УДК 658

Остапець Антон Олександрович
аспірант кафедри фінансового аналізу та аудиту
Державного торговельно-економічного університету
Ostapets Anton
Postgraduate Student of 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 Economic Sciences, Professor,
Professor at the Department of Financial Analysis and Audit
State University of Trade and Economics
ORCID: 0000-0001-6506-6965

DOI: 10.25313/2520-2294-2024-9-10265

ФОРМУВАННЯ КЛЮЧОВИХ ПОКАЗНИКІВ РИЗИКУ ДЛЯ ПРОЦЕСУ РИЗИК-МЕНЕДЖМЕНТУ ПІДПРИЄМСТВ ГАЛУЗІ ІТ

DEVELOPMENT OF KEY RISK INDICATORS FOR THE RISK MANAGEMENT PROCESS IN IT INDUSTRY ENTERPRISES

Анотація. *Вступ. У сучасних умовах стрімкого розвитку інформаційних технологій та цифровізації, підприємства галузі ІТ стикаються з численними викликами та ризиками, які можуть негативно вплинути на їх діяльність. Одним із ключових інструментів для забезпечення стабільного функціонування ІТ-компаній є ефективний ризик-менеджмент. Процеси аналізу та контролю ризиків передбачають формування мір та величин, відносно до яких здійснюватиметься оцінювання та контроль за потенційними загрозами. В системі ризик-менеджменту ці величини мають назву ключових показників ризику (KRI). У цій статті розглядаються методологічні підходи до формування KRI для підприємств галузі ІТ, а також їх роль у забезпеченні стійкості та безперервності бізнес-процесів в умовах невизначеності та змін.*

Мета. Мета дослідження полягає в розробці та обґрунтуванні ключових показників ризику (KRI) для підприємств галузі ІТ на основі класифікації ризиків, розробленій і опублікованій авторами в попередніх публікаціях, та які можуть бути ефективно застосовані в процесі управління ризиками на підприємствах галузі. Це дозволить забезпечити своєчасне виявлення, оцінку, моніторинг та мітигацію ризиків, що сприятиме підвищенню стійкості та конкурентоспроможності підприємств у динамічному середовищі галузі інформаційних технологій.

Матеріали і методи. Матеріалами дослідження є: 1) найкращі практики провідних вітчизняних та іноземних організацій галузей інформаційних технологій та підприємницького ризик-менеджменту; 2) праці вітчизняних та зарубіжних авторів, що здійснюють дослідження в сфері ризик-менеджменту підприємств; 3) минулі публікації авторів статті, що будуть використані в якості класифікаційної основи.

В процесі здійснення дослідження було використано наступні наукові методи: теоретичного узагальнення та групування (для характеристики поняття ключових показників ризику та його функцій); формалізації, аналізу та синтезу (для порівняння ключових показників ризику з ключовими показниками ефективності, формування показників у відповідності до наведеної раніше класифікації); логічного узагальнення результатів (формулювання висновків).

Результати. У науковій статті розкрито послідовність формування ключових показників ризику, що будуть використані в подальшому у процесах аналізу та контролю ризиків підприємств галузі ІТ, їх характеристики, процес формування. Запро-

понований ряд показників буде сприяти поліпшенню процесу аналізу та контролю ризиків і використовуватись як базові величини для оцінки потенційних втрат за умови настання ризику та для здійснення управлінських рішень по їх контролю.

Перспективи. У майбутніх наукових дослідженнях буде проведено кількісну оцінку ключових показників ризику, їхніх метричних характеристик і допустимого рівня ризику для підприємств на основі реальних даних компаній. Крім того, значення ключових показників ризику можуть бути адаптовані або масштабовані в залежності від розміру підприємства. Це дозволить покращити процеси управління ризиками та зменшити потенційні втрати у разі настання ризику.

Ключові слова: *risk, key risk indicator, key performance indicator, risk management, IT industry enterprise, risk analysis and control.*

Summary. *Introduction. In the context of modern rapid development in information technology and digitalization, IT industry enterprises face numerous challenges and risks that can adversely affect their operations. One of the key tools for ensuring the stable functioning of IT companies is effective risk management process. The processes of risk analysis and control involve the establishment of metrics and values against which potential threats will be assessed and monitored. In the risk management system, these metrics are referred to as key risk indicators (KRI). This article examines the methodological approaches to forming KRIs for IT enterprises, as well as their role in ensuring business process resilience and continuity in conditions of uncertainty and change.*

Purpose. The purpose of the study is to develop and substantiate key risk indicators (KRIs) for IT industry enterprises based on the risk classification previously developed and published by the authors. These KRIs can be effectively applied in the risk management process within IT companies, enabling timely identification, assessment, monitoring, and mitigation of risks. This approach will contribute to enhancing the resilience and competitiveness of enterprises in the dynamic environment of the information technology sector.

Materials and methods. Research materials include: 1) best practices of leading domestic and foreign organizations in the fields of information technology and enterprise risk management; 2) articles and works written by Ukrainian and foreign authors who conduct research in the field of enterprise risk management; 3) previous publications by the authors of the article, which will be used as a classification basis.

