

DOI: <https://doi.org/10.32782/2524-0072/2026-90-4>

УДК 339.9:004:330.131.7(477)

ПРОБЛЕМИ ТА РИЗИКИ ДІЯЛЬНОСТІ МІЖНАРОДНИХ КОМПАНІЙ ІТ СЕКТОРУ В УКРАЇНІ

CHALLENGES AND RISKS FACING INTERNATIONAL IT COMPANIES OPERATING IN UKRAINE

Булкот Оксана Вікторівнакандидат економічних наук, доцент,
Київський національний університет імені Тараса Шевченка
ORCID: <https://orcid.org/0000-0002-6311-1459>**Кузнецов Олександр Євгенович**магістр,
Київський національний університет імені Тараса Шевченка
ORCID: <https://orcid.org/0009-0001-0962-7892>**Bulkot Oksana, Kuznetsov Oleksandr**
Taras Shevchenko National University of Kyiv

Стаття присвячена дослідженню проблем і ризиків діяльності міжнародних компаній ІТ-сектору в Україні в умовах повномасштабної війни, економічної нестабільності та трансформації глобального попиту на цифрові послуги. Розкрито значення ІТ-сектору для експортного потенціалу України та інтеграції у міжнародний ринок цифрових послуг. Систематизовано основні групи ризиків, зокрема воєнно-безпекові, економічні, регуляторні, кадрові, технологічні та кібербезпекові. Визначено їхній вплив на операційну стабільність, довіру іноземних замовників, інвестиційну привабливість і конкурентоспроможність компаній. Запропоновано напрями мінімізації ризиків шляхом диверсифікації ринків, розвитку кадрового потенціалу, посилення кіберстійкості та адаптації бізнес-моделей. Обґрунтовано практичне значення системного управління ризиками для збереження стійкості галузі.

Ключові слова: міжнародні ІТ-компанії, ІТ-сектор України, ризики, цифрові послуги, цифрова трансформація, економічна система, бізнес середовище, воєнні виклики.

The article examines the problems and risks faced by international IT companies operating in Ukraine under conditions of full-scale war, macroeconomic instability, regulatory uncertainty and transformation of global demand for digital services. The relevance of the study is determined by the strategic role of the Ukrainian IT sector in the national economy, its export orientation, contribution to foreign currency revenues and integration into the global market for digital services. The article identifies the specific features of international IT companies' activities in Ukraine, where global client orientation is combined with local risks of the Ukrainian business environment. The main groups of risks are systematized, including military and security risks, economic risks, regulatory and tax risks, human capital risks, technological risks and cybersecurity risks. Particular attention is paid to the impact of full-scale war on business continuity, infrastructure stability, staff safety, mobilization processes and foreign customers' trust. The article also analyzes the dependence of Ukrainian IT companies on external demand, the shift from traditional outsourcing models to more complex product-oriented and high-tech solutions, and the growing importance of artificial intelligence, cloud technologies, data analytics and cybersecurity. The study emphasizes that the risks faced by international IT companies in Ukraine are interconnected and may simultaneously affect operational stability, export potential, investment attractiveness and long-term competitiveness. The practical value of the article lies in the proposed directions for risk minimization, including business continuity planning, diversification of markets and client portfolios, development of product-based models, investment in employee skills, strengthening of cybersecurity, regulatory monitoring and improvement of institutional support for the IT sector. The findings may be useful for international IT companies, Ukrainian technology enterprises, investors, business associations and public authorities involved in shaping policies for digital business development and resilience.

Keywords: international IT companies, Ukrainian IT sector, risks, digital services, digital transformation, economic system, business environment, wartime challenges.



Постановка проблеми. Сучасний розвиток ІТ-сектору відбувається в умовах посилення глобальної конкуренції, цифрової трансформації бізнесу, зростання ролі штучного інтелекту, хмарних технологій, кібербезпеки та зміни структури міжнародного попиту на цифрові послуги. Для України ця проблематика має особливе значення, оскільки ІТ-сектор залишається однією з найбільш експортно орієнтованих галузей національної економіки та важливим інструментом інтеграції країни у глобальний ринок цифрових послуг.

Водночас діяльність міжнародних компаній ІТ-сектору в Україні супроводжується комплексом ризиків, зумовлених повномасштабною війною, макроекономічною нестабільністю, змінами регуляторного середовища, кадровими обмеженнями, міграцією фахівців, кіберзагрозами та трансформацією глобального попиту на ІТ-послуги. Ці чинники впливають на операційну стабільність компаній, довіру іноземних замовників, інвестиційну привабливість сектору та довгострокову конкурентоспроможність українських ІТ-команд на міжнародному ринку. Саме тому актуальним є дослідження проблем і ризиків діяльності міжнародних ІТ-компаній в Україні, а також визначення можливих напрямів їх мінімізації в умовах воєнної, економічної та технологічної невизначеності.

