УДК 658

Остапець Антон Олександрович
аспірант кафедри фінансового аналізу та аудиту
Державного торговельно-економічного університету
Ostapets Anton
Postgraduate Student at the Department of Financial Analysis and Audit
State University of Trade and Economics
ORCID: 0000-0001-7048-6112

Парасій-Вергуненко Ірина Михайлівна
доктор економічних наук, професор,
професор кафедри фінансового аналізу та аудиту
Державний торговельно-економічний університет
Parasii-Verhunenko Iryna
Doctor of Sciences (Economics), Professor,
Professor at the Department of Financial Analysis and Audit
State University of Trade and Economics
ORCID: 0000-0001-6506-6965

DOI: 10.25313/2520-2294-2025-2-10724

МЕТОДИКИ ЯКІСНОГО АНАЛІЗУ РИЗИКІВ ПІДПРИЄМСТВ ГАЛУЗІ ІТ

METHODS OF QUALITATIVE RISK ANALYSIS FOR IT INDUSTRY ENTERPRISES

Анотація. *Вступ. В сучасних умовах стрімкого розвитку інформаційних технологій і впливу факторів зовнішнього середовища, українські підприємства галузі ІТ приділяють значну увагу процесам аналізу ризиків. Динамічність ринку, швидкий технологічний прогрес, кіберзагрози та нестабільність економічного середовища роблять процес управління ризиками важливою складовою успішного ведення бізнесу. Аналіз ризиків є важливим елементом процесу управління ризиками і здійснюється після їх ідентифікації. Якісний аналіз дозволяє зробити прогнозування можливих наслідків, що можуть виникнути у разі настання ризику, а також розробити стратегії щодо мінімізації наслідків. У цій статті розглянуто методики якісного аналізу ризиків, що можуть бути застосовані підприємствами галузі ІТ, їхні особливості та здійснено їх компаративний аналіз з метою обрання оптимальних для конкретного підприємства методик.*

Мета. Метою дослідження є аналіз і узагальнення сучасних методик якісного аналізу ризиків, що можуть бути застосовані підприємствами галузі ІТ в процесі ризик-менеджменту. Дослідження спрямоване на визначення характеристик кожної з них, їх порівняння та вибір оптимальних, для певних підприємств галузі. Результатами роботи можуть бути рекомендації з вибору оптимальних методик якісного аналізу ризиків, що можуть бути використані підприємством і включені до стратегії управління ризиками.

Матеріали і методи. Матеріалами дослідження є: 1) найкращі практики провідних вітчизняних та іноземних організацій галузі інформаційних технологій та ризик-менеджменту; 2) праці вітчизняних та зарубіжних авторів, що здійснюють дослідження в сфері управління ризиками; 3) минулі публікації авторів статті.

В процесі здійснення дослідження було використано наступні наукові методи: теоретичного узагальнення та групування (для надання характеристики методик якісного аналізу ризиків та визначення їх особливостей); формалізації, аналізу та синтезу (для порівняння методик якісного аналізу ризиків за певними визначеними критеріями та обрання оптимальних з них); логічного узагальнення результатів (формулювання висновків).

Результати. У науковій статті розкрито питання якісного аналізу ризиків та методик, що можуть бути використані для нього, їх характеристики та особливості. Також запропоновано рекомендації щодо вибору певних з методик для процесу аналізу ризиків в залежності від роду діяльності компаній та їх масштабів. Ці обрані методики можуть бути використані як база перед подальшим процесом кількісного аналізу ризиків, оскільки буде надана можливість вибору найбільш пріоритетних для аналізу ризиків.

Перспективи. У майбутніх наукових дослідженнях увага буде зосереджена на розробці інтегрованих підходів, що будуть поєднувати методи якісного та кількісного аналізу ризиків. Також актуальним може бути використання штучного інтелекту для потенційної заміни запрошених експертів в таких методиках як метод Дельфі, метод FMEA тощо. Крім того, перспективним напрямком є адаптація існуючих методик ризик-менеджменту до специфічних викликів, таких як кіберзагрози, регуляторні зміни та швидка еволюція технологій. Дослідження ефективності цих підходів на практиці дозволить покращити стратегії управління ризиками та підвищити конкурентоспроможність IT-компаній.

Ключові слова: *ризик, фінансовий аналіз, стратегічний аналіз, якісний аналіз ризиків, FMEA-аналіз, SWOT-аналіз, метод Дельфі, управління ризиками.*

Summary. *Introduction. In the modern era of rapid technological development and external environmental influences, Ukrainian IT enterprises place significant emphasis on risk analysis processes. The dynamic nature of the market, rapid technological progress, cyber threats, and economic instability make risk management a crucial component of successful business operations. Risk analysis is an essential element of the risk management process and is conducted after risk identification. Qualitative analysis enables the forecasting of potential financial consequences that may arise if a risk materializes, as well as the development of strategies to mitigate its impact. This article examines qualitative risk analysis methods that can be applied by IT enterprises, explores their characteristics, and conducts a comparative analysis to determine the most suitable methods for specific companies.*

Purpose. The objective of this study is to analyze and summarize modern qualitative risk analysis methods that can be employed by IT enterprises as part of their risk management processes. The research aims to define the characteristics of each method, compare them, and identify the most effective ones for different IT companies. The study's findings may serve as recommendations for selecting optimal qualitative risk analysis methods that can be integrated into an enterprise's risk management strategy.

Materials and methods. The study is based on the following materials: 1) Best practices of leading domestic and international organizations in the fields of information technology and risk management; 2) works of domestic and foreign authors conducting research in risk management; 3) previous publications by the article's authors.

The research uses the following scientific methods: theoretical generalization and classification (to describe qualitative risk analysis methods and identify their features); formalization, analysis, and synthesis (to compare qualitative risk analysis methods based on predefined criteria and select the most effective ones); and logical generalization of results (to formulate conclusions).

Results. The scientific article outlines the sequence of forming key risk indicators that will be used in the subsequent processes of risk analysis and control for IT industry enterprises, along with their characteristics and the formation process. The proposed set of indicators will contribute to improving the risk analysis and control process and will be used as baseline metrics for assessing potential losses in the event of a risk occurrence and for making management decisions regarding their control.

Discussion. Future research will focus on developing integrated approaches that combine qualitative and quantitative risk analysis methods. Additionally, the potential use of artificial intelligence to replace expert input in methods such as the Delphi method and FMEA will be explored. Another promising direction is the adaptation of existing risk management methods to address specific challenges, including cyber threats, regulatory changes, and rapid technological evolution. Studying the practical effectiveness of these approaches will enhance risk management strategies and improve the competitiveness of IT companies.

Key words: *risk, financial analysis, strategic analysis, qualitative risk analysis, FMEA-analysis, SWOT-Analysis, Delphi method, risk management.*

Постановка проблеми. В сучасних умовах невизначеності та стрімких змінах у зовнішньому середовищі, все більша увага надається аналізу потенційних ризиків, перед якими можуть постати підприємства галузі IT, а також оцінці потенційного впливу на фінансові показники підприємства у разі їх виникнення. Динамічність ринку, швидкий технологічний прогрес, кіберзагрози вплив воєнних дій на можливість забезпечення діяльності підприємств, роблять процеси якісного і кількісного аналізу ризиків дуже важливою складовою успішного ведення та збереження бізнесу. В даній статті буде проведено дослідження процесу та методик якісного аналізу ризиків, проведено компаративний аналіз методик і надано рекомендації щодо використання певних методик в залежності від масштабу то роду діяльності компаній. Наукове обґрунтування рекомендацій дозволить значно спростити і отримати більш кращі результати якісного аналізу ризиків і сконцентрувати увагу зацікавлених осіб на найбільш пріоритетних ризиках з метою їх подальшого кількісного аналізу.

