

О.А. ЖУРАН, Л.С. ФОНАР, О.С. КОНОВАЛОВ, В.О. ПАНІН
Національний університет «Одеська політехніка»

АНАЛІЗ РИЗИКІВ ІТ-ПРОЄКТУ ВЕБРЕСУРСУ ДЛЯ КОМУНІКАЦІЇ ОСВІТНІХ ЗАКЛАДІВ

Метою дослідження є аналіз ризиків, пов'язаних із реалізацією ІТ-проєкту адміністрування вебресурсів, призначеного для покращення комунікації між освітнім закладом і стейкхолдерами. Використання он-лайн соціальних мереж може спростити розповсюдження новин кафедри, здобутків здобувачів і викладачів, цікавих подій, пропозицій навчання, стажування, участі в конкурсах тощо. Створення сторінок у соціальних мережах дасть змогу структурному підрозділу допомогти випускникам залишатися в контакті, знаходити можливості співпраці, обмінюватися досвідом, а також організувати зустрічі, заходи та спільні проєкти в реальному житті. Основні причини невдач ІТ-проєктів можуть включати таке: погане управління, недостатнє залучення зацікавлених сторін, недостатній аналіз вимог, зміни вимог під час розробки, недостатню комунікацію тощо. Усі ці фактори є ризиками щодо успішності реалізації проєкту й відповідності запланованим показникам за вартістю, часом, термінами або якість. Крім того, під час управління проєктними ризиками варто враховувати той фактор, що більшість ІТ-проєктів унікальні, а іноді взагалі не мають аналогів. Саме тому й ризики для кожного з таких проєктів мають особливість. Важливо розглядати ризики ІТ-проєкту вебресурсу для комунікації освітніх закладів, ураховуючи організаційні особливості й структурних підрозділів навчального закладу і властивості соцмереж та інтернет-спілкування, а також проблеми, які виникають у процесі використання сторонніх веб-ресурсів, на які виконавці не можуть впливати. У статті проведено комплексний огляд потенційних ризикових ситуацій, що можуть виникнути. Визначено 4 ризики внутрішнього й 4 ризики зовнішнього середовища проєкту. Для кожного ідентифікованого ризику з'ясовано причину його виникнення – фактор ризику. Найчастіше факторами ризику обраного проєкту є людські ресурси й форс-мажор. Підсумковий аналіз ризиків дає змогу розробникам, управлінцям і зацікавленим сторонам краще зрозуміти важливість аспектів безпеки та планування для успішної реалізації запропонованого ІТ-проєкту з мінімізацією можливих негативних наслідків.

Ключові слова: ІТ-проєкт, заклад вищої освіти, управління проєктами, SWOT аналіз, ризики, соцмережі.

O.A. ZHURAN, L.S. FONAR, O.S. KONOVALOV, V.O. PANIN
Odesa Polytechnic National University

RISK ANALYSIS OF AN IT PROJECT FOR A WEB RESOURCE AIMED AT COMMUNICATION IN EDUCATIONAL INSTITUTIONS

The aim of the conducted research is to analyze the risks associated with the implementation of an IT project for the administration of web resources aimed at improving communication between educational institutions and stakeholders. The use of online social networks can facilitate the dissemination of departmental news, achievements of students and teachers, interesting events, educational offers, internships, participation in competitions, and more. Creating pages on social networks will allow the department to help graduates stay in touch, find collaboration opportunities, exchange information, and also organize meetings, events, and joint real-life projects. The main causes of IT project failures can include poor management, insufficient engagement of stakeholders, inadequate requirement analysis, changing requirements during development, insufficient communication, and more. All these factors pose risks to the success of project implementation and adherence to planned metrics in terms of cost, time, deadlines, or quality. Additionally, in managing project risks, it is important to consider that most IT projects are unique and sometimes have no analogs. Therefore, risks for each such project have their own specificity. It is crucial to examine the risks of an IT project for a web resource in communication with educational institutions, taking into account the organizational characteristics and structural departments of the educational institution, properties of social networks and online communication, as well as the problems arising from the use of third-party web resources that project executors cannot influence. Within the article, a comprehensive overview of potential risk situations that may arise is conducted. Four internal and four external environmental risks of the project are identified. For each identified risk, the cause of its occurrence – the risk factor is determined. The most common risk factors for the chosen project are human resources and force majeure. The cumulative risk analysis enables developers, managers, and stakeholders to better understand the importance of security aspects and planning for the successful implementation of the proposed IT project while minimizing potential negative consequences.