Аналіз останніх досліджень і публікацій.

Проблематика розвитку ІТ-сектору України, його експортного потенціалу, інтернаціоналізації та адаптації до умов воєнної й економічної нестабільності активно досліджується у наукових працях і галузевих аналітичних звітах. У сучасних дослідженнях увага зосереджується на стійкості українських ІТ-компаній, їхній ролі у зовнішній торгівлі послугами, кадрових викликах, регуляторних змінах, технологічній трансформації та залежності галузі від глобального попиту.

У працях, присвячених функціонуванню ІТ-сектору України в умовах повномасштабної війни, підкреслюється здатність галузі зберігати операційну стійкість, підтримувати експортну активність і швидко адаптувати бізнес-процеси до кризового середовища [1]. Водночас науковці наголошують, що воєнні ризики, кадрові обмеження, міграція фахівців, зростання країнового ризику та зміна міжнародного попиту суттєво впливають на перспективи подальшого розвитку українських ІТ-компаній [2; 3].

Окремий напрям досліджень стосується експортної орієнтації українського ІТ-сектору

та його інтеграції у міжнародні ринки. У наукових публікаціях зазначається, що залежність від зовнішнього попиту є одночасно джерелом конкурентних переваг і чинником вразливості до глобальних економічних коливань [4; 2].

Галузева аналітика доповнює наукові дослідження актуальними даними про стан української технологічної індустрії. Матеріали IT Ukraine Association, Lviv IT Cluster, НБУ та Centre for Economic Strategy дають змогу оцінити динаміку ІТ-експорту, кадрову структуру галузі, вплив мобілізаційних процесів, зміну глобального попиту та роль ІТ-сектору у валютних надходженнях України [5-9]. Ці джерела підтверджують, що попри збереження стійкості галузі, українські ІТ-компанії працюють в умовах посилення воєнних, економічних і кадрових ризиків.

Регуляторний аспект діяльності ІТ-компаній розкривається у джерелах, присвячених спеціальному правовому режиму «Дія City», податковому навантаженню та інституційним умовам розвитку технологічного бізнесу в Україні [10-12]. Окремої уваги потребують також кібербезпекові та бізнес-ризики: матеріали CERT-UA та Держспецзв'язку свідчать про посилення кіберзагроз, а дослідження European Business Association та American Chamber of Commerce in Ukraine фіксують ключові виклики ведення бізнесу під час війни, зокрема безпеку персоналу, бронювання працівників, енергетичні ризики та регуляторну невизначеність [13-16].

Виділення невирішених частин проблеми. Попри наявність досліджень, присвячених розвитку ІТ-сектору України, його експортному потенціалу, адаптації до умов війни, кадровим викликам, регуляторному середовищу, кібербезпеці та технологічними змінам, недостатньо систематизованим залишається питання комплексного впливу цих чинників саме на діяльність міжнародних ІТ-компаній в Україні в умовах воєнного стану. Більшість наукових і аналітичних джерел розглядає окремі аспекти проблеми – експортну динаміку, кадровий потенціал, податкове регулювання, кіберризики або зміну глобального попиту, тоді як взаємозв'язок воєнно-безпекових, економічних, регуляторних, кадрових і технологічних ризиків потребує подальшого наукового узагальнення. Саме тому актуальним є комплексне дослідження проблем і ризиків діяльності міжнародних компаній ІТ-сектору в Україні та визначення напрямів їх мінімізації.

Формулювання цілей статті. Метою статті є систематизація проблем і ризиків діяльності міжнародних компаній ІТ-сектору в Україні та визначення напрямів їх мінімізації в умовах воєнної, економічної, регуляторної, кадрової й технологічної невизначеності.

Виклад основного матеріалу дослідження. ІТ-сектор України є одним із найбільш міжнародно-інтегрованих сегментів національної економіки. Його розвиток значною мірою пов'язаний з експортом цифрових послуг, співпрацею з іноземними замовниками, участю українських фахівців у глобальних проєктах та діяльністю міжнародних ІТ-компаній на українському ринку. Особливістю цього сектору є те, що значна частина створюваної доданої вартості базується не на матеріальних активах, а на людському капіталі, технологічній експертизі, професійних компетентностях і здатності компаній швидко адаптуватися до змін зовнішнього середовища.