Аналіз останніх досліджень і публікацій. Значний внесок у дослідження та розуміння обмежень методик якісного аналізу ризиків а також можливих шляхів їх усунення вніс норвезький вчений Я. Емблемсваг (J. Emblemsvåg) [1]. Також одним з основоположних досліджень, що стосуються методик якісного аналізу ризиків є робота британських вчених П. Краузе (P. Krause), Дж. Фокса (J. Fox), П. Хадсона (P. Hudson) [2]. Саме ці вчені довели корисність процесу якісного аналізу ризиків, особливо у випадках відсутності можливості проведення кількісного аналізу. Значну увагу структурованому поясненню методів якісного аналізу та їх використання в реальних умовах приділено в роботах фінського вченого Р. Тіусанена (R. Tiusanen) [3]. Окремим аспектам використання якісного аналізу для управління ризиками, пов'язаними з кіберзагрозами, приділяється

увага в дослідженнях південнокорейських вчених Ю. Йу (Y. Yoo) та Х. С. Парка (H.-S. Park) [4]. Серед українських вчених варто виокремити роботи О. Зоріної [5], в яких приділено увагу якісному аналізу ризиків як важливою складовою перед проведенням кількісного аналізу, а також запропоновано використання комбінованих методик оцінки ризиків. Критеріям вибору методик якісного аналізу ризиків в залежності від специфіки підприємства приділено увагу в роботах К. Шурди [6]. Окремим аспектам якісного аналізу податкових ризиків приділено увагу в роботах В. Канюка [7]. Значну увагу критеріям вибору методик аналізу та поєднанню процесів якісного і кількісного аналізу ризиків приділено в роботах О. Білоцерківського [8].

Мета статті. Полягає в вивченні методик якісного аналізу ризиків, що можуть бути використані підприємствами галузі ІТ, проведенні компаративного аналізу основних методик на основі критеріїв, визначених авторами, формулюванні рекомендацій щодо вибору певних методик в залежності від роду діяльності та розміру підприємства. Завдяки проведеному дослідженню та компаративному аналізу і наданим рекомендаціям, підприємства галузі отримають можливість спростити та пришвидшити процес якісного аналізу ризиків та на основі його визначити найбільш пріоритетні для подальшого кількісного аналізу ризики.

Матеріали і методи. Матеріалами дослідження є: 1) найкращі практики провідних вітчизняних та іноземних організацій галузі інформаційних технологій та ризик-менеджменту; 2) праці вітчизняних та зарубіжних авторів, що здійснюють дослідження в сфері управління ризиками; 3) минулі публікації авторів статті.

В процесі здійснення дослідження було використано наступні наукові методи: теоретичного узагальнення та групування (для характеристики методик якісного аналізу ризиків та визначення їх особливостей); формалізації, аналізу та синтезу (для порівняння методик якісного аналізу ризиків за певними визначеними критеріями та обрання оптимальних з них); логічного узагальнення результатів (формулювання висновків).

Виклад основного матеріалу. Для підприємств галузі ІТ, що діють в середовищі, що стрімко розвивається, в останні роки, проблематика аналізу потенційних ризиків набуває дуже високої актуальності. Аналіз ризиків є одним з ключових елементів процесу оцінки ризиків у відповідності до міжнародного стандарту ISO 31000 і є наступним кроком після процесу ідентифікації можливих загроз. Даний стандарт визначає аналіз ризиків як процес забезпечення достатньою інформацією для прийняття рішень щодо необхідності подальших дій, таких як управління або моніторинг ризиків. Процес аналізу ризиків дозволяє зрозуміти їх природу, їхні джерела та фактори впливу, а також можливі взаємозв'язки між ними.

Аналіз ризиків виконується у взаємодії з іншими етапами управління ризиками, такими як ідентифікація, оцінка та обробка ризиків. Процес аналізу ризиків включає в себе такі стадії:

1) вивчення контексту (об'єкту аналізу, розуміння зовнішнього та внутрішнього середовищ організації та визначення критеріїв ризиків та допустимого їх рівня);
2) ідентифікацію ризиків (виявлення потенційних ризиків, що можуть вплинути на досягнення цілей, визначення джерел виникнення ризиків, подій, ситуація, що можуть призвести до реалізації ризику);
3) аналіз імовірності виникнення ризикових подій (визначення ймовірності настання конкретної події, що може викликати ризикові наслідки за допомогою використання статистичних даних, експертних оцінок або різноманітних моделей для оцінки ймовірностей);
4) аналізу наслідків ризику (оцінка потенційних наслідків для організації в результаті настання ризикових подій, що включають в себе фінансові, правові, операційні та репутаційні наслідки);
5) визначення рівня ризику (визначення важливості ризику як комбінацію ймовірності настання та наслідків в результаті виникнення, а також використання матриць ризиків або інших інструментів для оцінки рівня і пріоритезація ризиків);
6) виявлення взаємозв'язків між ризиками (аналіз впливу одного ризику на інші або ймовірність виникнення інших ризиків в разі настання одного).

В процесі аналізу ризиків використовуються якісні та кількісні методики, їх взаємодія в загальному процесі аналізу ризиків наведена в наступній блок-схемі, запропонованій профільною організацією IzenBridge і наведеній на рис. 1.

У відповідності до даного процесу, вартим уваги є те, що кількісний аналіз ризиків доцільно проводити не для всіх ідентифікованих та зареєстрованих на попередніх етапах ризиків, а тільки для тих, які мають найбільшу ймовірність виникнення та мають найбільшу значущість з точки зору потенційних втрат. Також варто зазначити, що якісний аналіз передує кількісному, оскільки не вимагає використання значного масиву вхідних даних та складних моделей, але стає підґрунтям для визначення тих ризиків, які варті найбільшої уваги.

Якісний аналіз ризиків представляє собою сукупність методів, що базуються на суб'єктивних судженнях і експертному досвіді. Він не потребує великої кількості вхідних деталізованих даних і використовується для ідентифікації ризиків та визначення їх пріоритету. Також важливим аспектом якісного аналізу ризиків є те, що в ньому не використовуються складні математичні розрахунки.

До методів якісного аналізу належать:

- Ризик-матриці (використовується для виявлення ризиків, що мають найбільшу критичність та

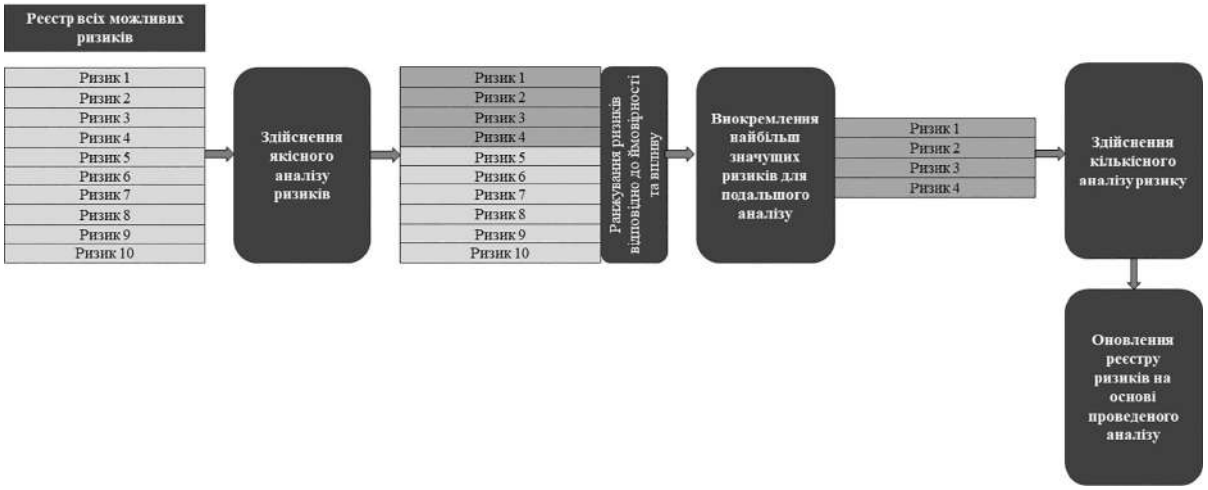

Рис. 1. Процес аналізу ризиків
Джерело: складено авторами за [9]

