

UDC 338.2:004:339.9
DOI: 0.24025/2306-4420.77(4).2025.347024

JEL Classification Code: F52, H5
Article's History:
Received: 11.09.2025; Revised: 22.09.2025; Accepted: 01.10.2025.

Volodymyr Blynkov
PhD Student
«KROK» University
03113, 30-32 Tabirna Str., Kyiv, Ukraine
<https://orcid.org/0009-0001-3409-5955>

The impact of globalisation on the economic security of the Ukrainian IT industry

Abstract. The information technology industry is actively developing in modern conditions due to the significant demand for digital technologies worldwide. Along with the intensive development of the IT industry, it is also necessary to note the presence of numerous risks associated with the desire to illegally seize information and financial resources of users and companies. The article examines the impact of globalisation on the economic security of the IT industry in Ukraine in wartime, with an emphasis on the challenges and prospects for development in the context of the European vector and ensuring the competitiveness of domestic IT enterprises in foreign markets. The main factors that affect the economic security of the IT sector, including significant dependence on the economic and political situation in the markets of other countries, cyber threats based on innovative malicious technologies, etc., are studied. The use of SWOT analysis made it possible to identify strengths and weaknesses, as well as opportunities and threats for the IT industry of Ukraine. Based on statistical data (McKinsey, World Bank, Statista) and examples of the activities of leading IT companies, an assessment of the vector of the information technology sector development was carried out. The positive impact of globalisation and digitalisation on the active development of the IT sector in Ukraine was determined by expanding its presence in foreign markets, attracting foreign investments, and adopting advanced technologies. Negative factors in the development of domestic companies in the field of information technology include dependence on foreign markets and cyberattacks, which is especially relevant in the conditions of war in Ukraine. Recommendations for the transformation of the IT industry of Ukraine in the conditions of global and military challenges, which will allow for intensive development in the conditions of post-war recovery, are presented

Keywords: digital technologies, investments, innovations, software, risks, cyberattacks, digitalization

*Corresponding author



Володимир Блинков

Аспірант

Університет економіки та права «КРОК»

03113, вул. Табірна, 30-32, м. Київ, Україна

<https://orcid.org/0009-0001-3409-5955>

Вплив глобалізації на економічну безпеку ІТ-галузі України

Анотація. Галузь інформаційних технологій активно розвивається в сучасних умовах у зв'язку зі значним попитом на цифрові технології у глобальному просторі. Поряд з інтенсивним розвитком ІТ-індустрії також необхідно відзначити наявність численних ризиків, які пов'язані з бажанням у незаконний спосіб заволодіти інформацією та грошовими ресурсами користувачів і компаній. У статті досліджується вплив глобалізації на економічну безпеку ІТ-галузі України в умовах війни з акцентом на виклики та перспективи розвитку в контексті європейського вектора та забезпечення конкурентоспроможності вітчизняних ІТ-підприємств на зовнішніх ринках. Досліджено основні фактори, які впливають на економічну безпеку ІТ-сектору, зокрема істотну залежність від економічної та політичної ситуації на ринках інших країн, кіберзагроз на основі інноваційних шкідливих технологій тощо. Використання SWOT-аналізу дозволило визначити сильні та слабкі сторони, а також можливості й загрози для ІТ-галузі України. На основі статистичних даних (McKinsey, Світовий банк, Statista) та прикладів діяльності провідних ІТ-компаній було проведено оцінювання вектора розвитку сфери інформаційних технологій. Визначено позитивний вплив глобалізації та цифровізації на активний розвиток ІТ-сектору в Україні шляхом розширення присутності на зовнішніх ринках, залучення іноземних інвестицій та передових технологій. До негативних чинників розвитку вітчизняних компаній у сфері інформаційних технологій відноситься залежність від іноземних ринків та кібератак, що особливо актуально в умовах війни на території України. Представлено рекомендації трансформації ІТ-галузі України в умовах глобальних і воєнних викликів, що дозволять інтенсивного розвиватися в умовах післявоєнного відновлення