The following scientific methods were used in the research process: theoretical generalization and grouping: to characterize the concept of key risk indicators and their functions; formalization, analysis, and synthesis: to compare key risk indicators with key performance indicators and to develop indicators in accordance with the previously presented classification; logical generalization of results: to formulate conclusions based on the research conducted.

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. In further research it is proposed to focus on the order of documentation and reflection in the accounts and in the reporting of expenses for remuneration of employees of the enterprise, as well as the development of appropriate methods of their analysis. This will improve the methodology and organization of accounting and cost analysis of employees.

Key words: *analysis, accounting, costs of remuneration of employees, labor costs, costs of social benefits, management accounting.*

Постановка проблеми. У сучасних умовах стрімкого розвитку інформаційних технологій та глобальної цифровізації, підприємства галузі ІТ України постійно стикаються з численними викликами та ризиками, які можуть суттєво вплинути на їхню стабільність та конкурентоспроможність. Ці ризики охоплюють як технічні, так і організаційні аспекти, починаючи від потенційних кіберзагроз до управління ресурсами та інновацій. Незважаючи на значний розвиток інструментів ризик-менеджменту, велика кількість ІТ-компаній не надає процесам ризик-менеджменту достатньої уваги і досі не мають чітких та адаптованих до специфіки їх діяльності ключових показників ризику (KRI), які б дозволяли своєчасно ідентифікувати загрози, оцінювати їхній потенційний вплив і ефективно управляти ними.

Відсутність таких показників призводить до того, що процес ризик-менеджменту в ІТ-компаніях є недостатньо систематизованим, що, в свою чергу, може спричинити зростання ймовірності фінансових та репутаційних втрат та порушення безперервності бізнес-процесів. З огляду на все вищезазначене, виникає необхідність у розробці науково обґрунтованих ключових показників ризику, адаптованих до умов і специфіки діяльності підприємств галузі ІТ, що дозволить підвищити ефективність ризик-менеджменту та забезпечити стійкий розвиток підприємств.

Аналіз останніх досліджень і публікацій. Значний внесок у формування базових концепцій формування ключових показників ризику, їх характеристик та використання у процесах ризик-менеджменту підприємства внесли американські вчені Дж. Девіс (J. F. Davies), М. Фінлі (M. Finlay), Т. Маклінеген (T. McLenaghen) та Д. Уілсон (D. Wilson) [1], також велику увагу процесам ризик-менеджменту підприємств та формуванню ключових

показників ризику приділено у книгах італійського науковця Серджіо Скандіццо (S. Scandizzo) [2]. Окремі аспекти методології впровадження та обчислення ключових показників ризику в сфері археології розглянуті в роботах словенських науковців Б. Печека (B. Pecek) та А. Ковачіча (A. Kovacic) [3]. Окрім вищезазначених авторів, ключові показники ризику і їх впровадження в процес ризик-менеджменту підприємств розглянуто в книгах А. Родрігес (A. Rodrigues) та В. Чадха (V. Chadha) [4]. Значну увагу типології та рольовій моделі впровадження ключових показників ризику приділено в статті українських науковців Д. Расшивалова та М. Ружковського [5]. Окремі аспекти порівняння ключових показників ефективності та ключових показників ризику і використання їх у стратегічному ризик-менеджменті розглянуті у статтях І. Федулової [6]. Також аспектам контролю за ризиками за допомогою ключових показників ризику та алгоритм взаємодії розглянуті у роботах К. Ратушної [7].

Метою статті. Мета дослідження полягає в розробці та обґрунтуванні ключових показників ризику (KRI) для підприємств галузі IT на основі класифікації ризиків, розробленій і опублікованій авторами в попередніх публікаціях, та які можуть бути ефективно застосовані в процесі управління ризиками на підприємствах IT-галузі. Це дозволить забезпечити своєчасне виявлення, оцінку, моніторинг та мітигацію ризиків, що, в свою чергу, сприятиме підвищенню стійкості та конкурентоспроможності підприємств у динамічному середовищі галузі інформаційних технологій.

Матеріали і методи. Матеріалами дослідження є: 1) найкращі практики провідних вітчизняних та іноземних організацій галузей інформаційних технологій та підприємницького ризик-менеджменту; 2) праці вітчизняних та зарубіжних авторів, що здійснюють дослідження в сфері ризик-менеджменту підприємств; 3) минулі публікації авторів статті, що будуть використані в якості класифікаційної основи

В процесі здійснення дослідження було використано наступні наукові методи: теоретичного узагальнення та групування (для характеристики поняття ключових показників ризику та його функцій); формалізації, аналізу та синтезу (для порівняння ключових показників ризику з ключовими показниками ефективності, формування показників у відповідності до наведеної раніше класифікації); логічного узагальнення результатів (формулювання висновків).

