Економіка

УДК 330.131.7:338.45

DOI https://doi.org/10.5281/zenodo.18168942

Якісний аналіз та кількісне оцінювання ризику підприємств в Україні за умов війни: фокус на ІТ-сектор

Лук'янова Валентина Вячеславівна,

д.е.н., професор, професор кафедри економіки, аналітики, моделювання та інформаційних технологій в бізнесі, Хмельницький національний університет, м. Хмельницький, Україна, https://orcid.org/0000-0003-0036-3138

Маліцький Роман Ігорович,

аспірант, Хмельницький національний університет, м. Хмельницький, Україна, https://orcid.org/ 0009-0004-0160-3441

Прийнято: 22.12.2025 | Опубліковано: 31.12.2025

Анотація. *Повномасштабна військова агресія проти України призвела до суттєвих змін у функціонуванні національної економіки, трансформації бізнес-середовища та різкого зростання рівня невизначеності для підприємств усіх форм власності та галузевої приналежності. У цих умовах ризики перестали бути виключно фінансовою категорією та набули системного характеру, охоплюючи операційні, кадрові, репутаційні, інституційні та воєнні загрози. Особливої актуальності набуває проблема управління ризиками у секторах, що мають високу частку експорту та ґрунтуються на людському капіталі, зокрема в ІТ-секторі України. Отже, управління ризиками набуває ключового значення, оскільки від здатності підприємств ідентифікувати, оцінювати та мінімізувати ризики залежить*

не лише їх фінансова стабільність, але й виживання в довгостроковій перспективі. Особливої актуальності набуває необхідність поєднання якісних і кількісних підходів до оцінювання ризику, що дозволяє більш повно відобразити складність сучасних загроз.

У статті систематизовано основні види ризиків, характерні для воєнного періоду, визначено їхні ключові джерела та наслідки для господарської діяльності. Запропоновано інтегровану модель оцінювання ризиків, що ґрунтується на поєднанні експертних оцінок, матричних методів і розрахунку інтегрального показника ризику. Основні акценти зроблено на ідентифікацію та оцінювання ризикових чинників, які породжені (або значно зросли) за умов військової агресії проти України. Отримані результати можуть бути використані для підвищення стійкості українських підприємств і вдосконалення системи управління ризиками в умовах тривалої нестабільності.

Ключові слова: *економічна безпека, матриця ризиків, інтегральний показник ризику, інтелектуальний аналіз даних, штучний інтелект, кризовий ризик-менеджмент.*

Risk assessment of enterprises in Ukraine under war conditions: focus on the IT sector

Valentyna Lukianova,

Doctor of Economics, Professor, Professor of the Department of Economics, Analytics, Modeling and Information Technologies in Business, Khmelnytskyi National University, Khmelnytskyi, Ukraine,

https//orcid.org/0000-0003-0036-3138

Roman Malitsky,
Postgraduate Student, Khmelnytskyi National University, Khmelnytskyi, Ukraine,
https://orcid.org/ 0009-0004-0160-3441

Abstract. *Full-scale military aggression against Ukraine has led to significant changes in the functioning of the national economy, the transformation of the business environment and a sharp increase in the level of uncertainty for enterprises of all forms of ownership and industry affiliation. In these conditions, risks have ceased to be exclusively a financial category and have acquired a systemic nature, encompassing operational, personnel, reputational, institutional and military threats. The problem of risk management in sectors with a high share of exports and based on human capital, in particular in the IT sector of Ukraine, is becoming particularly relevant. Therefore, risk management is becoming key, since not only their financial stability, but also their survival in the long term depends on the ability of enterprises to identify, assess and minimize risks. The need to combine qualitative and quantitative approaches to risk assessment, which allows for a more complete reflection of the complexity of modern threats, is becoming particularly relevant.*

The article systematizes the main types of risks characteristic of the war period, identifies their key sources and consequences for economic activity. An integrated risk assessment model is proposed, based on a combination of expert assessments, matrix methods and calculation of the integral risk indicator. The main emphasis is placed on the identification and assessment of risk factors that are generated (or significantly increased) under the conditions of military aggression against Ukraine. The results obtained can be used to increase the resilience of Ukrainian enterprises and improve the risk management system in conditions of prolonged instability.

