ISSN 2311-5149

Отримано: 19 листопада 2024 р.

Прорецензовано: 11 грудня 2024 р.

Прийнято до друку: 15 грудня 2024 р.

e-mail: oleksandr.novoseletskyy@oa.edu.ua

ORCID-ідентифікатор: https://orcid.org/0000-0003-3757-0552

e-mail: andrii.cherniavskyi@oa.edu.ua

ORCID-ідентифікатор: https://orcid.org/0009-0003-7774-7591

ORCID-ідентифікатор: https://orcid.org/0000-0002-4064-755X

DOI: 10.25264/2311-5149-2024-35(63)-71-78

Новоселецький О. М., Чернявський А. В., Данієлене Ю. Управління ризиками на різних етапах життєвого циклу розробки ІТ-проєктів. *Наукові записки Національного університету «Острозька академія». Серія «Економіка» : науковий журнал.* Острог : Вид-во НаУОА, грудень 2024. № 35(63). С. 71–78.

УДК: 005.334

JEL-класифікація: O22; L86

Новоселецький Олександр Миколайович,
кандидат економічних наук, доцент,
доцент кафедри економіко-математичного моделювання та ІТ
Національного університету «Острозька академія»
Чернявський Андрій Володимирович,
викладач кафедри економіко-математичного моделювання та ІТ
Національного університету «Острозька академія»
Данієлене Юрате,
викладач кафедри міжнародних відносин
Державного університету «Клайпедський державний коледж»

УПРАВЛІННЯ РИЗИКАМИ НА РІЗНИХ ЕТАПАХ ЖИТТЄВОГО ЦИКЛУ РОЗРОБКИ ІТ-ПРОЄКТІВ

У цьому дослідженні розглядаються основні ризики, які виникають протягом життєвого циклу ІТ-проекту, включаючи аналіз вимог, проектування системи, розробку програмного забезпечення, тестування, розгортання та обслуговування. Дослідження підкреслює різноманіття ризиків на кожному етапі, включаючи неоднозначність вимог, технічні вразливості, загрози кібербезпеці, обмеження масштабованості, організаційні та фінансові обмеження. Підкреслюється необхідність інтеграції управління ризиками в процес розробки програмного забезпечення, що дозволяє проактивно ідентифікувати та зменшувати невизначеності для запобігання збоям.

Структурований підхід до оцінки ризиків полегшує формулювання ефективних стратегій пом'якшення до того, як потенційні загрози посиляться. Основні методи включають повну документацію, автоматизоване тестування, безперервну інтеграцію та розгортання, гнучкі методології розробки та дотримання стандартизованих структур. Особлива увага приділяється заходам кібербезпеки, враховуючи зростаючу кількість витоків даних, несанкціонованого доступу та проблем, пов'язаних із відповідністю в ІТ-проектах. Крім того, дослідження підкреслює важливість ефективного спілкування та співпраці між зацікавленими сторонами проекту для забезпечення прозорості управління ризиками. Регулярна оцінка ризиків, активне залучення зацікавлених сторін і адаптивні процеси прийняття рішень сприяють підвищенню стійкості та гнучкості проекту. Крім того, інтеграція прогнозної аналітики та інструментів оцінки ризиків на основі штучного інтелекту визначено як засіб покращення стратегій виявлення ризиків і пом'якшення. Впроваджуючи цілісну структуру управління ризиками, ІТ-проектні групи можуть значно підвищити стабільність проекту, операційну ефективність і безпеку. Результати цього дослідження сприяють розвитку найкращих практик для пом'якшення невизначеності, оптимізації результатів проекту та забезпечення довгострокової стійкості в технологічному ландшафті, що розвивається.

