УДК 004.9:005.334]:519.87

МАТРИЧНІ МЕТОДИ ОЦІНЮВАННЯ РИЗИКІВ ПРИ ВПРОВАДЖЕННІ ІНФОРМАЦІЙНИХ СИСТЕМ НА ПІДПРИЄМСТВІ

Басараб Д.М.
e-mail: daria.basarab@nure.ua
Науковий керівник – канд. пед. наук, доц. Ситнікова Ю.В.
Харківський національний університет радіоелектроніки,
кафедра прикладної математики
м. Харків, Україна

The implementation of information systems in enterprises is accompanied by technical, organizational, financial, and personnel risks that may affect project deadlines, budgets, and system performance. This determines the relevance of improving practical approaches to risk identification and assessment during the digital transformation stage. The purpose of the study is to substantiate the expediency of using matrix methods for risk assessment during the implementation of information systems at an enterprise. The paper summarises scientific approaches to risk assessment, identifies the main risk factors and possible consequences, and proposes a probability-impact matrix for their analysis. The results obtained enable identification of the most critical combinations of risks and consequences and can be used to support managerial decision-making during the implementation of information systems.

Впровадження інформаційних систем на підприємстві сьогодні є одним із важливих напрямів підвищення ефективності управління, вдосконалення бізнес-процесів та забезпечення оперативного опрацювання інформації. Разом із перевагами цифровізації підприємства стикаються з низкою ризиків, які можуть впливати на строки реалізації проєкту, обсяг витрат, якість функціонування системи та рівень її прийняття персоналом. Саме тому питання своєчасного виявлення та оцінювання ризиків набуває особливого значення як у теоретичному, так і в прикладному аспектах [2, 4].

Метою дослідження є обґрунтування доцільності застосування матричних методів для оцінювання ризиків при впровадженні інформаційних систем на підприємстві та визначення найбільш критичних чинників, які потребують першочергової уваги з боку керівництва.

Аналіз наукових праць свідчить, що в дослідженнях ризиків інформаційних систем застосовуються якісні, кількісні та комбіновані підходи. Одним із найбільш зручних інструментів первинного аналізу є матриця ризиків, у межах якої поєднуються оцінка ймовірності виникнення ризикової події та сила її впливу на результат упровадження системи. Такий підхід дає змогу не лише структуровано подати можливі загрози, а й ранжувати їх за ступенем критичності, що є важливим для прийняття обґрунтованих управлінських рішень [3, 4].

Для прикладного аналізу доцільно виокремити п’ять типових факторів ризику, які найчастіше супроводжують процес упровадження інформаційних систем на підприємстві, як то: недостатнє фінансування проєкту, нестача кваліфікованого персоналу, технічні проблеми, опір працівників змінам та нечітко сформульовані вимоги до системи. Можливими наслідками реалізації таких ризиків є порушення строків виконання робіт, перевищення запланованого бюджету, зниження якості функціонування системи, втрата або пошкодження даних, а також труднощі з адаптацією користувачів до нової системи. Подібна логіка групування ризиків узгоджується із сучасними підходами до оцінювання ризиків у бізнес-процесах та інформаційних системах [1, 4].

Для побудови матриці ризиків можна використати п’ятибальну шкалу оцінювання, де 1 відповідає дуже низькому рівню, а 5 – дуже високому. Значення окремого елемента матриці ризиків визначається як добуток оцінки ймовірності виникнення ризику на оцінку сили його впливу:

$$r_{ij} = p_i \cdot l_j,$$

де r_{ij} – оцінка ризику для i-го фактора та j-го наслідку;

p_i – оцінка ймовірності виникнення i-го ризику;

l_j – оцінка сили впливу j-го наслідку.

Загальний вигляд матриці ризиків можна подати так:

$$R=\left(r_{ij}\right)_{m\times m},$$

де m – кількість факторів ризику; n – кількість можливих наслідків.

Для узагальнення результатів оцінювання визначають сумарний ризик за кожним фактором:

$$S_i = \sum_{j=1}^{n} r_{ij},$$

а також сумарний ризик за кожним наслідком:

$$Q_j = \sum_{i=1}^{m} r_{ij}.$$

Застосування цього підходу дає можливість встановити, які саме фактори ризику є найбільш небезпечними, а які наслідки є найбільш критичними для підприємства. Наприклад, високі значення для поєднання технічних проблем і втрати даних свідчать про потребу в посиленні технічного тестування, резервного копіювання та контролю стабільності системи. Якщо ж високі оцінки пов’язані з нестачею підготовленого персоналу або опором змінам, особливої уваги потребують навчання користувачів, внутрішня комунікація та поетапне впровадження системи [2, 3]. Крім того, матриця «ймовірність-вплив», аналізуючи поєднання ймовірності виникнення та потенційного впливу кожного фактора ризику, може слугувати простим, проте дієвим інструментом для систематизації цих ризиків та підтримки прийняття управлінських рішень [1, 4].

Практичне значення матричного підходу полягає в тому, що він дозволяє ще на початковому етапі реалізації проєкту виявити найбільш проблемні ділянки та визначити пріоритетність заходів реагування. На відміну від простого описового переліку ризиків, матриця дає змогу перейти до їх впорядкування та порівняння, що спрощує процес прийняття управлінських рішень і підвищує обґрунтованість вибору заходів мінімізації негативних наслідків [3, 4].

Дослідження демонструє, що матричні методи оцінювання ризиків є доцільними і практично зручними інструментами для аналізу ризиків при впровадженні інформаційних систем на підприємстві. Їх використання забезпечує структуроване подання факторів ризику, дозволяє виявити найбільш критичні комбінації ризиків і наслідків та створює основу для прийняття ефективних управлінських рішень.

Результати такого аналізу можуть бути використані під час планування ІТ-проєктів, організації навчання персоналу, вибору заходів зниження ризиків і вдосконалення системи управління цифровими змінами на підприємстві. Перспективою подальших досліджень є розширення матричної моделі за рахунок вагових коефіцієнтів, групового експертного оцінювання та інтеграції з програмними засобами підтримки ризик-менеджменту [2, 3].

Список використаних джерел:

1. Palko D., Babenko T., Bigdan A., Kiktev N., Hutsol T., Kuboń M., Hnatiienko H., Tabor S., Gorbovy O., Borusiewicz A. Cyber Security Risk Modeling in Distributed Information Systems. Applied Sciences. 2023. Vol. 13, No. 4. Article 2393. https://doi.org/10.3390/app13042393

2. Rosado D. G., Sánchez L. E., Varela-Vaca Á. J., Santos-Olmo A., Gómez-López M. T., Gasca R. M., Fernández-Medina E. Enabling security risk assessment and management for business process models. Journal of Information Security and Applications. 2024. Vol. 84. Article 103829. https://doi.org/10.1016/j.jisa.2024.103829

3. Stanojević P., Misita M., Đurić G., Kuzmanović B., Milošević M., Balos D. Innovative Approach to Conceptual Design of Enterprise Risk Management Software. Applied Sciences. 2024. Vol. 14, No. 23. Article 11255. https://doi.org/10.3390/app142311255

4. Tereshchenko E., Sosnovska O., Ushenko N., Andryeyeva V., Kovalova M. Risk Assessment Information System of Enterprise Business Processes. CEUR Workshop Proceedings. 2022. Vol. 3188. P. 214-220.