Keywords: *economic security, risk matrix, integrated risk indicator, data mining, artificial intelligence, crisis risk management.*

Постановка проблеми. Ризик є невід'ємною характеристикою підприємницької діяльності, однак у воєнних умовах його природа, інтенсивність і наслідки зазнають якісних змін. Війна створює багаторівневу систему загроз, які одночасно впливають на макроекономічне середовище, галузеві ринки та економічну безпеку окремих підприємств. Для українських компаній ризики війни проявляються не лише у вигляді фізичного знищення активів або логістичних обмежень, але й через втрату персоналу, зниження довіри іноземних контрагентів, регуляторну нестабільність та посилення кіберзагроз.

Особливе місце в економіці України займає IT-сектор, який до війни демонстрував стабільне зростання та був одним з ключових джерел валютних надходжень. Навіть за умов повномасштабної агресії IT-індустрія зберегла експортну орієнтацію та значну частину робочих місць, проте її стійкість значною мірою залежить від ефективного управління ризиками. Проблема полягає в тому, що більшість підприємств використовують фрагментарні або інтуїтивні підходи до оцінювання ризиків, які не дозволяють комплексно врахувати вплив воєнного чинника.

Наукова новизна дослідження полягає в обґрунтуванні та апробації інтегрованого підходу до оцінювання ризиків підприємств у воєнних умовах, який поєднує якісний аналіз ризиків, кількісне оцінювання їх ймовірності та впливу, а також галузеву статистику IT-сектору України. Уперше для українських умов запропоновано адаптовану інтегровану матрицю ризиків IT-підприємств, що враховує нефінансовий характер ключових загроз (кадрових, кібернетичних, репутаційних) та дозволяє кількісно інтерпретувати їхній економічний ефект.

Аналіз останніх досліджень і публікацій. У світовій економічній науці проблематика ризиків традиційно розглядається в межах концепцій невизначеності, теорії очікуваної корисності та корпоративного управління.

ISSN: 2786-9431

Міжнародні стандарти COSO ERM [1] та ISO 31000 [2] заклали основу системного підходу до управління ризиками на підприємствах. Проте їх застосування в умовах війни потребує адаптації, оскільки стандартні моделі не враховують високої динамічності та непередбачуваності середовища.

Зарубіжні дослідники (D. Hubbard, K. Winston, K. Mizrak) наголошують на необхідності поєднання якісних та кількісних методів оцінювання ризику, особливо в кризових ситуаціях [3-5]. В українських дослідженнях останніх років увага зосереджується на впливі війни на фінансову стійкість підприємств, трансформацію бізнес-моделей, діджиталізацію, інтелектуальний аналіз даних та роль державної підтримки. Вітчизняні дослідники підкреслюють, що війна створює унікальні виклики: знищення інфраструктури, перебої у ланцюгах постачання, неможливість планування понад короткостроковий горизонт, перебої в енергопостачанні і зростання витрат, нестача кадрів тощо [6-11]. Водночас галузеві аспекти ризиків, зокрема в IT-секторі, залишаються недостатньо систематизованими.

Дослідження останніх років підтверджують, що підприємства в кризових умовах повинні адаптувати свої інструменти управління ризиками. За результатами аналізу літератури [12], класичні методи мають обмежену застосовність без урахування динамічних змін середовища. Окремі автори розглядають особливості секторальних ризиків за сучасних умов воєнної невизначеності [13-14].

Окрему групу джерел становлять аналітичні матеріали IT Ukraine Association, які містять узагальнену статистику щодо експорту IT-послуг, чисельності фахівців та структури ринку [15]. Проте ці дані не часто знаходять застосування в наукових роботах для побудови формалізованих моделей оцінювання ризиків.

Виділення невирішених раніше частин загальної проблеми. період, низка аспектів залишається недостатньо дослідженою. Наразі, відсутній

єдиний підхід до систематизації ризиків підприємств з урахуванням воєнного чинника, що ускладнює порівняння результатів різних досліджень. Поряд з цим, більшість робіт зосереджується на окремих видах ризиків (фінансових або операційних), не враховуючи їх комплексний вплив [6, 8-11]. Також недостатньо розробленими є методи кількісного оцінювання ризиків у ситуаціях, коли статистичні дані є обмеженими або неповними[12]. Це особливо актуально для українських підприємств, які працюють в умовах швидких змін і часто не мають можливості накопичувати репрезентативні дані. Разом з тим, існує потреба в адаптації наявних міжнародних методик оцінювання ризиків до українського економічного та правового середовища[3-5]. Додатково можна виділити питання слабкої прив'язки теоретичних моделей до реальної галузевої статистики та обмежене використання кейс-аналізу реальних компаній як емпіричної бази дослідження.