Ключові слова: *ризик, управління ІТ-проектами, управління ризиками, життєвий цикл розробки програмного забезпечення, кібербезпека, стратегії зниження ризиків, прогнозна аналітика.*

Oleksandr Novoseletskyy,
Associate Professor of the Department of Economic-Mathematical Modeling and Informational Technologies
National University of Ostroh Academy
Andriy Chernyavskiy,
Lecturer at the Department of Economic-Mathematical Modeling and Informational Technologies
National University of Ostroh Academy
Jūratė Danielienė,
Lecturer at the Department of International Relations
Klaipėdos valstybinė kolegija / Higher Education Institution

RISK MANAGEMENT AT DIFFERENT STAGES OF THE IT PROJECT DEVELOPMENT LIFE CYCLE

This research explores the primary risks associated with the IT project lifecycle, covering stages such as requirement analysis, system design, software development, testing, deployment, and maintenance. The study emphasizes the varied nature of risks at each phase, including unclear requirements, technical weaknesses, cybersecurity threats, scalability issues, and organizational or financial limitations. It stresses the importance of embedding risk management into the software development process to proactively identify and address uncertainties, thereby minimizing disruptions. Effective identification, assessment, and mitigation of risks at various stages of the software development lifecycle are essential for ensuring system stability, security, and successful project execution. Risk management serves as a critical component in minimizing potential failures, optimizing resource utilization, and enhancing overall project efficiency.

A systematic approach to risk assessment enables the development of effective mitigation strategies before potential issues escalate. Key methods include thorough documentation, automated testing, continuous integration and deployment, agile practices, and compliance with standardized frameworks. Special focus is placed on cybersecurity measures due to the increasing prevalence of data breaches, unauthorized access, and compliance challenges in IT projects.

The study also highlights the critical role of communication and collaboration among stakeholders to ensure transparency in risk management. Regular risk evaluations, active stakeholder involvement, and adaptive decision-making processes enhance project resilience and adaptability. Additionally, the use of predictive analytics and AI-driven risk assessment tools is identified as a way to improve risk detection and mitigation.

By adopting a comprehensive risk management framework, IT project teams can enhance project stability, operational efficiency, and security. The findings of this study offer valuable insights for developing best practices to reduce uncertainties, optimize project outcomes, and ensure long-term sustainability in a rapidly evolving technological environment.

Keywords: *risk, IT project management, risk management, software development lifecycle, cybersecurity, risk mitigation strategies, predictive analytics.*

Постановка проблеми. В умовах швидкого розвитку інформаційних технологій та високої динаміки змін на ринку, управління ризиками в ІТ-проектах стає не лише важливим, а й критичним елементом для забезпечення стабільності і надійності розроблених систем. Враховуючи поточні виклики, такі як економічна нестабільність, геополітична ситуація в Україні та розвиток нових технологій, ефективне управління ризиками допомагає не лише забезпечити стабільну роботу системи, але й запобігти можливим загрозам, що можуть вплинути на її успішну реалізацію.

Актуальність цієї теми також підкріплюється необхідністю підвищення надійності та безпеки ІТ-проєктів у складних умовах, зокрема з урахуванням військових загроз, кібератак та проблем із персоналом через зовнішні обставини. Врахування таких чинників у системі управління ризиками є важливим для кожного етапу розробки, починаючи від ідеї до впровадження та супроводу. Оцінка ризиків дозволяє проактивно виявляти слабкі місця, своєчасно адаптувати стратегії та знижувати ймовірність негативних наслідків для проекту.

Аналіз останніх досліджень та публікацій. Останні дослідження та публікації в цій галузі демонструють різні підходи до ідентифікації, аналізу та мінімізації ризиків на різних етапах життєвого циклу ІТ-проєктів. Дослідження Френка Найта (Frank H. Knight) щодо ризику та невизначеності заклали теоретичні основи для розуміння природи ризиків у бізнесі та управлінні проектами [1]. У своїй праці він розрізняє ризик, який можна оцінити кількісно та невизначеність, яка не піддається точному вимірюванню. Ця концепція є важливою для розуміння ризиків у ІТ-проєктах, де часто доводиться працювати в умовах високої невизначеності.

Сучасні підходи до управління ризиками в ІТ-проєктах розглядаються у праці Дугласа Хаббард (Douglas W. Hubbard). У своїй книзі «The Failure of Risk Management: Why It's Broken and How to Fix It» він критично аналізує традиційні методи управління ризиками та пропонує нові підходи до їх оцінки та мінімізації [2]. Він наголошує на важливості використання кількісних методів для більш точного прогнозування ризиків. У контексті управління ризиками в ІТ-проєктах важливе значення мають стандарти, зокрема, «A Guide to the Project Management Body of Knowledge (PMBOK® Guide)» [5], який надає детальний опис процесів управління ризиками в рамках управління проектами. Цей стандарт є основним джерелом для багатьох фахівців у галузі проектного менеджменту.