Ключові слова: цифрові технології, інвестиції, інновації, програмне забезпечення, ризики, кібератаки, цифровізація

Вступ

Глобалізаційні процеси істотно впливають на більшість країн світу та види економічної діяльності на національному рівні. Інтеграція країни у міжнародне економічне середовище є важливою компонентою забезпечення сталого економічного розвитку завдяки отриманню доступу до міжнародних ринків, трансферу інноваційних технологій, залученню іноземних інвестицій тощо. Для України ІТ-галузь в останнє десятиліття почала відігравати дуже істотну роль, оскільки дає можливість експортувати високоякісні цифрові продукти, а вітчизняні компанії у сфері інформаційних технологій характеризуються високим рівнем конкурентоспроможності на глобальному ринку інновацій. ІТ-галузь України еволюціонує під впливом глобалізаційних процесів, адаптуючись до основних тенденцій на зовнішніх ринках з метою задоволення наявного попиту. Особливу увагу при формуванні ефективної політики стимулювання розвитку ІТ-ринку в Україні необхідно приділяти ключовим трендам в США та ЄС, які формують найбільший попит на цифрові продукти від українських компаній. Міжнародний ринок характеризується турбулентністю внаслідок дії комплексу соціально-економічних та політичних факторів, які в Україні посилюються завдяки війні, що призводить до багатьох викликів для національного ІТ-сектору. Актуальність дослідження пояснюється необхідністю визначення напрямів забезпечення сталого розвитку економіки України у

довгостроковій перспективі за рахунок ІТ-галузі, яка виступає важливим джерелом валютних надходжень. Наукова новизна роботи полягає у детальному оцінюванні викликів для економічної безпеки ІТ-галузі України з позиції глобалізації. Мета статті – провести комплексний аналіз впливу глобалізаційних процесів на економічну безпеку ІТ-сектору України в умовах воєнного часу, виявити ключові проблеми і можливості розвитку з урахуванням європейської інтеграції та підвищення конкурентоспроможності українських компаній на міжнародних ринках.

Огляд літератури

У дослідженнях О. Navryliuk *та ін.* (2023) та S. Spivakovskyy *та ін.* (2021) оцінюється вплив цифрових трансформацій на економічну безпеку в Україні. Проводиться комплексний аналіз дії цифровізації на національну економічну систему та потенційні вектори її трансформації. На основі статистичних даних McKinsey та Світового банку було ідентифіковано основні переваги та потенційні ризики функціонування економічної системи у цифровому середовищі. Значна увага приділяється проблемам економічної безпеки на рівні національної господарської системи та окремих видів економічної діяльності. До основних негативних чинників, які впливають на економічну безпеку, віднесено проблеми «цифрової нерівності», деструктивні явища на ринку праці, промислове шпигунство, незаконні дії з персональними даними тощо. Авторами представлено механізм нівелювання впливу негативних чинників цифрової трансформації на економічну безпеку України в сучасних умовах.

Комплексний аналіз загроз і ризиків екологічної та економічної безпеки України в умовах війни проведено у роботах S. Onyshchenko *та ін.* (2023), О. Yakushev *та ін.* (2024). Доведено, що військові дії в Україні суттєво вплинули на погіршення екологічної ситуації у багатьох регіонах країни. Знищення інфраструктурних об'єктів істотно збільшує ризики настання техногенних катастроф, а подолання наслідків забруднення вимагатиме значних ресурсів упродовж тривалого періоду часу. Розкрито взаємозв'язок між загрозами екологічній та економічній безпеці держави в умовах повномасштабного вторгнення. Руйнування інфраструктурних об'єктів призводить до погіршення екології, що має прямий та опосередкований вплив на економічну безпеку України. Авторами систематизовано ключові компоненти загроз екологічній та економічній безпеці країни, що дозволить забезпечити реалізацію заходів сталого розвитку України у період післявоєнного відновлення.

