УДК 336.7:005.33:004

Усачов Артем Ігорович
здобувач третього (освітньо-наукового) рівня вищої освіти
Державного науково-дослідного інституту інформатизації та моделювання економіки
Usachov Artem
PhD Student of the
State Research Institute of Informatization and Economic Modeling
ORCID: 0009-0008-9281-5640

DOI: 10.25313/2520-2294-2025-10-11503

ІНТЕГРАЛЬНА МОДЕЛЬ ОЦІНКИ ФІНАНСОВИХ РИЗИКІВ УКРАЇНСЬКИХ ІТ-КОМПАНІЙ: ВОЄННИЙ КОНТЕКСТ

INTEGRAL MODEL FOR FINANCIAL RISK ASSESSMENT OF UKRAINIAN IT FIRMS

Анотація. *У статті запропоновано інтегральну модель оцінювання фінансових ризиків українських ІТ-компаній у воєнному контексті, що поєднує експертний підхід із системою коригувальних коефіцієнтів (ІТ-специфіка, воєнний вплив, галузева значущість). Обґрунтовано виокремлення воєнно-специфічних ризиків поряд із класичними фінансовими та технологічними, що відповідає нинішнім умовам високої невизначеності. Теоретичною базою слугують положення ризик-менеджменту (Л. І. Донець) і стандарт ДСТУ IEC/ISO 31010:2013; інформаційну основу становлять аналітичні звіти DataDriven Research & Consulting (у співпраці з EBA, IT Ukraine Association, Aspen Institute Kyiv) та публікації щодо трансформації ринку ІТ у період війни. Модель передбачає двокомпонентну базову оцінку (ймовірність × вплив) з подальшим множенням на три безрозмірні коефіцієнти, що адаптують результат до галузевих і воєнних умов, та пропонує інтерпретаційну шкалу рівнів ризику для управлінських рішень. Порівняння з класичними підходами (VaR, Monte-Carlo) показує потенційну придатність запропонованої методики в умовах браку достовірних даних і швидкої зміни зовнішніх чинників. На умовних прикладах (кіберризик, кадровий, енергетичний) продемонстровано теоретичну узгодженість результатів та практичну логіку застосування для оперативної пріоритизації заходів мітигації, що є релевантним для стартапів і малих ІТ-компаній з обмеженими ресурсами. Перспективи досліджень охоплюють збір ширших емпіричних даних безпосередньо від ІТ-компаній, валідацію моделі в реальному середовищі та подальше вдосконалення параметрів з урахуванням сегментів ринку й післявоєнної динаміки.*

Вступ. Повномасштабна війна суттєво вплинула на фінансове середовище українських підприємств, зокрема ІТ-компаній, діяльність яких має високу залежність від зовнішніх ринків. Традиційні методи оцінки ризиків залишаються важливими, проте їх практичне застосування ускладнене браком достовірних даних і швидкою зміною зовнішніх чинників. Це зумовлює потребу у створенні спрощених, але методологічно обґрунтованих підходів, які дозволяють оперативно оцінювати ризики навіть за умов обмеженої інформації. Особливе значення така модель має для стартапів і малих ІТ-компаній, що не володіють великими статистичними масивами, але потребують швидких рішень у нестабільному середовищі.

Мета. Метою статті є розроблення інтегральної моделі оцінки фінансових ризиків українських ІТ-компаній, адаптованої до умов воєнної економіки та обмеженої статистичної інформації.

Матеріали і методи. Інформаційною базою дослідження стали наукові праці з економічних ризиків (зокрема, роботи Л. І. Донець), міжнародний стандарт ДСТУ IEC/ISO 31010:2013, аналітичні звіти DataDriven Research & Consulting, дослідження IT Ukraine Association, публікації вітчизняних авторів щодо управління фінансовими ризиками в умовах війни. У роботі застосовано методи логічного узагальнення, порівняльного аналізу, експертних оцінок і моделювання. Побудова інтегральної моделі ґрунтується на використанні системи коефіцієнтів, що враховують ІТ-специфіку, рівень воєнного впливу та галузеву критичність ризику.

Результати. Розроблено узагальнену формулу інтегральної оцінки фінансових ризиків, яка дозволяє кількісно визначати рівень ризику за умов невизначеності та обмеженої статистичної інформації. Обґрунтовано систему трьох коригувальних коефіцієнтів (воєнного стану, ІТ-специфіки та галузевої значущості), що забезпечують адаптивність моделі до зовнішніх умов. Порівняння з класичними підходами засвідчило потенційну ефективність і простоту використання моделі у ситуаціях

високої турбулентності. Результати апробації на умовних прикладах (кіберризик, кадровий, енергетичний) свідчать про її теоретичну узгодженість та методологічну доцільність для подальших досліджень.

Перспективи. Перспективи подальших досліджень полягають у зборі ширших емпіричних даних безпосередньо від українських IT-компаній, поглибленій перевірці моделі в реальних умовах та її вдосконаленні з урахуванням результатів практичного тестування. Це дозволить підвищити точність оцінювання ризиків і забезпечити інтеграцію моделі з кількісними методами аналізу у післявоєнний період.