Key words: IT project, higher education institution, project management, SWOT analysis, risks, social networks.

Постановка проблеми

Популярність соціальних мереж серед молоді, здобувачів та абітурієнтів постійно зростає. Вимушені умови дистанційного навчання, обмеженої соціалізації, пандемія, війна – усе це останніми роками значно підвищило важливість он-лайн соціальних мереж для спілкування, пошуку інформації та відгуків. Неможливість навчатися в аудиторному форматі для здобувачів, відвідувати дні відкритих дверей для абітурієнтів, евакуація та руйнування закладів освіти через війну – усе це негативно впливає на якість спілкування, самореалізації, соціального розвитку молоді.

Науково-викладацький склад також відчуває на собі наслідки он-лайн освіти, проблеми організаційного та виховного характеру під час роботи зі студентами через неможливість спілкуватися наживо.

Використання он-лайн соціальних мереж може допомогти вирішити деякі з перелічених проблем, покращити якість спілкування, спростити доведення новин кафедри, здобутків здобувачів і викладачів, цікавих подій, пропозицій навчання, стажування, участі в конкурсах тощо.

Також активна участь освітніх закладів у соцмережах збільшує охоплення потенційних абітурієнтів і їхніх батьків, підвищує обізнаність суспільства й наукової спільноти про здобутки кафедр, інститутів та університету загалом. Створення сторінок у соціальних мережах дасть змогу кафедрі залучити більше уваги і створити свій унікальний імідж серед студентів, співробітників і гостей. Здобувачі, які вже закінчили навчання, можуть залишатися в контакті через соціальні мережі, знаходити можливості співпраці, обмінюватися досвідом і підтримувати зв'язок зі своєю навчальною установою, а також організовувати зустрічі, заходи та спільні проекти в реальному житті.

Аналіз останніх досліджень та публікацій

Використання соціальних мереж та інших веб-ресурсів для комунікації освітніх закладів зі здобувачами – їх створення, адміністрування та просування – можна розглядати як ІТ-проект. У свою чергу, будь-який проект, безумовно, має ризики щодо його реалізації.

У вітчизняній науковій літературі розглянуто концептуальні положення управління ризиками ІТ-проектів з урахування особливостей впливу українського зовнішнього середовища [1].

Загальна характеристика методів і механізмів реагування на ризики ІТ-проектів висвітлені авторами в попередніх дослідженнях [2].

Зростання використання цифрових технологій майже в усіх сферах життя призвели до того, що велика частина особистих, корпоративних, фінансових і конфіденційних даних тепер зберігається та обробляється онлайн. У свою чергу, зростають злочини та зловживання особистою інформацією. Запобігання кіберзлочинності й безпека під час використання веб-технологій дистанційного навчання є першочерговими завданнями в управлінні проектними ризиками у сфері ІТ [3].

У роботах І.В. Рішняк розглядає ризики проекту як багатоаспектну систему та пропонує використовувати для аналізу методи імітаційного моделювання [4–5].

За даними деяких досліджень, близько 50% усіх ІТ-проектів вважаються невдалими, тобто вони завершуються або затримуються з порушенням термінів, бюджету або специфікацій. Близько 70% проектів зазнають затримок у термінах або вартості [1]. На жаль, зараз відсутня українська статистика щодо успішності реалізації ІТ-проектів і причин їх невдач. Також сучасна нестабільність зовнішнього середовища сильно впливає на хід реалізації проектів і також знижує їх результативність.

Використання веб-технологій в освітньому середовищі має свої переваги й недоліки [6; 7]. Основні причини невдач ІТ-проектів можуть включати погане управління, недостатнє залучення зацікавлених сторін, неповний аналіз вимог, зміни вимог під час розробки, недостатню комунікацію тощо. Усі ці фактори є ризиками щодо успішності реалізації проекту й відповідності запланованим показникам за вартістю, часом, термінами або якістю. Крім того, під

час управління проєктними ризиками варто враховувати той фактор, що більшість ІТ-проєктів унікальні, а іноді взагалі не мають аналогів. Саме тому й ризики для кожного з таких проєктів мають свою особливість.

