DOI: 10.31617/1.2023(149)08
УДК 005.334:658.15]:004.9

НАЗАРОВА Карина,
д. е. н., професор, завідувач кафедри фінансового аналізу та аудиту Державного торговельно-економічного університету
вул. Кіото, 19, м. Київ, 02156, Україна

ORCID: 0000-0002-5019-9244
k.nazarova@knute.edu.ua

ПАРАСІЙ-ВЕРГУНЕНКО Ірина,
д. е. н., професор, професор кафедри фінансового аналізу та аудиту Державного торговельно-економічного університету
вул. Кіото, 19, м. Київ, 02156, Україна

ORCID: 0000-0001-6506-6965
i.parasij-vergunenko@knute.edu.ua

ОСТАПЕЦЬ Антон,
аспірант кафедри фінансового аналізу та аудиту Державного торговельно-економічного університету
вул. Кіото, 19, м. Київ, 02156, Україна

ORCID: 0000-0001-7048-6112
a.ostapets@knute.edu.ua

КЛАСИФІКАЦІЯ РИЗИКІВ КОМПАНІЙ ІТ-ІНДУСТРІЇ

В умовах стабільно зростаючого ринку ІТ-послуг України актуальним є питання підвищення ефективності управління ризиками, з якими стикаються компанії. Класифікація ризиків є одним з найважливіших інструментів інформаційного забезпечення ризик-менеджменту задля підвищення конкурентоспроможності та фінансової стійкості компаній на такому турбулентному ринку, як ринок України. Метою дослідження є систематизація ризиків ІТ-компаній та вдосконалення їх класифікації для підвищення ефективності управління ними та їх мінімізації. У ході дослідження застосовано такі наукові методи: аналіз, синтез, індукція, дедукція, порівняння, ряди динаміки, середні та відносні величини, коефіцієнтний аналіз, абстрагування, аналогія та узагальнення.

NAZAROVA Karina,
Doctor of Sciences (Economics), Professor, Professor Head at the Department of Financial Analysis and Audit
State University of Trade and Economics
19, Kyoto St., Kyiv, 02156, Ukraine

ORCID: 0000-0002-5019-9244
k.nazarova@knute.edu.ua

PARASII-VERHUNENKO Iryna,
Doctor of Sciences (Economics), Professor, Professor at the Department of Financial Analysis and Audit
State University of Trade and Economics
19, Kyoto St., Kyiv, 02156, Ukraine

ORCID: 0000-0001-6506-6965
i.parasij-vergunenko@knute.edu.ua

OSTAPETS Anton,
Postgraduate Student at the Department of Financial Analysis and Audit
State University of Trade and Economics
19, Kyoto St., Kyiv, 02156, Ukraine

ORCID: 0000-0001-7048-6112
a.ostapets@knute.edu.ua

RISK CLASSIFICATION OF IT INDUSTRY COMPANIES

In the conditions of steadily growing market of IT services in Ukraine, the issue of increasing the effectiveness of risk management that companies face is urgent. Risk classification is one of the most important information provisioning tools for risk management directed to increase the competitiveness and financial stability of companies in such a turbulent market as the market of Ukraine. Scientific methods, such as: analysis, synthesis, induction, deduction, comparison, dynamics series, averages and relative values, coefficient analysis, abstraction, analogies, and generalizations were used in the research. The essence of political, economic, operational and legal risks has been researched. In addition to stated, risks classification and its consideration are one of the most important factors, ensuring a high level of competitiveness, saving of positive development trend, ensuring a high repu-

Copyright © Автор(и). Це стаття відкритого доступу, яка розповсюджується на умовах ліцензії Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/)

Досліджено сутність політичних, економічних, операційних та юридичних ризиків. Здійснено критичну оцінку підходів науковців до класифікації ризиків та доведено, що на діяльність ІТ-підприємства впливають як загальні, так і специфічні саме для галузі ІТ-ризики. При класифікації ризиків ІТ-підприємств запропо-новано враховувати такі ознаки, як сфера виникнення і наслідки ризику. Ризики класифіковано відповідно до джерел їх виникнення. Доведено доцільність поділу ризиків за рівнем впливу на діяльність підприємства та спричиненими наслідками на: допустимі (низькі і середні), високі, критичні, катастрофічні. Наведено характеристику кожного виду ризиків та розкрито їх значення для діяльності ІТ-компанії. На основі досвіду вітчизняних компаній доведено необхідність і доцільність виокремлення специфічних ризиків, пов'язаних з питаннями кадрового потенціалу, кіберзлочинності, проєктами тощо.

Ключові слова: фінанси, класифікація, ризик, управління ризикам, безпека, фактор, ІТ-проєкт, ІТ-компанія.

tation level, expanding the market share, ensuring business continuity etc. on such turbulent market as Ukrainian one. The critical assessment of scientifical approaches regarding risks classification is also performed and it's proven that not only general (applicable for all companies regardless their field of activity) risks, but specific for IT-industry ones are creating an impact on company's performance. Also it's important to state that the field of occurrence and risk consequences is worth to be considered in IT-companies' risks classification. The importance of risks division by the level of impact (affordable (low and medium), high, critical and catastrophic) on company's performance is also noted in current article. The characteristics of each risk types have been noted in current article and their value for company's performance has been shown. Based on the experience of domestic companies, the necessity and expediency of identifying specific risks related to issues of personnel potential, cybercrime, projects, etc. has been proven.

Keywords: finances, risk, risk management, security, factor, IT-project, IT-Company

JEL Classification: M15, M21, M41.

Вступ.

В умовах стабільно зростаючого протягом останніх років ринку ІТ-послуг України актуалізуються питання управління ризиками, з якими стикаються компанії упродовж свого функціонування.

Діяльність ІТ-компаній пов'язана з великою кількістю ризиків. За сучасних умовах стрімко зростаючого ринку ІТ-індустрії України та впливу на нього великої кількості негативних факторів (як-от пандемія *COVID*-19, воєнні дії, що спричинили проблеми з електропостачанням, курсовими коливаннями тощо) проблеми управління та контролю ризиків стають чи не найактуальнішим, оскільки для зазначених підприємств наразі гостро постає питання не просто забезпечення зростання бізнесу та збереження існуючої клієнтської бази, як раніше, а й виживання та залучення нових клієнтів в умовах ринкової нестабільності. За відсутності чіткого визначення ризиків та їх класифікації неможливо повною мірою передбачити ймовірність збитків та завчасно розробити заходи, що зможуть або зменшити їх наслідки чи уникнути настання ризику, або попередять ризикові події. Наявність численних різнопланових видів ризиків, які мають місце в нестабільній економіці, ускладнює їх систематизацію, що унеможливлює побудову єдиної їх класифікації. Водночас, така класифікація важлива тим, що вона створює методологічне підґрунтя для мінімізації їх впливу. Без належно організованої системи управління ризиками на

ІТ-підприємстві можуть бути відсутні заходи безпеки та належна оцінка можливих ризиків. Ідентифікація ризиків сприятиме удосконаленню їх класифікації з урахуванням специфіки діяльності досліджуваного підприємства та методів, які будуть застосовуватися для їх аналізу.

