УДК 004.056
DOI https://doi.org/10.32782/IT/2024-1-12

Тетяна САВЧЕНКО
кандидат технічних наук, доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки, Державний торговельно-економічний університет, вул. Кіото, 19, м. Київ, Україна, 02156
***ORCID:** 0000-0002-8884-5360*
***Scopus Author ID:** 57226103860*

Наталія ЛУЦЬКА
доктор технічних наук, професор, професор кафедри автоматизації та комп'ютерних технологій систем управління, Національний університет харчових технологій, вул. Володимирська, 68, м. Київ, Україна, 01601
***ORCID:** 0000-0001-8593-0431*
***Scopus Author ID:** 6603392462*

Лідія ВЛАСЕНКО
кандидат технічних наук, доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки, Державний торговельно-економічний університет, вул. Кіото, 19, м. Київ, Україна, 02156
***ORCID:** 0000-0002-2003-6313*
***Scopus Author ID:** 57202049156*

Бібліографічний опис статті: Савченко, Т., Луцька, Н., Власенко, Л. (2024). Аналіз ризиків при розробці та впровадженні електронної системи управління суб'єкта господарювання. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 1, 98–108, doi: https://doi.org/10.32782/IT/2024-1-12

АНАЛІЗ РИЗИКІВ ПРИ РОЗРОБЦІ ТА ВПРОВАДЖЕННІ ЕЛЕКТРОННОЇ СИСТЕМИ УПРАВЛІННЯ СУБ'ЄКТА ГОСПОДАРЮВАННЯ

Ефективне управління ризиками ІТ-проєктів відіграє ключову роль у процесі їх розробки та впровадження. Для успішного виконання проєкту потрібно ідентифікувати, аналізувати та керувати ризиками, які можуть виникнути на різних етапах проєкту. ***Метою роботи*** *є визначення, обґрунтування та аналіз основних ризиків ІТ-проєкту суб'єкта господарювання якісними та кількісними способами. В роботі розглядається приклад ІТ-проєкту електронної системи управління медичним закладом, що є ефективним інструментом для вдосконалення системи охорони здоров'я, підвищення якості медичного обслуговування та забезпечення більш ефективного використання ресурсів. Цілями ІТ-проєкту є збільшення ефективності управління медичним закладом, покращення якості медичних послуг, забезпечення точності та швидкості обліку медичних послуг і фінансів, а також передбачається забезпечення безпеки даних пацієнтів, що є особливо важливим для медичних закладів. Для впровадження даного ІТ-проєкту необхідно враховувати ряд чинників, які можуть сприяти успішній реалізації бізнес-плану. Основними з них є: підтримка керівництва медичного закладу; розуміння потреб і вимог користувачів; вибір правильної команди розробників; відповідність проєкту стандартам безпеки; фінансові ресурси.* ***Наукова новизна роботи*** *полягає у визначенні та аналізі чинників виникнення ризиків ІТ-проєкту при розробці електронної системи управління медичним закладом та формуванні рекомендованих заходів оптимізації цих ризиків. За попередніми оцінками, впровадження електронної системи управління медичним закладом дозволить зменшити витрати на бухгалтерський облік та кадрове управління на 30%, а також зменшити кількість помилок при розрахунку вартості послуг на 20%. Очікуваний дохід від використання нової системи становитиме близько 1 млн грн на рік, що дасть повну окупність проєкту через 5 років використання системи. Також під час реалізації проєкту були забезпечені додаткові робочі місця, що створило нові робочі місця для інженерів та адміністраторів системи.*

Ключові слова: *ІТ-проєкт, чинники виникнення ризиків, управління ризиками, експертні оцінки, ранжування чинників.*

Tetiana SAVCHENKO
Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Software Engineering and Cybersecurity, State University of Trade and Economics, 19, Kyoto Str., Kyiv, Ukraine, 02156, sv_t@ukr.net
ORCID: *0000-0002-8884-5360*
Scopus Author ID: *57226103860*

Nataliia LUTSKA
Doctor of Technical Sciences, Professor, Professor of Department of Integrated Automated Control Systems, National University of Food Technology, 68, Volodimirska Str., Kyiv, Ukraine, 01601, lutskanm2017@gmail.com
ORCID: *0000-0001-8593-0431*
Scopus Author ID: *6603392462*

Lidiia VLASENKO
Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Software Engineering and Cybersecurity, State University of Trade and Economics, 19, Kyoto Str., Kyiv, Ukraine, 02156, vlasenko.lidia1@gmail.com
ORCID: *0000-0002-2003-6313*
Scopus Author ID: *57202049156*

To cite this article: Savchenko, T., Lutska, N., Vlasenko, L. (2024). Analiz ryzykiv pry rozrobtsi ta vprovadzhenni elektronnoyi systemy upravlinnya sub'yekta hospodaryuvannya [Analysis of risks in the development and implementation of the electronic management system of a business entity]. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 1, 98–108, doi: https://doi.org/10.32782/IT/2024-1-12

ANALYSIS OF RISKS IN THE DEVELOPMENT AND IMPLEMENTATION OF THE ELECTRONIC MANAGEMENT SYSTEM OF A BUSINESS ENTITY

Effective risk management of IT projects plays a key role in the process of their development and implementation. For the successful implementation of the project, it is necessary to identify, analyze and manage the risks that may arise at various stages of the project. ***The purpose of the work*** *is to determine, substantiate and analyze the main risks of the business entity's IT project in qualitative and quantitative ways. The paper considers an example of an IT project of an electronic management system of a medical institution, which is an effective tool for improving the health care system, improving the quality of medical care and ensuring more efficient use of resources. The goals of the IT project are to increase the efficiency of the management of the medical institution, improve the quality of medical services, ensure the accuracy and speed of accounting for medical services and finances, and also provide for the security of patient data, which is especially important for medical institutions. For the implementation of this IT project, it is necessary to take into account a number of factors that can contribute to the successful implementation of the business plan. The main ones are: support of the management of the medical institution; understanding the needs and requirements of users; choosing the right development team; compliance of the project with safety standards; financial resources.* ***The scientific novelty*** *of the work consists in the identification and analysis of the risk factors of the IT project during the development of the electronic management system of the medical institution and the formation of recommended measures to optimize these risks. According to preliminary estimates, the introduction of an electronic management system for a medical facility will reduce the costs of accounting and personnel management by 30%, as well as reduce the number of errors when calculating the cost of services by 20%. The expected income from the use of the new system will be about UAH 1 million per year, which will give the project full payback after 5 years of using the system. Also, additional jobs were provided during the implementation of the project, which created new jobs for engineers and system administrators.*

