіл впливу ризиків у межах кожної окремої категорії. Такий підхід дає змогу візуально виокремити специфічні загрози з найвищим ступенем деструктивного впливу за обраним аспектом (рис. 5). Після завершення аналізу згенерованих даних система надає користувачеві можливість експортувати повний звіт у форматі HTML-документа для подальшого використання або архівування.

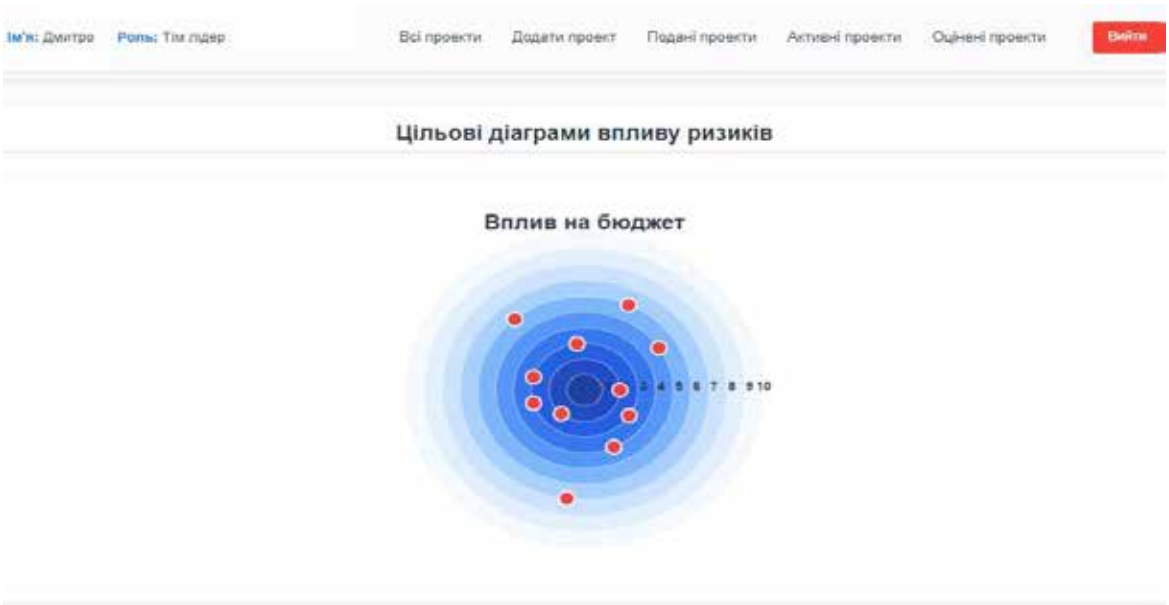

Рис. 5. Графічна інтерпретація впливу ризиків на бюджетну складову проєкту

Процедуру експертного оцінювання ідентифікованих загроз у системі регламентовано для користувачів із рівнем доступу «Проєктний менеджер». Робочий простір цього модуля реалізовано у вигляді ієрархічного класифікатора ризиків, згрупованих за відповідними категоріями.

Інструментарій системи дозволяє експерту здійснювати гнучке налаштування моделі оцінювання: самостійно вводити нові специфічні загрози, вилучати нерелевантні фактори та безпосередньо редагувати атрибути наявних записів. З метою мінімізації когнітивного навантаження на експерта процес квантифікації ризиків суттєво спрощено. Визначення ймовірності настання події здійснюється через дискретний вибір лінгвістичних термів, а фіксація рівня впливу – за допомогою візуальних інтерактивних шкал. Архітектурне рішення інтерфейсу передбачає механізм асинхронного збереження метрик у фоновому режимі одразу після завершення взаємодії з елементом управління, що підвищує загальну ергономічність системи. Згідно із закладеною методологією, алгоритм валідації сеансу оцінювання вимагає обов'язкової ініціалізації параметрів для повної множини ризиків проєкту, що гарантує математичну цілісність подальших розрахунків (рис. 6).