ймовірність настання і потребують першочергового реагування);

- Експертна оцінка (використовується для визначення ключових ризиків за допомогою залучення в процес аналізу стейкхолдерів організації або сторонніх груп експертів):
  – SWOT-аналіз (використовується для визначення сильних та слабких сторін організації, а також можливостей та загроз);
  – Метод Дельфі (Delphi) (використовується для прогнозування, прийняття рішень чи вирішення складних проблем, особливо у випадках, коли немає достатньої кількості даних для аналізу або ситуація є невизначеною);
  – Метод парного порівняння (використовується для оцінки ризиків шляхом порівняння кожного ризику з іншими в парі за певними критеріями);
  – Метод формування сценаріїв (використовується для визначення ймовірних варіантів майбутнього, оцінки їх впливу і допомоги в підготовці до можливих ризиків в складних і невизначених умовах);
  – Брейнстормінг (використовується для генерування великої кількості ідей і думок з приводу визначення ризиків, способів управління ними, ранжування та є менш структурованим на відміну від методу Дельфі);
  – FMEA-аналіз (використовується для визначення всіх можливих відмов у дизайні, виробничому або збірному процесі, чи у продукті або послузі).

Ризик-матриця представляє собою досить простий і ефективний метод, за допомогою якого здійснюється пріоритезація ризиків відповідно до ймовірності їх виникнення та впливу на об'єкт господарювання, а також характерною її особливістю є візуальне відображення.

Матриця ризиків є гнучким інструментом за рахунок можливості її масштабування та персоналізації в залежності від потреб організації. Загальноприйнятим є відображення матриці у вигляді таблиці, де рядки відповідають за ймовірність настання ризику, а стовпчики — за масштаб впливу на організацію. Найпростішим варіантом є матриця 3×3 (де виділяють низьку, середню та високу ймовірність виникнення ризику, а за рівнем впливу — незначний, середній та критичний), але останнім часом найбільшого розповсюдження набула матриця 5×5.

Даний різновид матриці передбачає градацію ризиків за ступенем ймовірності на дуже малоймовірні, малоймовірні, можливі, ймовірні та дуже ймовірні, а за ступенем впливу — несуттєві, низькі, середні, суттєві та катастрофічні. Також з метою візуалізації кожна клітинка в отриманій матриці зазвичай відображається кольором від зеленого (для найменш критичних ризиків) до червоного (для найбільш критичних і тих, шо потребують найбільшої уваги). Приклад ризик-матриці 5х5 наведено на рис. 2.

Варто зазначити, що кольорування може відрізнятись в залежності від обраної компанією стратегії ризик-менеджменту та ранжування ризиків у відповідності до ризик-рейтингу, який вираховується як значення по шкалі ймовірності перемножене на значення за шкалою впливу, де дуже малоймовірні ризики мають значення 1, а дуже ймовірні — 5. Зазвичай, розрізняють наступні ризики за рейтингом, що в свою чергу визначає колір зафарбування [10–11]:

- 1–6 — ризики низького рейтингу (зелений), які не можуть створити загрозу компанії/проекту;
- 7–12 — ризики середнього рейтингу (жовтий). Не викликають необхідності миттєвих дій по управлінню ними, але їх не варто ігнорувати;
- 13–25 — ризики високого рейтингу (червоний). Потребують особливої уваги, або ж негайних заходів по контролю.

Також важливою перевагою матриці ризиків є можливість деталізації описової складової рядків та стовпців, коли замість ймовірності настання ризи-

Ймовірність/ вплив на організацію	Несуттєві (1)	Низькі (2)	Середні (3)	Суттєві (4)	Катастрофічні (5)
Дуже ймовірні (5)	5	10	15	20	25
Ймовірні (4)	4	8	12	16	20
Можливі (3)	3	6	9	12	15
Малоймовірні (2)	2	4	6	8	10
Дуже малоймовірні (1)	1	2	3	4	5

Рис. 2. Приклад матриці ризиків
Джерело: складено авторами

ку може використовуватись частота їх виникнення (наприклад, раз на тиждень, раз на місяць, раз на квартал, раз на півріччя, раз на рік тощо), а також деталізація впливу у вигляді грошового виразу впливу на організацію (кількість грошових втрат, відсоток капіталу тощо). Приклад деталізованої ризик-матриці наведено на рис. 3.

Наступним методом якісної оцінки ризиків є метод експертної оцінки, що базується на знаннях, досвіді та судженнях експертів, обраних серед спеціалістів компанії чи запрошених зовні. Найчастіше цей метод використовується в ситуаціях, коли є недостатня кількість вхідних даних, а аналіз ризиків здійснюється на базі знань, досвіду та суджень запрошених експертів.

Як зазначено вище, однієї з методик експертної оцінки є SWOT-аналіз, що представляє собою потужний інструмент для стратегічного управління, який дозволяє компаніям здійснювати аналіз внутрішніх і зовнішніх аспектів свого бізнесу. Абревіатура SWOT походить від англійських слів: Strengths (сильні сторони), Weaknesses (слабкі сторони), Opportunities (можливості) та Threats (загрози). SWOT аналіз допомагає компаніям розібратися в їхніх внутрішніх перевагах і недоліках, а також в останніх тенденціях на ринку і можливих загрозах ззовні. [12]

До компоненти сильних сторін (S) належать внутрішні фактори та аспекти бізнесу, які надають організації перевагу над конкурентами. До сильних сторін можуть належати такі елементи як сильний

		Втрата в грошовому еквіваленті	Менше 10 тис. дол.	Від 10 тис. до 100 тис. дол.	Від 100 тис. до 1 млн. дол.	Від 1 до 10 млн. дол.	Більше 10 млн. дол.
Частота виникнення	Ймовірність відносно року	Ймовірність/ вплив на організацію	Несуттєві (1)	Низькі (2)	Середні (3)	Суттєві (4)	Катастрофічні (5)
Раз на тиждень	3,4-14%	Дуже ймовірні (5)	5	10	15	20	25
Раз на місяць	1,2-3,3%	Ймовірні (4)	4	8	12	16	20
Раз на квартал	0,25-1,1%	Можливі (3)	3	6	9	12	15
Раз на півріччя	0,28-0,54%	Малоймовірні (2)	2	4	6	8	10
Раз на рік	0,27%	Дуже малоймовірні (1)	1	2	3	4	5

Рис. 3. Розширена матриця ризиків
Джерело: складено авторами

і добре відомий бренд, висока якість продуктів компанії або послуг, що нею надаються, ефективна управлінська команда, доступ до використання унікальних технологій та інноваційність продукту/ послуги. Дані елементи допомагають привернути більше клієнтів.

До компоненти слабких сторін (W) належать недоліки або обмеження, що можуть стати перешкодою для досягнення компанією її цілей. До слабких сторін можуть належати такі елементи, як високі витрати на виробництво продуктів/надання послуг, низька урядова підтримка, нестабільність в постачаннях, слабка управлінська структура, відсутність інноваційності продукту, недостатнє фінансування тощо. Слабкі сторони можуть суттєво знижувати конкурентоспроможність бізнесу і потребують великого рівня уваги.

Наступною компонентою SWOT-аналізу є компонента можливостей (O), що представляє собою тенденції або обставини, які можуть бути використані для збільшення прибутку або розвитку бізнесу. До елементів даної компоненти можуть входити зростання попиту на продукти компанії чи послуги, що нею надаються, зміни в законодавстві, що сприяють розвитку бізнесу, вихід на нові ринки для експансії, впровадження технологічних інновацій, що полегшують процеси виробництва/ надання послуг або збуту.

Останньою компонентою SWOT-аналізу є компонента загроз (T), що представляє собою сукупність факторів або подій, що можуть спричинити негативний вплив на бізнес та його успішність. До елементів загроз можуть належати зростання рівня конкуренції, зміни в законодавчому регулюванні, економічні кризи, зміни в смаках або поведінці споживачів, технологічні загрози або зміни в ставленні до сталого розвитку. Компонента загроз вимагає від компанії гнучкості та можливості адаптації до змін задля зменшення їх негативного вплив на компанію.