Українські дослідження також внесли значний внесок у розвиток теорії та практики управління ризиками. Наприклад, роботи В. О. Москаленко [3] та О. А. Гавриш [4] присвячені аналізу проектних ризиків та їх впливу на успішність реалізації ІТ-проєктів. У своїх дослідженнях вони наголошують на важливості інтеграції ризик-менеджменту в загальну систему управління проектами. Дослідження О. Б. Данченко та ін. [7] присвячені інтегрованому управлінню ризиками в умовах невизначеності, що є особливо актуальним для ІТ-проєктів, де зміни вимог та зовнішні фактори можуть значно вплинути на результат. Вони пропонують методику, яка дозволяє враховувати як загрози, так і можливості, що виникають під час реалізації проекту.

Таким чином, аналіз останніх досліджень та публікацій демонструє, що управління ризиками в ІТ-проєктах є комплексним процесом, який вимагає інтеграції різних методів та підходів.

Мета і завдання дослідження: провести аналіз ризиків, що виникають на кожному етапі життєвого циклу розробки і впровадження ІТ-проєктів та визначити ефективні стратегій їх мінімізації.

Виклад основного матеріалу дослідження. Розробка ІТ-додатків є комплексним і багатогранним процесом, що включає кілька етапів, кожен із яких має свої особливі виклики та ризики. Серед цих етапів можна виділити аналіз вимог, проектування, розробку, тестування, впровадження, супровід і підтримку, а також оцінку результатів. Оскільки кожен етап має свою технічну і організаційну складність, ризики, які виникають, можуть значно вплинути на кінцевий результат проекту, зокрема, на його ефективність, терміни виконання та бюджет.

Забезпечення ефективного управління ризиками є важливою складовою успішного завершення проекту, оскільки несвоєчасне виявлення чи погане управління ризиками може призвести до серйозних проблем. На кожному етапі життєвого циклу ІТ-додатка ризики можуть проявлятися в різних формах – від технічних дефектів (помилки в коді чи архітектурі) до організаційних труднощів (неповне розуміння вимог замовника або затримок у тестуванні). Для мінімізації їхнього негативного впливу на кінцевий результат проекту необхідно мати чітку стратегію управління ризиками.

Аналіз вимог є ключовим етапом у процесі розробки ІТ-додатків, адже саме він визначає, які функціональні можливості та характеристики повинен мати майбутній продукт. Глибоке розуміння потреб замовника на цьому етапі є основою для успішної розробки, тестування та впровадження. Помилки або недоліки під час збору вимог можуть призвести до розбіжностей між очікуваннями замовника та кінцевим результатом.

Одним із найбільших викликів на цьому етапі є невизначеність вимог, яка часто виникає через відсутність чітких формулювань або недостатній досвід замовника чи кінцевих користувачів у визначенні бізнес-потреб. У результаті вимоги можуть виявитися занадто абстрактними або незрозумілими, що значно ускладнює процес розробки. Ефективним способом зниження цього ризику є створення докладної та зрозумілої документації, яка чітко описує функції продукту та технічні характеристики, необхідні для їх реалізації.

Ще однією поширеною проблемою є неповне розуміння потреб замовника. Це може траплятися, якщо замовник не в змозі повністю сформулювати свої очікування, або команда розробників неправильно інтерпретує ці вимоги. У таких ситуаціях можливі помилки в проектуванні та реалізації, що призводить до додаткових витрат і затримок. Для уникнення цього ризику важливо активно залучати замовника та кінцевих користувачів до процесу збору вимог, використовуючи методи інтерв'ю, опитувань або спільних воркшопів. Такий підхід дозволяє уточнити деталі та встановити чіткі пріоритети.

Зміни вимог у процесі розробки також можуть створити значні труднощі. Вони часто спричинені змінами в бізнес-цілях, зовнішніми обставинами або новими технологічними викликами. Це може викликати затримки в реалізації проекту, адже команда змушена адаптуватися до нових умов, що нерідко призводить до збільшення витрат. Для мінімізації цього ризику необхідно регулярно переглядати вимоги, проводити зустрічі із замовником та оперативно оцінювати можливий вплив змін на проект.