Мета дослідження

Метою проведеного дослідження є виконання детального аналізу ризиків, пов'язаних із реалізацією веб-ресурсу, призначеного для покращення комунікації між освітнім закладом і стейкхолдерами (здобувачами, абітурієнтами, випускниками, співробітниками, роботодавцями та ін.). У статті проведено комплексний огляд потенційних ризикових ситуацій, що можуть виникнути під час розробки й експлуатації цього веб-ресурсу. Підсумковий аналіз ризиків дає змогу розробникам, управлінцям і зацікавленим сторонам краще зрозуміти важливість аспектів безпеки та планування для успішної реалізації запропонованого ІТ-проєкту з мінімізацією можливих негативних наслідків.

Виклад основного матеріалу дослідження

Останніми роками здобувачі досить часто самостійно створюють групи спілкування для однокласників, однокурсників або загальні групи для здобувачів чи абітурієнтів того чи іншого навчального закладу. Найчастіше для цього використовують он-лайн соціальні мережі або месенджери: Телеграм-канали, Discord, Instagram, Facebook, Instagram, Twitter тощо. Бажання спілкуватися, ділитися новинами, враженнями й іншою інформацією – важливе питання для розвитку будь-якої особистості. Але часто такі групи мають суто неформальний характер і не несуть інформаційної цінності з погляду донесення до співробітників ВНЗ, здобувачів або абітурієнтів офіційної інформації чи поточних новин окремої кафедри.

Мета ІТ проєкту полягає в створенні й адмініструванні сторінок кафедри штучного інтелекту й аналізу даних Інституту штучного інтелекту та робототехніки Національного університету «Одеська політехніка» в трьох соціальних мережах. Для кожної онлайн мережі (Facebook, Twitter, Instagram) призначено окремого адміністратора, а також керівника групи.

Ухвалення проєктних рішень зазвичай відбувається в умовах ризику та невизначеності. Основними причинами їх наявності є:

- відсутність повної інформації про продукт проєкту, проєктне середовище, неможливість точного оцінювання необхідних для роботи параметрів проєкту;
- неможливість абсолютного прогнозування всіх чинників, що можуть вплинути на проєкт;
- наявність суб'єктивних чинників, пов'язаних з інтересами стейкхолдерів.

Багатоаспектність ризику як складного явища зумовлює існування кількох визначень понять ризику з різних поглядів. Наведемо визначення ризику за класикою проєктного управління з PMBOOK.

Ризик проєкту – це невизначена подія або умова, настання якої негативно чи позитивно позначається на цілях проєкту, змісті, розкладу, вартості та якості [8].

Найбільша увага в проєктному ризик-менеджменті приділяється саме негативним ризикам. Уже на етапі планування керівникові проєкту треба ідентифікувати, проаналізувати ризики й обрати метод реагування на них з метою нівелювання негативного впливу ризику на проєкт.

Для ідентифікування ризиків у контексті аналізу проєктів, у тому числі й у розробці веб-ресурсу для комунікації освітніх закладів, може бути використаний SWOT-аналіз [9].

SWOT-аналіз дає змогу розглянути внутрішні й зовнішні аспекти проєкту, оцінити його сильні та слабкі сторони, а також визначити можливості й загрози. Усі ці ризики важливо аналізувати та включити до плану управління ризиками для забезпечення успішної реалізації проєкту. Наприклад, для внутрішніх ризиків можуть бути розроблені плани резервного планування в разі втрати ключових осіб або відрахування студентів. Для зовнішніх ризиків можуть бути розглянуті плани резервного копіювання серверів і резервних шляхів доступу. З урахуванням виявлених сильних

сторін, слабких сторін, можливостей і загроз можна розробити конкретні стратегії для управління ризиками. Наприклад, розглянути можливість підготовки команди до можливих викликів.