Виклад основного матеріалу. Українські IT-компанії за сферою діяльності здебільшого спираються на іноземних клієнтів та співпрацюють з ними, що, в свою чергу, веде до необхідності інтеграції у світову IT-спільноту. Позитивною стороною даного процесу є використання багаторічних методів і практик стосовно аналізу та контролю ризиків. Оскільки за своїм визначенням, аналіз представляє собою процес детального вивчення об'єкта, явища або системи з метою розділення їх на складові частини і вивчення кожної з цих частин окремо, одним з важливих ключових елементів є визначення показників, що будуть аналізуватись. У сфері ризик-менеджменту використовується поняття ключових показників ризику (Key Risk Indicator). Спеціалісти профільної американської компанії Techtarget [8] визначають ключові показники ризику як метрику, призначену для вимірювання вірогідності того, що поєднана ймовірність настання події та її наслідків перевищить ризик-апетит організації та матиме надзвичайно негативний вплив на здатність організації бути успішною. Ключові показники ризику відіграють важливу роль у процесах управління ризиками підприємства і виступають в якості завчасного попередження про потенційні ризики, що можуть завдати шкоди організації та мати негативний вплив на її фінансовий стан. Також вони служать для постійного процесу моніторингу ризиків і виявлення слабких місць у цих процесах для подальшого їх удосконалення.

Дуже важливим аспектом в дослідженні поняття ключових показників ризику є розуміння того, що вони не мають спільного з ключовими показниками ефективності, не зважаючи на те, що вони є важливими інструментами для оцінювання ефективності операційних процесів і процедур організації. Ключові показники ефективності та ключові показники ризику виконують різні функції.

Ключові показники ефективності використовуються для оцінки того, наскільки організації досягають поставлених цілей та завдань, і здебільшого охоплюють позитивну складову, таку як зростання доходів, задоволеність клієнтів та операційну ефективність. Вони є важливими для відстеження прогресу, прийняття стратегічних рішень та покращення загальної ефективності.

На відміну від ключових показників ефективності, ключові показники ризику призначені для виявлення ризиків та вразливостей, які можуть вплинути на операції та цілі організації. Ключові показники ризику можуть бути як позитивними, так і негативними, вказуючи як на підвищений ризик, так і на ефективність зусиль з їх пом'якшення. Також вони допомагають організаціям передбачати потенційні проблеми.

Організаціям, від малих бізнесів до великих підприємств, необхідно підтримувати збалансований підхід до використання як ключових показників ефективності для оптимізації ефективності, так і ключових показників ризику для управління ризиками. Таким чином, обидва показники допомагають організаціям рухатися до довгострокового успіху та стійкості.

Відмінність між ключовими показниками ефективності та ключовими показниками ризику можна побачити в таблиці 1.

Оскільки створення і визначення ключових показників ризику є важливим етапів процесу ризик-

Таблиця 1

Порівняння ключових показників ефективності і ключових показників ризику

Фактор	Ключовий показник ефективності	Ключовий показник ризику
Персонал	• Повна зайнятість, необхідна для оптимальної роботи компанії; • Задоволеність працівників компанією та умовами роботи.	• Рівень відсутності працівників у проєкті; • Рівень незадоволеності працівників компанією та умовами праці.
Процеси	• Виробництво важливого продукту/ надання послуг підтримується на рівні, достатньому для задоволення попиту; • Існуючі характеристики продуктів/наданих послуг є задовільними та забезпечують очікувану цінність і результати для клієнтів.	• Падіння показників виробництва продуктів/ надання послуг до неприйнятного рівня; • Падіння показників продажів, зниження рівня конкурентоспроможності через невідповідність конструкції виробів сучасним вимогам.
Технології	• Мінімізація порушень роботи ІТ-систем через кібератаки шляхом регулярного оновлення систем кібербезпеки; • Мінімізація перебоїв у роботі бізнесу завдяки резервному копіюванню систем, файлів даних і баз даних до їх найновішої точки відновлення	• Невчасність рівня оновлення систем кібербезпеки організації; • Невідповідність періодичності резервного копіювання до поточного часу

менеджменту, доцільним є розуміння їх призначення. Отже, ключові показники ризику призначені для:

1. **Раннього попередження про ризики**. Ключові показники ризику служать в якості системи раннього попередження про ризики перед тим, як їх вплив у разі настання стане більшим, і вжиття заходів по контролю за ними;

2. **Ідентифікації та послаблення ризиків**. Завдяки вчасному виявленню ризиків або ж зміни в їх кількісних показниках, організації можуть негайно вжити міри з їх пом'якшення задля мінімізації потенційного або очікуваного негативного впливу;

3. **Грамотного розподілу ресурсів і підвищення ефективності організації**. Зосередження на пріоритетних ризиках та вчасне розподілення ресурсів на їх контроль роблять процеси ризик-менеджменту більш цілеспрямованими та стратегічними;

4. **Комунікації та звітності**. Ключові показники ризику надають стандартизований спосіб передачі інформації про ризики зацікавленим сторонам, від керівництва до членів ради директорів, що, в свою чергу, покращує процес звітності та сприяє підвищенню відповідальності у керуванні ризиками як спільною відповідальністю.