Успішне управління ризиками на етапі аналізу вимог залежить від створення детальної документації, активної участі замовника та кінцевих користувачів, а також постійного моніторингу змін. Такий підхід дозволяє не лише забезпечити чітке розуміння потреб, але й закласти надійну основу для подальших етапів розробки.

Аналізуючи вище наведене, можемо виокремити проаналізовану інформацію у схему (рис. 1).

Успішне управління ризиками на етапі аналізу вимог залежить від створення детальної документації, активної участі замовника та кінцевих користувачів, а також постійного моніторингу змін. Такий підхід дозволяє не лише забезпечити чітке розуміння потреб, але й закласти надійну основу для подальших етапів розробки.

Етап проектування є ключовим у створенні ІТ-додатка, оскільки саме тут закладаються основи архітектури, визначаються основні компоненти та їхня взаємодія. Рішення, прийняті на цьому етапі, впливають на функціональність, продуктивність, масштабованість і безпеку продукту.

Врахування вимог замовника та їх адаптація до технічних реалій є важливими аспектами. Типові ризики на етапі проектування включають ризики представлені в табл. 1.

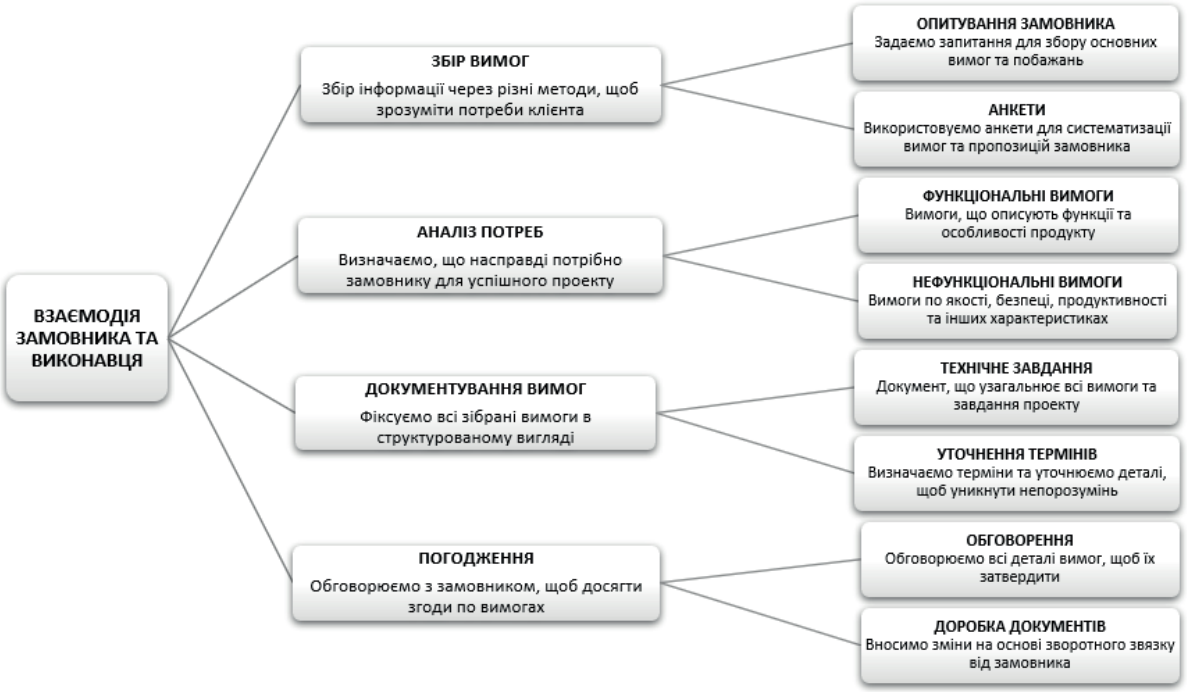

Рис. 1. Схема взаємодії замовника та виконавця

Таблиця 1

Оцінка можливих ризиків проектування

Ризик	Ймовірність	Вплив	Приклад наслідків	Стратегії управління
Помилки в архітектурі	Висока	Критичний	Погана продуктивність, збої у роботі додатка	Використання шаблонів, залучення експертів
Невідповідність технічним вимогам	Середня	Високий	Неможливість реалізувати всі функції, зазначені в документації	Регулярні ревізії, перевірка відповідності вимогам
Складність інтеграції з іншими системами	Середня	Середній	Затримки у розробці, додаткові витрати на доопрацювання інтеграції	Стандартизація інтерфейсів, тестування інтеграції