Ключові слова: *фінансові ризики, IT-компанії, воєнний стан, інтегральна модель, коефіцієнти ризику, ризик-менеджмент, оцінка ризиків.*

Summary. *The paper proposes an integral model for assessing the financial risks of Ukrainian IT companies under wartime conditions, combining an expert-based approach with a system of weighting coefficients (IT specificity, wartime impact, and industry significance). War-specific risks are distinguished alongside classical financial and technological risks, reflecting today's high uncertainty. The theoretical foundations refer to risk-management concepts (L. I. Donets) and DSTU IEC/ISO 31010:2013; the information base includes analytical market reviews by DataDriven Research & Consulting (in cooperation with EBA, IT Ukraine Association, Aspen Institute Kyiv) and studies on the wartime transformation of Ukraine's IT sector. The model starts with a two-factor basic score (probability × impact) and multiplies it by three dimensionless coefficients to adapt results to industry and wartime conditions; it also provides an interpretation scale to support managerial decisions. A comparison with classical approaches (VaR, Monte-Carlo) indicates potential applicability when reliable statistics are scarce and external factors change rapidly. On conditional examples (cyber, personnel, energy risks), we demonstrate theoretical consistency and a practical logic for rapid mitigation prioritization, which is especially relevant for startups and small IT firms with limited resources. Future work includes collecting broader firm-level data, validating the model in real settings, and refining parameters by market segments and post-war dynamics.*

Introduction. The full-scale war has significantly affected the financial environment of Ukrainian enterprises, particularly IT companies highly dependent on external markets. Traditional risk assessment methods remain important, yet their practical application is limited by the lack of reliable data and the rapid change of external factors. This necessitates simplified but methodologically sound approaches that enable quick risk assessment under information constraints. The proposed model is particularly relevant for startups and small IT firms that lack extensive statistical resources but require prompt decision-making in unstable conditions.

Purpose. The purpose of the article is to develop an integral model for assessing the financial risks of Ukrainian IT companies, adapted to the conditions of wartime economy and limited statistical data.

Materials and methods. The research is based on scientific works on economic risks (notably by L. I. Donets), the international standard DSTU IEC/ISO 31010:2013, analytical reports by DataDriven Research & Consulting, studies by the IT Ukraine Association, and Ukrainian publications on financial risk management under wartime conditions. The study applies methods of logical generalization, comparative analysis, expert evaluation, and modeling. The proposed integral model is built using a system of coefficients that account for IT specificity, wartime impact, and the criticality of each risk for the industry.

Results. A generalized formula for the integral assessment of financial risks has been developed, allowing quantitative estimation under uncertainty and limited statistical data. A system of three correction coefficients – wartime, IT-specific, and industry-significance – has been substantiated, ensuring the model's adaptability to external conditions. Comparison with classical approaches demonstrated its potential efficiency and simplicity in high-turbulence environments. Testing on conditional examples (cyber, personnel, and energy risks) confirms its theoretical consistency and methodological validity for further research.

Discussion. Future research should focus on collecting broader empirical data directly from Ukrainian IT companies, conducting an in-depth validation of the model in real conditions, and refining it based on practical testing results. This will improve the accuracy of risk assessment and enable the integration of the model with quantitative analysis methods in the post-war period.

Key words: *financial risks, IT companies, martial law, integral model, risk coefficients, risk management, risk assessment.*

Постановка проблеми. Повномасштабна війна в Україні створила нову конфігурацію фінансових ризиків для суб'єктів господарювання, особливо в IT-галузі, де економічна діяльність тісно пов'язана з міжнародними ринками, валютними коливаннями та безперервністю технологічних процесів. У таких умовах традиційні підходи до оцінки фінансових ризиків стикаються з обмеженнями, пов'язаними з дефіцитом достовірної статистичної інформації, високою динамікою зовнішнього середовища та впливом воєнних чинників. Це потребує адаптації методів ризик-менеджменту до умов невизначеності, що є особливо актуальним для малих IT-компаній і стартапів, які мають обмежені ресурси для аналітичної обробки даних. Таким чином, постає науково-практична проблема створення гнучкої моделі, здатної інтегрувати класичні підходи до оцінки фінансових ризиків із галузевою та воєнною специфікою українського IT-сектору.

Аналіз останніх досліджень і публікацій. Дослідження фінансових ризиків як складової системи економічної безпеки підприємств представлено у працях багатьох українських науковців. Зокрема, О. Кириленко [1] пропонує оптимізаційний підхід до уточнення сутності категорії «фінансові

ризики», обґрунтовуючи їх поділ за рівнем впливу на фінансову стійкість суб'єкта господарювання. С. Юдіна та С. Мондрієвський [2] розвивають системний підхід до оцінки ризиків у стратегічному управлінні, наголошуючи на важливості інтеграції ризик-менеджменту в загальну модель управління підприємством.

Засадничі теоретичні положення кількісного вимірювання економічних ризиків викладено у фундаментальній праці Л. І. Донець [3], яка заклала основи сучасних підходів до оцінювання невизначеності та використання безрозмірних коефіцієнтів при розрахунках ризику. Питання впливу війни на фінансову діяльність вітчизняних підприємств досліджують І. Макалюк та А. Лайкова [4], акцентуючи увагу на зміні структури ризиків і трансформації методів управління у кризових умовах.