Важливим для SWOT-аналізу є відповідь на певний перелік питань, які допомагають у аналізі ризиків з точки зору компонент SWOT-аналізу. Приклад SWOT-матриці з питаннями наведено на рис. 4.

Відповіді на наведені вище в матриці питання допоможуть компанії скористатися можливостями та розробити ефективні стратегії. Отримання чіткого та реалістичного уявлення про внутрішній стан компанії допоможе менеджменту знайти шляхи для кращого задоволення потреб клієнтів, досягнення цілей компанії і зміцнення слабких сторін, які впливають на ефективність роботи.

Провівши SWOT-аналіз, та визначивши сильні сторони, слабкості, можливості та загрози і заповнивши їх у відповідні квадранти матриці, керівний склад компанії має розробити відповідний план

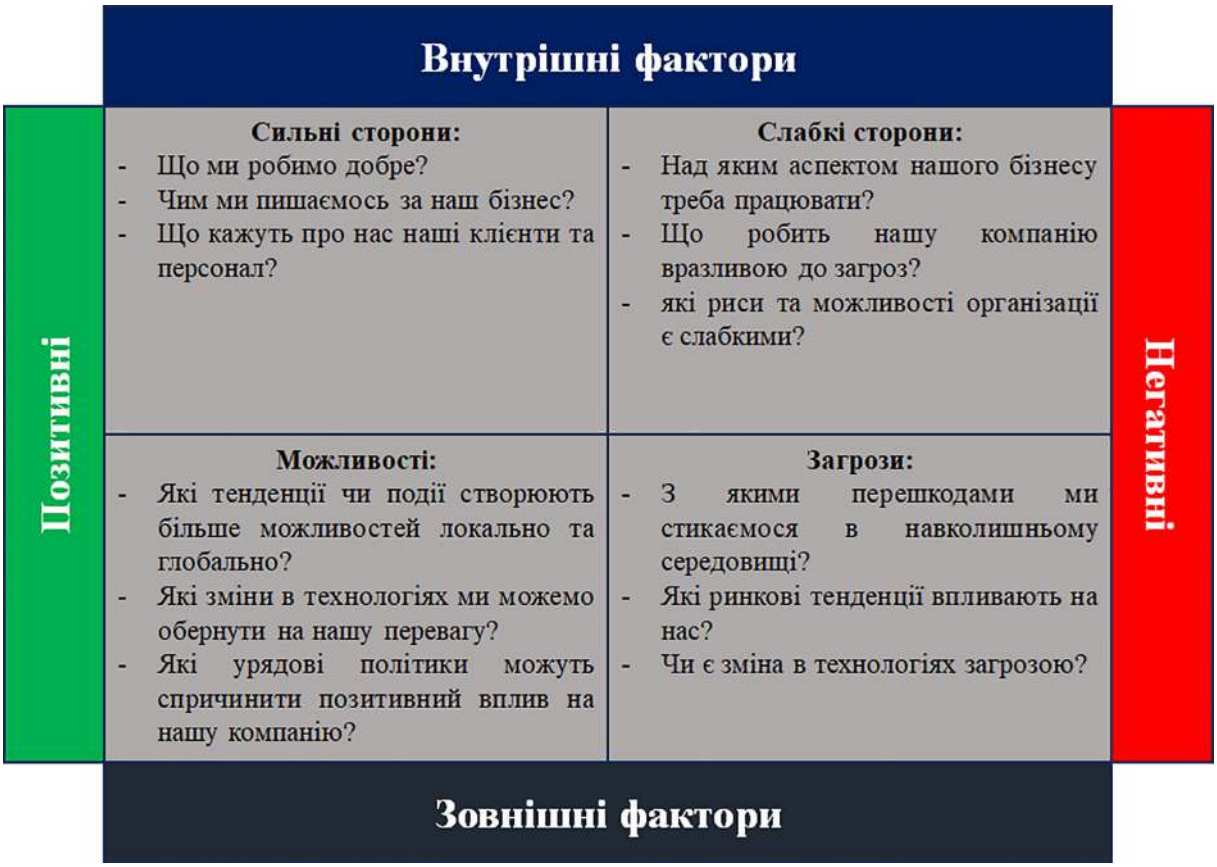

Рис. 4. Матриця SWOT-аналізу
Джерело: складено автором за [13]

реагування, відповівши на питання, що наведені на рис. 5.

Не зважаючи на те, що SWOT-аналіз здебільшого використовується для формування стратегії компаній, його також можна використовувати в аспекті управління ризиками. Для цього доцільним є переформулювання питань, що будуть задаватись співробітникам, що відповідають за аналіз ризиків. До прикладу:

- S — які сильні сторони компанії можна використати для зменшення ймовірності виникнення даного ризику?
- W — на які слабкі сторони компанії треба звернути особливу увагу для запобігання виникненню ризику?
- O — які додаткові можливості можна отримати в разі прийняття певного ризику?
- T — які загрози можуть викликати збільшення ймовірності чи впливу на компанію певного ризику?

Відповідно, пропрацювавши кожен ризик відповідно до матриці SWOT-аналізу, можна зробити якісну оцінку і сформувати подальшу стратегію компанії на основі аналізу отриманих результатів.

Окрім SWOT-аналізу, в якості методу експертної оцінки може використовуватись метод Дельфі, що представляє собою структуровану комунікаційну систему, яка базується на результатах кількох раундів анкетування групи експертів. Процес полягає в тому, що після кожного раунду анкетування експертам надається узагальнений підсумок попередніх відповідей, що дозволяє їм коригувати свої відповіді відповідно до групового підходу. Цей процес поєднує переваги експертного аналізу з елементами «мудрості натовпу». Результатом проведення оцінки має бути консенсусне рішення групи.

До характерних особливостей, що відрізняють метод Дельфі від інших стратегій групового прийняття рішення належать анонімність (запобігає отриманню нещирих відповідей за рахунок тиску інших колег-експертів), ітеративний зворотній зв'язок (учасники можуть отримати загальне уявлення про думки інших членів експертної групи, за допомогою чого можна адаптувати свою відповідь), групова відповідь (можливість адаптації відповіді експерта та доповнення інформації під час раундів зворотного зв'язку до моменту досягнення експертною групою консенсусу) та використання експертів (замість вибору випадкових учасників у якості експертної групи рекомендується залучення експертів з галузі, до якої належить організація).

Процедура аналізу ризиків за методом Дельфі складається з декількох основних етапів, які проілюстровано на рис. 6.

Першим етапом є постановка мети експертного дослідження, визначаються основні завдання, відповідно до яких в подальшому буде визначена експертна група.

Після постановки мети і завдань експертного дослідження проводиться підбір групи експертів,

		Внутрішні	
		Сильні сторони	**Слабкі сторони**
Зовнішні	**Можливості**	**Як використовуються сильні сторони компанії для отримання переваг від можливостей?**	**Як компанія може подолати слабкі сторони, які заважають скористатися цими можливостями?**
	Загрози	**Як компанія може використовувати свої сильні сторони, щоб зменшити ймовірність і вплив цих загроз?**	**Як можна подолати слабкі сторони, які зроблять ці загрози реальністю?**

Рис. 5. Перелік питань до менеджменту компанії після проведення SWOT-аналізу

Джерело: складено авторами за [13]

до яких можуть належати розробники програмного забезпечення, аналітики, архітектори систем, спеціалісти з кібербезпеки, проєктні менеджери.

Наступним процесом є розробка анкети для опитування, до якої можуть входити питання, подібні до наступних:

- Які основні ризики можуть здійснити вплив на проект?
- Наскільки висока ймовірність виникнення цих ризиків?
- Яким може бути вплив ризиків на проект чи організацію?