Дослідження С. McCaffrey та N. Poitiers (2024) присвячене проблемам забезпечення економічної безпеки ЄС у постпадемічний період, що характеризується комплексом соціально-економічних викликів, включаючи війну на території України. Проводиться комплексне дослідження загроз, які призводять до кризових явищ в економіках європейських країн. Наведено приклад економічного примусу Китаєм компаній з Литви шляхом торговельних обмежень і припинення співпраці у різних секторах економіки. Наголошується на необхідності комплексного оцінювання потенційних загроз економічній безпеці, оскільки значна кількість політиків приділяє увагу лише експортно-імпортним операціям. Розглянуто перспективи негативного впливу економічного примусу у перспективі, що пов'язано з відсутністю видимих короткострокових загроз і введенням в оману урядів країн ЄС. Автори наголошують на необхідності запровадження цілеспрямованої політики в певних видах економічної діяльності з метою оптимізації експортно-імпортних операцій завдяки застосуванню інструментів *ex-post*.

У науковій праці О. Pyash *та ін.* (2021) представлено теоретико-прикладну модель аналізу промислово-технологічного розвитку в системі економічної безпеки. Для комплексного оцінювання рівня економічної безпеки та її окремих складових запропоновано використовувати систему показників. На основі кореляційно-регресійного аналізу

досліджено взаємозв'язки промислово-технологічного розвитку та рівня економічної безпеки. Проведено прогнозування промислово-технологічного розвитку на основі системи показників, що дозволяє оцінити основні тенденції рівня економічної безпеки. Виокремлені ключові фактори впливу на промислово-технологічний розвиток доцільно використовувати для формування ефективних управлінських рішень, які дозволять забезпечити економічну безпеку у довгостроковій перспективі.

Інтелектуальний капітал в Суспільстві 5.0 розглядається як основний фактор формування економічної безпеки підприємств (Mishchuk *et al.*, 2022). Розглянуто перелік основних структурних складових інтелектуального капіталу та визначено істотність їх впливу на формування економічної безпеки підприємства. Ідентифіковано базові критерії оцінювання ефективності використання інтелектуального капіталу в процесі забезпечення економічної безпеки. Визначено, що існують ключові групи сучасних компетентностей працівників, які необхідні для формування економічної безпеки в умовах глобалізації та цифровізації. Оптимізація взаємозв'язків між структурними елементами інтелектуального капіталу сприяє стійкості економічної безпеки підприємства у довгостроковому періоді.

Y. Matyskevicius *та ін.* (2021) досліджують вплив технологій блокчейн на економічну безпеку в умовах цифрових трансформацій. Відповідно до особливостей функціонування блокчейн описано особливості негативного впливу на окремі види економічної діяльності та національну систему загалом з позиції економічної безпеки. Розкрито виклики, з якими може стикнутись економічна система в епоху цифрових трансформацій та зростання використання інформаційних систем на основі технологій блокчейн. Розглянуто основні риси багатогранної концепції економічної безпеки та важливість її розвитку на всіх рівнях для забезпечення ефективного функціонування економічної системи на всіх рівнях. Для дослідження впливу блокчейн було обрано такі галузі, як електронна комерція, платежі та логістика. Оскільки блокчейн відноситься до важливої складової Індустрії 4.0, обґрунтовано доцільність її використання у поєднанні зі штучним інтелектом, Інтернетом речей, великими даними тощо.

Дослідженню фінансової стабільності як важливої складової економічної безпеки присвячено наукову працю K. Anand *та ін.* (2022). Наголошується на істотному впливі кібератак на функціонування фінансово-банківських інституцій та інтенсивному зростанні панічних настроїв серед усіх учасників ринку у випадку виникнення загроз. Доведено, що сучасна цифрова інфраструктура виступає як дієвий інструмент захисту фінансового сектору. Забезпечення безпеки банків і фінансових компаній передбачає залучення достатнього обсягу інвестицій, а реалізовані заходи слугують формуванню сучасної системи економічної безпеки в країні на всіх рівнях.