Проблематику фінансової стабільності підприємств у період воєнного стану розглядають Л. Шевчук, Я. Шевчук і Я. Пась [5], які аналізують механізми управління ризиками та санаційні заходи, що дають змогу мінімізувати втрати в умовах підвищеної невизначеності. Значний внесок у формування методологічних основ обліку та аналізу ризиків IT-підприємств зробили О. Лаговська, І. Грабчук та Г. Лоскоріх [6], які запропонували облікову класифікацію ризиків, релевантну для цифрової економіки.

Інший аспект дослідження представлений у роботі О. Герасименко, Л. Гнилицької та А. Д'яченко [7], які розробили структуру класифікації ризиків IT-компаній із урахуванням галузевих технологічних особливостей та міжнародної практики управління ризиками. Емпіричні дані щодо динаміки розвитку українського IT-ринку в 2014–2024 роках наведено у звіті AIN [8], який висвітлює трансформацію структури експорту, розвиток стартапів і кадрові тенденції в галузі.

Нормативну базу ризик-менеджменту формує DSTU IEC/ISO 31010:2013 [9], що систематизує методи ідентифікації та оцінювання ризиків і визначає загальні принципи управління ними в економічних системах. Вагомим джерелом емпіричних даних є аналітичний звіт DataDriven Research & Consulting [10], підготовлений спільно з EBA, IT Ukraine Association та Аспен Інститутом Київ, який відображає стан ринку кібербезпеки України, рівень корпоративної стійкості та структуру фінансових ризиків IT-компаній.

Крім того, О. Тимків [11] аналізує сучасний стан і тенденції розвитку ринку інформаційних технологій України, визначаючи чинники його зростання та ризики дестабілізації. Своєю чергою, О. Лісік і Т. Моряк [12] досліджують особливості функціонування IT-сектору в умовах війни, вказуючи на зміни у фінансових потоках і структурі ризиків, що впливають на інвестиційну привабливість галузі. Актуальні питання інформаційної безпеки IT-компаній розкрито в аналітичному матеріалі DOU [13], який висвітлює причини й наслідки масштабних кібератак на державні та корпоративні системи даних.

Таким чином, результати попередніх досліджень охоплюють широкий спектр аспектів — від теоретичних засад управління ризиками до практичних проблем функціонування IT-бізнесу у воєнних умовах.

Метою статті є розроблення інтегральної моделі оцінки фінансових ризиків українських IT-компаній у воєнному контексті, яка поєднує експертний підхід із системою коригувальних коефіцієнтів, що враховують IT-специфіку, рівень воєнного впливу та галузеву критичність ризику, забезпечуючи можливість кількісної оцінки за умов обмеженої статистичної бази.

Матеріали і методи. Теоретичну основу дослідження становлять праці Л. І. Донець, у яких обґрунтовано принципи кількісного вимірювання економічних ризиків та використання безрозмірних коефіцієнтів для оцінки невизначеності. Методологічною базою є міжнародний стандарт DSTU IEC/ISO 31010:2013, що визначає загальні підходи до ідентифікації та оцінювання ризиків. Емпіричні дані сформовано на основі аналітичних звітів DataDriven Research & Consulting, EBA, IT Ukraine Association і публікацій, присвячених трансформації IT-ринку в умовах війни. У процесі дослідження застосовано методи логічного узагальнення, порівняльного аналізу, експертних оцінок і моделювання. Запропонована інтегральна модель передбачає використання системи коригувальних коефіцієнтів (воєнного стану, IT-специфіки та галузевої значущості), що дозволяє адаптувати класичні інструменти фінансового ризик-менеджменту до специфіки IT-компаній і підвищити точність оцінки в умовах воєнної невизначеності.

Виклад основного матеріалу. У сучасній економічній науці фінансовий ризик пояснюється як ймовірність фінансових втрат підприємства внаслідок негативних обставин в умовах нестабільного середовища [1,2,3]. Для IT-галузі це поняття набуває особливої актуальності через специфіку технологічного бізнесу та воєнний контекст функціонування українських компаній.

Ефективне управління фінансовими ризиками потребує їх класифікації, що передбачає поділ ризиків на кілька основних категорій.

Спочатку планувалося використовувати лише класичні фінансові ризики, однак аналіз специфіки воєнного часу змусив розширити класифікацію та додати категорію воєнно-специфічних ризиків, які виявилися критично важливими для українських IT-компаній в умовах повномасштабної війни.