Визначені ризики внутрішнього й зовнішнього середовища ІТ-проєкту для проєкту, що розглядається, подано в табл. 1.

Таблиця 1

Ризики внутрішнього та зовнішнього середовища ІТ-проєкту

Середовище проєкту	Ризики
Внутрішнє	Звільнення викладача Відрахування студента Ліквідація кафедри або інституту Особиста дисципліна виконавців
Зовнішнє	Відсутність інтернет-доступу Відсутність доступу до сервісу через «падіння» його серверу Відсутність доступу до сервісу через його власні блокування Блокування доступу до сервісу через унесення його до «чорного списку» сайтів

Для кожного ідентифікованого ризику визначено причину його виникнення – фактор ризику, проведено класифікацію ризиків за ознаками: час дії та керованість (табл. 2).

Таблиця 2

Класифікація ризиків

Ризик	Фактор ризику	Час дії	Керованість
Звільнення викладача	Людські ресурси підприємства	Після запуску проєкту	Керований
Відрахування студента	Людські ресурси підприємства	Після запуску проєкту	Керований
Ліквідація кафедри або інституту	Діяльність ВНЗ	Весь час існування проєкту	Керований
Особиста дисципліна виконавців	Особистий фактор	Весь час існування проєкту	Керований
Відсутність інтернет-доступу у виконавців	Форс-мажорні обставини	Весь час існування проєкту	Не керований
Відсутність доступу до сервісу через «падіння» його серверу	Форс-мажорні обставини	Весь час існування проєкту	Не керований
Відсутність доступу до сервісу через його власні блокування	Діяльність підприємства-власника сервісу	Весь час існування проєкту	Не керований
Блокування доступу до сервісу через унесення його до «чорного списку» сайтів	Загальнодержавна політика й законодавство	Весь час існування проєкту	Не керований

Основними інструментами якісного аналізу ризиків є матриця ймовірності й впливу (рейтинги ризиків на підставі комбінації та оцінювання їх ймовірності та ступеня впливу) [10].

Визначимо ранг кожного ідентифікованого ризику залежно від двох показників: ймовірність настання ризику та його впливу на проєкт. Після визначення ймовірності та впливу для кожного ризику вони комбінуються. Це допомагає визначити загальний ризикований ранг для кожного ризику.

Результати цього визначення рангів ризиків можуть бути використані для подальшого планування й розробки стратегій управління ризиками. Також це допомагає визначити, на які ризики потрібно звернути особливу увагу, якщо вони мають високий рівень впливу та ймовірності. Ступінь ризику визначені як добуток ймовірності появи ризику й величини втрат. Отримані результати представлено в табл. 3.

Таблиця 3

Ранжування ризиків проєкту

Ризик	Імовірність появи ризику	Величина втрат	Ступінь впливу ризику	Рівень загрози ризику
Звільнення викладача	Імовірна 3	Середня 3	Помірний 9	Виправданий 9
Відрахування студента	Малоймовірна 2	Мінімальна 1	Ігнорований 2	Прийнятний 2
Ліквідація кафедри або інституту	Слабоймовірна 1	Максимальна 5	Незначний 5	Виправданий 9
Особиста дисципліна виконавців	Імовірна 3	Середня 3	Помірний 9	Виправданий 9
Відсутність інтернет-доступу у виконавців	Імовірна 3	Мінімальна 1	Ігнорований 3	Прийнятний 2
Відсутність доступу до сервісу через «падіння» його серверу	Малоймовірна 2	Низька 2	Ігнорований 4	Прийнятний 2
Відсутність доступу до сервісу через його власні блокування	Слабоймовірна 1	Висока 4	Ігнорований 4	Прийнятний 2
Блокування доступу до сервісу через унесення його до «чорного списку» сайтів	Слабоймовірна 1	Висока 4	Ігнорований 4	Прийнятний 2

Вплив ризику на результативність ІТ проєкту зумовлюється зміною значень складників трикутника управління проєктами (час (time), вартість (cost), зміст (score) проєкту). Значення зміни параметрів, що відбуваються як результат впливу ризику, визначають експертним шляхом. Для адміністрування трьох соціальних мереж, якщо розглядаємо вплив ризиків на параметри проєкту (час, вартість, зміст), можна обґрунтувати силу впливу так (табл. 4).