Важливим аспектом оцінювання є те, що респондентам буде запропонована шкала для оцінки ймовірності та впливу на організацію. Наприклад, можна використовувати ранжування на низький, середній і високий рівні.

Після створення анкети запитань та її узгодження фасилітатором, проводиться перший раунд анонімного опитування експертів. Кожен з експертів дає відповідь базуючись на своїх знаннях і досвіді. Після завершення першого раунду опитування здійснюється агрегація та аналіз результатів опитування. Відповідно до проведеного аналізу учасникам надається зворотній зв'язок у вигляді узагальненої інформації про відповіді інших експертів без зазначення імен експертів. Наприклад, певна кількість експертів визначили, що певні ризики мають високий рівень впливу або високу ймовірність виникнення, а певні ризики, відповідно, середній та низький рівні.

Після проведення даного узагальнення проводяться наступні раунди дослідження, в яких експерти мають можливість переглянути свої відповіді, враховуючи результати групового зворотного зв'язку. Також можуть розглядатись додаткові питання або вноситись уточнення до попередніх. Результатом кожного раунду є аналіз і узагальнення результатів. Під час дослідження, зазвичай, від двох до чотирьох раундів опитування до моменту досягнення консенсусу експертами щодо найбільш пріоритетних ризиків.

Після досягнення консенсусу, результати дослідження оформлюються у вигляді звіту, що включає в себе підсумковий список найбільш пріоритетних ризиків. В подальшому, на основі цього звіту, розробляються стратегії управління ризиками (змен-

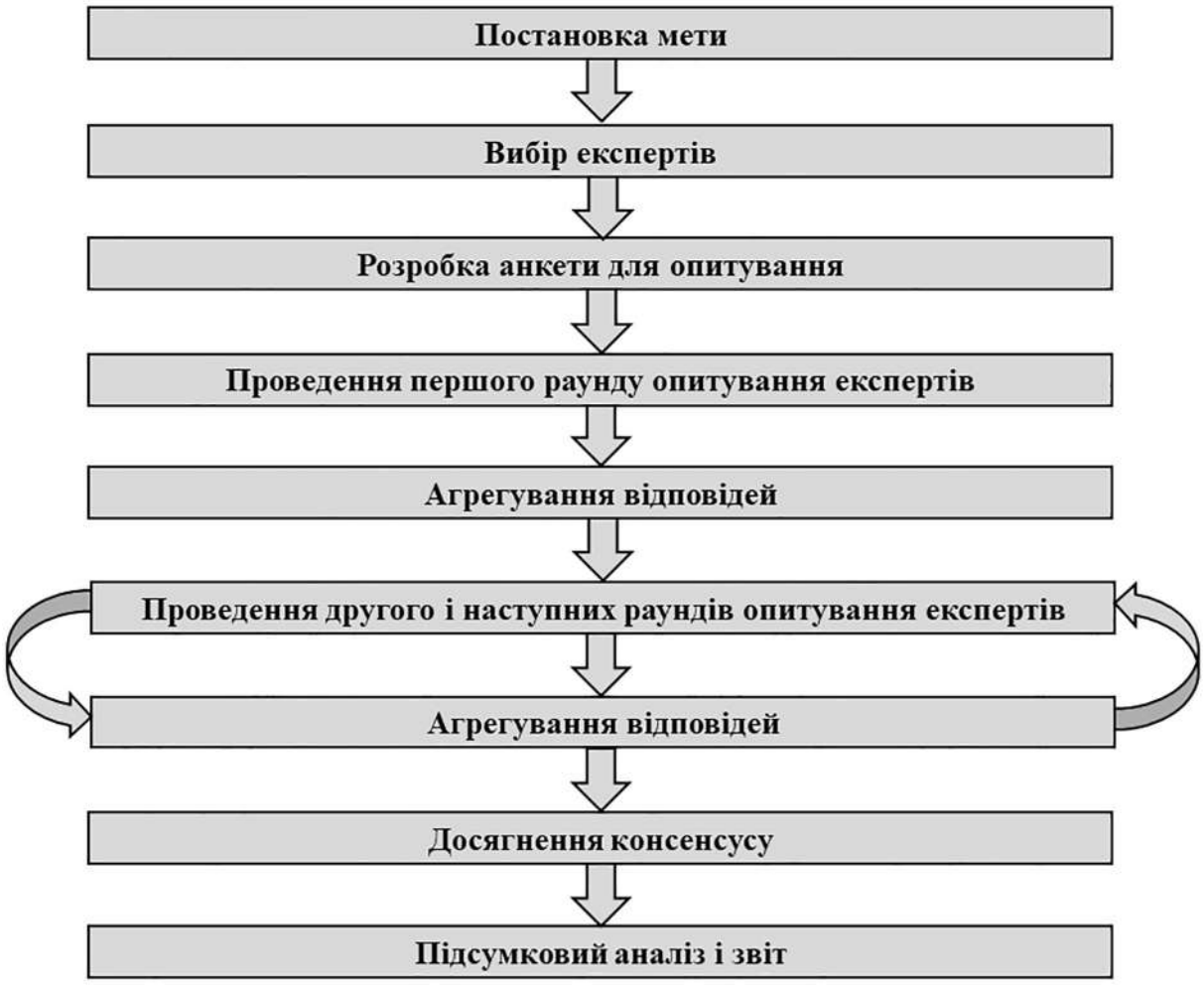

Рис. 6. Процес експертної оцінки методом Дельфі
Джерело: складено авторами за [14–15]

шення впливу, уникнення ризику, делегація ризику тощо).

Наступним методом, що може використовуватись для експертної оцінки, є метод парного порівняння, який використовується для оцінки ризиків шляхом зіставлення кожного ризику з іншим в парі. Таке порівняння дозволяє визначити пріоритетність ризику. Даний метод є ефективним у випадках, коли необхідно порівняти обмежену кількість ризиків та врахувати їх відносну важливість для цілей певного проекту чи організації.

Процес парного порівняння для оцінки ризиків складається з наступних етапів:

– Визначення списку ризиків (створення списку ризиків, що будуть в подальшому порівнюватись між собою);
– Формування матриці парного порівняння (представлення всіх ризиків у вигляді матриці, де одні ризики знаходяться в стовпчиках, інші — в рядках);
– Проведення порівнянь (визначення який з ризиків має більший вплив і ймовірність виникнення);
– Підрахунок сумарної оцінки (визначення суми оцінок для кожного ризику);
– Ранжування ризиків (визначення найбільш пріоритетних ризиків у відповідності до сумарної оцінки, де чим більше сумарна оцінка, тим вищим є пріоритет ризику).

Матриця порівняння ризиків заповнюється наступним чином: частина ризиків з загального списку записується в заголовках стовбців, частина — в заголовках рядків. Клітини заповнюються оцінками по шкалі 0–0.5–1, де значення 1 проставляється у випадку, коли ризик із рядка має більший вплив ніж ризик зі стовпця, 0.5 — якщо ризики мають рівнозначний вплив, 0 — якщо ризик з рядка має менший вплив ніж ризик зі стовпчика. Також для спрощення оцінок шкала може бути спрощена до значень 0–1, тобто в такому випадку не передбачається рівнозначність ризиків.

Приклад матриці парного порівняння наведено на рис. 7.

Як підсумок проведеного парного порівняння, здійснюється підрахунок сумарної оцінки, що представляє собою суму оцінок у кожному з рядків. У випадку наведеної вище матриці, найбільш пріоритетним є ризик пошкодження/виходу з ладу головного серверу, в той же час як в порівнянні з іншими ризиками, деактуалізація програмного коду має найменший пріоритет.