Дослідження українського ринку демонструють кардинальну трансформацію ризик-ландшафту внаслідок повномасштабної війни. Дані наведені в Огляді ринку кібербезпеки в Україні показують, що український ринок кібербезпеки зріс у 4 рази за останні 8 років і становить 138 млн. доларів США у 2024 році [10, с. 9]. Водночас сегмент мережевої

Таблиця 1

Класифікація фінансових ризиків українських ІТ-компаній

Категорія	Типи	Специфіка для ІТ-галузі
Класичні фінансові	Валютний, кредитний, ліквідності, інвестиційний, процентної ставки, податковий, інфляційний, політичний, неплатоспроможності, втрати контролю над активами	Висока залежність від долару США
ІТ-специфічні	Технологічний, інфраструктурний, кадровий, планувальний, кіберризик, витоку даних, інтеграційний, деактуалізації, масштабування	Швидкі зміни технологій
Воєнно-специфічні	Військовий, мобілізаційний, енергетичний, евакуаційний (переміщення), регуляторний	Унікальні для України від 2022 року

Джерело: складено автором на основі [3, с. 21–27; 4, с. 83–84; 5, с. 161; 6, с. 25–32; 7, с. 122–136]

безпеки переважає на ринку з часткою 36%, але хмарна безпека, безпека додатків та кінцевих точок демонструють найвищі темпи зростання (226%, 85,8% та 63,5% відповідно до 2029 року) [10, с. 11]. Кібербезпека має особливе значення через зростання кіберзагроз на 300% під час війни та необхідності захисту критичної інфраструктури [10, с. 8].

В свою чергу експорт ІТ-послуг досяг піку у 2022 році — 7,3 млрд. доларів США, проте у 2023 році вперше за багато років було зафіксовано зниження на 5,85% [11, с. 45]. Кількість спеціалістів у 50 найбільших ІТ-компаніях скоротилася з 99,5 тис. у січні 2022 року до 81,75 тис. у січні 2024 року [11, с. 47], а близько 50–57 тисяч ІТ-експертів (17–20% від загальної чисельності) виїхали за кордон після початку повномасштабного вторгнення, при цьому 70,8% ІТ-підприємств змушені були здійснити непередбачену релокацію [12]. Варто зауважити, що наведений діапазон (50–57 тисяч ІТ-експертів) відображає реальну невизначеність статистики воєнного часу, коли різні джерела подають дещо відмінні цифри через складність точного обліку під час конфлікту.

Географічна трансформація ІТ-галузі, що відображається у зміні розподілу спеціалістів (частка західних регіонів зросла з 16,5% до 24%, тоді як східних скоротилася з 27,8% до 10%, а південних — з 8,2% до 5% [12]), поєднується з валютними коливаннями (курс долара США зріс з 28–30 грн на початку 2022 року до понад 40 грн наприкінці року), технологічними ризиками від зростання популярності штучного інтелекту (кількість ШІ/ML спеціалістів зросла у 9 разів з 2013 по 2023 рік) [10, с. 12] та енергетичними викликами через регулярні відключення електроенергії.

Особливо значущим є те, що частка ІТ-послуг у структурі українського експорту зросла з 8,52% у 2021 році до 12,89% у 2022 році [12], що говорить про важливість ІТ-бізнесу в економіці України.

Специфіка воєнного контексту додає унікальні чинники ризику, що потребують адаптації традиційних методологій оцінки фінансових ризиків вітчизняних підприємств через відповідні коригуючі коефіцієнти, які враховують галузеву специфіку та розмір компанії [5, с. 83; 6, с. 160].

Згідно до Л. І. Донець [3, с. 59], сьогодні немає універсальної методики визначення економічного ризику, тому кожний підприємець самостійно обирає той чи інший підхід до аналізу економічного ризику. Це стало підставою для розробки власної методології, адаптованої до специфіки української ІТ-галузі в умовах воєнного стану.

З огляду на специфіку ІТ-сектору та обмежену статистичну базу внаслідок короткого періоду війни, застосування складних кількісних методів оцінки ризиків, таких як VaR або Monte Carlo, є ускладненим. Особливо це стосується стартапів та малих ІТ-компаній, які не мають достатніх ресурсів для впровадження складних статистичних систем, але потребують оперативних рішень для виживання в кризових умовах. За таких умов доцільно застосовувати метод експертних оцінок.

Оцінка ризиків передбачає визначення двох параметрів: ймовірність настання ризику (P) та потенційний вплив на діяльність компанії (I). Кожен параметр оцінюється за шкалою від 1 до 3 балів, де:

- ймовірність: 1 — малоймовірно, 2 — можливо, 3 — дуже ймовірно;
- вплив: 1 — незначні втрати, 2 — відчутні втрати, 3 — критичні втрати.

Базова оцінка ризику (R_0) визначається як добуток оцінок ймовірності та впливу:

$$R_0 = P \times I \ .$$

Значення R_0 інтерпретуються наступним чином:

1–3 бали відповідають прийнятним ризикам і потребують базового моніторингу;

4–6 балів — значним ризикам, що потребують планування заходів;

7–9 балів — критичним ризикам, які вимагають негайного реагування.

Більш точна оцінка інтегрального рівня ризику потребує застосування системи вагових коефіцієнтів. У розробці моделі автор спирався на концепцію коефіцієнтів ризику Л. І. Донець, згідно з якою «для знаходження компромісу і врахування величини власних коштів, вводять безрозмірні показники, які називаються коефіцієнтами ризику» [3, с. 57].