Таблиця 4

Обґрунтування сили впливу

Параметр	Час	Вартість	Зміст
Звільнення викладача	6 Сильний вплив, оскільки втрата викладача може призвести до необхідності перерозподілу обов'язків і часу інших членів команди	2 Слабкий вплив, можливість замінити відповідальну особу	3 Слабкий вплив, можливі зміни в змісті мало залежать від виконавця
Відрахування студента	3 Слабкий вплив, можливий невеликий перерозподіл часу для роботи над проєктом	2 Слабкий вплив, можливі незначні додаткові витрати на взаємодію з іншими студентами	1 Відсутній вплив, відрахування студента не має суттєво впливати на зміст проєкту
Ліквідація кафедри або інституту	9 Сильний вплив, можуть знадобитися значні зусилля для адаптації проєкту до змін у структурі університету	8 Сильний вплив, можливі великі додаткові витрати на адаптацію та зміни в проєкті	7 Середній вплив, можливі зміни в програмі та змісті проєкту під нові умови
Особиста дисципліна виконавців	4 Середній вплив, можливі невеликі відхилення в графіку роботи над проєктом	2 Слабкий вплив, можливі незначні додаткові витрати на контроль	3 Слабкий вплив, дисципліна виконавців не повинна впливати на зміст проєкту
Відсутність інтернет-доступу у виконавців	7 Сильний вплив, можлива втрата робочого часу й переривання в роботі над проєктом	5 Середній вплив, можливі додаткові витрати на забезпечення інтернет-доступу	7 Сильний вплив, доступ до ресурсів для проєкту може бути обмеженим

Закінчення таблиці 4

Параметр	Час	Вартість	Зміст
Відсутність доступу до сервісу через «падіння» його серверу	7 Сильний вплив, можливе переривання роботи над проектом через недоступність сервісу	6 Середній вплив, можливі додаткові витрати на відновлення роботи сервера	5 Середній вплив, зміни в змісті можуть бути обмежені
Відсутність доступу до сервісу через його власні блокування	5 Середній вплив, можливі незначні перерви в роботі над проектом	4 Середній вплив, можливі додаткові витрати на відновлення доступу	4 Середній вплив, можуть виникнути зміни в змісті через обмеження доступу
Блокування доступу до сервісу через унесення його до «чорного списку» сайтів	7 Сильний вплив, можливі перерви в роботі над проектом через обмеження доступу	7 Сильний вплив, можливі додаткові витрати на забезпечення доступу до інших ресурсів	5 Середній вплив, можливі зміни в змісті через обмеження доступу й використання інших сервісів з іншими вимогами до змісту

Використовуючи дані таблиці 3, побудуємо діаграми ризиків для кожного з параметрів трикутника ІТ-проекту, на яких відобразимо ступені впливу ситуацій ризику на відповідні параметри (рис. 1).

Сформована так інформаційна панель наочно демонструє силу впливу визначених факторів ризику проекту.

Грунтуючись на ймовірності настання того чи іншого фактору ризику, можемо робити висновок щодо ризикованості проекту загалом і доцільності його впровадження.

У наведеному проекті найбільш впливові ризику слабкоймовірні, тому можна обрати тактику реагування на них – прийняття ризику.

Висновки

У роботі обрано варіант ідентифікування ризиків проекту, який полягає в створенні й адмініструванні сторінок кафедри штучного інтелекту й аналізу даних Інституту штучного інтелекту та робототехніки Національного університету «Одеська політехніка» в трьох соціальних мережах (Facebook, Twitter, Instagram), застосовуючи метод SWOT-аналізу.

Визначено чотири ризики внутрішнього й чотири ризики зовнішнього середовища проекту. Для кожного ідентифікованого ризику визначено причину його виникнення – фактор ризику. Найчастіше факторами ризику обраного проекту є людські ресурси та форс-мажор.

Проведено класифікацію ризиків за ознаками: час дії, керованість. Усі ризики мають вплив протягом усього існування проекту. Внутрішні ризики обраного проекту, на відміну від зовнішніх, керовані.