Відсутність аналізу, контролю та управління ризиками в сфері ІТ призводить до зростання незахищеності підприємств в умовах нестабільного ринкового середовища, втрати ключових ринків та клієнтів, що, в свою чергу, може зумовити непередбачуваний рівень витрат та економічних втрат у випадку настання того чи іншого ризику. Для достеменного аналізу та подальшого контролю ризиків найважливішим фактором, що впливає на ці процеси, є їх класифікація, визначення та оцінка ймовірності настання, адже переоцінений ризик може завдати навіть більшого збитку, ніж недооцінений.

Теорію та методики аналізу ризиків досліджували такі закордонні науковці, як: Д. Лендолл *(D.J. Landoll,* 2021); К. Сріванас (*K. Srivanas,* 2019); Д. Хабберд (*D.W. Hubbard*, 2020) та ін., а також українські науковці (І. Іщенко, 2021) та ін. Окремим аспектам класифікації ризиків компаній сфери послуг та ІТ-сфери приділено увагу в дослідженнях І. Нечаєвої, Є. Дьордій (2018) та Ю. Дуднєвої (2018), систем управління різними видами ризиків – у працях М. Тимошик (2019), О. Данченко, В. Занора (2019), А. Д'яченко (2022). Ризики з точки зору менеджменту проєктів вивчала О. Герасименко (2021).

У найбільш актуальних дослідженнях з цієї тематики питання ризиків розглянуто здебільшого в контексті формування системи антикризового управління підприємствами. Відтак, подальшого дослідження потребує ідентифікація різних видів ризику, вдосконалення їх класифікації, методики аналізу та оцінки їх впливу на фінансові результати діяльності компаній сфери ІТ, формування системи контролю за наявними і потенційними ризиками, системи аналітичних показників, що характеризують ризики, які виникають в ІТ-середовищі, та інші аспекти.

Метою дослідження є систематизація ризиків ІТ-компаній та вдосконалення їх класифікації для підвищення ефективності управління ними та їх мінімізації.

Використано загальнонаукові та спеціальні методи дослідження явищ і процесів у їх взаємозв'язку і розвитку, а саме: під час дослідження тенденцій розвитку ринку ІТ-послуг України – ряди динаміки; для проведення аналізу кількості ІТ-спеціалістів в різних країнах – прийоми порівняння та коефіцієнтний аналіз; для побудови класи-фікації ризиків за різними класифікаційними ознаками – індукція, дедукція, аналіз, синтез, групування; для розроблення пропозицій з удосконалення класифікації джерел виникнення ризиків – узагальнення та абстрагування; для дослідження спільних та відмінних

рис існуючих класифікацій ризиків – методи аналогії, порівняння та систематизації. Рекомендаційний метод застосовано для формулювання пропозицій та висновків на основі проведеного дослідження.

1. Стан ринку ІТ-технологій України.

Дедалі більший інтерес дослідників привертає галузь інформаційних технологій України, яка, попри складні умови зовнішнього середовища, зумовлені пандемією *COVID*-19 та воєнними діями на території нашої держави, продовжує розвиватись, залучати іноземні інвестиції і створювати додаткові робочі місця.

За часткою експортного прибутку галузі інформаційних та комп'ютерних технологій у ВВП входять до трійки лідерів серед країн Східної Європи (*рис. 1*).

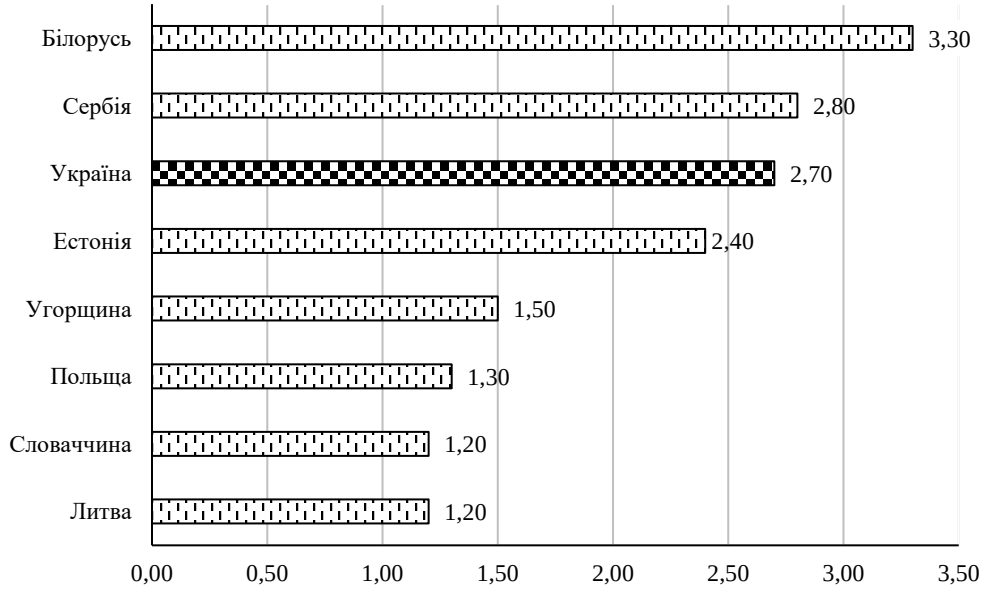

Рис. 1. Частка експорту комп'ютерних послуг у ВВП країн Східної Європи у 2021 р.

Джерело: IT Ukraine Association report for 2021 (2022).

Відповідно до даних Асоціації "IT *Ukraine*", станом на 1 червня 2022 р. ІТ-компанії та приватні особи-підприємці, які працюють в ІТ-галузі, перерахували до зведеного бюджету України податкових платежів та зборів на суму 29 млрд 558 млн грн, отже, ця сфера продовжує розвиватись і збільшує своє значення драйвера економіки України.

За останні чотири роки експорт ІТ-послуг збільшився вдвічі і, за даними асоціації ІТ, у 2021 р. він сягнув показника 6.83 млрд дол. США. Відповідно до показників 2022 р., темп зростання експорту ІТ-послуг зменшився в 6 разів порівняно з 2020–2021 рр., але, попри воєнні дії, експорт послуг збільшився на 6 %, що у кількісному

вираженні становило 470 млн дол. США (*рис. 2*).