Key words: *IT project, risk factors, risk management, expert assessments, factor ranking.*

Постановка проблеми. IT-проєкт – це система взаємопов'язаних цілей та програм, спрямованих на досягнення інноваційних результатів. Ця система включає науково-дослідницькі, дослідницько-конструкторські, виробничі, організаційні, фінансові, комерційні та інші заходи, які правильно організовані та документовані у проєктній документації. Вона спрямована на ефективне вирішення конкретних науково-технічних завдань, які вимірюються кількісними показниками. Однак, розробка вітчизняними підприємствами IT-проєктів завжди пов'язана з ризиками (Blyznyukova, 2020), а відмова від проєктної діяльності може призвести до втрати

підприємством своїх ринкових позицій. У зв'язку з цим, дослідження проблем ризиків IT-проєктів стає особливо актуальним.

Управління ризиками IT-проєктів є важливим етапом процесу розробки та реалізації. Для успішного виконання проєкту потрібно ідентифікувати, аналізувати та керувати ризиками, які можуть виникнути на різних етапах проєкту, основні з цих етапів наведені на рис. 1.

Зменшення ризиків IT-проєктів досягається завдяки систематичному підходу до їх оцінки та аналізу, їхньої класифікації, встановлення пріоритетів, планування запобіжних заходів та моніторингу їх реалізації. В результаті проведення управління ризиками можна зменшити вплив потенційно негативних подій на проєкт, знизити ймовірність їх виникнення та мінімізувати можливі втрати. Крім того, управління ризиками дозволяє збільшити впевненість у виконанні проєкту вчасно та в межах запланованого бюджету. Проте, важливо зазначити, що повністю виключити ризики неможливо, оскільки вони пов'язані з невизначеністю та непередбачуваністю. Тому, незалежно від рівня управління ризиками, проєкт повинен бути готовий до того, що негативні події можуть відбутись, та мати запасні плани для їх подолання.

Аналіз останніх досліджень і публікацій. Огляд існуючих підходів до аналізу ризиків при розробці та впровадженні електронної системи управління суб'єкта господарювання демонструє різноманітність методів і моделей, що використовуються в практиці (Natarajan, 2022; Sorooshian, 2020; Чубаєвський, 2023). Один з таких підходів – це аналіз ризиків на основі відомих стандартів, таких як ISO 31000 (Hubarieva, 2023), який надає загальні принципи управління ризиками та визначає процеси їх ідентифікації, оцінки та контролю. Інший підхід (Грабіна, 2023; Грабіна, 2023) полягає в застосуванні конкретних методів, таких як аналіз SWOT (Strengths, Weaknesses, Opportunities, Threats), який дозволяє виявити внутрішні сильні та слабкі сторони суб'єкта господарювання, а також зовнішні можливості та загрози, пов'язані з впровадженням електронної системи управління.

Додатково, існують кілька спеціалізованих підходів (Карпович, 2021; Замула, 2011; Поліщук, 2021), таких як аналіз ризиків інформаційної безпеки, який акцентує на виявленні та запобіганні потенційним загрозам для конфіденційності, цілісності та доступності даних у системі управління. Також варто відзначити підхід, що базується на використанні матриць ризиків (Deshmukh, 2020), де ідентифікуються конкретні ризики та їхній вплив на бізнес-процеси підприємства. Врахування різноманітності підходів дозволяє здійснювати комплексний аналіз ризиків та розробляти ефективні