5. **Моніторингу відповідності**. Ключові показники ризику можуть допомагати організаціям контролювати та забезпечувати дотримання нормативних вимог і стандартів задля уникнення юридичних та регуляторних проблем;

6. **Підтримки прийняття рішень**. Чітке уявлення про ризиковий ландшафт допомагає організаціям приймати більш обґрунтовані та стратегічні рішення, ефективно розподіляти ресурси та коригувати свої стратегії за потреби;

7. **Безперервного вдосконалення**. Знання, отримані на основі наданих ключовими показниками ризику даних, можуть бути використані для вдосконалення стратегій та процесів управління ризиками, а також для загального покращення діяльності організації.

Також окрім зазначеного вище призначення ключових показників ризику, кожен показник має відповідати наступним характеристикам:

8. **Кількісність** (пов'язана з числовими показниками витрат або потенційних втрат);

9. **Вимірюваність** (точність вимірювання і чіткість показників);

10. **Підтверджуваність** (висока ступінь впевненості в можливості настання);

11. **Відповідність** (вимірювання необхідності прийняття рішень).

Зважаючи на наведені вище характеристики та призначення, процес створення ключових показників ризику (KRI) вимагає ретельного і вдумливого підходу з метою забезпечення ефективного моніторингу потенційних ризиків в організації. Даний процес включає в себе 8 етапів, що мають бути пройдені відповідним підрозділом організації і відповідати характеристикам, наведеним в таблиці 2.

На першому етапі створення ключових показників ризику співробітники підрозділу, що займається їх аналізом та контролем, разом топ-менеджментом компанії, а також з зацікавленими особами, проводять всебічну оцінку потенційних загроз, що можуть негативно вплинути на досягнення стратегії та цілей компанії. В подальшому після розуміння цілей та стратегії важливим аспектом є категоризація та класифікація ризиків, з якими компанія може стикатись під час своєї діяльності. Відповідно до класифікації, що була визначена в минулих публікаціях авторів [10], стає можливим визначення ключових показників ризиків для організації галузі ІТ. На основі даної класифікації, ключові показники ризику, що можуть бути використані під час процесу ризик-менеджменту, наведені в табл. 3.

Таблиця 2

Процес створення ключових показників ризику

Етап	Опис
Розуміння організації	Глибоке розуміння цілей, операцій, галузі та ландшафту ризиків. Даний процес допомагає визначенню області, в якій потрібно здійснювати моніторинг ризиків. Обов'язковим є врахування внутрішніх та зовнішніх факторів, які можуть вплинути організацію.
Визначення категорій ризиків	Категоризація типів ризиків, з якими стикається організація. Найбільш поширеними типами є фінансові, операційні та комплаєнс-ризики. Розуміння цих категорій допомагає визначити обсяг розробки ключових показників ризику.
Залучення зацікавлених сторін	Залучення вищого менеджменту, керівників підрозділів та команди з управління ризиками до процесу створення ключових показників ризиків. Спільні обговорення можуть допомогти визначити ключові проблемні області та інформацію, необхідну для ефективного моніторингу цих областей.
Визначення факторів ризику	Визначення в кожній категорії ризиків конкретних факторів ризику, які є специфічними, вимірюваними та пов'язаними з цілями організації. Наприклад, для моніторингу фінансових ризиків, факторами можуть бути коефіцієнти ліквідності, рівень заборгованості або концентрація доходів.
Встановлення порогів та тригерів	Пороги представляють допустимий діапазон для кожного фактора ризику. За умови перевищення порогу, відбувається сповіщення або подальше розслідування. Пороги повинні базуватися на історичних даних, галузевих еталонах та ризиковому апетиті організації.
Визначення джерел та методів вимірювання даних для кожного KRI.	До даних можуть належати фінансові звіти, операційні дані, регуляторні документи та галузеві еталони. Також необхідним є розробка методів для збору та вимірювання даних, пов'язаних з кожним ключовим показником ризику.
Аналіз, звітування та візуалізація зібраних даних.	Розрахунок значень KRI може здійснюватися за допомогою математичних формул або статистичного аналізу, залежно від природи фактора ризику. Також необхідним є створення системи для звітування та візуалізації ключових показників ризику, наприклад, через інформаційні панелі та звіти.
Документація всієї структури ключових показників ризиків.	Включення обґрунтування вибору конкретних ключових показників ризиків та їхніх відповідних порогів. Потім необхідно задокументувати політики та процедури моніторингу ключових показників ризиків для забезпечення їх легкої доступності.

Джерело: узагальнено авторами за [8]

В таблиці 3 наведена велика кількість ключових показників ризику, не всі з яких можуть стосуватись діяльності конкретної IT-компанії, тож після формування переліку, важливим етапом є залучення зацікавлених сторін, а саме керівників підрозділів, проектів, топ-менеджменту з метою визначення ключових слабких місць та аспектів, що потребують найбільшої уваги. В результаті переговорного процесу кількість показників ризику може змінюватись в кількості, але під його кінець, перелік має бути сформований і відбутись більш детальний процес стосовно визначення факторів виникнення ризикових подій.

Наступним етапом є кількісна оцінка і встановлення порогів, за яких значення ключового показнику ризику набуде величини, достатньої для приділення йому уваги. Дані пороги або тригери можуть бути використані як сигнал для необхідності початку процесу контролю ризику.