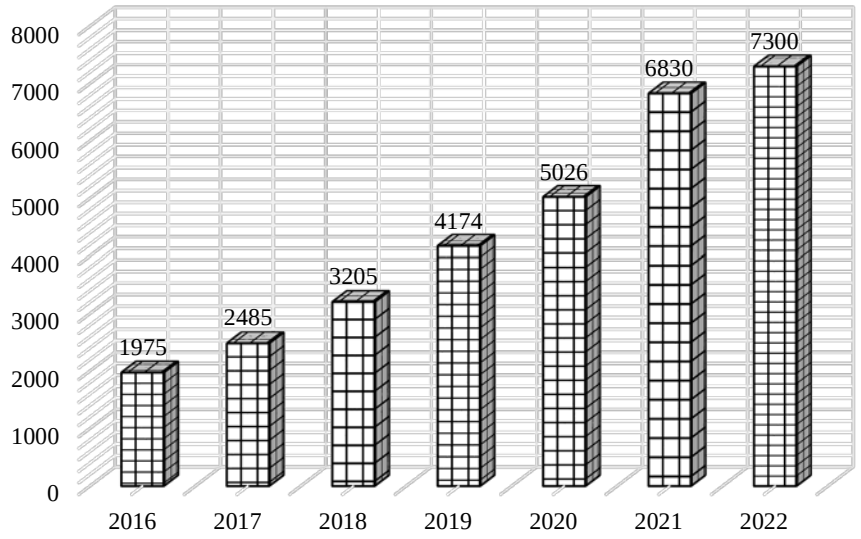

Рис. 2. Експорт послуг ІТ-галузі України, млн дол. США

Джерело: IT Ukraine Association report for 2021 (2022) та стаття *Forbes* "50 головних експортерів України 2022" (2023).

П’ятірку найбільших ІТ-компаній-експортерів України у рейтингу за 2022 р. представлено на *рис. 3*.

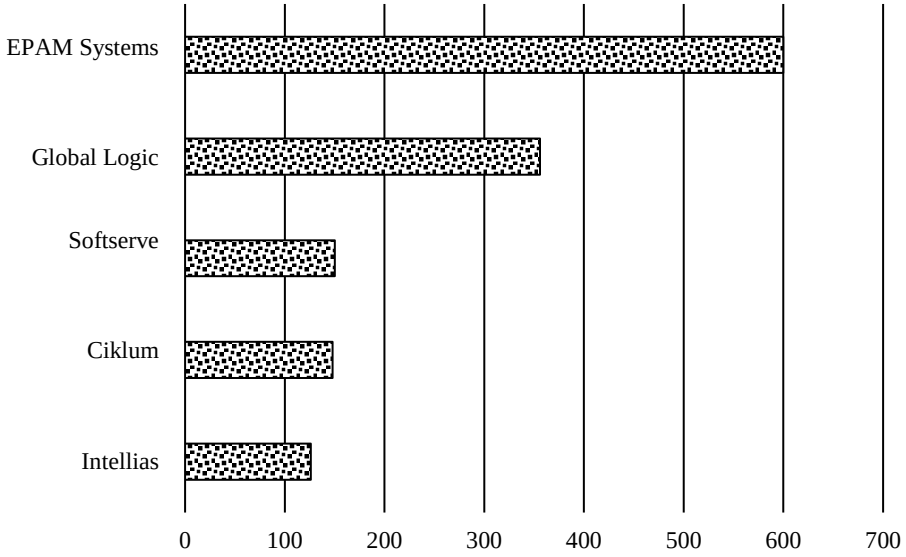

Рис. 3. ТОП-5 українських компаній сфери ІТ за рівнем експорту, млн дол. США

Джерело: 50 main exporters of Ukraine in 2022. (2023).

Україна також посідає друге місце на ринку Східної Європи за кількістю спеціалістів сфери інформаційно-комп’ютерних технологій (*рис. 4*).

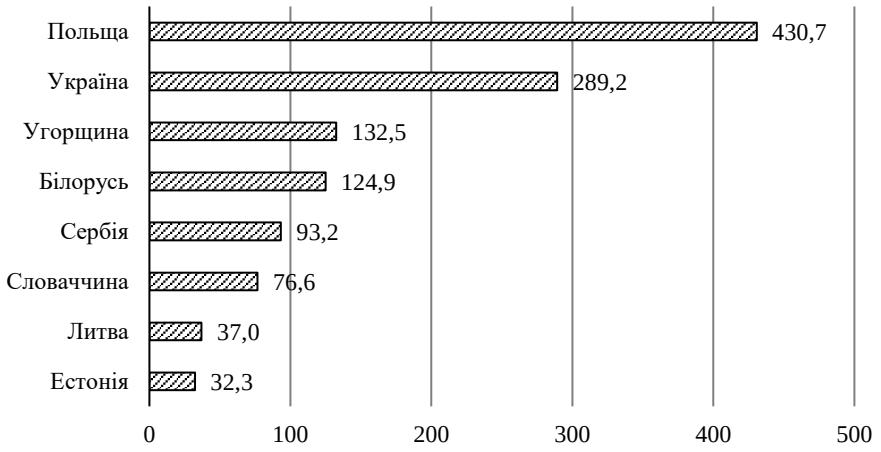

Рис. 4. Кількість ІТ-спеціалістів у країнах регіону, тис. осіб

Джерело: IT Ukraine Association report for 2021 (2022).

Україна демонструє щорічний приріст експорту інформаційних послуг на 27 % і, за даними 2020 р., основними імпортерами є США, Великобританія, Мальта, Ізраїль та Кіпр (2022). Фахівці з України розробляють програмне забезпечення для найскладніших медичних приладів, військової техніки, автомобілів майбутнього, освоєння космосу тощо. Завдяки українським ІТ-фахівцям, які працюють сьогодні на західних замовників, Україна через 10–15 років може перетворитися на найбільший технологічний центр Європи та світу.

Отже, ІТ-галузь дуже стрімко набула стадії зрілості, що сприяє посиленню конкурентної боротьби не лише за частку ринку, а й за потенційні інвестиції, стабільний розвиток, кваліфікований персонал тощо.

2. Загальні ризики компаній.

Компанії галузі ІТ діють у правовому та економічному полі України як і багато інших компаній, що належать до різних галузей, тому доцільно розглянути основні ризики, без урахування яких неможливе посилення конкурентної позиції компанії, особливо за мінливих ринкових умов.

2.1. Ризики компаній за сферою виникнення.

Проведене дослідження дало змогу виокремити чотири *основні групи ризиків* відповідно до сфери їх виникнення та визначити рівень їх впливу на діяльність та ключові показники компанії. До цих груп належать політичні, економічні, операційні та юридичні ризики.

Політичні ризики – це ризики, які можуть спонукати інвесторів відмовитись чи обмежити інвестиції внаслідок політичних змін або нестабільності в країні. Нестабільність, що впливає на прибуток від інвестицій, може бути наслідком зміни уряду, законодавчих органів, інших осіб, що розробляють зовнішню політику, або військового

контролю. Політичні ризики також відомі як "геополітичні ризики", і стають все більш значущим фактором, оскільки часовий горизонт повернення інвестицій стає більш тривалим.