Інтегральна оцінка ризику доповнює формулу загальної оцінки наступним чином:

$$R=\left(P\times I\right)\times k_{IT}\times k_w\times k_s$$

де: P — ймовірність настання ризику,
I — сила впливу на діяльність компанії,
k_{IT} — коефіцієнт IT-специфіки,
k_w — воєнний коефіцієнт,
k_s — коефіцієнт значущості.

Коефіцієнт воєнного стану (k_w) враховує специфіку ведення бізнесу в умовах збройного конфлікту. Його значення базується на концепції зонування ризиків за Л. І. Донець.

Градація значень коефіцієнта k_w обґрунтовується емпіричними даними впливу різних рівнів конфлікту на українську IT-галузь. Базове значення 1,0 відповідає нормальним умовам функціонування без корекції ризиків. Проміжне значення 1,5 для локальних військових дій базується на досвіді 2014–2021 років, коли конфлікт на сході України обмежено впливав на IT-сектор — галузь продовжувала демонструвати зростання експорту на 27% щорічно, а ризики локалізуваись переважно в окремих регіонах на сході країни [8, 12].

Значення 2,0 застосуується в умовах повномасштабної війни та відображає кардинальну зміну ризик-ландшафту з 2022 року: скорочення експорту IT-послуг на 5,85% у 2023 році після багаторічного зростання, зменшення кількості спеціалістів на 17,8% та вимушена релокація 70,8% підприємств [11, с. 45; 12]. Прогресія (1,0 → 1,5 → 2,0) для коефіцієнтів обґрунтовується природою воєнних ризиків — їх вплив зростає не лінійно, а стрибкоподібно при переході від локальних конфліктів до повномасштабної війни. Це підтверджується різким погіршенням всіх показників IT-галузі після 24 лютого 2022 року.

Коефіцієнт IT-специфіки (k_{IT}) адаптує класичні методи оцінки ризиків під особливості IT-бізнесу. Його розрахунок ґрунтується на принципах β-коефіцієнта, який відображає ступінь коливань результатів діяльності конкретної галузі порівняно із загальними ринковими показниками [3, с. 88]. Л. І. Донець обґрунтовує можливість застосування β-коефіцієнта не лише для оцінки цінних паперів, але й для аналізу галузевих інвестиційних рішень, що дає методологічну основу для адаптації його принципів до оцінки ризиків у конкретних галузях економіки.

Базове значення 1,0 відображає рівень ризику, аналогічний середньоринковому [3, с. 88], коли класичні фінансові ризики (валютний, кредитний, ліквідності) впливають на IT-компанії без галузевої специфіки.

Значення 1,2 застосовується для ризиків з помірною IT-специфікою. Це обґрунтовується емпіричними даними про технологічні особливості галузі: коротшими циклами оновлення технологій (2–3 роки проти 10–15 років у традиційних галузях), підвищеною валютною експозицією (понад 90% IT-контрактів українських компаній номіновані в доларах США [12]) та специфікою віртуальних активів (програмний код, бази даних, інтелектуальна власність), що ускладнює їх оцінку та захист.

Коефіцієнт 1,5 застосовується для ризиків, що мають найвищий ступінь IT-специфіки. Обґрунтування базується на структурних особливостях технологічного сектору: критичній залежності від кібербезпеки (особливо для компаній, що працюють з фінансовими даними, де кіберризик може призвести до повної втрати бізнесу), високій кадровій мобільності IT-фахівців (що створює ризики втрати ключових розробників, особливо критичні для стартапів та малих компаній) та унікальній енергетичній залежності від безперервного електропостачання для функціонування серверів та дата-центрів.

Для верифікації запропонованих значень автором застосовано порівняльний аналіз з типовими

Таблиця 2

Коефіцієнт воєнного стану

Умови ведення бізнесу	Коефіцієнт (k_w)	Характеристика зони ризику
Мирний час	1,0	Припустима зона економічного ризику
Локальні військові дії	1,5	Критична зона економічного ризику
Повномасштабна війна	2,0	Катастрофічна зона економічного ризику

Джерело: складено автором на основі [3, с. 52]

Таблиця 3

Коефіцієнт IT-специфіки

Тип ризику	Коефіцієнт (k_{IT})	Відхилення від середньоринкового рівня
Класичні фінансові ризики	1,0	Ризик на рівні середнього по ринку
Помірна IT-специфіка	1,2	Ризик вищий за середньоринковий
Висока IT-специфіка	1,5	Ризик значно вищий за середньоринковий

Джерело: складено автором на основі [3, с. 87; 3, с. 88]

β-коефіцієнтами різних галузей: комунальні послуги (β = 0,6–0,8), будівництво (β = 1,2–1,6), технології (β = 1,4–1,8), фінансові послуги (β = 1,1–1,3). Прогресія 1,0 → 1,2 → 1,5 узгоджується з міжнародною практикою оцінки технологічного сектору як більш ризикованого порівняно з середнім по ринку, але не надмірно спекулятивного.

Коефіцієнт галузевої значущості (k_s) показує, наскільки важливим є конкретний ризик для окремої ІТ-компанії. Різні компанії по-різному реагують на одні й ті самі ризики залежно від того, чим вони займаються та як організована їх робота. Наприклад валютний ризик буде критичним для аутсорсингової ІТ-компанії, що експортує послуги до США, але не критичним для компанії, що працює виключно на українському ринку та отримує оплату в національній валюті.