Етап проектування є ключовим для успішної реалізації ІТ-додатка, оскільки саме тут визначаються основні параметри, в рамках яких працюватиме вся команда. Неправильні рішення, ухвалені на цьому етапі, можуть не тільки затримати розробку, але й спричинити значні витрати на виправлення помилок, що може привести до перевищення бюджету.

Етап розробки є критичним у створенні ІТ-додатків, адже саме тут концепція стає реальним продуктом, що відповідає вимогам замовника. Важливо реалізувати програмний код, інтегрувати компоненти системи та забезпечити відповідність технічним вимогам. Однак цей етап пов’язаний з ризиками, які можуть виникнути через помилки в коді, невідповідність вимогам або певні технічні труднощі. Вони можуть спричинити затримки, збільшення витрат і погіршення якості продукту.

Для зменшення ймовірності помилок потрібно використовувати стандарти кодування, проведення перевірок коду та автоматизоване тестування. Важливо також забезпечити ефективну комунікацію в команді, щоб вчасно виявляти розбіжності у вимогах. Такі інструменти як CI/CD, профілювальники продуктивності та статичний аналіз коду допомагають підтримувати якість на високому рівні. Адаптивність до змін вимог і злагоджена робота з іншими етапами життєвого циклу допомагають уникати значних втрат у часі чи якості.

Особливо важливим є виявлення і корекція програмних помилок, технічних проблем із сумісністю та продуктивністю, а також ризиків, пов’язаних з неефективною комунікацією. Використання гнучких методологій і систем управління проектами дозволяє знизити ймовірність затримок і покращити координацію в команді. Застосування цих стратегій дає можливість зменшити ризики та підвищити ефективність етапу розробки.

Таблиця 2

Ризики та стратегії управління на етапі розробки

Ризик	Ймовірні наслідки	Стратегії управління
Програмні помилки	Затримки в розробці, збої в роботі, помилки в даних	Стандарти кодування, code review, автоматизоване тестування коду
Невідповідність вимогам функціональності	Некоректна робота програми, додаткові витрати	Поетапна розробка, прототипування, регулярні перевірки відповідності функціоналу
Технічні проблеми	Зниження продуктивності, проблеми з сумісністю чи безпекою	Регулярне проведення перформанс-тестів, інструменти оптимізації, стандарти безпеки
Комунікаційні проблеми в команді	Непорозуміння, дублювання роботи, затримки	Впровадження агільних методів, використання систем управління проектами, підтримка відкритої комунікації
Невиконання термінів через недооцінку складності завдань	Затримки в розробці, перевищення бюджету	Оцінка складності завдань, перегляд оцінок і планів, гнучкість у плануванні

Використання ефективних стратегій, таких як стандарти кодування, ревізія коду, автоматизоване тестування, а також забезпечення відкритої комунікації в команді та гнучкість у плануванні, допомагає зменшити ймовірність помилок, покращити продуктивність і забезпечити сумісність і безпеку системи. Зважене та стратегічне управління ризиками на етапі розробки забезпечує стабільність і надійність кінцевого продукту, що дозволяє задовольнити вимоги замовника і досягти бізнес-цілей.

Тестування є ключовим етапом у розробці ІТ-додатків, адже саме на цьому етапі виявляються дефекти, які можуть вплинути на стабільність і продуктивність системи. Воно дозволяє оцінити відповідність продукту вимогам, виявити помилки та потенційні проблеми, що можуть виникнути за змінених умов або підвищеного навантаження.

Разом із тим тестування не позбавлене ризиків. Основні з них – невиявлені дефекти, затримки через недостатнє тестування та проблеми із сумісністю на різних платформах. Ці ризики можуть призвести до помилок після запуску продукту, затримок у графіку або необхідності переробки компонентів.