Економічні ризики – комбінація подій, пов'язаних з діяльністю підприємства, які впливають на нього; імовірності цих подій та їх наслідків, що унеможливлюють досягнення запланованих цілей і внаслідок цього позначаються на доходах підприємства. За сферою виникнення економічні ризики зазвичай поділяють на внутрішні та зовнішні. Під зовнішніми слід розуміти виникнення таких умов, які підприємець, як правило, не може змінити, але повинен враховувати. Джерелами внутрішніх ризиків є саме підприємство. Першопричиною виникнення таких ризиків можуть бути прорахунки в системі управління ризиками, недосконалість маркетингових стратегій, некваліфіковані дії менеджерів, корпоративне шахрайство.

Також економічні ризики визначають як ймовірність, що відображає можливі коливання, які можуть мати місце в різних сценаріях функціонування компанії. Таким чином, економічні ризики вимірюють невизначеність, породжену різними можливими подіями, які можуть відбутися з часом, що може мати прямий вплив на компанію. Важливість вимірювання цих ризиків полягає в тому, що фінансові результати діяльності компаній залежать від них. Для цього багато компаній формують карти ризиків, які враховують силу їх впливу.

Операційні ризики – ризики можливих втрат та збитків, які виникають в операційній діяльності підприємства і зазвичай, є наслідками некваліфікованого управління, шахрайських дій з боку управлінців, неякісного надання послуг, невмінням керівництва швидко реагувати на загрози та негативні фактори, що впливають на діяльність компанії у найближчій та віддаленій перспективі. Ці ризики виникають внаслідок зловживань працівниками компанії своїми повноваженнями, шахрайських дій, або дій, які суперечать професійній етиці, що у підсумку може призводити до погіршення конкурентної позиції компанії на ринку, а іноді й до банкрутства (ризик зловживання). Інші аспекти операційного ризику, що притаманні IT-компаніям, стосуються критичних збоїв у роботі систем інформаційних технологій, пошкодження обладнання та інфраструктури.

Під *юридичним ризиком* розуміють існуючий або потенційний ризик зменшення доходів і капіталу компанії, спричинений порушенням або недотриманням компанією законів, нормативних актів, угод, загальноприйнятої практики чи етики, а також можливої неоднозначності тлумачення встановлених законів чи нормативних актів. Зазвичай, юридичні ризики виникають під час формування ділових відносин компанії з великою кількістю клієнтів, контрагентів, кредитних установ, фінансових посередників, а також державних інституцій та податкових органів. Негативними наслідками юридичних

ризиків можуть бути втрати підприємства від сплати адміністративних штрафів, пені, неустойок та погіршення репутаційного іміджу компанії.

Юридичний ризик також містить комплаєнс-ризик, який виникає через невиконання або порушення законів, інституційних стандартів, нормативних актів, що регулюють її діяльність. Тобто юридичний та репутаційний ризики є основними компонентами комплаєнс-ризику.

2.2. Ризики компаній за рівнем впливу та наслідками.

Для аналізу та контролю ризиків важливим фактором є можливість проведення оцінки їх рівня впливу та наслідків настання того чи іншого ризику.

За цими критеріями ризики поділяють на: катастрофічні, критичні, високі, середні, низькі (*табл. 1*).

Таблиця 1

Класифікація ризиків за потенційними наслідками

Рівень наслідків		Зміст	Вид ризику	Короткий опис або приклад
Катастрофічні		Втрати підприємства можуть спричинити його банкрутство	Юридичні	Ризики, що перевищують розмір майна підприємства. На прикладі Компанії Veon – виплата штрафу в розмірі 795 млн дол. США за порушення міжнародного антикорупційного законодавства за фінансові зв'язки з чиновниками Узбекистану задля розбудови мережі
Критичний		Наявні втрати можуть перевищувати прибуток підприємства за певний проміжок часу	Політичні	Ризики, пов'язані з веденням бізнесу в Україні (воєнний стан, зміна керівництва в законодавчих та виконавчих органах влади тощо)
			Операційні	Проблеми безпеки, що можуть бути зумовлені несанкціонованим доступом, втратою та розповсюдженням інформації тощо
Високий		Є висока ймовірність настання значних негативних наслідків. Наприклад, ризик потрапити на ненадійного контрагента має високу ймовірність і значні негативні наслідки	Фінансово – економічні	Ризики, пов'язані з коливанням курсу валют, високою інфляцією, дефіцитом, профіцитом, погашенням кредитів або зменшенням кредитних рейтингів фінансових установ
			Операційні	Ризики, пов'язані зі швидкою та значною зміною технологій, методологій, галузевих стандартів
Допустимий	Середній	Наявні втрати не будуть перевищувати розмір очікуваного прибутку	Економічні	Ймовірність обмеження вільної торгівлі та підвищення тарифів на товари та послуги, податкові реформи
			Юридичні	Порушення договорів конфіденційності та прав інтелектуальної власності
	Низький	Наявні втрати не впливають на прибуток підприємства, він може виникати лише в окремих підрозділах, або на який можна вплинути суто операційною діяльністю	Операційні	Дефекти програмних помилок, залежність від підрядних працівників та організацій, конкуренція і відсутність достатньої кількості кваліфікованих фахівців на ринку

Джерело: складено авторами.

Наведені у *табл. 1* ризики притаманні не лише ІТ-індустрії і не є специфічними.

Попри те, що виокремлення ризиків за їх наслідками характерне для усіх підприємств, без їх врахування неможливо побудувати класифікацію, яка забезпечить ефективне управління всією діяльністю ІТ-підприємства. Для ідентифікації ризиків за їх наслідками використовуються методи і технології прогнозного сценарного аналізу (розрахунок песимістичного, реалістичного та оптимістичного варіантів прогнозу або бізнес-кейсу). На діяльність ІТ-компаній впливають такі ж самі фактори, що й на підприємства інших видів діяльності, водночас, специфіка діяльності ІТ-бізнесу супроводжується ще й специфічними факторами впливу.

2.2. Ризики компаній з точки зору управління.

З погляду управління компанією та стратегічного планування, запропоновано виокремити *стратегічні* та *тактичні* ризики і додати їх до групи загальних ризиків.

Business dictionary визначає *стратегічні ризики* як можливе джерело збитків, що може виникнути внаслідок здійснення невдалого бізнес-плану. Більш узагальнено можна надати таке визначення: це ризики, що впливають на забезпечення довгострокового існування підприємства на ринку і формування та/або збереження своєї конкурентної переваги; це ризики, пов’язані із функціонуванням і розвитком ринку або галузі та поведінкою підприємства на ринку.