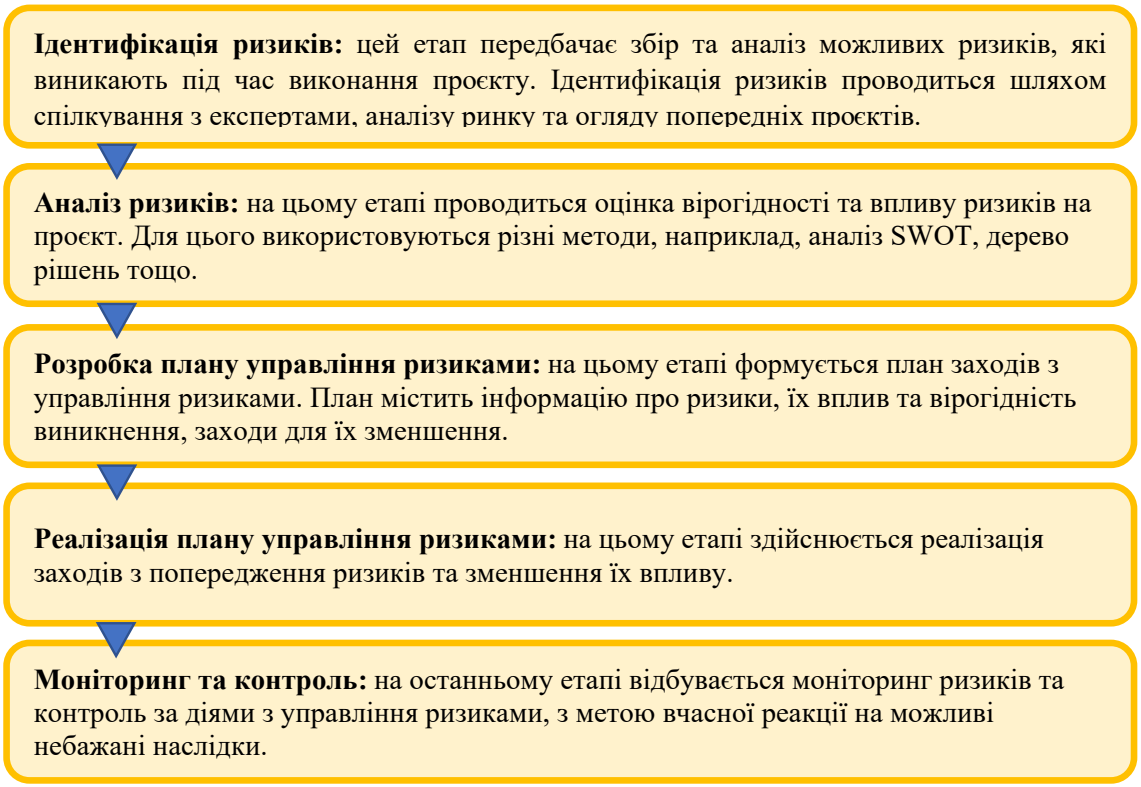

Рис. 1. Основні етапи управління ризиками IT-проєктів

стратегії їхнього управління під час впровадження ІТ-проєкту.

Мета статті. Метою роботи є визначення, обґрунтування та аналіз основних ризиків ІТ-проєкту суб'єкта господарювання якісними та кількісними способами. ІТ-проєкт передбачає розробку та впровадження програмного забезпечення для автоматизації бухгалтерського обліку, кадрового управління, обліку медичних послуг та інвентаризацію.

Виклад основного матеріалу дослідження. У роботі розглядається приклад ІТ-проєкту електронної системи управління медичним закладом, що є ефективним інструментом для вдосконалення системи охорони здоров'я, підвищення якості медичного обслуговування та забезпечення більш ефективного використання ресурсів. Такі проєкти можуть включати в себе різноманітні компоненти та функціональності, спрямовані на поліпшення ефективності управління та надання якісної медичної допомоги.

Цілями ІТ-проєкту є збільшення ефективності управління медичним закладом, покращення якості медичних послуг та забезпечення точності та швидкості обліку медичних послуг і фінансів. Функції системи включають управління пацієнтами, запис на прийом, ведення медичних карток, контроль лікування та розрахунок вартості послуг. Крім того, передбачається забезпечення безпеки даних пацієнтів, що є особливо важливим для медичних закладів.

Основні фактори, які сприяють успішній реалізації бізнес-плану, включають в себе належне фінансування проєкту, відповідну кваліфікацію та компетенції розробників та фахівців, які займаються впровадженням системи, а також ефективне управління проєктом та вчасне виявлення та вирішення можливих проблем.

Для впровадження даного ІТ-проєкту необхідно враховувати ряд чинників, які можуть сприяти успішній реалізації бізнес-плану. Основними з них є: підтримка керівництва медичного закладу; розуміння потреб і вимог користувачів; вибір правильної команди розробників; відповідність проєкту стандартам безпеки; фінансові ресурси.

Основні обмеження реалізації даного проєкту можуть включати: часові обмеження; технічні обмеження; фінансові обмеження; людські ресурси.

Організаційна структурна схема ІТ-проєкту, як правило, включає наступні складові: керівництво проєкту; команда розробників; команда користувачів; команда технічної підтримки. Кожен з вищезгаданих відділів має свої завдання та обов'язки, що пов'язані з розробкою та впровадженням електронної системи управління медичним закладом. Взаємодія між цими відділами та командами є дуже важливою для успішної реалізації проєкту. Крім основних учасників, в проєкт можуть бути включені й інші сторони, наприклад, пацієнти, представники медичного персоналу, консультанти з питань проєктування та розробки програмного забезпечення тощо. В організаційній структурі можуть бути також вказані інші підрозділи, наприклад, відділ забезпечення безпеки даних, відділ контролю якості, відділ підтримки користувачів тощо.

Успішне впровадження електронної системи управління медичним закладом залежить від ефективної співпраці всіх учасників проєкту та їх здатності вирішувати виникаючі питання та проблеми в процесі розробки та впровадження системи. Крім того, успіх проєкту залежить від чіткого планування проєкту, розуміння вимог та очікувань замовника, виконання умов договору та дотримання термінів реалізації проєкту. Важливо також враховувати вимоги та стандарти, які регулюють діяльність медичних закладів, а також вимоги до захисту конфіденційної інформації пацієнтів. Крім технічних аспектів, важливо враховувати людський фактор, зокрема, готовність користувачів до використання нової системи та необхідність проведення навчання. Також важливо забезпечити підтримку та технічне обслуговування системи після впровадження.

Економічна ефективність реалізації проєкту полягає в зменшенні витрат на управління медичним закладом за рахунок автоматизації процесів та покращенні якості медичних послуг за рахунок більш точного та швидкого контролю за діяльністю медичного закладу. Крім того, використання електронної системи управління може збільшити кількість пацієнтів, що обслуговуються, та покращити їх задоволеність якістю обслуговування. За попередніми оцінками, впровадження електронної системи управління медичним закладом дозволить зменшити витрати на бухгалтерський облік та кадрове управління на 30%, а також зменшити кількість помилок при розрахунку вартості послуг на 20%. Очікуваний дохід від використання нової системи становитиме близько 1 млн грн на рік, що дасть повну *окупність проєкту* через 5 років використання системи. Також під час реалізації проєкту були забезпечені додаткові робочі місця, що створило нові робочі місця для інженерів та адміністраторів системи.

Джерела фінансування проєкту: кошти медичного закладу, який є замовником проєкту. Фінансові показники виконання і реалізації проєкту: вартість розробки та впровадження програмного забезпечення, вартість придбання обладнання та витрати на роботу спеціалістів, що займаються встановленням та налаштуванням системи. Фінансові аспекти проєкту включають оцінку вартості проєкту, визначення джерел фінансування, аналіз вартості та користі, оцінку ризиків, пов'язаних з проєктом.