На основі отриманих даних найбільш впливові на успішність проекту за всіма трьома параметрами час, вартість, зміст – ситуація ризику: ліквідація кафедри або інституту, відсутність інтернет-доступу у виконавців і блокування доступу до сервісу через унесення його до «чорного списку» сайтів.

Найменше впливають на успішність проекту за параметрами часу, вартості та змісту параметри особиста дисципліна виконавців і відрахування студента.

Практична цінність дослідження полягає в можливості подальшого використання розроблених шаблонів та інформаційних панелей для аналізу ризиків аналогічних проектів.

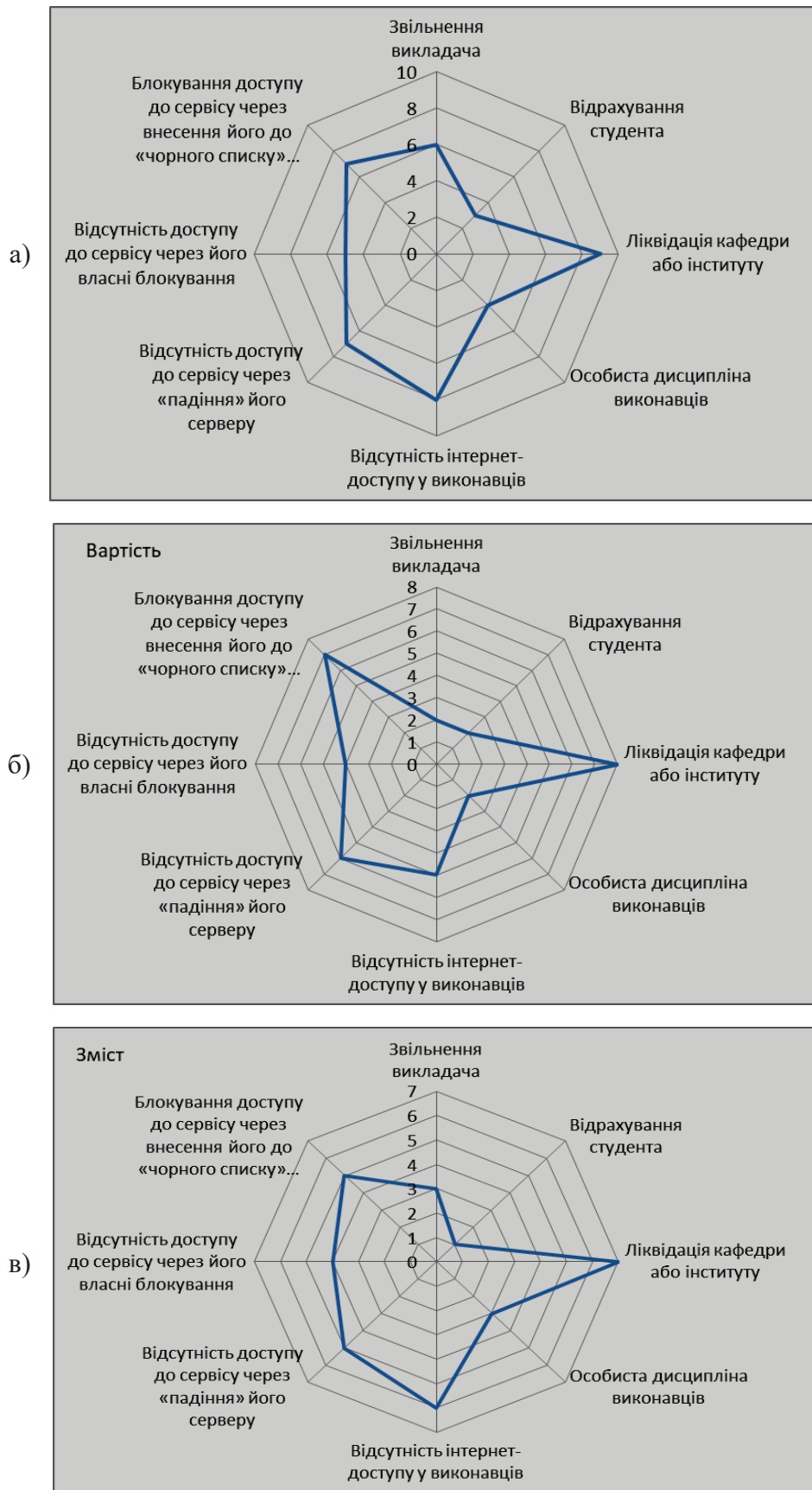


Рис. 1. Вплив ситуацій ризику на час (а), вартість (б), зміст (в)