Стратегічні ризики є дуже важливою одиницею ризик-менеджменту, оскільки вони можуть дуже швидко завдати серйозної шкоди організації, можуть уражати ланцюги постачання, інфраструктуру, технології, персонал, капітал, репутацію та базові чинники створення цінності компанії. Стратегічні, як і будь-які інші ризики, несуть, з одного боку, загрозу, але з іншого – великі можливості, які допоможуть збільшити вартість існуючого бізнесу, знайти нові джерела доходу чи принаймні стабільно утримувати його на існуючому рівні.

А. Сливоцький (2010) визначає 7 груп стратегічних ризиків (*табл. 2*).

Тактичні ризики мають тісний зв’язок зі стратегічними і пов’язані з конкретними діями, спрямованими на досягнення стратегічної мети у конкретний проміжок часу на будь-якому з етапів реалізації затвердженої стратегії. Тактичні ризики здебільшого можуть виникати через визначені дії менеджменту компаній, обрання неправильних/недоцільних на цей момент методів досягнення мети, управління, бізнес-моделей тощо.

Таблиця 2

Групування стратегічних ризиків

Група ризиків	Сутність	Способи мінімізації впливу
Галузеві	Ризики, притаманні для окремої галузі та обумовлені специфікою її діяльності	Відмова постачальників від послуг посередників та вихід на кінцевого споживача; збільшення вартості капітальних витрат по галузі; стрімкі процеси щодо лібералізації цін; консолідація постачальників; збільшення вартості досліджень та розробки для високотехнологічних компаній
Технологічні	Ризики, пов'язані з використанням тої чи іншої технології. Здебільшого стосуються використання технологій та бізнес-моделей, що значно перевершують існуючі	Перехід на онлайн-торгівлю замість роздрібної; перехід на смартфони і додатки до них замість традиційних ПК та інтернет-додатків; використання цифрових телефонів замість аналогових; розвиток електроавтомобілів та гібридних технологій
Ризики бренду	Ризики, пов'язані з іменем компанії (брендом), її репутацією на ринку і ступенем довіри до неї споживачів та контрагентів	Збереження відповідності продукту стандартам бренду; відповідність позиціонування бренду розроблюваним продуктам (наприклад, IT-компанія позиціонує себе як одна з найкращих для молодіжної аудиторії, але, при цьому розроблює продукти, орієнтовані на людей старшого віку (ставки на біржі) – є прикладом невідповідності); відповідність розроблюваних нових продуктів сталому іміджу бренду (наприклад, якщо компанія *Revision* розробить нову систему для проведення досліджень, вірогідність того, що її сприймуть споживачі є великою, оскільки компанія має сталу репутацію в розробці програмного забезпечення для систем дослідження)
Ризики конкуренції	Ризики, пов'язані з появою і діями конкурентів, які можуть швидше виявляти і якісніше задовольняти потреби своїх споживачів та контрагентів, а також спроможні оптимізувати собівартість виробництва аналогічних товарів / надання послуг, що може становити серйозну загрозу для підприємств	Таргетування на нові групи споживачів; втрата маржинальності продукту за рахунок вимушеної цінової конкуренції; додаткові витрати на збільшення відповідності продукту до продуктів конкурентів; вихід на нові ринки; диверсифікація пропозиції новими інноваційними продуктами
Ризик стагнації	Ризики, пов'язані з процесом розвитку компаній, коли продаж, прибутки і вартість компанії загалом досягають певної межі і припиняють зростати	Використання інноваційних технологій; відмова від консервативних бізнес-моделей; постійний аналіз розвитку та тенденцій галузі і розробка способів відповідності до них

Закінчення таблиці 2

Група ризиків	Сутність	Способи мінімізації впливу
Проєктні	Ризики, пов'язані з реалізацією нових проектів	Створення нових продуктів, що відповідають споживацькому попиту; вихід на нові притаманні компанії ринки; спрощення виробничих процесів; спроби виходу на нові (закордонні) ринки (наприклад, вихід логістичної компанії "Нова Пошта" на ринок Польщі)
Ризики споживачів	Ризики, пов'язані з поведінкою споживачів, роботу над утриманням існуючих і залученням нових	Збір, аналіз і використання даних про споживачів; збільшення точок контактів з клієнтами; створення цільових пропозицій; розширення портфеля пропозицій; оптимізація структури і збалансованість продукції

Джерело: узагальнено авторами за А. Сливоцьким (2010).

3. Специфічні для ІТ-сфери ризики.

Дослідженню проблем управління ризиками діяльності різних суб'єктів господарювання з позиції використання облікових технологій присвячено праці вітчизняних учених, зокрема Л. Гнилицької (2014), І. Чібісової, Б. Левчунь (2016) та ін. Цілком імовірно, що методичні підходи до управліннями різними видами ризиків, запропоновані цими вченими, можуть бути використані і в практиці ризик-менеджменту *ІТ*-компаній, хоча специфіка їх діяльності породжує низку специфічних видів ризику, яку потребують нестандартних підходів до їх вивчення. Зокрема до таких специфічних ризиків належить виробничий ризик, який пов'язаний з невиконанням зобов'язань щодо надання послуг, розроблення програмного забезпечення у зв'язку з негативним впливом зовнішніх факторів та недостатньо ефективним використанням внутрішнього потенціалу компанії.

Специфічні або особливі ризики визначаються характером діяльності підприємства конкретної галузі. Серед особливих (специфічних) ризиків є типові, що впливають як на всі ІТ-підприємства загалом, так і на окремі з них – відповідно до сфери діяльності. Врахування особливостей впливу типових ризиків уможливлює використання досвіду інших ІТ-компаній, що забезпечує формування дієвих механізмів мінімізації негативного впливу факторів ризику. Інші конкретні загрози та фактори ризику можна визначити, вивчивши план конкретного ІТ-проєкту, на основі якого визначаються дії для усунення ризику або запобігання чи зменшення його наслідків. Узагальнення, зроблене авторами з різних джерел, виокремлюють *макроризики*, *загальні* ризики підприємства, *особливі* ризики. Останні відображають специфіку діяльності в цій сфері та враховують такі ризики:

за часом (пов'язані з невиконанням часових рамок, відведених на роботу з проєктом);

за витратами (призводять до значного збільшення витрат на реалізацію проєкту, пов'язаних з виникненням помилок під час його розроблення, використання невідповідних технологій та програмних засобів тощо та передбачають перевищення бюджету ІТ-проєкту);

за якістю (невідповідність отриманого результату першопочатковим узгодженим з клієнтом вимогам характеризує невідповідність якісних параметрів проєкту).