Для України ІТ-сектор має важливе макроекономічне значення, оскільки забезпечує валютні надходження, підтримує зайнятість висококваліфікованих фахівців і сприяє інтеграції країни у міжнародний ринок цифрових послуг. ІТ-послуги залишаються однією з ключових складових експорту послуг України, а комп'ютерні послуги формують основну частину українського експорту ІКТ-послуг [5; 7]. Водночас у 2024 р. спостерігалось погіршення експортної динаміки ІТ-сектору, що було пов'язано як із воєнними ризиками всередині країни, так і зі зниженням глобального попиту на окремі види ІТ-послуг [5; 17].

Специфіка діяльності міжнародних компаній ІТ-сектору в Україні полягає у поєднанні глобальної клієнтської орієнтації з локальними ризиками українського бізнес-середовища. Такі компанії можуть працювати через власні офіси, R&D-центри, дочірні структури, контрактні команди або партнерські моделі співпраці з українськими підрядниками. У кожному з цих випадків їхня діяльність залежить від стабільності операційних процесів, доступності кваліфікованих кадрів, передбачуваності регуляторного середовища, якості цифрової інфраструктури та рівня довіри з боку міжнародних клієнтів.

Ключовою групою ризиків для міжнародних ІТ-компаній в Україні є воєнно-безпекові ризики. Вони проявляються у загрозах для фізичної безпеки персоналу, атаках на енергетичну та цифрову інфраструктуру, перебоях електропостачання, необхідності релокації

працівників, мобілізаційних процесах і зростанні країнового ризику. Для міжнародних компаній ці фактори ускладнюють виконання довгострокових контрактів, дотримання сервісних угод і підтримання довіри іноземних замовників.

Одним із найбільш критичних проявів воєнно-безпекових ризиків є загроза порушення безперервності бізнес-процесів. Для ІТ-компаній це особливо важливо, оскільки їхня діяльність часто пов'язана з підтримкою цифрових продуктів, виконанням проєктів для іноземних клієнтів, роботою команд у різних часових поясах і необхідністю дотримання визначених строків. Водночас український ІТ-сектор продемонстрував високий рівень адаптивності завдяки віддаленим форматам роботи, хмарним технологіям, резервним каналам зв'язку, розподіленням команд і планам безперервності бізнесу [1; 5; 6]. Саме гнучкість бізнес-моделей і цифровий характер послуг стали важливими чинниками стійкості галузі в умовах війни.

Разом із тим воєнні ризики мають не лише операційний, а й репутаційний вимір. Підвищений країновий ризик може впливати на рішення іноземних замовників щодо співпраці з українськими командами, особливо у випадку критично важливих, довгострокових або високоавантажених проєктів. Частина клієнтів може прагнути диверсифікувати портфель підрядників або переносити окремі завдання до країн із нижчим рівнем безпекових ризиків. У такій ситуації для міжнародних ІТ-компаній важливого значення набувають прозора комунікація з клієнтами, підтвердження операційної стійкості, наявність резервної інфраструктури та здатність гарантувати безперервність надання послуг.

Економічні ризики зумовлені високою залежністю українського ІТ-сектору від зовнішнього попиту. Оскільки значна частина ІТ-послуг України орієнтована на іноземних замовників, компанії є чутливими до змін глобальної економічної кон'юнктури, скорочення ІТ-бюджетів клієнтів, коливань інвестиційної активності та посилення конкуренції з боку інших аутсорсингових центрів [2; 4]. Висока експортна орієнтація є водночас перевагою і джерелом вразливості: вона забезпечує валютні надходження та доступ до міжнародних клієнтів, але водночас підвищує залежність від ситуації на ключових зовнішніх ринках.

Окремим економічним викликом є зміна структури міжнародного попиту на ІТ-послуги.

Глобальний ринок поступово переходить від традиційної аутсорсингової моделі до складніших інтегрованих, продуктових і високотехнологічних рішень, пов'язаних зі штучним інтелектом, автоматизацією, хмарними сервісами, аналітикою даних і кібербезпекою [18]. Збереження високих темпів глобальних ІТ-витрат підтверджує, що міжнародний попит на цифрові рішення залишається значним, однак його структура дедалі більше зміщується у бік AI, хмарної інфраструктури, кібербезпеки та автоматизації [19]. Для компаній, які спеціалізуються переважно на сервісному аутсорсингу, це створює ризик поступової втрати конкурентних переваг у разі недостатньої інноваційної активності, слабкої продуктової експертизи або повільного оновлення компетентностей персоналу. До економічних ризиків також належать валютна нестабільність, інфляційний тиск, зростання операційних витрат та загальна невизначеність бізнес-середовища.