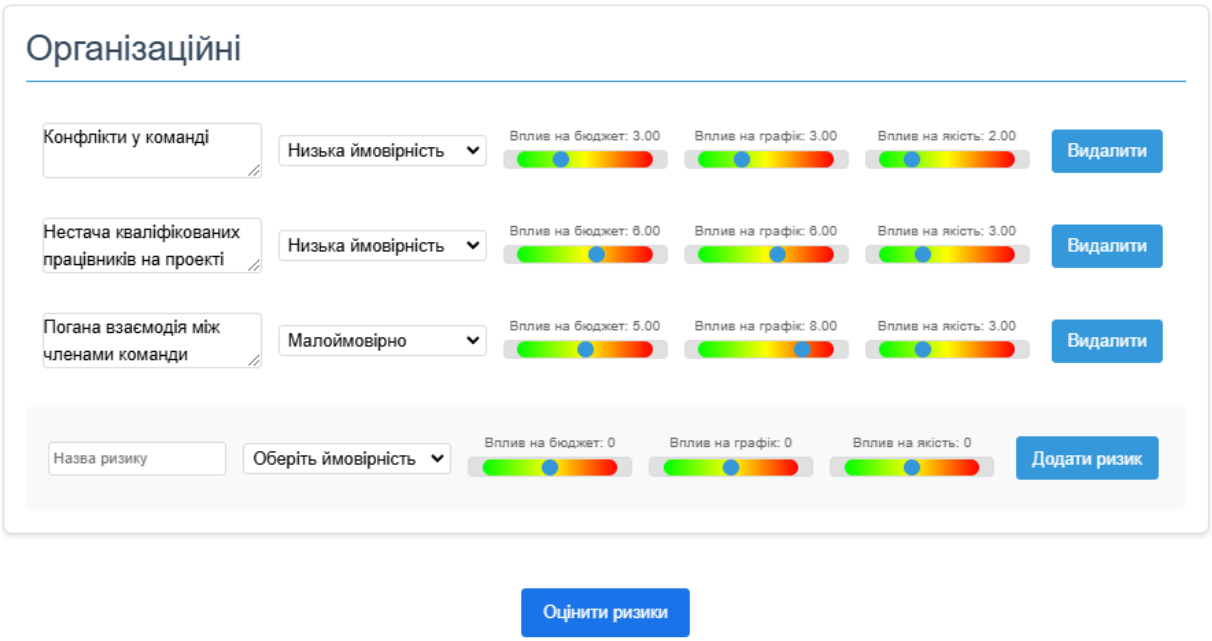

Рис. 6. Інтерфейс оцінювання ризиків

Обговорення. Отримані результати свідчать, що розроблена веборієнтована система успішно формує надійне інструментальне середовище для підтримки прийняття управлінських рішень під час роботи з ризиками в IT-проєктах. Автоматизація етапу кількісного вимірювання (обробки експертних оцінок за інтегрованими математичними моделями) дозволяє не лише зручно накопичувати та структурувати дані про загрози, але й об'єктивно оцінювати їхній деструктивний вплив на ключові обмеження проєкту.

Для верифікації розроблених алгоритмів та підтвердження адекватності математичного апарату було проведено функціональне тестування програмного забезпечення. В якості тестової вибірки використано набір вихідних даних, що імітує реальний IT-проєкт на стадії планування. Для цього проєкту було сформовано реєстр із типових загроз (зокрема, відхилення в графіку розробки, перевитрати виділеного бюджету, зниження якості програмного коду) із заздалегідь визначеними експертними оцінками ймовірності настання та рівня впливу.

Для перевірки коректності роботи модуля обчислення загальних впливів ризику та їхніх інтегральних показників було виконано серію еталонних мануальних розрахунків, результати яких зіставлялися зі значеннями, обчисленими інформаційною системою. За результатами порівняльного аналізу не було виявлено жодних математичних чи логічних розбіжностей. Усі отримані автоматизованим шляхом показники абсолютно точно відповідають очікуваним еталонним значенням, що беззаперечно підтверджує точність алгоритмічних обчислень. Результати верифікації інтегральних показників для тестового проєкту наведено в табл. 3.