Комплексний аналіз економіки кібербезпеки проведено у роботі M. Kianpour *та ін.* (2021) з метою визначення напрямів сталого розвитку цифрових екосистем. Обґрунтовано доцільність досліджень щодо ідентифікації напрямів оптимізації управління процесами у сфері кібербезпеки, що дозволяє досягти стійкості економіки на мікро-, макро- та мезорівнях. Авторами узагальнено досвід з наукових статей та досліджень у сфері економіки кібербезпеки відповідно до її мультидисциплінарності, оскільки відзначається поєднання економіки, соціології, психології, права, політології та інформатики. Зазначено, що значна кількість моделей економіки кібербезпеки характеризувалася нереалістичністю або спрощенням фундаментальних передумов. Проте в останні роки в наукових колах відзначається переорієнтація на динамічні, стохастичні та узагальнюючі моделі, які дозволяють більш точно описувати процеси в економіці кібербезпеки.

T. Shmatkovska *та ін.* (2022) досліджують особливості забезпечення економічної безпеки підприємств в умовах активного розвитку та впровадження інформаційних технологій. Доведено, що процеси цифровізації приводять до активної трансформації діяльності підприємств та формування якісно нових моделей бізнес-стратегій. Завдяки

інноваціям підприємства отримують можливість посилити рівень економічної безпеки та забезпечити конкурентоспроможність упродовж тривалого часового періоду. Автори розглядають економічну безпеку підприємства як структуровану систему елементів управління суб'єктом підприємницької діяльності, які використовуються для забезпечення ефективного розвитку підприємств в умовах турбулентності зовнішнього середовища.

Визначенню ролі цифрової трансформації в забезпеченні економічної безпеки присвячено роботи О. Kalinin *та in.* (2024), О. Якушев (2024). Наголошується на важливості цифрових технологій у процесі покращення інвестиційного клімату, що стимулює економічне зростання національної системи та сприяє її стійкості в довгостроковій перспективі. Ефективність і прозорість інвестиційної політики держави істотно збільшують ймовірність залучення грошових ресурсів на зовнішніх ринках та сприяють інтенсифікації економічного розвитку (Новицька, 2014)). Доведено, що активний розвиток штучного інтелекту, автоматизації, великих даних та інших цифрових технологій позитивно впливає на економічну безпеку.

Представлені напрями наукових досліджень є важливими для сталого розвитку національної економічної системи, проте доцільно розширити дослідницьку діяльність шляхом вивчення особливостей формування економічної безпеки ІТ-сектору, який відіграє ключову роль в Україні та виступає як важливе джерело наповнення Державного бюджету.

Мета статті – дослідження впливу процесів глобалізації на економічну безпеку ІТ-галузі України в умовах війни, визначення основних викликів та перспектив розвитку у контексті європейського вектора розвитку та забезпечення конкурентоспроможності вітчизняних підприємств на зовнішніх ринках.

Матеріали та методи

Інформаційною базою статті слугували наукові праці вітчизняних та зарубіжних авторів, статистичні дані міжнародних організацій та компаній (McKinsey, Світовий банк, Statista), а також власні узагальнення. Методологічною основою дослідження є системний підхід, що дозволив комплексно оцінити причинно-наслідкові зв'язки між процесами глобалізації, військовими викликами та економічною безпекою ІТ-галузі України. SWOT-аналіз використано для ідентифікації сильних і слабких сторін, можливостей та загроз для ІТ-сектору України. Формулювання висновків та рекомендацій щодо посилення економічної безпеки ІТ-галузі базується на методах узагальнення, синтезу та порівняльного аналізу.

Результати та обговорення

Українська економічна система характеризується значним розвитком аграрного та промислового секторів, досягаючи високих конкурентних позицій за окремими напрямками на міжнародних ринках. Поряд з цим, наявна система освіти в країні дозволяє населенню отримати актуальні знання та практичні навички, які роблять робочу силу конкурентоспроможною на глобальному рівні. Свідченням якості економічно активного населення в країні є розвиток індустрії інформаційних технологій, що характеризується високим рівнем оплати праці та посідає друге місце в українському експорті. За 2024 р. у структурі ВВП питома вага експорту ІТ-індустрії становила 3,4 % (Ukrainian IT industry..., 2025). Незважаючи на війну в Україні, розробка програмного забезпечення відноситься до пріоритетних сфер діяльності, акумулюючи значні інвестиційні ресурси та дозволяючи забезпечити економічне зростання у довгостроковій перспективі. На рисунку 1 представлено динаміку фактичних і прогнозних значень доходів ІТ-сектору в Україні за 2016–2030 рр.