Відповідно, після проведення ранжування ризиків згідно до їх сумарних оцінок, отримаємо

	Пошкодження / вихід з ладу головного серверу	Деактуалізація програмного коду	Витік інформації про персональні дані споживачів	Масивна DDoS-атака на сервери	Сумарна оцінка ризику
Пошкодження / вихід з ладу головного серверу		1	1	0,5	2,5
Деактуалізація програмного коду	0		0	0	0
Витік інформації про персональні дані споживачів	0	1		0,5	1,5
Масивна DDoS-атака на сервери	0,5	1	0,5		2,0

Рис. 7. Приклад матриці парного порівняння ризиків
Джерело: складено авторами за [16–17]

наступне: 1 місце з точки зору пріоритету посідає ризик пошкодження/виходу з ладу головного серверу, 2 місце — масивна DDoS-атака на сервери, 3 місце — витік інформації про персональні дані споживачів і останнє місце займає ризик деактуалізації коду.

Метод парного порівняння дозволяє отримати чітку картину пріоритетності ризиків та допомагає ефективно розподілити ресурси для їхнього управління.

Ще одним з методів експертної оцінки є метод формування сценаріїв. Даний метод представляє собою потужний інструмент для аналізу ризиків, завдяки якому передбачаються можливі варіанти розвитку подій і здійснюється оцінка їхнього впливу на організацію чи проєкт. Такий підхід дозволяє здійснювати моделювання різних сценаріїв майбутнього з урахуванням невизначеності та можливих змін у зовнішньому середовищі. Суть методу полягає в розробці кількох сценаріїв того, як можуть розвиватись події в залежності від ключових факторів ризику. Кожен сценарій містить опис умов, що можуть виникнути і наслідки для організації [18].

Методика сценарного аналізу складається з наступних етапів:

- Визначення цілей для аналізу (формування чіткої мети для аналізу. Наприклад, оцінити вплив кібератаки на ІТ-інфраструктуру підприємства, або ж підготовка до змін на ринку через нові регуляторні вимоги);
- Визначення основних факторів невизначеності (формування переліку факторів, що можуть впливати на проєкт чи організацію);
- Формування можливих сценаріїв (пропрацювання та формування декількох видів розвитку подій);
- Аналіз впливу сценаріїв (здійснення оцінки ймовірності виникнення та впливу на організацію у разі настання);
- Розробка плану дій (напрацювання покрокового плану дій на випадок настання сценарію);
- Моніторинг і перегляд (відслідковування розвитку подій і перегляд сценаріїв в залежності від змін у зовнішньому і внутрішньому середовищі організації).

До факторів, невизначеності, що можуть чинити вплив на організацію, можуть належати економічні показники (зміни в рівні інфляції, зміни валютних курсів, зміни в показниках рівня сплати праці тощо), технологічні зміни (поява нових технологій, оновлення існуючих продуктів тощо), зміни в політичній ситуації (зміни в законодавстві, війни, санкції, зміни в міждержавних торговельних відносинах тощо).

Зазвичай, під час сценарного аналізу розробляється декілька сценаріїв. Здебільшого прийнято використовувати такі види сценаріїв: оптимістичний (всі фактори складаються сприятливо), песимістичний (виникають найгірші можливі умови) та реалістичний (збалансований розвиток між позитивними і негативними наслідками). Після формування і опису переліку сценаріїв здійснюється оцінка рівня впливу і ймовірності реалізації сценарію. За результатами оцінки пропрацьовується подальший план дій: стратегії розвитку для оптимістичного сценарію, заходи мінімізації наслідків для песимістичного і комбінація підходів у випадку настання реалістичного сценарію.

В цілому, метод формування сценаріїв допомагає організаціям краще зрозуміти ризики та бути готовими до непередбачуваних обставин.

Останнім в запропонованому переліку методів експертного оцінювання є метод мозкового штурму або брейнстормінг, що представляє собою колективне генерування ідей задля виявлення, аналізу та оцінки різноманітних ситуацій. Може також використовуватись в процесі ризик-менеджменту і бути ефективним для створення повного переліку потенційних ризиків і розробки стратегій по роботі з ними.

До основних етапів проведення процесу брейнстормінгу належать [19–20]:

- Визначення мети сесії (чітке визначення цілей і завдань, що ставляться перед експертами перед проведенням процесу);
- Формування команди експертів (залучення до процесу фахівців з різних сфер, пов'язаних з проектом);
- Проведення сесії (учасники висловлюють свої ідеї з приводу запропонованого об'єкту);
- Фіксація результатів (документування всіх думок, висловлених під час сесії);
- Аналіз отриманих результатів (обробка результатів сесії з метою виявлення найбільш-пріоритетних викликів);
- Розробка подальшого плану (обміркування щодо плану подальших дій стосовно контролю за найбільш пріоритетними ризиками).

Брейнстормінг, зазвичай, має певний регламент і правила. Зазвичай, до правил відносяться прийняття будь-яких ідей без оцінок та критики, заохочується найбільша кількість ідей, певні ідею/думки можуть доповнюватись іншими учасниками чи об'єднуватись з іншими. Також з точки зору генерації ідей можна виділити спонтанну генерацію, або ж генерація може мати структурований підхід (генерування за певними категоріями). Важливим аспектом є фіксація всіх ідей чи результатів в режимі реального часу, наприклад, на дошці або за допомогою спеціального програмного забезпечення (Miro, Microsoft Teams, Trello, Google Docs).

Метод брейнстормінгу є дієвим способом створення переліку ризиків на ранніх етапах проєктів, особливо в динамічній ІТ-сфері.

Наступним і останнім з перерахованих вище методів якісного аналізу ризиків є FMEA-аналіз (Аналіз видів і наслідків відмов). Він представляє собою структурований метод ідентифікації та аналізу потенційних видів відмов у процесах, системах, продуктах або послугах і визначення їхніх можливих наслідків. Основна мета FMEA — запобігання можливим помилкам та мінімізація їх впливу.

Головними цілями FMEA є ідентифікація видів відмов (визначення потенційних помилок в системах), оцінка наслідків відмов (аналіз можливих наслідків, що можуть настати в разі відмови), оцінка критичності ризиків (пріоритезація ризиків на основі рівня їх небезпеки) та розробка заходів для усунення або зниження ризиків (визначення способів запобігання відмовам або зменшення їх впливу).

Процес проведення FMEA-аналізу наведений на рис. 8.

На першому етапі процесу здійснюється розбиття процесу чи системи на окремі частини чи етапи та визначаються всі можливі види відмов/ризиків, що можуть виникати на кожному етапі. Наступним етапом виступає визначення всіх можливих причин відмов/виникнення ризиків. Після визначення причин наступним кроком йде аналіз потенційних наслідків відмов/настання ризику. В подальшому після аналізу наслідків проводиться оцінка ризиків за показником RPN (Risk Priority Number), що представляє собою перемножені між собою показники S (Severity — серйозність, оцінюється по шкалі від 1 до 10, де 10 — найсерйозніший ризик), O (Occurrence — ймовірність виникнення, також по шкалі від 1 до 10) та D (Detection — здатність системи виявити відмову/ризик до того, як вони настануть). Після розрахунку RPN проводиться визначаються міри по зменшенню впливу ризику або його уникненню і розробляються відповідні кроки. Найбільш важливими для розгляду є ризики з найбільшим числом RPN. Останнім етапом є перегляд та оновлення списку відмов.

FMEA є потужним інструментом для управління ризиками, особливо корисним в IT-сфері для оцінки ризиків, пов'язаних з кібербезпекою, розробкою програмного забезпечення та IT-інфраструктурою, завдяки якому забезпечується надійність систем і мінімізація впливу ризиків та відмов.

Серед наведених вище методів якісного аналізу ризиків в IT-компаніях частіше за все застосовуються методики брейнстормінгу, SWOT-аналізу, сценарного аналізу та метод Дельфі. Після використання даних методик і для визначення пріоритетності ризиків для подальшого кількісного аналізу найбільш важливих ризиків може бути використаний метод парного порівняння.

Узагальнення характеристик та особливостей методик якісного аналізу ризиків наведено в таблиці 1.

Для вибору оптимального методу якісної оцінки ризиків доцільним буде провести порівняльний аналіз за наступними характеристиками:

- Рівень складності методу з точки зору необхідних знань та навичок;
- Вимогливість до обсягу і точності необхідних даних для проведення аналізу;
- Точність результатів;
- Часо- та ресурсомісткість;
- Залежність від експертної думки.