Коефіцієнт визначає управлінська команда компанії (CEO, CTO, CFO) на основі власного розуміння бізнесу. Методологічною основою слугують принципи міжнародного стандарту ДСТУ IEC/ISO 31010:2013, який при встановленні критеріїв ризику вимагає враховувати готовність організації до ризику [9, с. 10].

Градація забезпечує помірне зростання впливу (на 10% та 30% відповідно), що відповідає принципу достатньої чутливості моделі без створення псевдоточності, характерної для ризик-менеджменту в умовах невизначеності [3, с. 58].

Для коректної інтерпретації результатів інтегральної оцінки необхідно визначити межі діапазонів ризику. Максимально можливе значення розраховується як добуток максимальних значень усіх компонентів:

$$R_{\max} = (3 \times 3) \times 1,5 \times 2,0 \times 1,3 = 35,1 \text{ бали.}$$

Цей теоретичний максимум (35,1 бали) визначає верхню межу шкали для подальшої градації ризиків.

Міжнародний стандарт ДСТУ IEC/ISO 31010:2013 рекомендує розділяти ризики на три діапазони [9, с. 9]. Методологічною основою градації слугує класифікація зон ризику за Л. І. Донець, яка виділяє «припустиму зону економічного ризику», «критичну зону економічного ризику» та «катастрофічну зону економічного ризику» [3, с. 53]. Цей принцип, а також теоретичний максимум, дозволили сформувати наступну градацію:

- 1–5 балів — низький рівень ризику, що потребує базового моніторингу;
- 6–15 балів — помірний рівень ризику, що вимагає планування заходів реагування;
- 16+ балів — високий рівень ризику, що потребує негайного втручання.

Доцільність застосування запропонованої інтегральної моделі підтверджує порівняння, наведені у таблиці 5, з класичними підходами оцінки фінансових ризиків, які найчастіше використовуються у практиці міжнародних компаній.

Як видно з таблиці, методи VaR та Монте-Карло забезпечують високу точність оцінок, однак мають суттєві обмеження щодо використання в умовах воєнної економіки. Їх застосування потребує великих обсягів історичних даних [3, с. 89] та значних обчислювальних ресурсів, що є малодоступним для українських ІТ-компаній які становлять близько 70% ринку [12].

Натомість запропонована інтегральна модель базується на коригувальних коефіцієнтах і може застосовуватися навіть за умов браку статистичної інформації. Вона є простою у використанні, гнучкою та придатною для оперативної оцінки ризиків у кризових ситуаціях, що робить її зручним інструментом для ІТ-компаній в умовах воєнного часу. Важливо також підкреслити певні обмеженнях: у стабільних макроекономічних умовах класичні методи (зокрема VaR і Монте-Карло) можуть забезпечувати вищу точність і деталізацію результатів [3, с. 89]. Таким чином, запропонована модель є оптимальним рішенням саме для умов невизначеності та воєнних ризиків, тоді як у довгостроковій перспективі доцільним є комбінування її з традиційними кількісними методами.

Практичну застосовність розробленої моделі демонструє оцінка трьох актуальних ризиків українських ІТ-компаній в поточних умовах: кіберризик, кадровий та енергетичний ризики.

Спочатку розглянемо приклад застосування моделі для оцінки кіберризику: 19 грудня 2024 року хакери заявили про злам інфраструктури та видалення даних ДП «Національні інформаційні системи» (НАІС), яке адмініструє державні реєстри Мін'юсту [13]. Відповідно, ймовірність (P) та вплив (I) оцінено у 3 бали кожен, а коефіцієнти:

k_w = 2,0 (повномасштабна війна),

k_{IT} = 1,5 (висока ІТ-специфіка реєстрів);

k_s = 1,3 (критично-важливий ризик [8, 10, 13]).

Інтегральна оцінка: $R = 9 \times 1,5 \times 2,0 \times 1,3 = 35,1$ бали (високий ризик).

Аналогічні розрахунки для кадрового ризику ІТ-стартапу (з урахуванням міграції 50–57 тисяч ІТ-експертів [12]) та енергетичного ризику хостинг-провайдера

Таблиця 4

Коефіцієнт значущості

Рівень критичності	Коефіцієнт (k_s)	Характеристика
Помірна критичність	1,0	Ризик на базовому рівні для конкретної компанії
Значна критичність	1,1	Ризик може суттєво вплинути на діяльність компанії
Висока критичність	1,3	Ризик є критично важливим для бізнес-моделі компанії

Джерело: складено автором на основі [3, 9]

Таблиця 5

Порівняльна характеристика методів оцінки фінансових ризиків

Критерій	VaR/статистичні	Монте-Карло	Класичні експертні	Запропонована модель
Потреба в історичних даних	Висока	Висока	Відсутня	Мінімальна
Адаптивність до війни	Низька	Низька	Середня	Висока
Придатність для стартапів	Неможлива	Неможлива	Обмежена	Повна
Швидкість результату	Години	Дні	Години	<1 години
Врахування ІТ-специфіки	Ні	Потребує програмування	Ні	Так

Джерело: складено автором на основі [3, с. 63, 88–89; 9, с. 10]

Таблиця 6

Результати апробації інтегральної моделі оцінки ризиків

Ризик	Тип компанії	P	I	k_{IT}	k_w	k_s	R	Рівень ризику
Кадровий	ІТ-стартап	3	2	1,5	2,0	1,3	11,88	Помірний
Енергетичний	Хостинг-провайдер	3	3	1,2	2,0	1,3	28,08	Високий

Джерело: складено автором

(в умовах регулярних відключень електроенергії) показали результати продемонстровані в таблиці 6.