Для їх мінімізації важливе ретельне планування, використання різних рівнів тестування (модульного, інтеграційного, системного) та автоматизація процесів. Це підходи, які забезпечують якість, стабільність і відповідність продукту бізнес-цілям.

Таблиця 3

Типи тестів та їх роль у зменшенні ризиків

Тип тесту	Роль у зменшенні ризиків
Модульне тестування	Виявляє помилки на рівні окремих компонентів, що дозволяє виправити їх на ранніх етапах.
Інтеграційне тестування	Перевіряє взаємодію між компонентами, що допомагає виявити проблеми сумісності та інтеграції.
Системне тестування	Перевіряє продукт в цілому, забезпечуючи виявлення проблем на рівні всієї системи.
Тестування продуктивності	Виявляє проблеми з навантаженням та ефективністю, що дозволяє уникнути збоїв при високому навантаженні.
Тестування безпеки	Виявляє вразливості та потенційні загрози для системи, забезпечуючи її захищеність.

Тестування відіграє ключову роль у забезпеченні якості ІТ-додатків і зниженні ризиків, пов'язаних із невиявленими помилками, затримками або несумісністю. Для ефективного управління цими ризиками важливо застосовувати різні рівні перевірки, автоматизовані тести та ретельно продуманий план тестування. Модульне, інтеграційне та системне тестування дозволяють виявляти помилки на різних етапах розробки, забезпечуючи стабільність і надійність фінального продукту.

Етап впровадження є ключовим для переходу ІТ-додатку до реального використання, адже від його успішності залежить стабільна робота системи та задоволеність користувачів. Однак цей процес супроводжується ризиками, які можуть вплинути на ефективність інтеграції та продуктивність після запуску.

Технічні виклики включають можливу несумісність із наявними системами, недостатнє тестування інтеграції та збої в роботі через відсутність стандартів або належної документації. Рішенням є створення тестових середовищ, поетапне впровадження та дотримання стандартів обміну даними.

Організаційні проблеми часто виникають через недостатню підготовку користувачів. Це ускладнює адаптацію, збільшуючи навантаження на підтримку. Навчальні матеріали, інтерактивні інструкції та підтримка на початковому етапі впровадження сприяють зменшенню цих ризиків.

Бізнесові ризики, такі як втрата довіри через збої чи низьку продуктивність, загрожують репутації продукту. Їх можна мінімізувати завдяки стрес-тестуванню, системам моніторингу та резервному копіюванню даних.

Безпекові загрози, пов'язані з неправильною конфігурацією чи застарілими методами аутентифікації, створюють уразливості до кібератак. Для їх запобігання потрібні регулярні аудити, багаторівнева аутентифікація та оновлення систем захисту.

Налагоджена комунікація між командами розробників, тестувальників і технічної підтримки є критично важливою. Відсутність координації може призвести до затримок або помилок, тому варто використовувати інструменти для управління завданнями та регулярно узгоджувати прогрес.

Якісний користувацький досвід забезпечує інтуїтивний інтерфейс, розроблений з урахуванням відгуків користувачів і тестувань прототипів, що сприяє кращій адаптації системи.

Аналіз ризиків етапу розробки наведено в наступній таблиці.