Саме ці невирішені питання зумовлюють необхідність подальших наукового пошуку у даному напрямі.

Формулювання цілей статті (постановка завдання). Метою статті є розробка та обґрунтування комплексного підходу до якісного аналізу та кількісного оцінювання ризиків підприємств в Україні за умов війни. Для досягнення поставленої мети передбачено вирішення таких завдань: систематизувати основні види ризиків підприємств у воєнний період, у т.ч. з врахуванням специфіки ІТ-сектору; обґрунтувати доцільність поєднання якісних і кількісних методів оцінювання ризику; розробити інтегровану модель кількісної оцінки ризику; проаналізувати реальний кейс ІТ-компанії з використанням галузевої статистики; сформулювати практичні рекомендації щодо управління ризиками в умовах війни

Виклад основного матеріалу дослідження. Ризик у діяльності підприємства доцільно розглядати як імовірність відхилення фактичних результатів від запланованих під впливом внутрішніх і зовнішніх чинників. В

умовах війни домінують зовнішні ризики, проте внутрішні управлінські помилки можуть суттєво посилювати їхній негативний ефект.

Якісний аналіз передбачає ідентифікацію ризиків, визначення їхніх джерел, характеру впливу та можливих наслідків. Він базується на експертних оцінках, аналізі бізнес-процесів та зовнішнього середовища. Таблиця 1 містить основні види ризиків за умов військових загроз.

Таблиця 1

Основні ризики підприємств в Україні за умов війни

Вид ризику	Характеристика	Потенційні наслідки
Військовий	Загроза руйнування активів	Повна або часткова втрата виробництва
Фінансовий	Інфляція, девальвація	Зниження платоспроможності
Операційний	Перебої в логістиці	Зупинка діяльності
Інформаційний	Нестача та викривлення інформації, використання ШІ	Низька обґрунтованість прийнятих рішень
Соціальний	Втрата персоналу	Падіння продуктивності

Джерело: побудовано авторами

ІТ-сектор характеризується домінуванням нематеріальних активів, тому ключову роль відіграють наступні ризики. (таблиця 2). Конкретизація і звуження ризикових чинників проводиться у контексті функціонування конкретної ІТ-компанії.

Таблиця 2

Основні ризики ІТ-підприємств України

Вид ризику	Характеристика	Потенційні наслідки
Група ризиків	Зміст	Потенційні наслідки
Кадрові	Міграція фахівців, мобілізація	Втрата проєктів
Кібернетичні	Атаки, витік даних	Фінансові та репутаційні втрати
Операційні	Перебої електроенергії	Зрив дедлайнів
Контрактні	Форс-мажори	Штрафи, розірвання угод
Репутаційні	Недовіра клієнтів	Втрата ринку

Джерело: побудовано авторами

ISSN: 2786-9431

Якісний аналіз передбачає експертну оцінку значущості кожного ризику, визначення тригерів та наслідків. Для ІТ-компаній особливо важливою є оцінка критичності ризику втрати ключових розробників та замовників.

Базова кількісна оцінка ризику здійснюється шляхом визначення ймовірності реалізації ризику та величини можливих втрат. Інтегральний показник ризику може бути представлений у вигляді добутку цих величин. Приклад такого оцінювання подано у табл. 3.

Таблиця 3

Приклад кількісної оцінки ризиків ІТ-компанії

Ризик	Імовірність	Наслідки – розмір втрат (тис. дол.)	Ризик
Втрата ключового клієнта	0,4	500	200
Кіберінцидент	0,3	300	90
Масова релокація персоналу	0,5	400	200

Джерело: побудовано авторами

На основі отриманих значень можна сформувати матрицю ризиків, яка дозволяє ранжувати загрози та визначати пріоритети управління. Найвищий пріоритет мають ризики з високим значенням ризику.

Інтегрована матриця ризиків формується на основі двох ключових параметрів:

– ймовірність реалізації ризику (P) –оцінюється експертно за шкалою від 1 до 5;

– рівень впливу (I) – визначається за ступенем фінансових, операційних та репутаційних втрат також за шкалою від 1 до 5.