Список використаної літератури

1. Лазарева С.Ф, Ткаченко М.А. Управління ризиками ІТ-проектів в Україні в сучасних умовах. *Формування ринкових відносин в Україні*. 2015. № 6(169). С. 169–174.
2. Журан О.А., Глава М.Г. Управління ризиками в ІТ-проектах. *Project, Program, Portfolio Management. P3M*. 2016. Vol. 1. С. 46–48.
3. Фонар Л.С., Коновалов О.С., Філіппов Є.Г. Дослідження загроз інформаційної безпеки при використанні веб-технологій дистанційного навчання. *Прикладні питання математичного моделювання*. 2022. Т. 5. № 1. С. 101–107.
4. Рішняк І.В. Система управління ризиками ІТ-проектів. *Інформаційні системи та мережі : збірн. наук. праць*. Львів : Видавництво Національного університету «Львівська політехніка», 2011. С. 250–259.
5. Рішняк І.В. Застосування імітаційних моделей для управління ризиками ІТ-проектів. *Інформаційні системи та мережі : збірн. наук. праць*. Львів : Видавництво Національного університету «Львівська політехніка», 2010. С. 171–181.
6. Назар М.М. Специфіка психологічного впливу навчання користувачів мережі Інтернет. *Освіта дорослих в Україні : матеріали ІХ Міжнар. наук.-практ. конф.* (Київ, 11–17 вер. 2008 р.). Київ : ЕКМО, 2008. С. 102–104.
7. Середа Х.В. Основні принципи побудови інформаційних систем освіти на основі веб-технологій. *Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку : матеріали Всеукраїнської науково-практичної Інтернет-конференції / Черкаський національний університет імені Богдана Хмельницького*. Черкаси, 2013. С. 203–205.
8. A Guide to the Project Management Body of Knowledge (PMBOK® Guide). 7th Edition. Project Management Institute, 2021. 250 p.
9. Шляхта О.М. SWOT-аналіз як інструмент стратегічного менеджменту підприємства. *Економічний простір / Придніпровська державна академія будівництва та архітектури*. 2012. № 68. С. 301–309. URL: http://nbuv.gov.ua/UJRN/ecpros_2012_68_35 (дата звернення: 20.08.2023).
10. ДСТУ ІЕС/ISO 31010:2013 (ІЕС/ISO 31010:2009 IDT). Керування ризиком. Методи загального оцінювання ризику.

References

1. Lazareva, S.F. & Tkachenko, M.A. (2015). Upravlinnia ryzykamy IT-proektiv v Ukraini v suchasnykh umovakh – [IT Project risk management in Ukraine under modern conditions]. *Formuvannia rynkovykh vidnosyn v Ukraini*. Vol. 6(169). P. 169–174. [in Ukrainian]
2. Zhuran, O. A. & Hlava, M.H. (2016).Upravlinnia ryzykamy v IT-proektakh – [Risk Management in IT Projects]. *Project, Program, Portfolio Management. P3M*. Vol. 1. P. 46–48. [in Ukrainian]
3. Fonar, L.S., Konovalov, O.S. & Filippov Ye.H. (2022). Doslidzhennia zahroz informatsiinoi bezpeky pry vykorystanni veb-tekhnohii dystantsiinoho navchannia – [Research on snformation security threats in the use of web technologies for remote learning]. *Prykladni pytannia matematychnoho modeliuвання*. Vol. 5. Is. 1. P. 101–107. [in Ukrainian]
4. Rishniak, I.V. (2011). Systema upravlinnia ryzykamy IT-proektiv – [IT Project risk management system]. *Informatsiini systemy ta merezhi : zbir. nauk. prats*. Lviv : Vydavnytstvo Natsionalnoho universytetu “Lvivska politekhnika”. P. 250–259. [in Ukrainian]
5. Rishniak, I.V. (2010). Zastosuvannia imitatsiinykh modelei dlia upravlinnia ryzykamy IT-proektiv – [Application of Simulation Models for IT Project Risk Management]. *Informatsiini systemy ta merezhi : zbir. nauk. prats*. Lviv : Vydavnytstvo Natsionalnoho universytetu “Lvivska politekhnika”. P. 171–181. [in Ukrainian]