Таблиця 4

Результати аналізу ризиків на етапі впровадження

Тип ризику	Ризик	Ймовірність	Вплив	Стратегія вирішення
Технічний	Несумісність з існуючими системами	Висока	Високий	Тестування у тестовому середовищі, використання стандартів обміну даними (REST, GraphQL)
	Невірна конфігурація серверного оточення	Середня	Високий	Детальне налаштування серверного оточення, перевірка налаштувань перед запуском
	Проблеми з масштабуванням при високих навантаженнях	Середня	Високий	Стрес-тестування, використання балансування навантаження
Організаційний	Недостатнє навчання користувачів	Середня	Середній	Розробка навчальних матеріалів, тестовий період для користувачів
	Відсутність чіткої документації про нову систему	Висока	Середній	Створення детальної документації, відео-інструкцій
	Низька залученість співробітників до процесу впровадження	Середня	Середній	Проведення мотиваційних заходів, організація зустрічей з користувачами
Бізнесовий	Втрата довіри користувачів через технічні збої	Висока	Високий	Впровадження моніторингу в реальному часі, резервне копіювання та стрес-тестування
	Відставання від конкурентів через затримки впровадження	Середня	Середній	Планування поетапного запуску, ретельний моніторинг конкурентів
	Недостатнє фінансування для масштабування системи	Середня	Високий	Оцінка потреб в ресурсах на ранніх етапах, пошук додаткових інвестицій
Безпековий	Неправильна конфігурація системи	Низька	Високий	Аудит безпеки, багаторівнева аутентифікація, регулярні оновлення безпеки
	Витік даних через ненадійні канали зв'язку	Середня	Високий	Використання шифрування, захищені протоколи передавання даних
	Атаки через вразливості в сторонніх бібліотеках чи компонентах	Низька	Високий	Регулярне оновлення сторонніх компонентів, використання тільки перевірених бібліотек
Комунікаційний	Недостатня взаємодія між командами	Середня	Середній	Регулярні зустрічі та використання платформ для комунікації (Jira, Slack)
	Невизначеність у комунікаціях щодо змін вимог і часу впровадження	Середня	Середній	Постійні зустрічі зі всіма зацікавленими сторонами, чітке документування змін
	Відсутність чіткої координації між розробниками та відділом технічної підтримки	Висока	Середній	Спільна робота на всіх етапах проєкту, регулярні оновлення статусу
Користувацький	Низька прийнятність системи серед користувачів	Середня	Високий	Тестування інтерфейсу, збір відгуків, залучення користувачів до тестування прототипів
	Висока складність у використанні нової системи	Середня	Середній	Спрощення інтерфейсу, організація тренінгів та навчальних сесій
	Відсутність належної адаптації інтерфейсу до потреб користувачів	Середня	Середній	Опитування користувачів, регулярні оновлення та адаптація інтерфейсу

Ця таблиця дає більш детальний огляд ризиків, що можуть виникнути під час впровадження IT-додатку з огляду на різні аспекти. Для кожного ризику визначено ймовірність, вплив на проект і можливі стратегії вирішення. Натомість, якщо розглядати кожен етап впровадження окремо, можемо визначити ряд ризиків, які відображаються в наступній таблиці.

Таблиця 5

Основні ризики відповідно до різних етапів впровадження

Етап впровадження	Основні ризики	Заходи мінімізації ризиків
Планування	Неправильне визначення вимог, недоліки в ресурсному плануванні	Докладний аналіз вимог, залучення ключових зацікавлених осіб, створення резерву ресурсів
Тестування	Невиявлені баги або вразливості, неповне тестування	Проведення різних типів тестування: функціонального, навантажувального, безпеки
Навчання	Недостатня підготовка користувачів, опір змінам	Організація навчальних сесій, підтримка користувачів, залучення тренерів
Пілотний запуск	Проблеми під час запуску, невідповідність очікуванням	Обмежене впровадження на обраних користувачах, зворотний зв'язок для корекції
Масштабування	Складнощі з масштабуванням системи, проблеми з продуктивністю	Поетапне масштабування, забезпечення гнучкості архітектури, резервне планування
Підтримка	Збої в роботі системи, відсутність швидкого реагування	Постійний моніторинг, створення команди підтримки, планування резервних заходів

Цією таблицею ми відображаємо основні ризики для кожного етапу процесу впровадження та кроки для мінімізації цих ризиків.

Висновки. Таким чином, ми проаналізували етапи життєвого циклу ІТ-додатку до його впровадження, розглянули характерні ризики та стратегії їх мінімізації. На етапі аналізу вимог ключовими проблемами є невизначеність та неповне розуміння потреб замовника, що вирішується шляхом створення чіткої документації та регулярного перегляду вимог. Під час проектування та розробки ризики, пов'язані з архітектурними і програмними помилками, зменшуються завдяки використанню шаблонів проектування та паралельному тестуванню. Етап тестування спрямований на зниження кількості дефектів за допомогою багаторівневого підходу та автоматизації. Впровадження супроводжується викликами, пов'язаними з інтеграцією у продуктивному середовищі та адаптацією користувачів, які вирішуються поетапним підходом і планом відновлення. Для кращого розуміння та контролю процесів управління ризиками використовуються схеми й таблиці, що забезпечують візуалізацію ключових аспектів.