Таблиця 3

Результати верифікації обчислень інтегральних показників ризиків проєкту

	Очікуване значення	**Отримане значення**
Загальний показник ризику проєкту	39.40	39.40
Показник ризику за бюджетом	12.00	12.00
Показник ризику за строком	17.80	17.80
Показник ризику за якістю	9.60	9.60

Поряд із підтвердженою алгоритмічною точністю обчислень, ключова наукова та практична цінність розробки визначається ефективністю запропонованого методологічного підходу. Модель, що базується на інтеграції методів експертного оцінювання з цілеспрямованим математичним аналізом деструктивних загроз, демонструє високу результативність з огляду на специфіку IT-галузі. Перетворення якісних, переважно нечітких експертних суджень щодо потенційних ризиків у формалізовані кількісні метрики їхнього впливу на базові проєктні обмеження (бюджет, строки та якість) формує об'єктивне підґрунтя для системної підтримки прийняття управлінських рішень.

Практичне впровадження розробленої вебсистеми слугує інструментальним базисом для реалізації зазначеного підходу. Автоматизація процесів дозволяє повністю нівелювати вплив людського фактору на етапі математичної обробки даних та забезпечує безперервний аналітичний моніторинг стану проєкту. Завдяки механізмам автоматизованого ранжування та візуалізації розподілу ризиків, керівники проєктів отримують інструментарій для переходу від реактивного усунення наявних проблем до проактивного управління загрозами. Таким чином, інтеграція запропонованої інформаційної технології в корпоративне середовище розробки програмного забезпечення формує дієвий механізм пріоритезації завдань, підвищує загальну життєздатність проєктів і сприяє превентивній мінімізації фінансових та часових втрат.

Висновки

У роботі розроблено та апробовано веборієнтовану інформаційну систему оцінювання ризиків IT-проєктів, яка забезпечує комплексну підтримку процесів ідентифікації, кількісного вимірювання та аналізу потенційних загроз. Вебсистема дозволяє ефективно трансформувати нечіткі лінгвістичні експертні оцінки у строгі математичні показники, формуючи об'єктивне підґрунтя для системної підтримки прийняття управлінських рішень.

Реалізовані функціональні можливості включають ведення ієрархічного реєстру проєктів і класифікатора загроз, проведення експертного оцінювання за допомогою візуальних інтерактивних шкал, а також автоматизовану генерацію розширеної аналітичної звітності. Вбудований інструментарій візуалізації, зокрема побудова класичної матриці ризиків та цільових діаграм, забезпечує керівникам проєктів наочну ідентифікацію найбільш критичних факторів, що впливають на бюджет, строки та якість розробки.

Система побудована за клієнт-серверною архітектурою на основі патерну MVC, що гарантує надійність, гнучкість масштабування та чіткий розподіл бізнес-логіки. Серверна частина реалізована мовою PHP з використанням фреймворку Laravel, а динамічна взаємодія та реактивне оновлення інтерфейсу в режимі реального часу забезпечуються технологією Livewire у поєднанні із шаблонізатором Blade. Проведене тестування підтвердило абсолютну алгоритмічну точність обчислень, засвідчивши повне нівелювання впливу людського фактору на етапі математичної обробки даних.

Впровадження розробленого програмного продукту в діяльність IT-компаній забезпечує зміщення управлінського фокусу з подолання вже наявних кризових ситуацій на стратегію їх системного запобігання. Такий інструментарій підвищує ймовірність успішності реалізації проєктів, створюючи надійне підґрунтя для захисту виділених бюджетів та затверджених графіків виконання робіт в умовах високої динаміки розробки програмного забезпечення.

Список використаної літератури

1. Pimchangthong Pimchangthong D., Boonjing V. Effects of Risk Management Practice on the Success of IT Project. *Procedia Engineering*. 2017. Vol. 182. P. 579–586. URL: https://doi.org/10.1016/j.proeng.2017.03.158

2. Hrytsiuk Y. I., Zhabych M. R. RISK MANAGEMENT OF IMPLEMENTATION OF PROGRAM PROJECTS. *Scientific Bulletin of UNFU*. 2018. T. 28, № 1. C. 150–162. URL: https://doi.org/10.15421/40280130

3. Eldash K. PROJECT RISK MANAGEMENT. 2012. 173 p. URL: https://www.researchgate.net/publication/271909639_PROJECT_RISK_MANAGEMENT_COURSE_NOTES

4. The role of data analytics within operational risk management: A systematic review from the financial services and energy sectors / N. Cornwell et al. *Journal of the Operational Research Society*. 2022. P. 1–29. URL: https://doi.org/10.1080/01605682.2022.2041373