В подальшому після формування порогів та тригерів важливим етапом є визначення джерел отримання інформації. Джерелами отримання інформації можуть бути як внутрішні, так і зовнішні, до них входять фінансові звіти, операційні дані різних підрозділів компанії, нормативні документи та галузеві контрольні показники. Увесь перелік даних має пройти усесторонню обробку з метою оцінки відповідності даних ключовим показникам ризику та можливості їх подальшого застосування.

Результатом процесу аналізу даних є можливість їх інтеграції в існуючі інструменти обробки з метою їх подальшої візуалізації та можливості проведення певних репортингових маніпуляцій. Окрім інтеграції в існуючі системи, такі як, Tableau, Microsoft Power BI, Qlik Sense, Looker, проаналізовані дані можуть бути використані для розробки власних інструментів для звітування та візуалізації про ризикові події.

Останнім етапом створення ключових показників ризику є чітка і послідовна документація, що спростить в подальшому можливість роботи з даними та інструментами різними підрозділами компанії.

Запропоновані в таблиці 3 ключові показники ризику в подальшому будуть використані в процесах аналізу та контролю за ризиковими подіями.

Висновки і перспективи подальших досліджень. Результатом проведеного в даній статті дослідження є сформований перелік ключових

Таблиця 3

Ключові показники ризику IT-компанії згідно до авторської класифікації

Тип/вид ризику та опис	Ключові показники ризику
Юридичні (Ризики, пов'язані з законами, зовнішніми та внутрішніми правилами, політиками та рекомендаціями, внутрішніми питаннями чи етикою).	• Кількість змін у регуляторних вимогах, що стосуються організації, за певний період; • Частота та серйозність регуляторних штрафів або санкцій; • Кількість невдалих регуляторних аудитів або перевірок; • Кількість випадків порушень політик організації; • Кількість та частота сповіщень про конфлікт інтересів; • Кількість скарг або запитів на захист даних (наприклад, запити згідно з GDPR); • Кількість поточних судових справ; • Юридичні витрати у відсотках від доходу; • Кількість скарг клієнтів, пов'язаних з юридичними питаннями.
Політичні (Ризики, пов'язані за змінами к політичній обстановці в країні, зміною законодавства тощо, які можуть спонукати інвесторів відмовитись чи обмежити інвестиції).	• Кількість та частота прийняття нових законів або змін до існуючого законодавства; • Частота та масштаб регуляторних змін, які можуть вплинути на конкретні галузі або ринки; • Частота змін уряду або керівництва країни, яка може вплинути на політичний курс; • Кількість міжнародних конфліктів або суперечок, які можуть вплинути на торгівлю або інвестиції; • Кількість та частота змін у торговельних угодах; • Частота та результати виборів, які можуть призвести до змін у політичному ландшафті; • Частота змін у законах про працю, які можуть вплинути на зайнятість та трудові витрати; • Частота змін у податковій політиці, які можуть вплинути на фінансові результати компанії; • Зміни у політиці національної або міжнародної безпеки, які можуть вплинути на операційну діяльність компанії.
Операційні (Ризики, пов'язані з внутрішніми процесами, системами, людьми та зовнішніми подіями).	• Кількість інцидентів відмови критично важливого обладнання; • Рівень продуктивності праці у порівнянні з встановленими нормами; • Кількість рекламацій на випущений продукт/надані послуги; • Кількість випадків затримок в наданні послуг; • Відхилення фактичних витрат від бюджетних показників; • Кількість інцидентів, пов'язаних з невиконанням зобов'язань постачальниками; • Кількість скарг клієнтів, пов'язаних з якістю обслуговування, якістю продукту; • Час реагування на запити та скарги клієнтів; • Кількість проектів, що виходять за рамки бюджетних або часових обмежень.
Економічні (Ризики, пов'язані з ситуацією в економічному середовищі, що можуть негативно вплинути на фінансовий стан, операційну діяльність організації, стратегії розвитку та загальну стійкість компанії).	• Рівень інфляції в країні чи регіоні; • Коливання обмінного курсу валюти; • Відсоток доходів або витрат в іноземній валюті; • Рівень заборгованості компанії щодо власного капіталу; • Кредитний рейтинг компанії; • Рівень дефолтів серед клієнтів або постачальників; • Коливання на фондовому ринку та їхній вплив на капіталізацію компанії; • Рівень кредитоспроможності основних банківських партнерів; • Частота та масштаби банківських криз; • Рівень прямих іноземних інвестицій; • Індекси інвестиційної привабливості, стабільності країни або регіону.
Стратегічні (Ризики, пов'язані з прийняттям рішень на рівні стратегії компанії, які можуть вплинути на досягнення її довгострокових цілей і місії).	• Темпи зростання або скорочення ринку, на якому оперує компанія; • Зміни в ринкових частках основних конкурентів; • Частота нових регуляторних ініціатив, що впливають на галузь; • Рівень інвестицій у дослідження та розробки; • Кількість нових технологій або інновацій, впроваджених на ринку; • Зміни у вподобаннях та потребах клієнтів; • Рівень задоволеності клієнтів та їх лояльності; • Кількість конкурентів на ринку, поява нових; • Частота значних змін у стратегіях та показниках основних конкурентів; • Частота та серйозність репутаційних криз; • Надійність та стабільність ключових постачальників і партнерів; • Рівень стабільності у країнах, де компанія здійснює операційну діяльність; • Зміни у торговельних угодах або політичні санкції; • Частота змін у керівництві компанії; • Кількість стратегічних проектів, що виконуються поза графіком і за межами бюджету; • Частота невдач або затримок у реалізації стратегічних ініціатив.