Основні типи ризиків, які можуть бути ідентифіковані в проєкті «Розробка та впровадження

Таблиця 1

Види ризиків IT-проєктів та їх характеристика

№	Види ризиків	Характеристика
1.	Технічні ризики	Пов'язані з можливими проблемами зі створенням, тестуванням та впровадженням програмного забезпечення та апаратного забезпечення (несумісність з іншими системами, незадовільна продуктивність, технічні збої в роботі обладнання, недостатня функціональність, незручність у використанні, помилки в програмному забезпеченні тощо).
2.	Фінансові ризики	Пов'язані з можливими перевищеннями бюджету, незапланованими витратами та іншими фінансовими проблемами, такими як затримки у фінансуванні, витрати на придбання обладнання та програмного забезпечення, оплату послуг фахівців тощо.
3.	Ризики управління проєктом	Пов'язані з можливими проблемами з плануванням, координацією та керуванням проєктом, затримками у розробці та впровадженні системи, що може призвести до зміни планових термінів (затримки у графіку, втрата зв'язку між різними членами команди проєкту, недостатній контроль над виконанням завдань та затримки в процесі прийняття рішень).
4.	Ризики безпеки	Пов'язані з можливими проблемами безпеки даних, які можуть бути збережені в електронній системі управління медичним закладом, можливістю злому системи управління медичним закладом або втратою конфіденційної інформації (можливість несанкціонованого доступу до конфіденційної інформації про пацієнтів, можливість атаки хакерів на систему, витік конфіденційної інформації через недостатні заходи безпеки тощо.
5.	Ризики пов'язані з людським фактором	Пов'язані з можливими помилками при введенні даних, використанні системи не за призначенням, недостатньою кваліфікацією користувачів, можливими проблемами з взаємодією з користувачами системи, такими як недостатня зрозумілість, незадовільна якість обслуговування та інші.
6.	Технологічні ризики	Пов'язані зі значними змінами у технології, що можуть виникнути під час розробки та впровадження системи управління медичним закладом (необхідність переходу на нові технології або використання нових інструментів розробки).
7.	Ризики залежності від постачальників	Пов'язані з можливими проблемами з постачанням необхідних компонентів, послуг та інших ресурсів, можливими проблемами з постачальниками обладнання, програмного забезпечення та іншого необхідного для розробки та впровадження системи (зміни у вимогах до системи можуть призвести до змін у поставках постачальників).
8.	Ризики щодо прийняття системи	Пов'язані з можливим недовір'ям або неприйняттям системи управління медичним закладом користувачами (можливість втрати даних або проблеми з їхньою конфіденційністю можуть спричинити недовіру користувачів до системи).
9.	Ризики щодо потреб користувачів	Пов'язані з можливою недостатньою здатністю системи управління медичним закладом задовольняти потреби користувачів (можливість втрати даних або збоїв в системі можуть призвести до незадоволеності користувачів).
10.	Ризики щодо масштабування системи	Пов'язані з можливою недостатньою здатністю системи управління медичним закладом масштабуватися при зростанні кількості користувачів або обсягу обробки даних (можливість затримок або втрати даних при великому обсязі вхідної інформації).
11.	Ризики щодо правової сумісності	Пов'язані з відповідністю системи управління медичним закладом правовим вимогам і стандартам, таким як законодавство про захист персональних даних, вимоги щодо безпеки медичної інформації тощо.
12.	Ризики бізнесу	Пов'язані з можливістю втрати фінансових ресурсів та недосягнення планованих цілей, що може виникнути в результаті затримок у розробці, втрати даних або проблем з безпекою і т.д.
13.	Ризики кадрової нестабільності	Пов'язані з можливими проблемами зі збереженням та підбором кваліфікованих працівників, необхідних для розробки, впровадження та підтримки системи управління медичним закладом, проблемами у складанні команди, звільненням ключових працівників, недостатнім рівнем кваліфікації персоналу або недостатньою кількістю спеціалістів для виконання проєкту.

електронної системи управління медичним закладом», наведені в табл. 1. Всі ці ризики можуть суттєво вплинути на успішність проєкту та призвести до небажаних наслідків.

Для успішної реалізації проєкту необхідно визначити всі можливі ризики та розробити план дій з їх управління, що дозволить уникнути можливих проблем та забезпечить успішну реалізацію проєкту. Використання планів управління ризиками дозволяє зменшити вплив ризиків та забезпечити успішну реалізацію проєкту. Для того, щоб оцінити чинники виникнення ризиків IT-проєкту, проведено їхню ідентифікацію та групування за класифікаційними ознаками, при цьому одному ризику може відповідати кілька чинників. Умови та обставини, що породжують ризики, можна розділити на контрольовані, тобто ті, що піддаються впливу управлінських рішень підприємства, та неконтрольовані, які зазвичай виникають внаслідок об'єктивної появи випадкових подій.

Отже, за *рівнем управління чинники* згруповано:

Контрольовані: недостатня кваліфікація персоналу (Ч1); недостатня кількість ресурсів (бюджет, людські ресурси, час) (Ч2); необхідність зміни в бізнес-процесах (Ч3); недостатня комунікація між учасниками проєкту (Ч4); недостатній контроль та моніторинг робіт (Ч5).

Неконтрольовані: технічні проблеми з обладнанням та програмним забезпеченням (Ч6); негативний вплив зовнішніх умов (погодні умови, катастрофи, економічні зміни) (Ч7); поява нових конкурентів, технологій та інновацій (Ч8); втрата ключових учасників проєкту через відхід або хворобу (Ч9); зміна пріоритетів та цілей замовника (Ч10).

За *рівнем утворення чинники* розділено:

Внутрішні: недостатня кваліфікація персоналу (Ч1); недостатня кількість ресурсів (бюджет, людські ресурси, час) (Ч2); необхідність зміни в бізнес-процесах (Ч3); недостатня комунікація між учасниками проєкту (Ч4); недостатня контроль та моніторинг робіт (Ч5); технічні проблеми з обладнанням та програмним забезпеченням (Ч6).

*Зовнішні: н*егативний вплив зовнішніх умов (погодні умови, катастрофи, економічні зміни) (Ч7); поява нових конкурентів, технологій та інновацій (Ч8); втрата ключових учасників проєкту через відхід або хворобу (Ч9); зміна пріоритетів та цілей замовника (Ч10).