6. Nazar, M.M. (2008). Spetsyfika psykholohichnoho vplyvu navchannia korystuvachiv merezhi Internet – [Specificity of psychological influence of training of Internet users]. *Osvita doroslykh v Ukraini* : IX Mizhnar. nauk.-prakt. konf., (Kyiv, 11–17 ver. 2008 r.). Kyiv : EKMO. P. 102–104. [in Ukrainian]
7. Sereda, Kh.V. (2013). Osnovni pryntsypy pobudovy informatsiinykh system osvity na osnovi veb-tekhnologii. *Avtomatyzatsiia ta kompiuterno-intehrovani tekhnologii u vyrobnytstvi ta osviti: stan, dosiahnennia, perspektyvy rozvytku* : Vseukrainska naukovo-praktychna Internet-konferentsiia / Cherkaskyi natsionalnyi universytet imeni Bohdana Khmelnytskoho. Cherkasy. P. 203–205. [in Ukrainian]
8. A Guide to the Project Management Body of Knowledge (PMBOK® Guide). 7th Edition. Project Management Institute. 250 p. [in English]
9. Shliakhta, O.M. (2012). SWOT-analiz yak instrument stratehichnoho menedzhmentu pidpriemstva. [SWOT analysis as a tool of strategic enterprise management]. *Ekonomichnyi prostir. Prydniprovska derzhavna akademiia budivnytstva ta arkhitektury*. Vol. 68. P. 301–309. URL: http://nbuv.gov.ua/UJRN/ecpros_2012_68_35 (accessed 20.08.2023).
10. DSTU IES/ISO 31010:2013 (IES/ISO 31010:2009,IDT). Keruvannia ryzykom. Metody zahalnoho otsiniuvannia ryzyku.

Журан Олена Анатоліївна – к.е.н., доцент кафедри штучного інтелекту та аналізу даних Національного університету «Одеська політехніка», e-mail: juran@ukr.net, ORCID: 0000-0001-8487-9072.

Фонар Людмила Сергіївна – к.т.н., доцент кафедри штучного інтелекту та аналізу даних Національного університету «Одеська політехніка», e-mail: fonar_1_s@ukr.net, ORCID: 0000-0002-7478-6742.

Коновалов Олександр Сергійович – аспірант кафедри штучного інтелекту та аналізу даних Національного університету «Одеська політехніка», e-mail: akonovalov.lux@gmail.com, ORCID: 0000-0001-8023-9633.

Панін Віктор Олександрович – аспірант кафедри штучного інтелекту та аналізу даних Національного університету «Одеська політехніка», e-mail: panin.8142017@stud.op.edu.ua.

Zhuran Olena Anatoliivna – PhD in Economics, Associate Professor at the Department of Artificial Intelligence and Data Analysis of the Odesa Polytechnic National University, e-mail: juran@ukr.net, ORCID: 0000-0001-8487-9072.

Fonar Liudmyla – PhD in Technology, Associate Professor at the Department of Artificial Intelligence and Data Analysis of the Odesa Polytechnic National University, e-mail: fonar_1_s@ukr.net, ORCID: 0000-0002-7478-6742.

Konovalov Oleksandr Serhiiiovych – Graduate Student at the Department of Artificial Intelligence and Data Analysis of the Odesa Polytechnic National University, e-mail: akonovalov.lux@gmail.com, ORCID: 0000-0001-8023-9633.

Panin Victor Oleksandrovych – Graduate Student at the Department of Artificial Intelligence and Data Analysis of the Odesa Polytechnic National University, e-mail: panin.8142017@stud.op.edu.ua.