Результати апробації демонструють практичну цінність та ефективність розробленої моделі для українських ІТ-компаній в умовах воєнного стану. Методологія дозволяє компаніям швидко оцінювати актуальні ризики на основі аналізу ринкової ситуації, пріоритизувати заходи мітігації та ефективно розподіляти обмежені ресурси між найбільш критичними загрозами.

Це дослідження дозволило розробити інтегральну модель оцінки фінансових ризиків українських ІТ-компаній, яка враховує специфіку воєнного часу. Пропонуємий підхід ґрунтується на модифікації експертного методу через систему коригувальних коефіцієнтів, що дозволяє адаптувати традиційні інструменти до умов обмеженої статистичної інформації та підвищеної турбулентності.

Модель має ключову перевагу — можливість застосування у ситуаціях, коли класичні методи втрачають ефективність через недоступність або неактуальність даних. Апробація на прикладах кіберризику та енергетичних викликів підтвердила практичну придатність методики для використання управлінськими командами ІТ-компаній у оперативній і комплексній оцінці ризиків та обґрунтуванні управлінських рішень у кризових умовах.

Водночас модель має певні обмеження, які важливо враховувати при практичному застосуванні: суб'єктивність експертних оцінок може призводити до розбіжностей у результатах між різними оцінювачами; при зміні умов ведення бізнесу (наприклад, зміна статусу ризику з помірного на критичний) потрібно переглядати застосування відповідних коефіцієнтів.

Подальший розвиток дослідження включає тестування на ширшій вибірці компаній, удосконалення коефіцієнтів для різних сегментів ІТ-ринку та інтеграцію з кількісними методами у післявоєнний період, що дозволить поєднати гнучкість експертної оцінки з точністю математичного моделювання.

Українська ІТ-галузь стала першою у світі, що змушена адаптувати ризик-менеджмент до умов повномасштабної війни при збереженні глобальної конкурентоспроможності. Це створює унікальний досвід, який може бути цінним для інших країн у подібних ситуаціях.

Література

1. Кириленко О.І. Оптимізація визначення категорії «фінансові ризики». *Молодий вчений.* 2024. № 1 (125). С. 114–120. DOI: https://doi.org/10.32839/2304-5809/2024-1-125-23

2. Юдіна С.В., Мондрієвський С.А. Системний підхід до оцінки фінансових ризиків під час стратегічного управління. *Економіка та суспільство.* 2024. № 67. С. 242–249. DOI: https://doi.org/10.32782/2524-0072/2024-67-54

3. Донець Л.І. Економічні ризики та методи їх вимірювання: навч. посіб. Київ : Центр навчальної літератури, 2006. 312 с.

4. Макалюк І.В., Лайкова А.О. Фінансові ризики вітчизняних підприємств в умовах війни. *Бізнес, інновації, менеджмент: проблеми та перспективи: зб. тез доп. V Міжнар. наук.-практ. конф.,* Київ, 25 квіт. 2024 р. Київ : КПІ ім. Ігоря Сікорського, 2024. С. 83–84. URL: https://confmanagement-proc.kpi.ua/article/view/303665

5. Шевчук Л. Т., Шевчук Я. В., Пась Я. І. Управління фінансовими ризиками та санація підприємств в умовах воєнного стану. *Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична.* 2024. Вип. 41. С. 158–167. DOI: https://doi.org/10.5281/zenodo.13609386

6. Лаговська О. А., Грабчук І. Л., Лоскоріх Г. Л. Класифікація ризиків ІТ-підприємств: обліковий аспект. *Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу.* 2020. Вип. 3 (47). С. 25–32.

7. Герасименко О., Гнилицька Л., Д'яченко А. Risk classification of IT industry companies. *Scientia Fructuosa*. 2023. № 4. С. 122–136.

8. AIN. Топ-компанії, обсяги експорту, стартапи та найбільш затребувані стеки: як змінився ринок українського ІТ з 2014 до 2024. Київ, 2025. 139 с.

9. Керування ризиком. Методи загального оцінювання ризику: ДСТУ IEC/ISO 31010:2013. Київ : Мінекономрозвитку України, 2015. 73 с.

10. DataDriven Research & Consulting. Огляд ринку кібербезпеки в Україні: дослідження / DataDriven Research & Consulting; EBA; Асоціація ІТ Ukraine; Аспен Інститут Київ. Київ, 2025. 43 с.