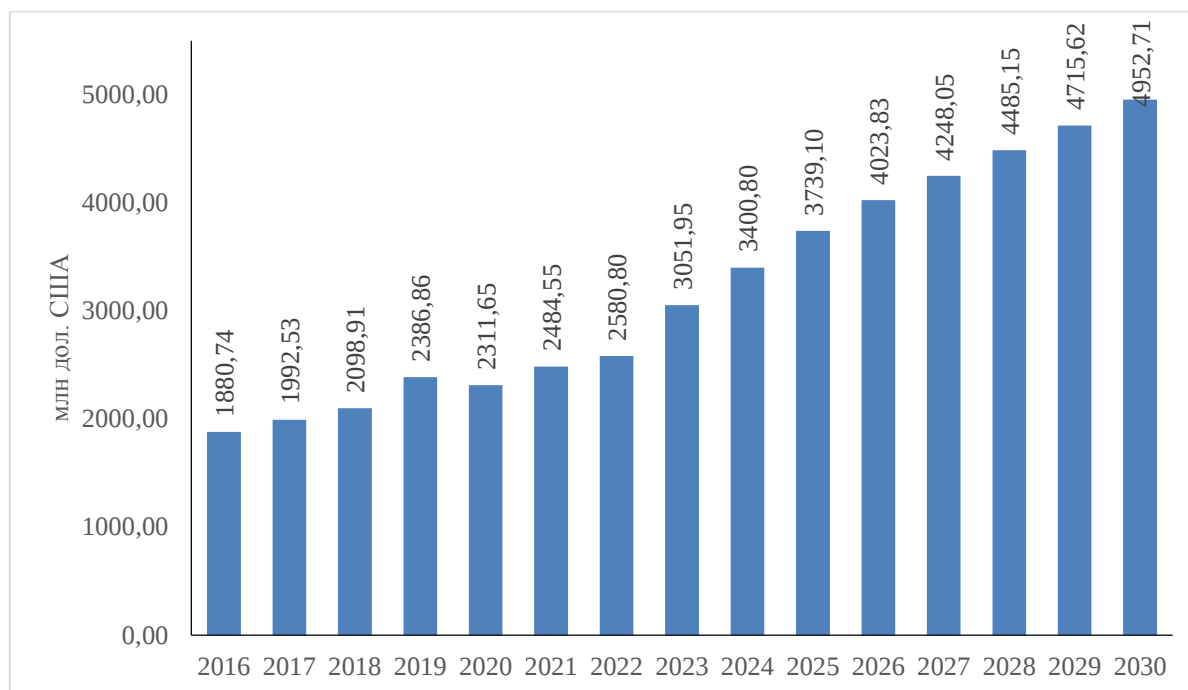


Рисунок 1. Динаміка доходів ІТ-галузі в Україні за 2016–2030 рр.

Джерело: складено автором за (IT Services – Ukraine, 2025)

За оцінками Statista Market Insights, незважаючи на військові дії, в Україні очікується поступове зростання ринку ІТ. Так, до кінця 2025 р. оціночне значення доходів передбачається близько 3,74 млрд дол., а в 2030 р. значення досліджуваного показника може зрости до 4,95 млрд дол. Середньорічне значення темпу зростання ІТ-сектору в Україні впродовж 2025–2030 рр. прогнозується на рівні 5,78 %. У структурі індустрії інформаційних технологій лідируюче місце посідає ІТ-аутсорсинг, що пов'язано з активною співпрацею вітчизняних компаній з іноземними замовниками. Привабливість ІТ-індустрії для висококваліфікованої робочої сили в Україні пояснюється високим рівнем оплати праці. Слід відзначити, що наявні прогнозні значення можуть бути відкориговані відповідно до зміни ситуації в Україні та на зовнішніх ринках упродовж майбутніх періодів часу. Турбулентність зовнішнього економічного середовища та інтенсифікація процесів діджиталізації відносяться до важливих факторів, які безперервно впливають на економіку України, включаючи сектор інформаційних технологій.