Відповідно до політики Гонконгського університету науки і технологій щодо використання ІТ-ресурсів (2021) можна провести узагальнення наведених ризиків, враховуючи такі види ризиків, притаманні для цього виду діяльності:

технологічні (пов'язані з використанням відповідних до вимог проєкту технологій, програмного забезпечення та обладнання);

пов'язані з ІТ-*інфраструктурою* (пов'язані з мережевою інфраструктурою, засобами резервування даних, забезпечення мір надмірності (*redundancy*), засобів протидії вірусам тощо);

втрати кадрового потенціалу (пов'язані із забезпеченням можливості обміну унікальними знаннями всередині колективу, запобіганням можливості накопичення унікальних знань у однієї особи (групи осіб), залишення компанії якими понесе незворотну втрату даних по проєкту тощо);

втрата або витік інформації (пов'язані із забезпеченням дотримання правил кібербезпеки співробітниками, збережен-ням та поводженням з даними, дотриманням умов *NDA* тощо);

соціальні (пов'язані з рівнем освіти, демографічною ситуацією тощо);

проєктні (пов'язані з достатньою кількістю досвіду, необхідного для виконання проєктів, можливістю внесення змін, грамотним проджект-менеджментом тощо);

юридичні (пов'язані із забезпеченням відповідності проєкту, продукту, послуги усім нормам законодавства України та країни-реципієнта);

ринкові (пов'язані із ситуацію на ринку країни, нестабільністю ринкової кон'юнктури, коливаннями валютного курсу, ситуацією на міжнародному ринку послуг ІТ).

Враховуючи детальну характеристику видів ризику, окремі групи можуть бути наведені для характеристики ризиків за факторами їх виникнення.

Також ризики технологічних компаній можна класифікувати відповідно до джерел їх виникнення. Цю типологію наводять польські науковці М. Кураш та А. Заяц (*M. Kuraś, A. Zając,* 1999) (*табл. 3*).

Таблиця 3

Класифікація джерел виникнення ризиків

Джерело	Короткий опис
Соціально-економічне середовище	Недосконалість системи освіти; нестабільна економічна та правова обстановка; зміни ситуації на ринку; недостатнє розуміння організації та ролі сфери *IT*; відсутність мережевих стандартів; низька інформаційна культура
Технологічне середовище	Недостатній рівень розвитку телекомунікаційних технологій; відсутність мережевих технологічних стандартів; недостатньо розвинений ринок комп'ютерного обладнання та програмного забезпечення; недостатній високий та сучасний рівень використовуваного програмного забезпечення
Організація	Відсутність у менеджменту компаній бачення та стратегії розвитку, невизначені цілі просування продуктів; консерватизм та нездатність до змін; складнощі в управлінні інформаційними технологіями; відсутність досвіду підприємництва в галузі; неналежний стиль управління підприємством; раптові зміни структури; недосконалість системи контролю всередині підприємства; труднощі з пошуком кваліфікованих кадрів та підвищення кваліфікації працюючих у компанії; відсутність очікувань щодо ефективності; відсутність координованої співпраці між менеджментом та користувачами із фахівцями підрозділів IT
Розробники IT-проєкту	Недостатній рівень знань щодо питань організації праці та управління командою; відсутність гнучкості та врахування змін у межах проєкту; недостатній глибокий рівень консультування клієнтів (користувачів); поверхневий підхід до реалізації проєкту; недостатнє знання методів, прийомів та інструментів; невміння працювати в команді
Проєкт	Обсяг і загальна складність проєкту; фрагментарне проєктування та програмування IT-проєкту; відсутність чіткого графіка та кошторису на проєктні роботи; обмежений обсяг аналізу; поверхневе врахування питань інформаційної безпеки; загроза конфліктів всередині команди та із замовниками проєкту

Джерело: узагальнено авторами за М. Кураш та А. Заяц (1999).

Запропонована типологія має стати основою для систематизації ризиків, притаманних сфері IT.

Також, крім загальних ризиків, важливою складовою для врахування є ризики, пов'язані з *конкретними* IT-проєктами. Враховуючи, що IT-проєкт є важливою складовою діяльності IT-підприємства (особливо для ауторсингових компаній, які здебільшого

винаймають спеціалістів під конкретний проєкт), вважаємо за доцільне розкрити це питання більш детально в подальших дослідженнях.

Враховуючи специфіку діяльності ІТ-компаній, пов'язану з використанням безлічі різноманітних сучасних технологій та мов програмування, для цієї галузі дуже важливим ресурсним потенціалом виступає людський капітал, тож, крім зазначених, серед специфічних ризиків запропоновано виокремити *ризик кадрового потенціалу,* що пов'язаний з плинністю кадрів, забезпеченням їх високого рівня кваліфікації та підготовки, регулярним підвищенням рівня знань тощо. Ризик кадрового потенціалу належить до одного з важко прогнозованих ризиків, оскільки винайнятий працівник не може забезпечити високої продуктивності і виконувати складні завдання та проєкти в короткий термін. Навіть для висококваліфікованого спеціаліста велика частина часу та ресурсів витрачається на ознайомлення з проєктом та його специфікою. Важливим ризиком з точки зору кадрового потенціалу є також вміння співробітників працювати в команді, оскільки неграмотний менеджмент персоналу може призвести до значних затримок у виконанні проєктів та неналежної їх якості. Не менш важливим фактором є створення резервів під компенсації та пільгові виплати, навчання персоналу, забезпечення його належними умовами для праці (у тому числі віддаленої, що нині є особливо актуальним), мотиваційні програми тощо. Невчасне врахування цих ризиків може призвести до фінансових втрат, зумовлених невчасним або неякісним виконанням зобов'язань по проєктах або ж їх зриву.

Оскільки сфера ІТ розвивається дуже динамічно і тісно пов'язана з використанням різноманітного обладнання і технологій, ризикам, що виникають безпосередньо через них, варто приділити особливу увагу. З огляду на це, запропоновано вдосконалити класифікацію специфічних ризиків ІТ-сфери завдяки більш детальному розподіленню технологічних ризиків, а саме виокремленню таких: *ризики деактуалізації коду програмного забезпечення*, *інтеграційні ризики* та *ризики кіберзлочинності*.

Ризики деактуалізації коду програмного забезпечення пов'язані із забезпеченням актуальності використаної мови програмування, її версії (підтримки як нових, так і більш старих версій), доступності на будь-яких платформах. Настання цього ризику може призвести до значних витрат підприємства на вдосконалення існуючого коду програмного забезпечення або ж необхідності створення програмного забезпечення з самого початку з метою його відповідності умовам поточного часу і технологій.

Інтеграційні ризики мають велику значущість у діяльності ІТ-підприємств, оскільки вони пов'язані з розміщенням та впровадженням розробленого програмного забезпечення на різних технологічних платформах, платформах замовників програмного забезпечення

та забезпеченням крос-платформного взаємозв'язку, що суттєво впливає на майбутнє потенційне розширення сфери діяльності виокремленого ІТ-підприємства, здобуття нових джерел доходів або навіть спрощення взаємодії між системами всередині компанії.