Література:

1. Frank H. Knight. Risk, Uncertainty and Profit. <https://www.econlib.org/library/Knight/knRUP.html> (2024, December, 02).

2. Hubbard D. W. (2020). Failure of Risk Management: Why It's Broken and How to Fix It. Wiley & Sons, Incorporated, John, 2020. 384 с.

3. Москаленко В. О. (2013). Теоретичні аспекти аналізу проектних ризиків. Наукові праці Національного університету харчових технологій. 2013. № 52. С. 129-136.

Moskalenko V. O. (2013). Teoretychni aspekty analizu proektnykh ryzykiv [Theoretical aspects of project risk analysis]. Naukovi pratsi Natsionalnoho universytetu kharchovykh tekhnolohii [Scientific works of the National University of Food Technologies]. 2013. № 52. S. 129-136. [in Ukrainian].

4. Гавриш О. А., Мельникова В. А. (2021). Роль проектного ризику в загальній системі ризик-менеджменту. Бізнес, інновації, менеджмент: проблеми та перспективи : зб. тез доп. II Міжнар. наук.-практ. конференції, 22 квітня 2021 р. Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. С. 50-51.

Havrysh O. A., Melnykova V. A. (2021). Rol proektnoho ryzyku v zahalnii systemi ryzyk-menedzhmentu [The role of project risk in the general risk management system.]. Biznes, innovatsii, menedzhment: problemy ta perspektyvy: zb. tez dop. II Mizhnar. nauk.-prakt. konferentsii, 22 kvitnia 2021 r. [Business, innovation, management: problems and prospects: collection of abstracts of the II International Scientific and Practical Conference (April,22,2021)] Kyiv: KPI im. Ihoria Sikorskoho, Vyd-vo «Politekhnika» [Kyiv: Igor Sikorsky Kyiv Polytechnic Institute, Publishing House "Polytechnica"], 2021. S. 50-51. [in Ukrainian].

5. A Guide to the Project Management Body of Knowledge (PMBOK). (7 Ed.) (2019). Chicago: Project Management Institute, 2019.

6. Danchenko E., Bakulich O., Teslenko P., Bedrii D., Bielova O., Semko I. (2021). Information technology of integrated risk management of scientific projects under uncertainty and behavioral economy. Scientific Journal of Astana IT University. Vol. 5, March 2021. Astana, 2021. P. 63-76.

7. Шендрик В. В., Данченко О. Б., Грабіна К. В. (2020). Синергетичний ефект від управління загрозами та можливостями в ІТ-проєктах Project, Program, Portfolio Management. V міжнародна науково-практична конференція (м. Одеса, 04-05 грудня 2020 року). Одеса: ОНПУ, 2020. С. 26-30.

Shendryk V. V., Danchenko O. B., Hrabina K. V. (2020). Synerhetychnyi efekt vid upravlinnia zahrozamy ta mozhlyvostiamy v IT-proiektakh Project, Program, Portfolio Management.[Synergistic effect of threat and opportunity management in IT projects Project, Program, Portfolio Management.]. V mizhnarodna naukovo-praktychna konferentsiia

(m. Odesa, 04-05 hrudnia 2020 roku) [V international scientific and practical conference (Odessa, December 4-5, 2020).]. Odesa: ONPU, 2020. С. 26-30. [in Ukrainian].

8. Бедрій Д. І. (2021). Інтегроване протиризикове управління науковими проєктами в умовах невизначеності та переходу до циркулярної економіки: дис.... д-ра техн. наук : 05.13.22. Одеса: Держ. ун-т «Одеська політехніка», 2021.

Bedrii D. I. (2021). Intehrovane protyryzykove upravlinnia naukovymy proiektamy v umovakh nevyznachenosti ta perekhodu do tsyrkuliarnoi ekonomiky [Integrated risk management of scientific projects in conditions of uncertainty and transition to a circular economy]: dys.... d-ra tekhn. nauk [diss.... Dr. Tech. Science]: 05.13.22. Odesa: Derzh. un-t «Odeska politekhnika» [Odesa: State University”Odesa Polytechnic”], 2021. [in Ukrainian].