Продовження табл. 3

Пов'язані з IT-інфраструктурою (Ризики, пов'язані з інформаційними технологіями та системами організації).	• Кількість збоїв у роботі IT-систем; • Час відновлення роботи систем після збоїв; • Відсоток часу безвідмовної роботи систем; • Час відгуку критичних систем та додатків; • Час реагування на інциденти безпеки; • Частота відмов критичного обладнання (сервери, мережеві пристрої); • Середній час відновлення після відмови; • Відсоток систем, які працюють не на останніх версіях програмного забезпечення; • Середній час встановлення оновлень та патчів; • Кількість і частота інцидентів, викликаних плановими роботами; • Рівень використання мережевої пропускної здатності; • Відсоток невдало завершених резервних копій; • Час реагування IT-персоналу на запити користувачів; • Кількість скарг від користувачів на роботу IT-систем; • Відсоток відповідності IT-послуг договірним угодам про рівень обслуговування; • Кількість порушень SLA; • Рівень виконання планів з обслуговування та модернізації IT-інфраструктури; • Кількість виявлених вразливостей в IT-системах; • Час між виявленням вразливості та її усуненням.
Пов'язані з кадровим потенціалом (Ризики, пов'язані з людським фактором, які можуть вплинути на ефективність та стійкість бізнесу).	• Коефіцієнт плинності кадрів (відсоток працівників, які залишили компанію протягом певного періоду); • Коефіцієнт плинності серед ключових працівників та керівництва; • Результати опитувань щодо задоволеності працівників; • Рівень залученості та мотивації працівників; • Середня тривалість лікарняних та неоплачуваних відпусток; • Відсоток невиконання планів та завдань працівниками; • Кількість випадків порушення дисципліни або кодексу поведінки; • Кількість дисциплінарних заходів та звільнень; • Час, необхідний для заповнення вакантних посад; • Відсоток нових працівників, які не пройшли випробувальний термін; • Відсоток витрат на персонал у загальних операційних витратах компанії; • Кількість внутрішніх конфліктів та скарг працівників; • Час, необхідний для вирішення конфліктів та скарг; • Кількість порушень трудового законодавства та регуляторних вимог.
Пов'язані з втратою чи витоком інформації (Ризики, пов'язані із захистом інформаційних активів, збереженням, резервуванням даних та інформації)	• Кількість інцидентів безпеки, пов'язаних з втратою даних або витоком інформації; • Кількість спроб несанкціонованого доступу до інформаційних систем; • Кількість успішних атак, що призвели до витоку даних; • Відсоток чутливих даних, які зберігаються в зашифрованому вигляді; • Кількість інцидентів, пов'язаних з незашифрованими даними; • Кількість порушень політик доступу до даних; • Відсоток працівників, які пройшли навчання з інформаційної безпеки; • Кількість випадків втрати або крадіжки фізичних носіїв даних (наприклад, ноутбуків, USB-накопичувачів); • Кількість випадків, коли фізичні носії даних були залишені без нагляду або незахищеними; • Частота проведення перевірок та аудитів інформаційної безпеки; • Кількість виявлених аномалій у системах моніторингу; • Відсоток систем, які відповідають галузевим стандартам безпеки (наприклад, ISO/IEC 27001); • Час, необхідний для повного розслідування та усунення наслідків інциденту; • Кількість звітів про підозрілі активності, поданих працівниками.
Соціальні (Ризики, пов'язані із соціальними аспектами діяльності.)	• Кількість негативних згадок у ЗМІ та соціальних мережах; • Індекс репутації компанії у галузі (наприклад, за результатами опитувань або досліджень); • Рівень задоволеності клієнтів за результатами опитувань; • Кількість скарг клієнтів та час їх вирішення; • Рівень дотримання стандартів корпоративної соціальної відповідальності; • Рівень задоволеності працівників умовами праці; • Кількість страйків або інших форм протестів серед працівників; • Рівень задоволеності працівників програмами інклюзії; • Кількість скарг на дискримінацію та їхнє вирішення; • Відсоток постачальників, які відповідають соціальним стандартам компанії;