Результати компаративного аналізу якісних методів аналізу ризиків наведено в таблиці 2.

Відповідно до проведеного вище компаративного аналізу якісних методик аналізу ризиків, невеликі компанії та стартапи можуть здебільшого

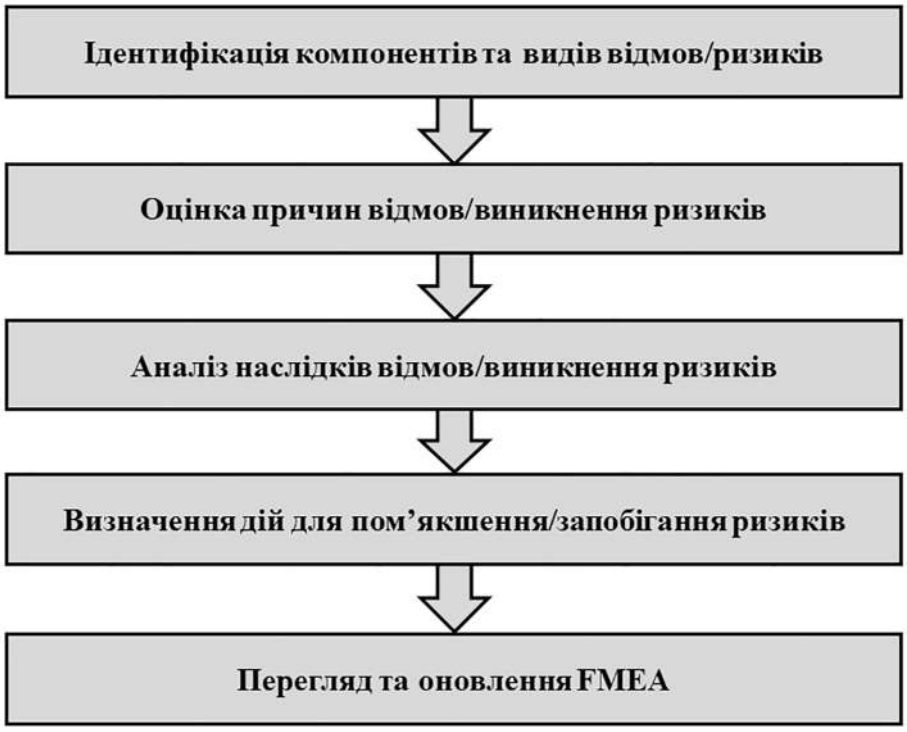

Рис. 8. Процес проведення FMEA
Джерело: складено авторами за [21–22]

Таблиця 1

Характеристики методів якісного аналізу ризиків

Метод	Переваги	Недоліки
Ризик-матриця	• Візуалізація результатів аналізу; • Легка пріоритезація ризиків	• Суб'єктивність результатів оцінки; • Неврахування зв'язків між ризиками; • Обмежена деталізація складних ризиків
SWOT-аналіз	• Простота у використанні; • Універсальність; • Поглиблене розуміння середовища	• Суб'єктивність; • Поверховість; • Неможливість кількісної оцінки
Метод Delphi	• Можливість дистанційного проведення; • Анонімність; • Можливість переосмислення думок експертами	• Відсутність живого спілкування між експертами; • Довготривалість дослідження; • Ймовірність втрати частини учасників; • Ризик конформізму
Метод парного порівняння	• Простота; • Зручність для невеликої кількості ризиків; • Об'єктивність	• Велика витрата часу та складність у разі аналізу значної кількості ризиків; • Суб'єктивність
Метод формування сценаріїв	• Можливість передбачення наслідків; • Гнучкість; • Покращення рівня готовності до невизначеностей	• Суб'єктивність; • Складність; • Невизначеність;
Брейнстормінг	• Широта охоплення; • Креативність; • Простота	• Суб'єктивність; • Обмеженість; • Ризик домінування
FMEA-аналіз	• Структурованість; • Пріоритезація ризиків; • Універсальність	• Суб'єктивність; • Трудомісткість; • Складність для великих систем

Джерело: узагальнено авторами

використовувати більш легкі та менш ресурсномісткі методи, такі як SWOT-аналіз, брейнстормінг, метод ранжування та ризик-матриць для якісного аналізу ризиків. Ці методи не вимагають серйозної експертизи від спеціалістів, потребують менших часових затрат і не вимагають залучення сторонніх консультантів.

В той же час, великі ІТ-компанії здебільшого приділяють велику увагу процесам аналізу та контролю за ризиками, мають окремі підрозділи, що складаються зі спеціалістів, які мають високий кваліфікаційний рівень в сфері управління ризиками, матеріальні та технологічні можливості, тож такі компанії можуть використовувати більш складні методики якісного аналізу ризиків, такі як метод Дельфі, FMEA-аналіз та метод сценарного аналізу. Також великі компанії галузі ІТ можуть залучати сторонніх експертів та консалтингові компанії для проведення процесу аналізу.

Висновки і перспективи подальших досліджень. Результатом проведеного в даній статті дослідження є формування рекомендацій підприємствам галузі ІТ щодо вибору найбільш оптимальних методів якісного аналізу ризиків. Враховуючи стрімкі зміни в зовнішньому середовищі діяльності українських підприємств ІТ індустрії, запропоновані рекомендації

Таблиця 2

Компаративний аналіз якісних методів аналізу ризиків

Метод / Характеристика	Ризик-матриці	SWOT-аналіз	Метод Дельфі	Метод парного порівняння	Метод формування сценаріїв	Брейнстормінг	FMEA-аналіз
Складність	Низька	Низька	Висока	Середня	Висока	Низька	Висока
Вимогливість до вхідних даних	Помірна	Низька	Висока	Помірна	Висока	Низька	Висока
Точність результатів	Середня	Низька	Висока	Середня	Висока	Низька	Висока
Часо- та ресурсомісткість	Низька	Низька	Висока	Середня	Висока	Низька	Висока
Залежність від експертної думки	Середня	Висока	Дуже висока	Висока	Висока	Дуже висока	Низька

Джерело: узагальнено авторами

можуть значно спростити процес якісного аналізу ризиків і пришвидшити перехід до кількісного аналізу.

В подальших дослідження пропонується зосередити увагу на більш докладній адаптації досліджених методик до підприємств галузі ІТ, формуванні шаблонів анкет для таких методик, як метод Дельфі та брейнстормінг з урахуванням потреб та специфіки діяльності конкретних організацій.

Література

1. Emblemsvåg, Jan. (2006). Qualitative risk analysis: Some problems and remedies. Management Decision. 44. 395–408.

2. Krause, P. J., Fox, J., & Judson, P. (1995). Is there a role for qualitative risk assessment? In Proceedings of the Eleventh Conference on Uncertainty in Artificial Intelligence (pp. 290–297). Montreal, Quebec, Canada: Morgan Kaufmann Publishers Inc.

3. Tiusanen, R. (2018). Qualitative Risk Analysis. In N. Möller, S. O. Hansson, J.-E. Holmberg, & C. Rollenhagen (Eds.), Handbook of Safety Principles (pp. 463–492). *Wiley.* https://doi.org/10.1002/9781119443070.ch21.

4. Yoo, Y., & Park, H.-S. (2021). Qualitative Risk Assessment of Cybersecurity and Development of Vulnerability Enhancement Plans in Consideration of Digitalized Ship. *Journal of Marine Science and Engineering,* 9(6), 565. https://doi.org/10.3390/jmse9060565.

5. Зоріна, О. А. (2011). Методи аналізу фінансових ризиків. *Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу,* (2 (20)), 221–229.

6. Шурда, К. Е. (2020). Методи якісного та кількісного аналізу ризиків. *Збалансоване природокористування,* (4), 64–72.

7. Канюк, В. М. (2015). Вибір методів аналізу ризиків для оцінювання податкових ризиків суб'єктів підприємництва. *Науковий вісник Херсонського державного університету. Сер.: Економічні науки,* (12 (1)), 182–186.