ІТ-сектор в Україні функціонує згідно з тенденціями, які притаманні для глобальної індустрії інформаційних технологій. На національному ринку функціонують продуктові та аутсорсингові компанії, які працюють за різними моделями реалізації бізнес-процесів. У цьому секторі близько 80 % українських компаній працює за моделлю аутсорсингу, співпрацюючи з клієнтами з високорозвинених країн (США, ЄС та Канада). Співпраця передбачає розробку та тестування програмного забезпечення, а також його підтримку. Поряд з цим, продуктові компанії мають значний потенціал до зростання завдяки можливості розробки власних конкурентоспроможних продуктів та виведенню їх на глобальний ринок.

На рисунку 2 наведено лідерів ІТ-сектору в Україні за доходами у 2024 р., серед яких лідируючі позиції займає EPAM. Лідер ринку надає послуги у таких сферах, як розробка програмних продуктів, консалтинг, цифрова трансформація, штучний інтелект, аналітика даних, запровадження інноваційних рішень тощо. Україна входить до 50 країн, в яких розміщені представництва EPAM. Компанія не лише є великим платником податків та роботодавцем у країні, а також реалізує низку освітніх проєктів у рамках співпраці з українськими університетами. Офіси EPAM розміщуються в 11 містах України, а лідерами за чисельністю спеціалістів є Київ (понад 4700 осіб), Львів (понад 2600 осіб) та Харків (понад 1000 осіб) (EPAM, n.d.).

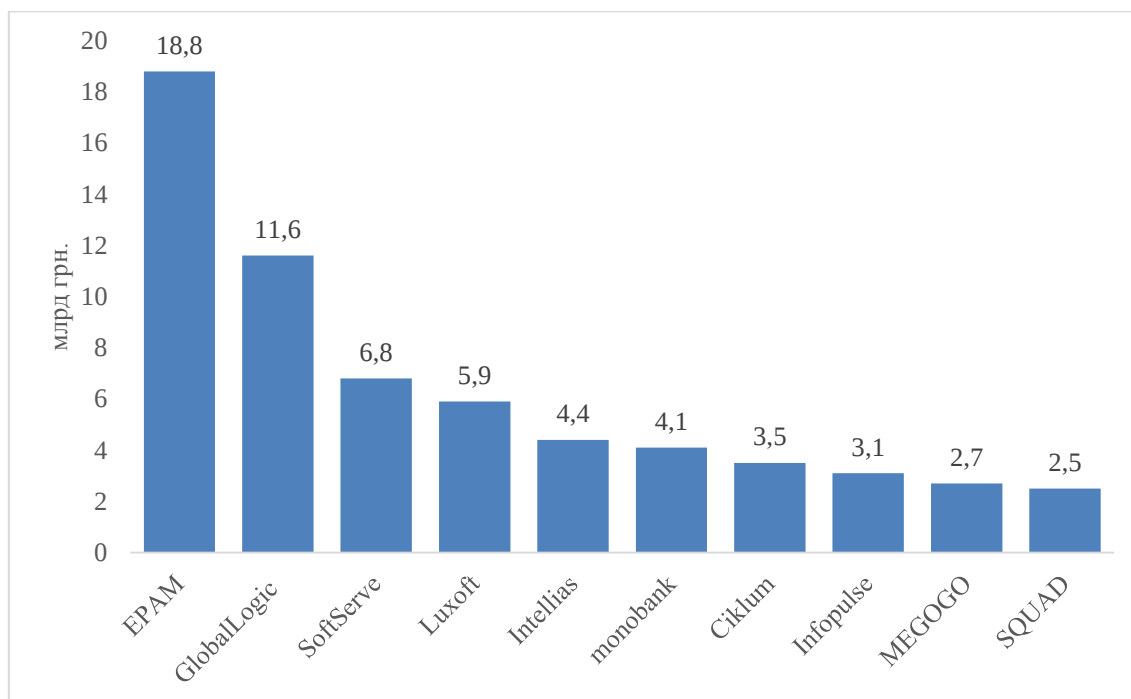


Рисунок 2. Топ-10 ІТ-компаній в Україні за доходами у 2024 р.