ISSN: 2786-9431

Інтегральний рівень ризику визначається як добуток цих двох величин. У таблиці 4 подано лінгвістичну шкалу оцінювання, яка придатна для практичного застосування. Отримане значення використовується для ранжування ризиків та визначення пріоритетів при прийняття управлінських рішень.

Таблиця 4

Шкала оцінювання ймовірності та впливу ризиків

Бал	Ймовірність (P)	Вплив (I)
1	Дуже низька	Незначний
2	Низька	Обмежений
3	Середня	Помірний
4	Висока	Значний
5	Дуже висока	Критичний

Джерело: побудовано авторами

Тоді, інтегрована матриця ризиків одержить наступний вигляд (табл.5). Дана матриця – є шаблоном для визначення зони ризику. Разом з тим, за потреби розширення або звуження (зміни рівня деталізації) можна застосовувати і інші можливі інтервали, наприклад – від 1 до 3 чи від 1 до 10.

Таблиця 5

Інтегрована матриця ризиків IT-підприємств

Ймовірність \ Вплив	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

Джерело: побудовано авторами

Для подальшого формування і конкретизації системи антиризикових заходів пропонуємо виділяти наступні зони ризику:

1-5 – низький ризик (прийнятний);

6-12 – середній ризик (потребує контролю);

15-25 – високий / критичний ризик (потребує негайного управління).

Важливо відзначити, що IT-індустрія України продовжує залишатися одним із найстійкіших секторів економіки навіть у воєнний період. За даними асоціації IT Ukraine Association [16]:

– експорт IT-послуг у 2024 році становив близько $6,4 млрд, що відповідає приблизно 37,4 % експорту послуг країни та 11,5 % загального експорту України; частка IT-послуг зберігається на високому рівні попри війну;

– у секторі налічувалося 266,8 тис. платників податків, з яких 96,8 % – фізичні підприємці (ФОПи), що підкреслює гнучку структуру ринку праці IT-сфери;

– експортні IT-послуги постачалися до 147 країн, причому 37,2 % припадає на США, що підкреслює орієнтацію галузі на глобальні ринки.

Ці дані ілюструють важливість IT-індустрії як економічного драйвера України в умовах війни та необхідність ефективного управління ризиками для збереження цих позицій.

На основі експертних оцінок ймовірності та впливу ризиків та аналітичних матеріалів IT Ukraine Association [15] було сформовано інтегровану матрицю ризиків IT-підприємств України(табл. 6).

Таблиця 6

Інтеграція основних ризиків IT-підприємств

Ризик	P	I	R	Рівень
Втрата ключового клієнта	4	5	20	Критичний
Масова міграція персоналу	4	4	16	Високий
Кіберінциденти	3	5	15	Високий
Перебої електроенергії	5	3	15	Високий
Контрактні санкції	3	4	12	Середній

ISSN: 2786-9431

Валютні коливання	2	3	6	Середній
Регуляторні зміни	2	2	4	Низький

Джерело: побудовано авторами

Побудована інтегрована матриця свідчить, що для IT-підприємств України в умовах війни найбільшу загрозу становлять ризики втрати клієнтів, кадрові ризики та кібернетичні загрози, які потрапляють у червону зону матриці. Саме ці ризики повинні бути пріоритетними в системі управління. Ризики середнього рівня потребують постійного моніторингу та превентивних заходів, тоді як низькі ризики можуть бути прийняті без значних управлінських втручань.

На основі результатів матричного аналізу можна сформувати комплекс заходів управління ризиками:

1. Управління клієнтським ризиком:
- диверсифікація клієнтського портфеля;
- укладання контрактів з гнучкими параметрами;
- регулярна комунікація з клієнтами щодо безперервності бізнесу.

2. Управління кадровими ризиками:
- створення розподілених команд у різних регіонах;
- перегляд політики управління інтелектуальним капіталом;
- розширення співпраці з фрілансерами та підрядниками.

3. Управління операційними ризиками:
- забезпечення автономних джерел живлення;
- резервні канали інтернет-зв’язку;
- перехід на повністю віддалену модель роботи.

4. Кібербезпека:
- збільшення бюджету на інформаційну безпеку;
- впровадження багатофакторної аутентифікації;
- застосування процедур інтелектуального аналізу даних;

– регулярні аудити безпеки.