Ризики кіберзлочинності – ризики, які полягають в отриманні прямих чи побічних збитків економічними суб'єктами внаслідок їх функціонування у кіберпросторі. Ця категорія ризиків пов'язана з несанкціонованим доступом до програмного забезпечення, його вихідного коду та баз даних користувачів з метою неправомірного використання інформації користувачів або заподіяння збитку компанії шляхом виведення з ладу програмного продукту. На відміну від компаній інших галузей економічної діяльності, компанії сфери ІТ є найбільш вразливими від настання ризиків кіберзлочинності, оскільки вони вражають не окрему сферу або систему компанії, а її основний продукт, що може призвести до повної зупинки діяльності підприємства, ураження та зупинення систем партнерів, контрагентів, постачальників та інших суб'єктів взаємодії.

Серед ризиків кіберзлочинності варто враховувати такі загрози для діяльності ІТ:

- шкідливе програмне забезпечення, що зашкоджує діяльності продукту та може спричинити втрату продуктивності системи, витрати на відновлення та навіть заміну обладнання;
- фішинг або компрометація ділової електронної пошти, що використовуються для отримання доступу до різноманітних систем. При переході за посиланням, що вказане у фішинговому листі, злочинець отримує доступ до конфіденційних даних компанії;
- атаки на кінцеві точки, що використовуються для отримання доступу до великих мереж, створення надзвичайного навантаження на них, у тому числі з метою виведення з ладу обладнання;
- атаки третіх осіб, коли кіберзлочинці використовують вразливість системи безпеки зовнішнього постачальника з метою отримання доступу до мережі більшої організації;
- атаки з використанням машинного навчання і штучного інтелекту, що використовуються для отримання доступу до критично важливих мереж та конфіденційних баз даних;
- гостра нестача фахівців та недостатнє приділення уваги питанням кібербезпеки. За деякими оцінками, у світі налічується понад 1 млн незаповнених вакансій фахівців протидії кіберзагрозам.

4. Консолідована класифікація ризиків ІТ-компаній.

Наведені в статті дані стали основою для створення *консолідованої класифікації ризиків для компаній галузі інформаційних технологій*, які враховують такі групи ризиків: *загальні* (притаманні для

будь-яких компаній незалежно від сфери їх діяльності) та *специфічні* для досліджуваної сфери (*рис. 5*).

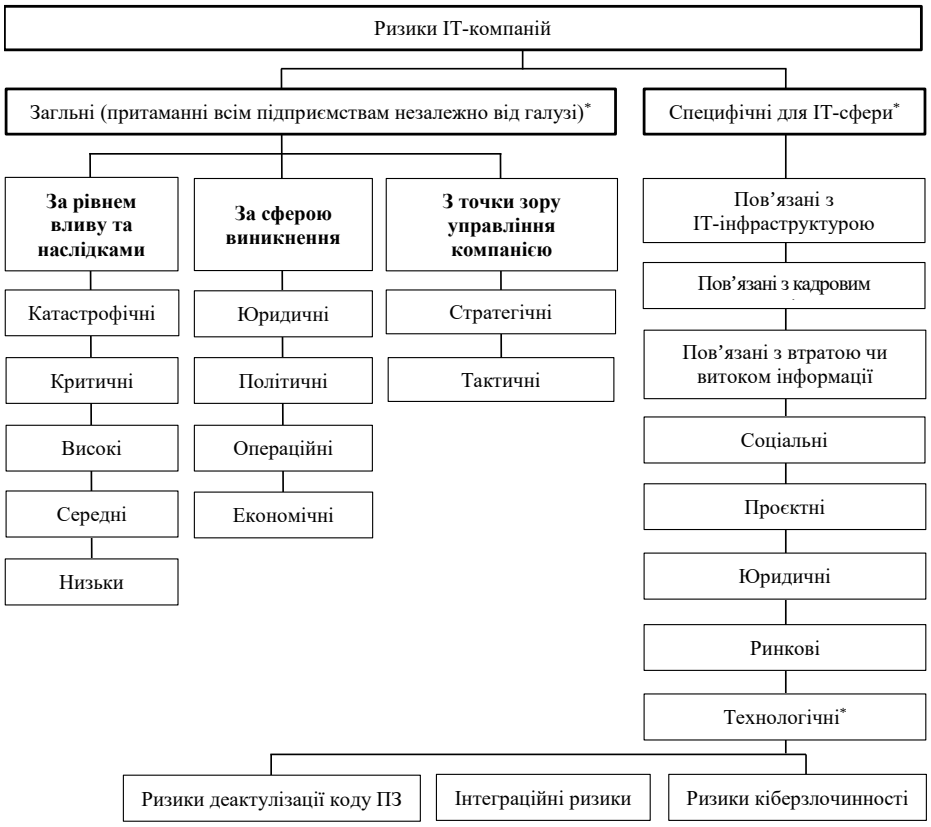

Рис. 5. Класифікація ризиків ІТ-компаній

* *Класифікаційна ознака, запропонована авторами дослідження.*
Джерело: складено авторами.

Запропоновану авторами класифікацію ризиків в подальшому можна використовувати як опорну систему для подальшого вдосконалення аналізу та контролю ризиків організацій сфери ІТ.

Висновки.

Типологізація та ідентифікація ризиків є невід'ємним етапом для подальшого забезпечення їх аналізу та побудови процедур і систем управління ними. Попри те, що повністю уникнути та запобігти виникненню ризиків неможливо, персонал та менеджмент ІТ-підприємства має розробляти та впроваджувати заходи, призначені для зменшення ймовірності їх виникнення або мінімізації наслідків у разі настання того чи іншого ризику. Враховуючи напрацювання науковців і дослідження аспектів діяльності підприємств сфери інформаційних технологій, *запропоновано класифікувати* ризики ІТ-компаній на *загальні*, що притаманні всім підприємствам, незалежно від сфери їх діяльності, та *специфічні – для ІТ-сфери*. До групи загальних ризиків віднесено ризики, класифіковані відповідно до рівня впливу, сфери виникнення і

безпосередньої значущості в управлінській діяльності; до групи *специфічних ризиків* ІТ-підприємств – технологічні (пов'язані з обраними засобами та технологіями, що використовують), ризики ІТ-інфраструктури (пов'язані зі збереженням даних, забезпеченням зв'язку, системами резервування тощо), ризики кадрового потенціалу (пошуком нових співробітників, навчанням та підвищенням рівня їх кваліфікації тощо), ризики втрати чи витоку інформації (пов'язані з питаннями конфіденційності даних, прав інтелектуальної власності), соціальні (пов'язані з рівнем освіти, обізнаністю громадян про сферу тощо), ризики проєкту (пов'язані з часом виконання, витратами та якістю), юридичні (пов'язані з дотриманням відповідності продуктів та наданих послуг законодавству України та країни-реципієнта) та ринкові (пов'язані із загальною ситуацією на ринку).