Регуляторні та податкові ризики впливають на умови ведення бізнесу, вартість операційної діяльності, інвестиційну привабливість і передбачуваність довгострокового планування. Для міжнародних компаній важливими є стабільність податкового режиму, прозорість адміністрування, валютне регулювання та можливість ефективного здійснення зовнішньоекономічних операцій. Нестабільність правового середовища або часті зміни правил можуть ускладнювати фінансове планування, структурування контрактів і прийняття рішень щодо розширення присутності в Україні.

Одним із ключових інструментів підтримки ІТ-сектору в Україні є спеціальний правовий режим «Дія City», який спрямований на створення сприятливих умов для розвитку технологічного бізнесу, залучення інвестицій і формалізацію нових моделей зайнятості в ІТ-сфері. Водночас для міжнародних компаній важливим є не лише існування такого режиму, а й стабільність його умов. Зміни у податковому навантаженні, критеріях резидентства, правилах оподаткування гіг-спеціалістів або порядку адміністрування можуть формувати додаткову невизначеність для компаній, які планують довгострокову діяльність в Україні [10-12].

Кадрові ризики є одними з найбільш критичних, оскільки основним ресурсом ІТ-сектору є людський капітал. Конкурентоспроможність ІТ-компаній значною мірою залежить від наявності кваліфікованих розробників, інженерів, аналітиків, фахівців із кібербезпеки,

менеджерів проєктів та спеціалістів із новітніх цифрових технологій. В умовах війни кадрові ризики посилюються через мобілізаційні процеси, міграцію фахівців, психологічне навантаження, складність довгострокового планування команд і глобальну конкуренцію за таланти.

За даними галузевих досліджень, українська технологічна індустрія зберігає значний кадровий потенціал, однак водночас стикається з викликами, пов'язаними з мобілізацією працівників, переміщенням фахівців за кордон і необхідністю збереження стабільності команд [6; 7]. Для міжнародних ІТ-компаній ці фактори є особливо важливими, оскільки якість і безперервність роботи команд прямо впливають на виконання контрактів, рівень довіри клієнтів і конкурентоспроможність на глобальному ринку.

Окрім кількісного дефіциту кадрів, актуальним є ризик невідповідності компетентностей фахівців новим вимогам міжнародного ринку. Зростання ролі штучного інтелекту, хмарних технологій, великих даних, кібербезпеки та автоматизації бізнес-процесів підвищує попит на спеціалістів із більш складними технологічними навичками. Компанії, які не інвестують у навчання персоналу, розвиток R&D-напрямів і підвищення кваліфікації команд, можуть втрачати конкурентні позиції на користь гравців, здатних пропонувати більш комплексні й технологічно складні рішення [20; 3; 18].

Технологічні ризики діяльності міжнародних компаній ІТ-сектору в Україні пов'язані з високою швидкістю змін на глобальному ринку цифрових послуг. Розвиток штучного інтелекту, автоматизації, хмарних технологій, великих даних і платформних бізнес-моделей змінює структуру попиту на ІТ-послуги та підвищує вимоги до складності рішень, які пропонують компанії. У таких умовах традиційна аутсорсингова модель, орієнтована переважно на виконання окремих технічних завдань, поступово поступається місцем комплексним рішенням, що поєднують розробку, аналітику, автоматизацію, кібербезпеку, інтеграцію систем і стратегічний цифровий консалтинг.

Для міжнародних ІТ-компаній, що працюють в Україні, технологічна трансформація створює подвійний ефект. З одного боку, вона відкриває можливості для виходу у більш високодохідні сегменти ринку, розвитку продуктових рішень, R&D-напрямів, послуг зі штучного інтелекту, кібербезпеки та аналітики даних. З іншого боку, вона формує ризик

втрата конкурентоспроможності для компаній, які не встигають адаптувати бізнес-модель, оновити компетентності персоналу або перейти від сервісної моделі до створення рішень із вищою доданою вартістю [20; 3; 18].

Кібербезпекові ризики є ще одним критично важливим чинником для міжнародних ІТ-компаній в Україні. В умовах війни Україна залишається об'єктом інтенсивних кібератак, спрямованих на державні установи, критичну інфраструктуру, бізнес, телекомунікаційні системи та цифрові сервіси. Для ІТ-компаній це створює ризики порушення конфіденційності даних, збоїв у роботі цифрових продуктів, фінансових втрат, репутаційних наслідків і зниження довіри міжнародних клієнтів [13; 14].