8. Білоцерківський, О. (2021). Аналіз методів оцінки підприємницького ризику. *Вісник Національного технічного університету» Харківський політехнічний інститут» (економічні науки),* (4), 65–70.

9. Saket Bansal (2019). Differentiating quantitative risk analysis and qualitative risk analysis. *Izenbridge.* URL: https://www.izenbridge.com/blog/differentiating-quantitative-risk-analysis-and-qualitative-risk-analysis/ (дата звернення: 25.01.2025).

10. Knutson, B., & Huettel, S. A. (2015). The risk matrix. *Current Opinion in Behavioral Sciences,* 5, 141–146.

11. Duijm, N. J. (2015). Recommendations on the use and design of risk matrices. *Safety science,* 76, 21–31.

12. Ukrainian Digital Community (2024). SWOT аналіз — що це, приклади та особливості свот аналізу. *Ukrainian Digital Community.* URL: https://ukrainiandigital.com/swot-analiz/ (дата звернення: 29.01.2025).

13. Business Development Bank of Canada (BDC). (2022). SWOT analysis: An easy tool for strategic planning. URL: https://www.bdc.ca/en/articles-tools/business-strategy-planning/define-strategy/swot-analysis-easy-tool-strategic-planning (дата звернення: 15.02.2025).

14. Куртов, А. І., Полікашин, О. В., Потіхенський, А. І., & Александров, В. М. (2017). Експертні оцінки. Метод Делфі як технологія прийняття управлінських рішень. *Збірник наукових праць Харківського університету Повітряних Сил,* (1), 118–122.

15. Sourani, A., & Sohail, M. (2015). The Delphi method: Review and use in construction management research. *International journal of construction education and research,* 11(1), 54–76.

16. Silverstein, D. A., & Farrell, J. E. (2001). Efficient method for paired comparison. *Journal of Electronic Imaging,* 10(2), 394–398.

17. Tarrow, S. (2010). The strategy of paired comparison: Toward a theory of practice. *Comparative political studies,* 43(2), 230–259.

18. Hassani, B., & Hassani, B. K. (2016). Scenario analysis in risk management. *Springer International Publishing Switzerland.*

19. Mohd-Nassir, M. D., Mohd-Sanusi, Z., & Ghani, E. K. (2016). Effect of brainstorming and expertise on fraud risk assessment. *International Journal of Economics and Financial Issues,* 6(4S).

20. Landis, M., Jerris, S. I., & Braswell, M. (2008). Better brainstorming. *Journal of Accountancy,* 206(4), 70

21. Carbone, T. A., & Tippett, D. D. (2004). Project risk management using the project risk FMEA. *Engineering management journal,* 16(4), 28–35.

22. Curkovic, S., Scannell, T., & Wagner, B. (2013). Using FMEA for supply chain risk management. *Modern management science & Engineering,* 1(2), 251–265.

References

1. Emblemsvåg, Jan. (2006). Qualitative risk analysis: Some problems and remedies. *Management Decision*. 44. 395–408.

2. Krause, P.J., Fox, J., & Judson, P. (1995). Is there a role for qualitative risk assessment? In Proceedings of the Eleventh Conference on Uncertainty in Artificial Intelligence (pp. 290–297). Montreal, Quebec, Canada: Morgan Kaufmann Publishers Inc.

3. Tiusanen, R. (2018). Qualitative Risk Analysis. In N. Möller, S. O. Hansson, J.-E. Holmberg, & C. Rollenhagen (Eds.), Handbook of Safety Principles (pp. 463–492). *Wiley.* https://doi.org/10.1002/9781119443070.ch21.

4. Yoo, Y., & Park, H.-S. (2021). Qualitative Risk Assessment of Cybersecurity and Development of Vulnerability Enhancement Plans in Consideration of Digitalized Ship. *Journal of Marine Science and Engineering,* 9(6), 565. https://doi.org/10.3390/jmse9060565.

5. Zorina O. (2011). Metody analisu finansovykh ryzykiv. [Methods of financial risk analysis] *Problemy teoriii ta metodologiii buhgalters'koho obliku, kontroliu i analizu,* (2 (20)), 221–229.

6. Shurda K. (2020). Metody iakisnoho ta kil'kisnoho analisu ryzykiv. [Methods of Qualitative and Quantitative Risk Analysis]. *Zbalansovane pryrodokorystuvannia,* (4), 64–72 [in Ukrainian].

7. Kaniuk V. (2015). Vybir metodiv analisu ryzykiv dlia ociniuvanniuz podatkovyh ryzykiv sub'iektiv pidpryiemnytstva [Selection of risk analysis methods for assessing tax risks of business entities]. *Naukovyi visnyk Khersons'koho derzhavnoho universytetu. Seriia: Economichni nauky,* (12 (1)), 182–186 [in Ukrainian].

8. Bilotserkivskyi O. (2021). Analis metodiv otsinky pidpryiemnyts'koho ryzyku. [Analysis of methods for assessing entrepreneurial risk]. *Visnyk natsional'noho technichnoho universytetu "Kharkivs'kyi politechnichnyi instytut" (ekonomichni nauky),* (4), 65–70 [in Ukrainian].

9. Saket Bansal (2019). Differentiating quantitative risk analysis and qualitative risk analysis. *Izenbridge.* URL: https://www.izenbridge.com/blog/differentiating-quantitative-risk-analysis-and-qualitative-risk-analysis/.

10. Knutson, B., & Huettel, S. A. (2015). The risk matrix. *Current Opinion in Behavioral Sciences,* 5, 141–146.

11. Duijm, N. J. (2015). Recommendations on the use and design of risk matrices. *Safety science,* 76, 21–31.

12. Ukrainian Digital Community (2024). SWOT analis — shcho tse, pryklady ta osoblyvosti svot-analisu. [SWOT Analysis — What It Is, Examples, and Features of SWOT Analysis.] *Ukrainian Digital Community.* URL: https://ukrainiandigital.com/swot-analiz/ [in Ukrainian].

13. Business Development Bank of Canada (BDC). (2022). SWOT analysis: An easy tool for strategic planning. URL: https://www.bdc.ca/en/articles-tools/business-strategy-planning/define-strategy/swot-analysis-easy-tool-strategic-planning.

14. Kurtov A., Polikashyn O., Potikhens'kyi A., Aleksandrov V. (2017). Ekspertni otsinky. Metod Delphi iak tekhnolohiia pryiniatt'ia rishen'. [Expert assessments. The Delphi Method as a management decision-making technology]. *Zbirnyk naukovykh prac' Kharkivs'koho universytetu Povitrianykh Syl,* (1), 118–122 [in Ukrainian].

15. Sourani, A., & Sohail, M. (2015). The Delphi method: Review and use in construction management research. *International journal of construction education and research,* 11(1), 54–76.

16. Silverstein, D. A., & Farrell, J. E. (2001). Efficient method for paired comparison. *Journal of Electronic Imaging,* 10(2), 394–398.

17. Tarrow, S. (2010). The strategy of paired comparison: Toward a theory of practice. *Comparative political studies,* 43(2), 230–259.

18. Hassani, B., & Hassani, B. K. (2016). Scenario analysis in risk management. *Springer International Publishing Switzerland.*

19. Mohd-Nassir, M. D., Mohd-Sanusi, Z., & Ghani, E. K. (2016). Effect of brainstorming and expertise on fraud risk assessment. *International Journal of Economics and Financial Issues*, 6(4S).

20. Landis, M., Jerris, S. I., & Braswell, M. (2008). Better brainstorming. *Journal of Accountancy,* 206(4), 70.

21. Carbone, T. A., & Tippett, D. D. (2004). Project risk management using the project risk FMEA. *Engineering management journal,* 16(4), 28–35.

22. Curkovic, S., Scannell, T., & Wagner, B. (2013). Using FMEA for supply chain risk management. *Modern management science & Engineering,* 1(2), 251–265.