Перспективами подальших досліджень є використання запропонованої класифікації для систематизації прогнозування, досконалого аналізу та розроблення механізму ефективного управління ризиками у сфері діяльності ІТ-підприємств.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	**REFERENCES**
Герасименко, О. (2021). *Ризик-орієнтоване управління в системі економічної безпеки підприємства.* [Дис. д-ра екон. наук. Черкаський національний університет імені Богдана Хмельницького].	Herasymenko, O. (2021). Risk-oriented management in the system of economic security of the enterprise. [Doctor's thesis. Bohdan Khmelnytsky National University of Cherkasy].
Гнилицька, Л. (2014) *Інформаційне забезпечення ризиками підприємницької діяльності: обліковий аспект. Економічні інновації.*	Hnylytska, L. (2014). Informational support of entrepreneurship risks: accounting aspect. *Economical innovations.*
Д'яченко, А. (2022). *Аналіз операційних ризиківта їх взаємодії з іншими ризиками.* [Дис. на здобуття ступеня магістра. Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"].	D'iachenko, A. (2022). Analysis of operational risks and their interactions with other risks. [Doctor's thesis. National Technical University "gor Sikorsky Kyiv Polytechnic Institute"].
Данченко О., & Занора В. (2019). *Проектний менеджмент управління ризиками та змінами в процесах прийняття управлінських рішень:* монографія. ФОП Чабаненко І. А.	Danchenko, O., & Zanora, V. (2019). Project management: managing risks and changes in management decision-making processes. Chabanenko I. A.
Дуднєва, Ю. (2018). Ризики організацій сфери послуг: підходи до класифікації. *Адаптивне управління: теорія і практика, 5(10).*	Dudnieva, I. (2018). Risks of service sector organizations: approaches to classification. *Adaptive management: theory and practices.* Series of economics, *5(10).*
Іщенко, І. (2021). *Управління ризиками інвестицій-них проектів торговельних підприємств.* [Дис. д-ра екон. наук. Полтавський університет економіки і торгівлі].	Ishchenko, I. (2021). Risk management of investment projects of trade enterprises. [Doctor`s thesis. Poltava University of Economics and Trade, Poltava.].
Нечаєва, І., & Дьордій, Є. (2018). Управління ризиками підприємства в секторі ІТ-послуг як інстру-мент підвищення цього конкурентно-спроможнос-ті. *Ефективна економіка,* 12.	Nechayeva, I., & Dordiy, E. (2018). Risk management of the enterprise in the it service sector as an instrument for improving it competitiveness. *Efficient economy, 12.*

Сливоцький, А. (2010). *Прорив*. Український католичний університет.	Slyvots'kyj, A. (2010). *Proryv* [Breakthrough]. Ukrainian Catholic University.
Тимошик, М. (2019). *Формування системи управління ризиками промислових підприємств.* Тернопільский національним технічний університет імені Івана Пулюя.	Tymoshyk, M. (2019). Formation of the risk management system of industrial enterprises [Thesis abstract]. Ternopil Ivan Puluj National Technical University.
Чібісова, І., & Левчунь, Б. (2016). Бухгалтерський облік як інструмент управління ризиками на підприємст-ва. *Проблеми системного підходу в економіці, (2),* 113-116.	Chibisova, I., & Levchun', B. (2016). Accounting as tool for risk control in companies. *Problems of the systemic approach in economics*, *2*, 113-116.
50 main exporters of Ukraine in 2022. Forbes Ukraine (2023, March 7). https://forbes.ua/ratings/50-naybilshikh-eksporteriv-ukraini-2022-02032023-12098?fbclid=IwAR28JIUE5r5ylFrKDMh0UeZpu3D030X-xv1tlIsqMVwQ2RIdLttrHa1jt_E	*50 main exporters of Ukraine in 2022*. Forbes Ukraine (2023, March 7). https://forbes.ua/ratings/50-naybilshikh-eksporteriv-ukraini-2022-02032023-12098?fbclid=IwAR28JIUE5r5ylFrKDMh0UeZpu3D030X-xv1tlIsqMVwQ2RIdLttrHa1jt_E
Hubbard, D. (2020). The *Failure of Risk Management* (2nd ed.). Wiley.	Hubbard, D. (2020). The *Failure of Risk Management* (2nd ed.). Wiley.
IT Ukraine Association report for 2021. https://drive.google.com/file/d/1LujaT9pHEGhgpRRojfnlZgQikkyiIlbE/view	*IT Ukraine Association report for 2021*. https://drive.google.com/file/d/1LujaT9pHEGhgpRRojfnlZgQikkyiIlbE/view
Kuraś M., & Zając A. (1999). Czynniki powodzenia i ryzyka projektów informatycznych. *Zeszyty Naukowe, Akademia Ekonomiczna w Krakowie*, *522*, 159-182.	Kuraś, M., & Zając, A. (1999). Success and risk factors of IT projects. *Zeszyty Naukowe*. [Science notebooks]. Krakow University of Economics, *522*, 159-182 [in Polish].
Landoll, D. J. (2021) *The Security Risk Assessment Handbook* (3-nd ed.). Boca Raton, FL: CRC Press.	Landoll, D. J. (2021). *The Security Risk Assessment Handbook* (3-nd ed.). Boca Raton, FL: CRC Press.
Risk Classification Examples of Common IT Resources. Retrieved from https://itsc.hkust.edu.hk/it-policies-guidelines/ risk-classification	*Risk Classification Examples of Common IT Resources*. Retrieved from https://itsc.hkust.edu.hk/it-policies-guidelines/risk-classification
Srinivas, K. (2019). *Process of Risk Management*. IntechOpen.	Srinivas, K. (2019). *Process of Risk Management*. IntechOpen.

Конфлікт інтересів. Автори заявляють, що вони не мають фінансових чи нефінансових конфліктів інтересів щодо цієї публікації; не мають відносин із державними органами, комерційними або некомерційними організаціями, які могли б бути зацікавлені у поданні цієї точки зору. З огляду на те, що автори працюють в установі, яка є видавцем журналу, що може зумовити потенційний конфлікт або підозру в упередженості, остаточне рішення про публікацію цієї статті (включно з вибором рецензентів та редакторів) приймалося тими членами редколегії, які не пов'язані з цією установою.

Назарова К., Парасій-Вергуненко І., Остапець А**.** Класифікація ризиків компаній ІТ-індустрії. *Scientia fructuosa*. 2023. № 4. С. 120-137. https://doi.org/10.31617/1.2023(150)08

Надійшла до редакції 08.03.2023.
Прийнято до друку 15.05.2023.
Публікація онлайн 05.09.2023.