Особливо актуальними ці ризики є для компаній, які працюють із персональними даними, фінансовими сервісами, хмарною інфраструктурою, критичними бізнес-процесами клієнтів або мають доступ до інформаційних систем іноземних замовників. У таких умовах кібербезпека перестає бути допоміжною функцією і стає обов'язковим елементом конкурентоспроможності. Міжнародні клієнти

дедалі частіше оцінюють не лише вартість і якість ІТ-послуг, а й рівень захисту даних, відповідність стандартам інформаційної безпеки, наявність процедур реагування на інциденти та здатність компанії забезпечити безперервність роботи.

Систематизацію основних ризиків і напрямів їх мінімізації подано в табл. 1.

Ризики діяльності міжнародних компаній ІТ-сектору в Україні мають комплексний і взаємопов'язаний характер. Найбільш критичними у короткостроковому періоді є воєнно-безпекові, кадрові та кібербезпекові ризики, оскільки вони безпосередньо впливають на безперервність операційної діяльності, стабільність команд і довіру міжнародних клієнтів. У середньо- та довгостроковій перспективі особливого значення набувають економічні, регуляторні й технологічні ризики, які визначають інвестиційну привабливість, конкурентоспроможність і здатність компаній адаптуватися до змін глобального ІТ-ринку.

Мінімізація зазначених ризиків потребує формування комплексної адаптаційної стратегії. Для міжнародних ІТ-компаній така стратегія має поєднувати плани безперервності

Таблиця 1

Систематизація ризиків діяльності міжнародних ІТ-компаній в Україні та напрямів їх мінімізації

Група ризиків	Основні прояви	Напрями мінімізації
Воєнно-безпекові	Воєнні дії, загрози інфраструктурі, перебої електропостачання, ризики для персоналу, мобілізаційні процеси	Розподілені команди, плани безперервності бізнесу, резервні канали зв'язку, хмарна інфраструктура, релокаційні сценарії
Економічні	Залежність від зовнішнього попиту, коливання експорту, валютна нестабільність, зростання операційних витрат	Диверсифікація ринків збуту, розширення клієнтського портфеля, розвиток продуктових рішень, довгострокові контракти
Регуляторні та податкові	Зміни податкового законодавства, умови режиму «Дія City», валютні обмеження, складність адміністрування ЗЕД	Моніторинг законодавчих змін, податкове планування, комплаєнс, оцінка умов участі в режимі «Дія City»
Кадрові	Мобілізація, міграція спеціалістів, конкуренція за таланти, психологічне навантаження, дефіцит нових компетентностей	Утримання талантів, навчання персоналу, формування кадрового резерву, підтримка ментального здоров'я, гнучкі формати роботи
Технологічні	Розвиток AI, автоматизація, зміна структури попиту, потреба в інноваціях і R&D	Інвестиції в R&D, розвиток AI-, cloud-, data- та cybersecurity-компетентностей, перехід до рішень із вищою доданою вартістю
Кібербезпекові	Кібератаки, витоки даних, вразливість цифрової інфраструктури, порушення роботи сервісів	Аудит інформаційної безпеки, моніторинг кіберзагроз, захист даних, навчання персоналу, процедури реагування на інциденти

Джерело: сформовано авторами на основі [1-3; 5; 7; 10; 11; 13-16; 18]

бізнесу, диверсифікацію ринків збуту, розвиток продуктових і високотехнологічних напрямів, посилення кібербезпеки, інвестування у підвищення кваліфікації персоналу та системний моніторинг регуляторних змін. Для держави важливими залишаються стабільність податкового середовища, підтримка цифрової інфраструктури, розвиток людського капіталу, вдосконалення механізмів бронювання критичних фахівців і посилення кіберстійкості бізнесу.

Висновки. Проведене дослідження дозволило встановити, що діяльність міжнародних компаній ІТ-сектору в Україні відбувається в умовах комплексного впливу воєнно-безпекових, економічних, регуляторних, кадрових, технологічних і кібербезпекових ризиків. Їхня особливість полягає не лише в наявності окремих загроз, а й у тісному взаємозв'язку між ними. Воєнні ризики посилюють кадрову нестабільність, впливають на довіру іноземних замовників і ускладнюють довгострокове планування. Економічні ризики пов'язані з високою залежністю від зовнішнього попиту, зміною глобальної кон'юнктури та поступовою трансформацією міжнародного ринку ІТ-послуг. Регуляторні й податкові ризики визначають передбачуваність умов ведення бізнесу, тоді як кадрові та технологічні чинники безпосередньо впливають на конкурентоспроможність компаній.