5. Crespo Márquez A., Crespo Del Castillo A., Gómez Fernández J. F. Integrating artificial intelligent techniques and continuous time simulation modelling. Practical predictive analytics for energy efficiency and failure detection. *Computers in Industry*. 2020. Vol. 115. P. 103164. URL: https://doi.org/10.1016/j.compind.2019.103164

6. Mazumder R. K., Salman A. M., Li Y. Failure risk analysis of pipelines using data-driven machine learning algorithms. *Structural Safety*. 2021. Vol. 89. P. 102047. URL: https://doi.org/10.1016/j.strusafe.2020.102047

7. A Data-Driven Artificial Neural Network Approach to Software Project Risk Assessment / M. N. Alatawi et al. *IET Software*. 2023. Vol. 2023. P. 1–19. URL: https://doi.org/10.1049/2023/4324783

8. McNeil A. J. Extreme Value Theory for Risk Managers. 1999. P. 1–22. URL: https://www.researchgate.net/publication/2470539_Extreme_Value_Theory_for_Risk_Managers

9. Probabilistic Risk Assessment (PRA). *NRC Web*. URL: https://www.nrc.gov/about-nrc/regulatory/risk-informed/pra.html

10. Каверіна Н. О. Науково-методичні підходи до аналізу та оцінки ризиків інноваційної діяльності. *ScienceRise*. 2014. Т. 5, № 3. С. 74. URL: https://doi.org/10.15587/2313-8416.2014.34799

11. Грабіна К. В. Моделі та методи інформаційної технології управління ризиками в IT-проєктах : дис. … канд. техн. наук : 122. Суми, 2024. 185 с. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/97100/1/Hrabina_K_PhD_thesis.pdf

References

1. Pimchangthong, D., & Boonjing, V. (2017). Effects of risk management practice on the success of IT project. *Procedia Engineering, 182*, 579–586. https://doi.org/10.1016/j.proeng.2017.03.158

2. Hrytsiuk, Y. I., & Zhabych, M. R. (2018). Risk management of implementation of program projects. *Scientific Bulletin of UNFU, 28*(1), 150–162. https://doi.org/10.15421/40280130

3. Eldash, K. (2012). *Project risk management*. https://www.researchgate.net/publication/271909639_PROJECT_RISK_MANAGEMENT_COURSE_NOTES

4. Cornwell, N., et al. (2022). The role of data analytics within operational risk management: A systematic review from the financial services and energy sectors. *Journal of the Operational Research Society*, 1–29. https://doi.org/10.1080/01605682.2022.2041373

5. Crespo Márquez, A., Crespo Del Castillo, A., & Gómez Fernández, J. F. (2020). Integrating artificial intelligent techniques and continuous time simulation modelling: Practical predictive analytics for energy efficiency and failure detection. *Computers in Industry, 115*, 103164. https://doi.org/10.1016/j.compind.2019.103164

6. Mazumder, R. K., Salman, A. M., & Li, Y. (2021). Failure risk analysis of pipelines using data-driven machine learning algorithms. *Structural Safety, 89*, 102047. https://doi.org/10.1016/j.strusafe.2020.102047

7. Alatawi, M. N., et al. (2023). A data-driven artificial neural network approach to software project risk assessment. *IET Software, 2023*, 1–19. https://doi.org/10.1049/2023/4324783

8. McNeil, A. J. (1999). *Extreme value theory for risk managers*. https://www.researchgate.net/publication/2470539_Extreme_Value_Theory_for_Risk_Managers

9. NRC Web. (n.d.). *Probabilistic risk assessment (PRA)*. https://www.nrc.gov/about-nrc/regulatory/risk-informed/pra.html

10. Kaverina, N. O. (2014). Scientific and methodological approaches to the analysis and assessment of risks in innovative activity. *ScienceRise, 5*(3), 74. https://doi.org/10.15587/2313-8416.2014.34799

11. Hrabina, K. V. (2024). *Models and methods of information technology for risk management in IT projects* [Doctoral dissertation, Sumy State University]. https://essuir.sumdu.edu.ua/bitstream-download/123456789/97100/1/Hrabina_K_PhD_thesis.pdf

Дата першого надходження статті до видання: 28.02.2026
Дата прийняття статті до друку після рецензування: 30.03.2026
Дата публікації (оприлюднення) статті: 07.05.2026