Переважно аналіз чинників виникнення ризиків проводять за допомогою експертного оцінювання (Afzal, 2021), яке базується на особистому оцінюванні конкретних показників індивідуальними експертами, такими як консультанти або спеціалісти з конкретних питань. Цей метод застосовується у випадках, коли неможливо здобути необхідний обсяг статистичної інформації або коли аналогів такого розвитку подій ще не існує. Наведений метод дозволяє скласти перелік ризиків та їх можливих процесів виникнення, а також провести оцінку цих чинників за десятибальною шкалою та побудувати матрицю рангів для подальшого аналізу. Для оцінки погодженості відповідей експертів використовується коефіцієнт конкордації, що обчислюється за наступною формулою:

$$W = \frac{\sigma_{ф}^2}{\sigma_{\max}^2} = \frac{\sum_{i=1}^{m}\left\{a_i - \frac{1}{2}\cdot n\cdot(m+1)\right\}^2}{\frac{1}{12}\cdot n^2\cdot m\cdot(m^2-1)}, \qquad (1)$$

де $\sigma_{ф}^2$ – фактична дисперсія (середньоквадратичне відхилення) підсумкових оцінок, наданих експертами; $\sigma_{\max}^2$ – дисперсія підсумкових оцінок при умові повного збігу думок експертів; a_i – сумарна оцінка, отримана *i*-м об'єктом; *m* – кількість об'єктів, що досліджується; *n* – кількість експертів.

Визначено ранги чинників виникнення ризиків в IT-проєкті, шляхом присвоєння кожному чиннику певного рангу у послідовності. Результати ранжування чинників виникнення ризиків представлені у табл. 2. Істотність коефіцієнту конкордації перевіряємо за допомогою критерію Пірсона за формулою $\chi^2 = W\cdot n\cdot(m-1)$ з $(m-1)$ числом ступенів свободи.

Оскільки величина коефіцієнта конкордації за (1) становить *W = 0,899*, розрахункове значення $\chi^2_{розр}$ = 0,899·10·9 = 80,91, для якого для (10 – 1) ступенів свободи та довірчої імовірності 0,95 є більшим за табличне $\chi^2_{табл}$ = 16,92 (для довірчої імовірності 0,99 $\chi^2_{табл}$ = 21,69), то можна вважати, що в оцінці впливу ризиків думки експертів є добре узгодженими.

Вагомість чинників розраховується за формулою:

$$w = \frac{l_j + m_j}{\sum_{i=1}^{j}(l_j + m_j)}, \qquad (2)$$

де l_j – сукупна частота переваг *j-ої* групи за рядком; m_j – сукупна частота переваг *j-ої* групи за стовпцем. Результати визначення вагомості чинників виникнення ризиків IT-проєкту представляємо у вигляді матриці (табл. 3).

Загальний бал *h* для кожного чинника виникнення ризику обчислюється за формулою (табл. 4):

Таблиця 2

Оцінювання чинників виникнення ризиків методом експертних оцінок

Чинник	Екс.1	Екс.2	Екс.3	Екс.4	Екс.5	Екс.6	Екс.7	Екс.8	Екс.9	Екс.10	S
Ч1	1	2	2	3	3	2	1	1	2	1	18
Ч2	2	1	1	2	1	1	3	2	3	2	18
Ч3	6	3	4	5	5	5	4	4	5	3	44
Ч4	3	5	6	6	6	4	2	3	4	5	44
Ч5	7	8	8	7	9	9	8	7	8	9	80
Ч6	5	4	3	1	2	6	6	5	1	6	39
Ч7	10	9	10	9	10	10	10	10	9	8	95
Ч8	9	10	9	10	7	8	7	8	10	7	85
Ч9	8	7	7	8	8	7	9	9	7	10	80
Ч10	4	6	5	4	4	3	5	6	6	4	47

Таблиця 3

Матриця вагомості чинників виникнення ризиків ІТ-проєкту

Чинники	Ч1	Ч2	Ч3	Ч4	Ч5	Ч6	Ч7	Ч8	Ч9	Ч10	Сукупна частота переваг за рядком (l_j)	Сукупна частота переваг за стовпцем (m_j)	Сукуп-на частота переваг (l_j+m_j)	Ваговий коефіцієнт, w
Ч1	–	Ч2	Ч3	Ч4	Ч5	Ч6	Ч1	Ч1	Ч9	Ч1	3	0	3	0,065
Ч2	–	–	Ч3	Ч2	Ч2	Ч6	Ч2	Ч2	Ч2	Ч2	6	1	7	0,152
Ч3	–	–	–	Ч3	Ч3	Ч6	Ч3	Ч8	Ч9	Ч10	3	3	6	0,130
Ч4	–	–	–	–	Ч4	Ч6	Ч7	Ч4	Ч9	Ч10	2	1	3	0,065
Ч5	–	–	–	–	–	Ч6	Ч7	Ч5	Ч9	Ч5	2	1	3	0,065
Ч6	–	–	–	–	–	–	Ч6	Ч8	Ч6	Ч10	2	5	7	0,152
Ч7	–	–	–	–	–	–	–	Ч8	Ч9	Ч10	0	2	2	0,043
Ч8	–	–	–	–	–	–	–	–	Ч9	Ч8	1	3	4	0,087
Ч9	–	–	–	–	–	–	–	–	–	Ч9	1	6	7	0,152
Ч10	–	–	–	–	–	–	–	–	–	–	0	4	4	0,087
Разом											**20**	**26**	**46**	**1,00**

Таблиця 4

Ранжування чинників виникнення ризиків ІТ-проєкту

№ з/п	Чинники	Сума бальних оцінок, a_i	Середнє арифме-тичне значення бальної оцінки, v_i	Ваговий коефіцієнт, w_i	Загальний бал, $h = w_i \cdot v_i$	Рейтинг чинника
1.	Ч1	18	1,8	0,065	0,117	1
2.	Ч2	18	1,8	0,152	0,274	2
3.	Ч3	44	4,4	0,130	0,572	7
4.	Ч4	44	4,4	0,065	0,286	3
5.	Ч5	80	8,0	0,065	0,520	6
6.	Ч6	39	3,9	0,152	0,593	8
7.	Ч7	95	9,5	0,043	0,409	5
8.	Ч8	85	8,5	0,087	0,740	9
9.	Ч9	80	8,0	0,152	1,216	10
10.	Ч10	47	4,7	0,087	0,409	4

$$h_i = w_i \cdot v_i = w_i \cdot \frac{\sum_{k=1}^{n} a_{ik}}{K}, \qquad (3)$$

де a_{ik} – сума значень бальних оцінок i-го чинника k-м експертом; K – кількість експертів, залучених до експертного опитування, осіб; v_i – середнє значення бальної оцінки i-го чинника; w_i – ваговий коефіцієнт i-го чинника.