Встановлено, що попри повномасштабну війну та високий рівень невизначеності український ІТ-сектор зберігає значний потенціал для міжнародної діяльності. Його сильними сторонами залишаються високий рівень професійної підготовки фахівців, досвід роботи з іноземними замовниками, експортна орієнтація, гнучкість бізнес-моделей, поширення віддалених форматів роботи та здатність швидко адаптуватися до кризових умов. Водночас ці переваги не усувають наявних ризиків, а потребують системного управління ними з боку компаній, держави та інших стейкхолдерів.

У результаті дослідження систематизовано основні групи ризиків діяльності міжнародних компаній ІТ-сектору в Україні та визначено їхній вплив на операційну стабільність, експортний потенціал, інвестиційну привабливість і довгострокову конкуренто-

спроможність. Найбільш критичними у короткостроковому періоді є воєнно-безпекові, кадрові та кібербезпекові ризики, оскільки вони безпосередньо впливають на безперервність роботи компаній, виконання контрактів і довіру міжнародних клієнтів. У середньодовгостроковій перспективі особливого значення набувають економічні, регуляторні та технологічні ризики, які визначають здатність компаній масштабувати діяльність, залучати інвестиції та переходити до послуг із вищою доданою вартістю.

Практичне значення отриманих результатів полягає у можливості їх використання міжнародними ІТ-компаніями, українськими технологічними підприємствами, інвесторами, органами державної влади та бізнес-асоціаціями для формування ефективних стратегій управління ризиками. Для компаній пріоритетними напрямками є впровадження планів безперервності бізнесу, диверсифікація ринків збуту та клієнтського портфеля, розвиток продуктових і високотехнологічних напрямів, посилення кібербезпеки, інвестування у підвищення кваліфікації персоналу та підтримка кадрової стійкості. Для державної політики важливими залишаються стабільність регуляторного середовища, передбачуваність податкових умов, підтримка цифрової інфраструктури, розвиток людського капіталу та створення умов для збереження інвестиційної привабливості ІТ-сектору.