11. Тимків О. О. Ринок інформаційних технологій України: поточний стан і тенденції розвитку. *Актуальні проблеми економіки.* 2024. № 11 (281). С. 42–50. DOI: 10.32752/1993-6788-2024-1-281-42-50

12. Лісік О. А., Моряк Т. П. Аналіз стану ІТ-сектору України в умовах повномасштабної війни. *Економіка та суспільство.* 2023. Вип. 55. С. 158–164. DOI: https://doi.org/10.32782/2524-0072/2023-55-67

13. Кібератака на реєстри Мін'юсту: чому це могло статися і які наслідки. *DOU*. URL: https://dou.ua/lenta/articles/cyberattacks-on-registries-and-vendor-locks — дата звернення: 27.08.2025.

References

1. Kyrylenko, O. I. (2024). Optymizatsiia vyznachennia katehorii "finansovi ryzyky" [Optimization of the definition of the category "financial risks"]. Molodyi Vchenyi, 1 (125), 114–120. https://doi.org/10.32839/2304-5809/2024-1-125-23 [in Ukrainian].

2. Yudina, S. V., & Mondriievskyi, S. A. (2024). Systemnyi pidkhid do otsinky finansovykh ryzykiv pid chas stratehichnoho upravlinnia [A systematic approach to assessing financial risks during strategic management]. Ekonomika ta Suspilstvo, 67, 242–249. https://doi.org/10.32782/2524-0072/2024-67-54 [in Ukrainian].

3. Donets, L. I. (2006). Ekonomichni ryzyky ta metody yikh vymiriuvannia [Economic risks and methods of their measurement]. Kyiv: Tsentr Navchalnoi Literatury [in Ukrainian].

4. Makaliuk, I. V., & Laikova, A. O. (2024). Finansovi ryzyky vitchyznianykh pidpryiemstv v umovakh viiny [Financial risks of domestic enterprises under wartime conditions]. In Business, Innovations, Management: Problems and Prospects (Proc. of the V Int. Sci.-Pract. Conf., Kyiv, Apr 25, 2024) (pp. 83–84). Kyiv: KPI im. Ihori Sikorskoho. https://confmanagement-proc.kpi.ua/article/view/303665 [in Ukrainian].

5. Shevchuk, L. T., Shevchuk, Ya. V., & Pas, Ya. I. (2024). Upravlinnia finansovymy ryzykamy ta sanatsiia pidpryiemstv v umovakh voiennoho stanu [Financial risk management and enterprise rehabilitation under martial law]. Naukovi Zapysky Lvivskoho Universytetu Biznesu ta Prava. Seriia Ekonomichna. Seriia Yurydychna, 41, 158–167. https://doi.org/10.5281/zenodo.13609386 [in Ukrainian].

6. Lahovska, O. A., Grabchuk, I. L., & Loskorikh, H. L. (2020). Klasyfikatsiia ryzykiv IT-pidpryiemstv: oblikovyi aspekt [Classification of IT enterprises' risks: Accounting aspect]. Problemy Teorii ta Metodolohii Bukhhalterskoho Obliku, Kontroliu i Analizu, 3 (47), 25–32 [in Ukrainian].

7. Herasymenko, O., Hnylytska, L., & Diachenko, A. (2023). Risk classification of IT industry companies. Scientia Fructuosa, 4, 122–136 [in Ukrainian].

8. AIN (2025). Top-kompanii, obsiahy eksportu, startapy ta naibilsh zatrebuvani steky: iak zminyvsia rynok ukrainskoho IT z 2014 do 2024 roku [Top companies, export volumes, startups, and most in-demand stacks: How Ukraine's IT market has changed from 2014 to 2024]. Kyiv [in Ukrainian].

9. DSTU IEC/ISO 31010:2013 (2015). Keruvannia ryzykom. Metody zahalnoho otsiniuvannia ryzyku [Risk management — Risk assessment techniques]. Kyiv: Minekonomrozvytku Ukrainy [in Ukrainian].

10. DataDriven Research & Consulting (2025). Ohliad rynku kiberbezpeky v Ukraini [Overview of the cybersecurity market in Ukraine]. Kyiv: EBA, IT Ukraine Association, Aspen Institute Kyiv [in Ukrainian].

11. Tymkiv, O. O. (2024). Rynok informatsiinykh tekhnolohii Ukrainy: potochnyi stan i tendentsii rozvytku [The IT market of Ukraine: Current state and development trends]. Aktualni Problemy Ekonomiky, 11 (281), 42–50. https://doi.org/10.32752/1993-6788-2024-1-281-42-50 [in Ukrainian].

12. Lisik, O. A., & Moriak, T. P. (2023). Analiz stanu IT-sektoru Ukrainy v umovakh povnomasshtabnoi viiny [Analysis of Ukraine's IT sector under full-scale war conditions]. Ekonomika ta Suspilstvo, 55, 158–164. https://doi.org/10.32782/2524-0072/2023-55-67 [in Ukrainian].

13. DOU (2025). Kiberataka na reiestry MinJustu: chomu tse mohlo statysia i iaki naslidky [Cyberattack on the Ministry of Justice registries: Causes and consequences]. Retrieved from https://dou.ua/lenta/articles/cyberattacks-on-registries-and-vendor-locks [in Ukrainian].