Отже, найвпливовішими чинниками є (рис. 2): недостатня кваліфікація персоналу (Ч1), недостатня кількість ресурсів (Ч2), недостатня комунікація між учасниками проєкту (Ч4), зміна пріоритетів та цілей замовника (Ч10).

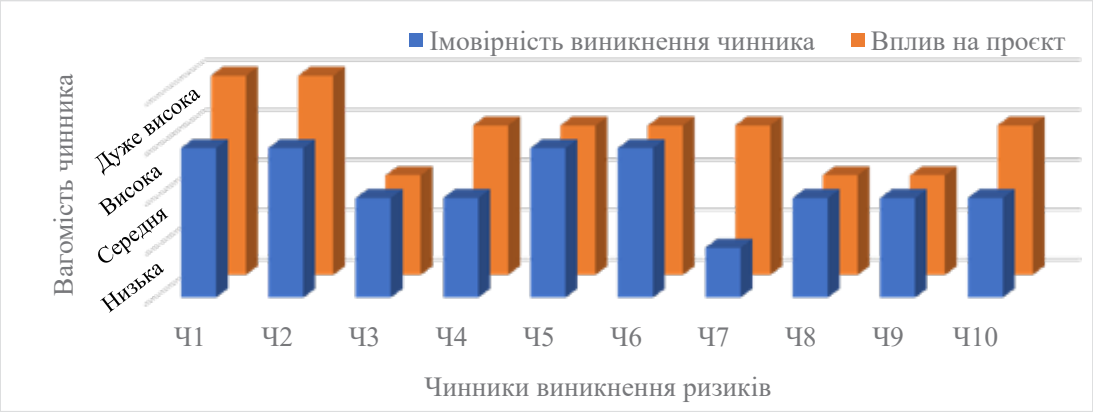

Рис. 2. Розподіл чинників виникнення ризиків ІТ-проєкту

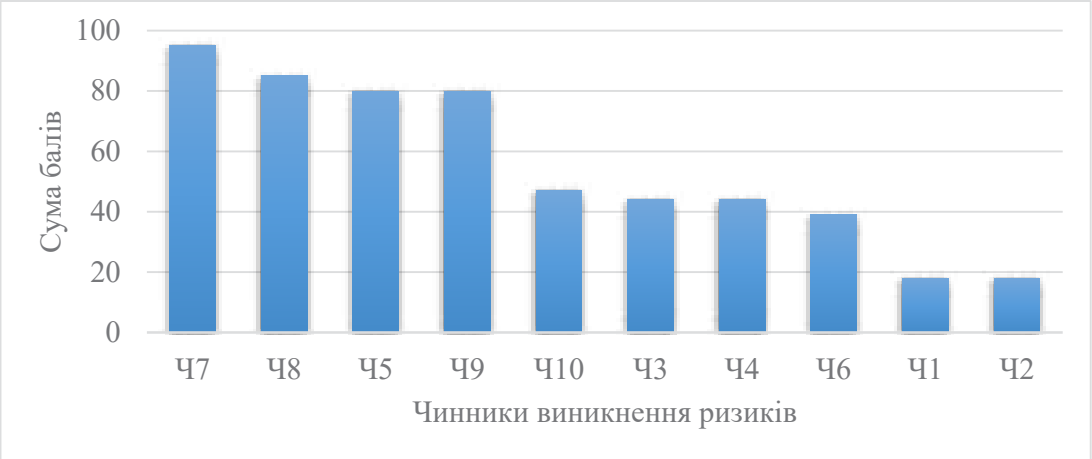

Рис. 3. Гістограма суми балів

Таблиця 5

Оцінювання ризиків методом експертних оцінок

Чинник	Експерти, *m*										Ймовірність, *P*	Рейтинг $R=m_{сер}$ Ч
	1	2	3	4	5	6	7	8	9	10		
Ч1	4	4	4	5	3	4	4	3	4	4	0,25	0,98
Ч2	5	4	5	4	5	4	5	4	5	3	0,2	0,88
Ч3	3	4	3	4	2	3	3	3	2	3	0,15	0,45
Ч4	4	3	4	4	5	3	4	4	4	4	0,1	0,39
Ч5	4	3	4	4	3	4	4	4	4	4	0,1	0,38
Ч6	3	4	4	3	2	3	3	3	2	3	0,05	0,15
Ч7	2	1	2	1	2	3	2	3	2	2	0,1	0,20
Ч8	2	1	2	2	1	2	3	3	2	2	0,025	0,05
Ч9	4	4	3	3	4	4	4	4	4	4	0,025	0,10
Ч10	4	4	4	3	4	3	4	4	4	4	0,05	0,19

Виокремимо основні та додаткові чинники виникнення ризиків за допомогою побудови гістограми суми балів (рис. 3).

В процесі дослідження було обрано метод експертних оцінок, оскільки неможливо скласти масив статистичних даних за минулі роки через недоступність. Оцінки виставляються від 1 до 5 балів, де 5 – найважливіший, 1 найменш важливий ризики (табл. 5).