Таким чином, конкурентоспроможність міжнародних компаній ІТ-сектору в Україні залежатиме від здатності поєднувати адаптацію до поточних воєнних і економічних викликів із довгостроковою технологічною трансформацією. Україна має потенціал залишатися важливим учасником глобального ринку ІТ-послуг, однак реалізація цього потенціалу потребує системного управління ризиками, розвитку інноваційних компетентностей, зміцнення кіберстійкості та підтримання довіри міжнародних партнерів. Перспективи подальших досліджень доцільно пов'язати з кількісною оцінкою впливу окремих груп ризиків на експорт ІТ-послуг, аналізом стратегій адаптації міжнародних ІТ-компаній в Україні та порівнянням українського досвіду з практиками інших країн, що функціонують в умовах підвищеної геополітичної нестабільності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Лісік О.А., Моряк Т.П. Аналіз стану ІТ-сектору України в умовах повномасштабної війни. *Економіка та суспільство*. 2023. № 55. DOI: <https://doi.org/10.32782/2524-0072/2023-55-67>
2. Ковтуненко Ю.В., Дукіна Д.М. Проблеми та перспективи розвитку вітчизняних підприємств ІТ-сфери на міжнародних ринках в умовах глобальних ризиків. *Економічний журнал Одеського політехнічного університету*. 2024. № 3(29). С. 20–26. DOI: <https://doi.org/10.15276/EJ.03.2024.3>
3. Посохов І.М., Пономарьов В.Д. Ризики українських ІТ-компаній в умовах інтеграції до Європейського Союзу та аналіз змін у сфері українських ІТ-технологій. *Вісник Національного технічного університету «ХПІ» (економічні науки)*. 2024. № 1. С. 82–87. DOI: <https://doi.org/10.20998/2519-4461.2024.1.82>
4. Попко О.В., Тивончук П.В. Стратегічний маркетинговий аналіз ринку ІТ-послуг в Україні. *Економіка та суспільство*. 2025. № 71. DOI: <https://doi.org/10.32782/2524-0072/2025-71-58>
5. IT Ukraine Association. Ukraine's IT Exports Declined by Over 4% in 2024. What's Next? 2025. URL: <https://itukraine.org.ua/en/ukraine-s-it-exports-declined-by-over-4-in-2024-what-next/> (дата звернення: 03.07.2026).
6. Lviv IT Cluster. IT Research Ukraine. URL: <https://itcluster.lviv.ua/en/projects/it-research-ukraine/> (дата звернення: 03.07.2026).
7. Lviv IT Cluster. Dynamics of Ukraine's Tech Industry: Results from IT Research Ukraine 2024. Resilience as the New Reality. 2024. URL: <https://itcluster.lviv.ua/en/dynamics-of-ukraines-tech-industry-results-from-it-research-ukraine-2024-resilience-as-the-new-reality/> (дата звернення: 03.07.2026).
8. Національний банк України. Статистика зовнішнього сектору. URL: <https://bank.gov.ua/en/statistic/sector-external> (дата звернення: 03.07.2026).
9. Centre for Economic Strategy. February Economic Review. 2025. URL: <https://ces.org.ua/wp-content/uploads/2025/02/ukrainian-economy-in-war-times-february-2025.pdf> (дата звернення: 03.07.2026).
10. UkraineInvest. IT. URL: <https://ukraineinvest.gov.ua/en/incentives/it/> (дата звернення: 03.07.2026).
11. BDO Ukraine. Diia.City – preferable special tax regime for IT industry in Ukraine. URL: <https://www.bdo.ua/en-gb/ukraine-recovery-1/information-guides-from-bdo-in-ukraine/ukraine-market-entry-and-reconstruction-guide/diia-city-preferable-special-tax-regime-for-it-industry-in-ukraine> (дата звернення: 03.07.2026).
12. PwC Ukraine. Tax & Legal support for Diia City residents. URL: <https://www.pwc.com/ua/en/services/tax-legal-support-diia-city.html> (дата звернення: 03.07.2026).
13. CERT-UA. CERT-UA recorded 4315 cyber incidents in 2024. 2025. URL: <https://cip.gov.ua/en/news/cert-ua-minulogo-roku-opracyovala-4315-kiberincidentiv> (дата звернення: 03.07.2026).
14. State Service of Special Communications and Information Protection of Ukraine. Russian Cyber Operations: H1 2024 Report. 2024. URL: <https://cip.gov.ua/services/cm/api/attachment/download?id=68768> (дата звернення: 03.07.2026).
15. European Business Association. Research and Analytics. URL: <https://eba.com.ua/en/research/doslidzhennya-ta-analityka/> (дата звернення: 03.07.2026).
16. American Chamber of Commerce in Ukraine, Citi Ukraine. Ukraine Wartime Business Assessment: AmCham/Citi Survey Results. 2024. URL: https://chamber.ua/wp-content/uploads/2024/06/AmCham_Citi_Survey_Results_11_06_EN.pdf (дата звернення: 03.07.2026).
17. Digital State UA. Ukraine IT Exports Rise to 43% of Total Trade. 2025. URL: <https://digitalstate.gov.ua/news/it-outsourcing/it-posluhy-staly-holovnym-drayverom-eksportu-ukrayiny-u-2025-rotsi> (дата звернення: 03.07.2026).
18. McKinsey & Company. Technology Trends Outlook 2024. URL: <https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/the-top-trends-in-tech-2024> (дата звернення: 03.07.2026).
19. Gartner. Gartner Forecasts Worldwide IT Spending to Grow 7.9% in 2025. 2025. URL: <https://www.gartner.com/en/newsroom/press-releases/2025-07-15-gartner-forecasts-worldwide-it-spending-to-grow-7-point-9-percent-in-2025> (дата звернення: 03.07.2026).
20. Анголенко В.С. Дослідження розвитку ІТ-ринку України в умовах невизначеності. Актуальні питання економічних наук. 2025. № 8. DOI: <https://doi.org/10.5281/zenodo.14974116>

REFERENCES:

1. Lysik O.A., Moriak T.P. (2023) Analiz stanu IT-sektoru Ukrainy v umovakh povnomasshtabnoi viiny [Analysis of the state of Ukraine's IT sector under full-scale war]. *Ekonomika ta suspilstvo – Economy and Society*, 55. DOI: <https://doi.org/10.32782/2524-0072/2023-55-67>
2. Kovtunenکو Ю.В., Dukina D.M. (2024) Problemy ta perspektyvy rozvytku vitchyznianskykh pidpriemstv IT-sfery na mizhnarodnykh rynkakh v umovakh hlobalnykh ryzykiv [Problems and prospects for the development of domestic

IT enterprises in international markets under global risks]. *Ekonomichnyi zhurnal Odeskoho politekhnichnoho universytetu – Economic Journal of Odessa Polytechnic University*, no. 3(29), pp. 20–26. DOI: <https://doi.org/10.15276/EJ.03.2024.3>

3. Posokhov I.M., Ponomarov V.D. (2024) Ryzyky ukrainskykh IT-kompanii v umovakh intehtatsii do Yevropeiskoho Soiuzu ta analiz zmin u sferi ukrainskykh IT-tekhnologii [Risks of Ukrainian IT companies in the context of EU integration and analysis of changes in Ukrainian IT technologies]. *Visnyk Natsionalnoho tekhnichnoho universytetu "KhPI" (Ekonomichni nauky) – Bulletin of the National Technical University "KhPI" (Economic Sciences)*, no. 1, pp. 82–87. DOI: <https://doi.org/10.20998/2519-4461.2024.1.82>