Проведений кейс-аналіз конкретної IT-компанії підтвердив доцільність використання інтегрованої матриці ризиків як інструменту прийняття управлінських рішень в умовах війни. Результати свідчать, що своєчасна ідентифікація та кількісна оцінка ризиків дозволяє мінімізувати негативні наслідки навіть за умов високої невизначеності.

Методологічну основу дослідження становить сукупність загальнонаукових та спеціальних методів пізнання, що забезпечили досягнення поставленої мети та обґрунтованість отриманих результатів.

У процесі дослідження застосовано метод аналізу та синтезу, який використано для розкриття сутності ризиків підприємств в умовах війни та систематизації чинників ризикового середовища. Системний підхід застосовано для розгляду ризиків підприємств як взаємопов'язаної багаторівневої системи, що формується під впливом зовнішніх (воєнних, макроекономічних, інституційних) та внутрішніх (організаційних, кадрових, фінансових) чинників.

Метод логіко-теоретичного узагальнення використано для аналізу наукових підходів до управління ризиками, узагальнення положень міжнародних стандартів (ISO 31000, COSO ERM) та адаптації їх до умов воєнного стану в Україні.

Метод класифікації застосовано для систематизації ризиків підприємств за функціональними ознаками з урахуванням галузевої специфіки IT-сектору, що дало змогу сформувати розширену типологію ризиків воєнного періоду.

Для ідентифікації та попереднього оцінювання ризиків використано експертний метод, який ґрунтувався на узагальненні думок керівників IT-підприємств, менеджерів проєктів та фахівців з управління ризиками. Метод контент-аналізу застосовано для аналізу аналітичних звітів IT Ukraine Association, публікацій професійних об'єднань та відкритих джерел.

ISSN: 2786-9431

Кількісне оцінювання ризиків здійснювалося з використанням методу експертного бального оцінювання, який передбачає визначення ймовірності реалізації ризику та рівня його впливу за п'ятибальною шкалою.

Для узагальнення результатів застосовано метод інтегральної оцінки ризику, відповідно до якого інтегральний показник ризику визначався як добуток ймовірності та впливу ризику. Отримані значення використано для ранжування ризиків та визначення пріоритетів управління.

З метою візуалізації результатів кількісного оцінювання використано метод матричного аналізу, що передбачає побудову інтегрованої матриці ризиків. Матриця дозволила класифікувати ризики за рівнем критичності та визначити зони допустимого, помірного і критичного ризику.

Висновки. Проведене дослідження демонструє, що в умовах війни українські підприємства потребують інтегрованих інструментів оцінювання ризиків, що поєднують якісний опис ризикових явищ із кількісними показниками впливу та ймовірності. IT-сектор України, попри відносну стійкість, зазнає значного впливу воєнних ризиків, які мають переважно нефінансовий характер, але призводять до суттєвих економічних втрат. Поєднання якісного аналізу та кількісного оцінювання дозволяє сформувати ефективну систему управління ризиками та підвищити адаптивність IT-підприємств. Запропонована модель дозволяє систематизувати ризики, оцінити їхній потенційний негативний вплив та розробити адаптивні стратегії управління.

Практичне значення проведеного дослідження полягає у можливості безпосереднього використання отриманих результатів у процесі управління ризиками підприємств України в умовах війни, зокрема в IT-секторі, який характеризується високою часткою експорту, домінуванням нематеріальних активів та підвищеною залежністю від людського капіталу.

ISSN: 2786-9431

Розроблений у статті інтегрований підхід до якісного аналізу та кількісного оцінювання ризиків може бути використаний керівниками та власниками ІТ-підприємств для системної ідентифікації ключових ризиків воєнного періоду; кількісного вимірювання потенційних втрат від реалізації нефінансових ризиків (кадрових, кібернетичних, репутаційних); визначення пріоритетів управління ризиками на основі інтегрованої матриці ризиків; обґрунтування управлінських рішень щодо диверсифікації клієнтського портфеля, розподілу ресурсів та інвестицій у кібербезпеку.

Запропонована інтегрована матриця ризиків може бути використана як прикладний інструмент внутрішнього контролю та ризик-моніторингу, а також як основа для формування корпоративної системи ризик-менеджменту відповідно до принципів ISO 31000 та COSO ERM, адаптованих до воєнних умов.

Таким чином, практичне значення дослідження полягає у створенні прикладного інструментарію, здатного підвищити адаптивність і стійкість підприємств України в умовах тривалої військової нестабільності.