В результаті проведеного експертного оцінювання можна зробити висновки за рейтингом, який оцінимо наступним чином: високий $1 < R \le 2{,}5$; середній $0{,}5 < R \le 1$; малий $0{,}25 < R \le 0{,}5$; відсутній $0 < R \le 0{,}25$. Так, на думку

експертів найважливішим і найбільш імовірним ризиком є недостатня кваліфікація персоналу (Ч1), а найменш важливим є поява нових конкурентів, технологій та інновацій (Ч8), а також невисока ймовірність даного ризику. За табл. 5 спостерігаємо, що більшість чинників створюють малий ризик або він взагалі відсутній, тому проєкт можливо втілити з невеликими витратами. Середній рівень ризику може бути при недостатній кваліфікації персоналу (Ч1) та недостатній кількості ресурсів (Ч2), тому на ці критерії слід звернути увагу при реалізації даного проєкту.

До виокремлених видів ризиків було обрано заходи їхньої оптимізації (мінімізації,

Таблиця 6

Рекомендовані заходи оптимізації ризиків ІТ-проєкту

№ з/п	Види ризиків	Заходи оптимізації ризиків
1.	*Технічні ризики*	Цей тип ризиків пов'язаний з технічними складнощами, що можуть виникнути в процесі розробки та впровадження системи. До них можуть відноситися: – Відмова обладнання або програмного забезпечення. *Оптимізація:* Перевірка обладнання та програмного забезпечення на початку проєкту, регулярні огляди та тестування, забезпечення резервних копій даних. – Проблеми з інтеграцією різних систем. *Оптимізація:* Ретельне планування та тестування інтеграції, залучення експертів, використання стандартизованих протоколів. – Проблеми з безпекою даних. *Оптимізація:* Розробка та впровадження міцних систем безпеки, забезпечення захисту конфіденційної інформації, використання шифрування та автентифікації.
2.	*Організаційні ризики*	Цей тип ризиків пов'язаний з організаційними аспектами проєкту, такими як забезпечення ресурсів, комунікації та управління ризиками. До них можуть відноситися: – Недостатній бюджет або ресурси. *Оптимізація:* Ретельне планування бюджету та ресурсів, залучення експертів для оцінки витрат, перегляд плану проєкту для зменшення надмірності. – Недостатнє управління проєктом. *Оптимізація:* Ретельне планування та контроль проєкту, використання керуючого ПО, яке дозволяє відстежувати терміни та ресурси проєкту, забезпечення чіткої комунікації між учасниками проєкту. – Недостатня підтримка від клієнта. *Оптимізація:* Ретельний аналіз потреб клієнта, встановлення зв'язку з клієнтом на початку проєкту та під час виконання проєкту, забезпечення чіткої комунікації з клієнтом.
3.	*Ризики, пов'язані зі змінами вимог*	Цей тип ризиків пов'язаний з можливістю зміни вимог до проєкту під час його розробки та впровадження. До них можуть відноситися: – Зміна вимог до функціональності системи. *Оптимізація:* Розробка гнучкого плану проєкту, що дозволяє змінюватися у відповідь на нові вимоги, ретельний аналіз вимог до системи на початку проєкту. – Зміна вимог до термінів виконання проєкту. *Оптимізація:* Розробка гнучкого плану проєкту, який дозволяє змінюватися у відповідь на нові вимоги, оцінка витрат на ресурси та терміни відповідно до нових вимог. – Зміна вимог до бюджету проєкту. *Оптимізація:* Розробка гнучкого плану проєкту, який дозволяє змінюватися у відповідь на нові вимоги, ретельний аналіз витрат та ресурсів на початку проєкту.
4.	*Ризик некомпетентності персоналу*	*Оптимізація:* Проведення навчання та тренінгів з персоналом, щоб забезпечити необхідну компетентність в області використання електронної системи управління медичним закладом. Встановлення процедур перевірки компетентності персоналу перед включенням їх до використання системи.
5.	*Ризик витоку даних*	*Оптимізація:* Встановлення політики безпеки та захисту даних, що охоплює контроль доступу до системи, шифрування та моніторинг активності користувачів. Застосування антивірусних програм та систем захисту від зломів та злочинних дій.
6.	*Ризик затримки термінів розробки та впровадження системи*	*Оптимізація:* Ретельне планування процесу розробки та впровадження системи з встановленням проміжних термінових дедлайнів. Систематичний моніторинг процесу розробки та впровадження системи з встановленням контрольних точок для визначення прогресу та вчасного виявлення можливих затримок.
7.	*Ризик несумісності системи з іншими системами медичного закладу*	*Оптимізація:* Вивчення технічних та функціональних характеристик інших систем медичного закладу та їх інтеграція в процесі розробки та впровадження системи управління. Тестування та перевірка сумісності системи з іншими системами.

регулювання). Існують різні заходи оптимізації ризиків, серед яких варто виокремити: уникнення ризику, передача ризику, прийняття ризику, зниження ризику. Табл. 6 містить основні види ризиків та рекомендовані заходи щодо їх оптимізації.

Крім того, ефективна оптимізація ризиків такого проєкту передбачає систематичне виявлення та аналіз ризиків на різних етапах розробки та впровадження системи, а також використання найкращих практик управління проєктами та ризиками.

Висновки. В роботі охарактеризовано ІТ-проєкт «Розробка та впровадження електронної системи управління медичним закладом», наведено його мету, цілі та завдання, основних учасників проєкту (власників, замовників, акціонерів, інвесторів, виконавців, постачальників), а також обумовлено життєвий цикл проєкту та його фінансову складову. Окрім цього, було проведено ідентифікацію ризиків, проаналізовано чинники виникнення ризиків та проведено їх якісну та кількісну оцінку. Також були обрані найбільш оптимальні заходи щодо запобігання визначених ризиків.

В цілому, успішне виконання ІТ-проєкту залежить від того, наскільки ефективно будуть виявлені та оптимізовані ризики, а також від здатності команди проєкту пристосовуватися до змін та виконувати роботу відповідно до найкращих практик управління проєктами. Управління ризиками є процесом, який повинен здійснюватися протягом усього життєвого циклу проєкту, від початкової розробки до підтримки та розвитку після впровадження. Оптимізація ризиків також може допомогти зменшити витрати на проєкт та збільшити його ефективність, тому її виконання необхідно розглядати як інвестицію в успішну реалізацію проєкту.