Продовження табл. 3

	• Кількість випадків порушення етичних норм та їхнє вирішення; • Рівень дотримання екологічних стандартів та нормативів.
Ринкові (Ризики, пов'язані з ринковими умовами, які можуть вплинути на діяльність та стратегії організації.)	• Кількість нових конкурентів на ринку; • Зміни в конкурентних стратегіях, таких як ціни, маркетингові кампанії та нові продукти; • Коливання цін на основні продукти або послуги; • Відхилення цін від середнього рівня на ринку; • Частота та обсяг цінових змін; • Зміни в обсягах продажів; • Коливання попиту на основні продукти або послуги; • Зміни в перевагах та поведінці споживачів; • Частота змін у законодавстві, що стосується галузі; • Вплив нових регуляцій на витрати та операційні процеси компанії, її продукти; • Рівень задоволеності клієнтів продукцією або послугами; • Частота технологічних інновацій та їх вплив на ринок; • Вплив міжнародних економічних та політичних подій на ринок; • Вплив глобальних криз, таких як пандемії або природні катастрофи; • Відсоток нових та втрачених клієнтів; • Рівень лояльності клієнтів; • Коливання доходів та прибутків компанії; • Відсоток невиконаних фінансових прогнозів; • Зростання або коливання відсотку дебіторської заборгованості; • Доступність кваліфікованої робочої сили.
Пов'язані з деактуалізацією коду програмного забезпечення (Ризики, пов'язані з застаріванням або недостатньою актуальністю програмного забезпечення)	• Кількість оновлень програмного коду, випущених за певний період; • Середній інтервал між випусками оновлень; • Відсоток коду, що використовує застарілі технології або фреймворки; • Кількість компонентів, які більше не підтримуються постачальником; • Кількість виявлених вразливостей у програмному коді; • Час, необхідний для виправлення виявлених вразливостей; • Число зареєстрованих дефектів або багів у програмному забезпеченні; • Відсоток критичних багів, що впливають на основну функціональність; • Відсоток коду, покритого автоматичними тестами; • Кількість тестів, що провалилися, під час інтеграційного тестування; • Повнота та актуальність технічної документації; • Кількість проблем сумісності при інтеграції з новими системами або технологіями; • Частота оновлень, що вимагаються для підтримки сумісності; • Частота та тривалість затримок у розробці нових функцій або релізів; • Загальні витрати на підтримку та обслуговування застарілого коду; • Відсоток бюджету на IT, витраченого на технічний борг; • Кількість критичних компонентів, розроблених сторонніми постачальниками; • Зростання витрат на інфраструктуру через неефективний або застарілий код; • Рівень задоволеності користувачів програмним забезпеченням; • Кількість скарг від користувачів щодо продуктивності або функціональності.
Інтеграційні (Ризики, пов'язані з процесом інтеграції інформаційних технологій.)	• Частота та тривалість затримок у виконанні етапів інтеграції; • Відсоток завершених завдань відповідно до запланованого графіку; • Перевищення бюджету на IT-інтеграцію; • Співвідношення фактичних витрат до запланованих витрат; • Кількість інцидентів, пов'язаних з проблемами якості даних; • Кількість збоїв або відмов після інтеграції; • Час простою системи через проблеми інтеграції; • Зміни у швидкості обробки даних та продуктивності системи; • Кількість скарг користувачів на зниження продуктивності; • Частота оновлень або виправлень для забезпечення сумісності; • Кількість виявлених вразливостей після інтеграції; • Час реагування на інциденти безпеки, пов'язані з інтеграцією; • Кількість запитів на технічну підтримку після інтеграції; • Рівень прийняття нових систем користувачами; • Кількість негативних відгуків або скарг від користувачів; • Повнота та актуальність документації щодо інтеграційних процесів; • Кількість бізнес-процесів, які зазнали змін через інтеграцію; • Кількість звернень до технічної підтримки, пов'язаних з інтеграцією; • Середній час вирішення інцидентів;

Продовження табл. 3

	• Відсоток ризиків, які були ідентифіковані та успішно усунені; • Кількість інцидентів, пов'язаних з невідповідністю нормативним вимогам.
Ризики кіберзлочинності (Ризики, пов'язані з впливом на організацію кіберзлочинів)	• Загальна кількість виявлених кіберінцидентів за певний період; • Частота виникнення кіберінцидентів; • Кількість інцидентів, пов'язаних з різними типами атак (фішинг, шкідливе ПЗ, DDoS, і т.д.); • Частота виникнення конкретних типів загроз; • Середній час виявлення кіберінциденту; • Середній час реагування на кіберінцидент; • Кількість виявлених вразливостей у програмному забезпеченні та системах; • Частота виявлення нових вразливостей; • Кількість інцидентів, що призвели до витоку даних; • Кількість інцидентів, що спричинили фінансові втрати; • Кількість інцидентів, що спричинили зупинку бізнес-процесів; • Відсоток систем, захищених останніми оновленнями безпеки; • Кількість користувачів, які стали жертвами фішингових атак; • Відсоток користувачів, які пройшли навчання з кібербезпеки; • Кількість виявлених аномалій у мережевому трафіку; • Частота спрацювання систем моніторингу безпеки; • Кількість кіберінцидентів, пов'язаних з постачальниками або партнерами; • Відсоток третіх сторін, які відповідають вимогам безпеки; • Результати оцінок безпеки (наприклад, рівень успішності пен-тестів); • Частка бюджету IT, витраченого на кібербезпеку; • Кількість інцидентів, що призвели до втрати або крадіжки даних; • Обсяг втрачених або викрадених даних; • Відсоток систем, що відповідають вимогам стандартів та нормативів безпеки (наприклад, GDPR, ISO/IEC 27001); • Кількість оцінених та ідентифікованих кіберризиків; • Рівень критичності оцінених ризиків; • Кількість скарг користувачів, пов'язаних з безпекою; • Рівень задоволеності користувачів заходами безпеки.