4. Popko O.V., Tyvonchuk P.V. (2025) Stratehichnyi marketynhovyi analiz rynku IT-posluh v Ukraini [Strategic marketing analysis of the IT services market in Ukraine]. *Ekonomika ta suspilstvo – Economy and Society*, 71. DOI: <https://doi.org/10.32782/2524-0072/2025-71-58>

5. IT Ukraine Association. (2025). Ukraine's IT exports declined by over 4% in 2024. What's next? Available at: <https://itukraine.org.ua/en/ukraine-s-it-exports-declined-by-over-4-in-2024-what-next/> (accessed July 3, 2026)

6. Lviv IT Cluster. (n.d.). IT Research Ukraine. Available at: <https://itcluster.lviv.ua/en/projects/it-research-ukraine/> (accessed July 3, 2026)

7. Lviv IT Cluster. (2024). Dynamics of Ukraine's tech industry: Results from IT Research Ukraine 2024. Resilience as the new reality. Available at: <https://itcluster.lviv.ua/en/dynamics-of-ukraines-tech-industry-results-from-it-research-ukraine-2024-resilience-as-the-new-reality/> (accessed July 3, 2026)

8. National Bank of Ukraine. (n.d.). External sector statistics. Available at: <https://bank.gov.ua/en/statistic/sector-external> (accessed July 3, 2026)

9. Centre for Economic Strategy. (2025). Ukrainian economy during the war: February 2025. Available at: <https://ces.org.ua/wp-content/uploads/2025/02/ukrainian-economy-in-war-times-february-2025.pdf> (accessed July 3, 2026)

10. UkraineInvest. (n.d.). IT. Available at: <https://ukraineinvest.gov.ua/en/incentives/it/> (accessed July 3, 2026)

11. BDO Ukraine. (n.d.). Diia.City – preferable special tax regime for IT industry in Ukraine. Available at: <https://www.bdo.ua/en-gb/ukraine-recovery-1/information-guides-from-bdo-in-ukraine/ukraine-market-entry-and-reconstruction-guide/diia-city-preferable-special-tax-regime-for-it-industry-in-ukraine>

12. PwC Ukraine. (n.d.). Tax & legal support for Diia City residents. Available at: <https://www.pwc.com/ua/en/services/tax-legal-support-diia-city.html> (accessed July 3, 2026)

13. CERT-UA. (2025). CERT-UA recorded 4315 cyber incidents in 2024. Available at: <https://cip.gov.ua/en/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv> (accessed July 3, 2026)

14. State Service of Special Communications and Information Protection of Ukraine. (2024). Russian cyber operations: H1 2024 report. Available at: <https://cip.gov.ua/services/cm/api/attachment/download?id=68768>

15. European Business Association. (n.d.). Research and analytics. Available at: <https://eba.com.ua/en/research/doslidzhennya-ta-analytyka/>

16. American Chamber of Commerce in Ukraine, & Citi Ukraine. (2024). Ukraine wartime business assessment: AmCham/Citi survey results. Available at: https://chamber.ua/wp-content/uploads/2024/06/AmCham_Citi_Survey_Results_11_06_EN.pdf

17. Digital State UA. (2025). Ukraine IT exports rise to 43% of total trade. Available at: <https://digitalstate.gov.ua/news/it-outsourcing/it-posluhy-staly-holovnym-drayverom-eksportu-ukrayiny-u-2025-rotsi> (accessed July 3, 2026)

18. McKinsey & Company. (2024). Technology trends outlook 2024. Available at: <https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/the-top-trends-in-tech-2024>

19. Gartner. (2025). Gartner forecasts worldwide IT spending to grow 7.9% in 2025. Available at: <https://www.gartner.com/en/newsroom/press-releases/2025-07-15-gartner-forecasts-worldwide-it-spending-to-grow-7-point-9-percent-in-2025> (accessed July 3, 2026)

20. Anholenko V.S. (2025) Doslidzhennia rozvytku IT-rynku Ukrainy v umovakh nevyznachenosti [Study of the development of Ukraine's IT market under uncertainty]. *Aktualni pytannia ekonomichnykh nauk – Current Issues of Economic Sciences*. no. 8. DOI: <https://doi.org/10.5281/zenodo.14974116>

Дата надходження статті: 07.07.2026

Дата прийняття статті до публікації: 18.09.2026

Дата публікації статті: 23.09.2026