ЛІТЕРАТУРА:

1. Blyznyukova I., Semko I., Kiyko S. Огляд сучасних методологій управління командами ІТ-проєктів. *Управління розвитком складних систем*. 2020. № 43. С. 60–66.

2. Natarajan A., Gopal G. IT Risk Management. Managing Information Technology Projects: Building a Body of Knowledge in IT Project Management. 2022. С. 282–314.

3. Sorooshian S., Mun S. Y. Literature review: Critical risk factors affecting information-technology projects. *Calitatea.* 2020. № 21(175). С. 157–161.

4. Чубаєвський В., Луцька Н., Савченко Т., Власенко Л., Синельник К. Підвищення криптографічної стійкості агрегованого цифрового підпису за рахунок комбінованої системи автентифікації. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2023. № 2(22). С. 39–53.

5. Hubarieva I., Trushkina N. Процес управління ризиками в ІТ-проєктах. *Scientific Notes of Ostroh Academy National University*. *Economics Series*. 2023. № 30 (58). С. 84–88.

6. Грабіна К. В., Шендрик В.В. Метод управління ризиками ІТ-проєктів з врахуванням загроз та можливостей. *Управління розвитком складних систем*. 2023. № 55. С. 18–28.

7. Грабіна К. В., Шендрик В.В. Information technology of integrated management of threats and opportunities in IT projects. *Вісник сучасних інформаційних технологій.* 2023. № 6(4). С. 363–374.

8. Карпович І., Гладка О., Бухало Ю. Технології моделювання і оцінки ризиків інформаційної безпеки. *Технічні науки та технології.* 2021. № 1(23). С. 62–68.

9. Замула О. А., Черниш В. І. Аналіз міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки. *Системи обробки інформації.* 2011. № 2. С. 53–56.

10. Поліщук Д. В., Захарова М. В., Люта М. В. Модель оцінки ризиків інформаційної системи. *Сучасні електромеханічні та інформаційні системи*. 2021. № 1. С. 102–106.

11. Deshmukh G. K., Mukerjee H. S., Prasad U. D. Risk management in global CRM IT projects. *Business Perspectives and Research.* 2020. № 8(2). С. 156–172.

12. Afzal F., Yunfei S., Nazir M., Bhatti S. M. A review of artificial intelligence based risk assessment methods for capturing complexity-risk interdependencies: Cost overrun in construction projects. *International Journal of Managing Projects in Business.* 2021. № 14(2). С. 300–328.

REFERENCES:

1. Blyznyukova, I., Semko, I. & Kiyko, S. (2020). Ohlyad suchasnykh metodolohiy upravlinnya komandamy IT-proyektiv [Overview of modern IT project team management methodologies]. *Upravlinnya rozvytkom skladnykh system – Management of the development of complex systems*, 43, 60–66 [in Ukrainian].

2. Natarajan, A. & Gopal, G. (2022). IT Risk Management. Managing Information Technology Projects: Building a Body of Knowledge in IT Project Management, 282–314.

3. Sorooshian, S. & Mun, S.Y. (2020). Literature review: Critical risk factors affecting information-technology projects. *Calitatea,* 21(175), 157–161.

4. Chubaevsky, V., Lutska, N., Savchenko, T., Vlasenko, L. & Synelnyk, K. (2023). Pidvyshchennya kryptohrafichnoyi stiykosti ahrehovanoho tsyfrovoho pidpysu za rakhunok kombinovanoyi systemy avtentyfikatsiyi [Increasing the cryptographic stability of the aggregated digital signature due to the combined authentication system]. *Elektronne fakhove naukove vydannya «Kiberbezpeka: osvita, nauka, tekhnika» – Electronic professional scientific publication "Cybersecurity: education, science, technology"*, 2(22), 39–53 [in Ukrainian].

5. Hubarieva, I. & Trushkina, N. (2023). Protses upravlinnya ryzykamy v it-proyektakh [Risk management process in IT projects]. *Scientific Notes of Ostroh Academy National University, Economics Series,* 30 (58), 84–88 [in Ukrainian].

6. Hrabina, K. V. & Shendryk, V. V. (2023). Metod upravlinnya ryzykamy IT-proyektiv z vrakhuvannyam zahroz ta mozhlyvostey [Method of risk management of IT projects taking into account threats and opportunities]. *Upravlinnya rozvytkom skladnykh system – Management of the development of complex systems*, 55, 18–28 [in Ukrainian].

7. Hrabina, K. V. & Shendryk, V. V. (2023). Information technology of integrated management of threats and opportunities in IT projects. *Visnyk suchasnykh informatsiynykh tekhnolohiy – Bulletin of modern information technologies*, 6.4, 363–374 [in Ukrainian].

8. Karpovich, I., Hladka, O. & Bukhalo, Yu. (2021). Tekhnolohiyi modelyuvannya ta otsinky ryzykiv informatsiynoyi bezpeky [Information security risk modeling and assessment technologies]. *Tekhnichni nauky ta tekhnolohiyi – Technical sciences and technologies*, 1(23), 62–68 [in Ukrainian].

9. Zamula, O. A. & Chernysh, V. I. (2011). Analiz mizhnarodnykh standartiv v haluzi otsinyuvannya ryzykiv informatsiynoyi bezpeky [Analysis of international standards in the field of information security risk assessment]. *Systemy obrobky informatsiyi – Information processing systems*, 2, 53–56 [in Ukrainian].

10. Polishchuk, D. V., Zakharova, M. V. & Lyuta, M. V. (2021). Model' otsinky ryzykiv informatsiynoyi systemy [A model of information system risk assessment]. Suchasni elektromekhanichni ta informatsiyni systemy – Modern electromechanical and information systems, 1, 102–106 [in Ukrainian].

11. Deshmukh, G. K., Mukerjee, H. S. & Prasad, U. D. (2020). Risk management in global CRM IT projects. *Business Perspectives and Research*, 8(2), 156–172.

12. Afzal, F., Yunfei, S., Nazir, M. & Bhatti, S. M. (2021). A review of artificial intelligence based risk assessment methods for capturing complexity-risk interdependencies: Cost overrun in construction projects. *International Journal of Managing Projects in Business*, 14(2), 300–328.