Джерело: узагальнено авторами

показників ризику, що можуть бути використані в процесах ризик-менеджменту підприємств галузі IT. Перелік даних показників може бути масштабований в залежності від специфіки бізнесу конкретної компанії а також від специфіки конкретного проекту. Враховуючи поточні умови зовнішнього середовища, в яких здійснюють діяльність українські IT-компанії, ризик-менеджмент є все більш важливою процедурою і компанії вимушені створювати окремі підрозділи для протидії і контролю за ризиками, тому наведені у статті ключові показники ризику можуть бути використані в процесах аналізу та контролю ризиків цими підрозділами.

В подальших наукових дослідженнях пропонується зосередити увагу на кількісних характеристиках наведених показників, документальному оформленню та впровадженню їх в існуючі системи аналізу та контролю ризиків. Це надасть змогу створити універсальну систему аналізу та контролю ризиків IT-компаній.

Література

1. Davies J., Finlay M., McLenaghen T., Wilson D. Key risk indicators — their role in operational risk management and measurement. ARM and RiskBusiness International. Prague, 2006. P. 1–32.

2. Scandizzo S. Risk Mapping and Key Risk Indicators in Operational Risk Management. *Economic Notes*. 2005. 34. P. 231–256.

3. Peček B., Kovačič A. Methodology of monitoring key risk indicators. *Economic Research-Ekonomska Istraživanja.* 2019. Vol. 32, No. 1. P. 3485–3501.

4. Rodriguez A., Chadha V. Key Risk Indicators. Risk Books, 2015. 202 p.

5. Rasshyvalov D., Rushkovskyi M. Use of the key risk indicators method in risk management strategies. *Actual Problems of International Relations.* 2022. No. 153. P. 69–80.

6. Fedulova, I. Risk management strategy. *Management and Entrepreneurship in Ukraine: the stages of formation and problems of development.* 2019. Vol. 2019, No. 1. P. 65–74.

7. Ратушна К. Розробка методики оцінювання та контролю системи управління даними у клінічних випробуваннях за допомогою ключових показників ризиків. *Клінічна фармація*. 2015. Т. 19, № 1. С. 17–24.

8. Kirvan P., Tucci L. What is a Key Risk Indicator (KRI) and Why is it Important?. *CIO.* URL: https://www.techtarget.com/searchcio/definition/key-risk-indicator-KRI (дата звернення: 01.09.2024).

9. What are Key Risk Indicators? URL: https://safetyculture.com/topics/risk-management/key-risk-indicators/ (дата звернення: 01.09.2024).

10. Назарова К., Парасій-Вергуненко І., Остапець А. Класифікація ризиків компаній ІТ-індустрії. *Scientia Fructuosa.* 2023. Т. 150, № 4. С. 120–137.

References

1. Davies, J., Finlay, M., McLenaghen, T., & Wilson, D. (2006). Key risk indicators — their role in operational risk management and measurement. *ARM and RiskBusiness International.* Prague. pp. 1–32.

2. Scandizzo, S. (2005). Risk Mapping and Key Risk Indicators in Operational Risk Management. *Economic Notes.* 34. pp. 231–256.

3. Peček, B., & Kovačič, A. (2019). Methodology of monitoring key risk indicators. *Economic Research-Ekonomska Istraživanja*. Vol. 32, no. 1. pp. 3485–3501.

4. Rodriguez, A., & Chadha, V. (2015). Key Risk Indicators. Risk Books. 202 p.

5. Rasshyvalov, D., & Rushkovskyi, M. (2022). Use of the key risk indicators method in risk management strategies. *Actual Problems of International Relations*. No. 153. pp. 69–80.

6. Fedulova, I. (2019). Stratehiia ryzyk-menedghmentu [Risk management strategy]. *Management and Entrepreneurship in Ukraine: the stages of formation and problems of development.* Vol. 2019, No. 1. pp. 65–74 [in Ukrainian].

7. Ratushna, K. (2015). Rozrobka metodyky otsiniuvannia ta kontroliu systemy upravlinnia danymy u klinichnykh vyprobuvanniakh za dopomohoiu kliuchovykh pokaznykiv ryzykiv [Development of a methodology for assessing and controlling the data management system in clinical trials using key risk indicators]. *Klinichna farmaciia.* Vol. 19, № 1. pp. 17–24.

8. Kirvan, P., Tucci L. What is a Key Risk Indicator (KRI) and Why is it Important?. *CIO.* URL: https://www.techtarget.com/searchcio/definition/key-risk-indicator-KRI.

9. What are Key Risk Indicators? URL: https://safetyculture.com/topics/risk-management/key-risk-indicators/

10. Nazarova, K., Parasii-Verhunenko, I., & Ostapets, A. (2023). Klasyfikaciia ryzykiv companiy IT-industriii [IT companies' risks classification] *Scientia Fructuosa*. Vol. 150, № 4. pp. 120–137.