Подальші дослідження можуть бути зосереджені на вдосконаленні моделей з урахуванням невизначених даних; використанні машинного навчання (інтелектуального аналізу даних, штучного інтелекту для прогнозування ризиків; формування галузевих ризик-індикаторів; адаптації моделі до конкретних секторів економіки та регіонів; порівняльний аналіз ризиків у різних секторах економіки.

Список використаних джерел

1. Приказюк Н., Мендрик Д. Модель управління ризиками COSO: еволюція та трансформація. *Економіка та суспільство*. 2020. № 22. https://economyandsociety.in.ua/index.php/journal/article/view/90.

 ISSN: 2786-9431

2. Роголь Г. Управління ризиками відповідно до стандарту ISO 31000:2018. *Тех Медіа Груп*. 2023. https://qualityexpert.com.ua/articles/657421-upravlinnya-ryzykamy-vidpovidno-do-standartu-iso-310002018.

3. Hubbard D. The Failure of Risk Management: Why It's Broken and How to Fix It (2nd Edition). 2020. https://hubbardresearch.com/shop/failure-risk-management-signed-author/

4. Winston K. J. Quantitative Risk and Portfolio Management Theory and Practice. *California Institute of Technology*. 2023. https://www.cambridge.org/highereducation/books/quantitative-risk-and-portfolio-management/8F70D4FBEE25210A2EE4E61193AA2BE0#overview.

5. Mizrak K. C. Crisis Management and Risk Mitigation: Strategies for Effective Response and Resilience. *Trends, Challenges, and Practices in Contemporary Strategic Managemen. 2024.* P. 254-278. https://www.igi-global.com/chapter/crisis-management-and-risk-mitigation/336799.

6. Вакуленко В.Л., Юнтао, Л., Сяовей Л. Система ризик-менеджменту логістичних систем в умовах воєнного стану України. *Сталий розвиток економіки*. 2025. №3 (54). С. 296-300.

7. Ярмусь Д. В. Ризик-менеджмент в умовах воєнного стану: адаптація моделей управління. *Вісник Херсонського національного технічного університету*. 2025. № 2(93) Том 1. https://journals.kntu.kherson.ua/index.php/visnyk_kntu/article/view/1010.

8. Лошенюк О. В., Мурована Т. О. Ризики ведення бізнесу в умовах воєнного стану та шляхи їх подолання. *Ефективна економіка*. 2023. №2. https://nayka.com.ua/index.php/ee/article/view/1166.

9. Хома І.Б., Боберський Р.І. Управління фінансовими ризиками в умовах війни. *Причорноморські економічні студії.* 2023. Вип. 84. https://bses.in.ua/journals/2023/84_2023/9.pdf

10. Чернишова Л. І., Бондар К. Р., Красіловська Л. О. Особливості управління ризиками в умовах дії воєнного стану: моделі поведінки сучасних підприємств. Науковий вісник Одеського національного економічного університету. 2024. № 3-4 (316-317). С. 126-136. http://n-visnik.oneu.edu.ua/collections/2024/316-317/pdf/126-136.pdf.

11. Макалюк І.В., Кривда О.В., Лайкова А.О. Якісний аналіз ризиків вітчизняних підприємств в умовах воєнного стану. *Економіка та суспільство.* 2024. № 62. https://economyandsociety.in.ua/index.php/journal/article/view/3950.

12. Balasubramaniam V. S., Mahadik S., Khair M. A., Goel O. Effective Risk Mitigation Strategies in Digital Project Management. *Innovative Research Thoughts*. 2023. № 9(1). P. 538-567. https://www.researchgate.net/publication/384274149_Effective_Risk_Mitigation_Strategies_in_Digital_Project_Management.

13. Ясіновська І. Ф., Шеремета Л. М. Управління банківськими ризиками в умовах війни. *Бізнес Інформ*. 2024. №11. С. 237–246. https://www.business-inform.net/export_pdf/business-inform-2024-11_0-pages-237_246.pdf.

14. Осіпчук Д.С. Управління ризиками у митній справі в умовах воєнного стану. *Економіка, управління та адміністрування*. 2024. №2 (108). С. 16-21.

15. IT Ukraine Association. https://itukraine.org.ua/.

16. Українська IT-індустрія сплатила понад $1 млрд податків у 2024 році – дослідження IT Ukraine Association. 2025. https://ain.ua/2025/03/24/it-ponad-1-mlrd-podatkiv/.