Джерело: складено автором за (Які українські ІТ-компанії..., 2025, Березень, 21)

Процеси глобалізації комплексно впливають на розвиток ІТ-сектору, що пов'язано з наявністю можливостей інтенсивного зростання та проявом системи потенційних ризиків. Забезпечення економічної безпеки ІТ-сектору в Україні в сучасних умовах передбачає реалізацією органами державного управління ефективної політики, яка сприятиме розвитку вітчизняних інноваційних підприємств відповідно до трендів глобального ринку. В таблиці 1 представлено SWOT-аналіз ІТ-галузі України, що дозволить ідентифікувати сильні та слабкі сторони, а також можливості і загрози.

На функціонування ІТ-галузі в Україні істотний вплив справляє війна, що призводить до явних негативних наслідків і потенційних ризиків у довгостроковій перспективі. Незважаючи на розміщення офісів компаній у відносно безпечних регіонах, деструктивні чинники військових дій негативно впливають на моральний стан працівників, можливість забезпечувати ефективність функціонування різноманітних підрозділів ІТ-компаній, укомплектованість висококваліфікованим персоналом, економічно обґрунтований рівень рентабельності тощо.

Таблиця 1. SWOT-аналіз ІТ-галузі України

Сильні сторони	Слабкі сторони
- Відповідність менеджменту ІТ-компаній сучасним міжнародним стандартам, що дозволяє забезпечити сталий розвиток у довгостроковій перспективі на глобальних ринках. - Присутність у глобальному просторі вітчизняних ІТ-компаній, які мають сильні бренди та виступають як важливий експортер послуг в Україні, займаючи важливу частку у податкових надходженнях країни. - Орієнтація на запровадження інновацій та розробку передових продуктів (штучний інтелект, блокчейн тощо), які користуються підвищеним попитом у глобальному середовищі. - Позитивний вплив на ринок праці завдяки створенню попиту на висококваліфікованих працівників та конкурентоспроможному рівню заробітної плати.	- Залежність від іноземних клієнтів, дефіцит власної елементної бази, що призводить до вразливості національної ІТ-галузі в системі глобальних ланцюгів постачань. - Відсутність сучасної корпоративної культури у багатьох національних ІТ-компаніях, що проявляється на умовах праці та стимулюванні ефективної роботи. - Невідповідність розвитку ринку праці сучасним стандартам, що проявляється у низькій адаптивності системи освіти до інтеграції інновацій, відставанні профільного законодавства від глобальних тенденцій та наявній системі соціально-трудових відносин.

Продовження таблиці 1

Можливості	Загрози
- Вдосконалення державної програми щодо розвитку ринку ІТ-технологій та стимулювання вітчизняних розробників цифрових продуктів активізувати діяльність на глобальних ринках. - Інтенсивне зростання глобальної економічної системи та підвищення попиту на сучасні цифрові продукти. - Вдосконалення цифрової інфраструктури та розвиток різноманітних сервісів державного і приватного секторів, які сприятимуть розвитку ІТ-ринку в Україні. - Підписання угод з транснаціональними корпораціями та урядами інших країн з метою отримання інвестицій та передових технологій, які будуть актуальними в період післявоєнного відновлення України.	- Нестабільність функціонування компаній внаслідок війни: знищення інфраструктури, блекауту, вплив та мобілізація фахівців, зниження довіри замовників з інших країн. - Складна демографічна ситуація внаслідок скорочення чисельності населення та зростання частки людей старших вікових груп, що посилюється внаслідок міграції значної чисельності населення в умовах війни, призводить до стагнації ІТ-галузі у довгостроковій перспективі. - Кризові явища на міжнародному ринку в умовах значної конкуренції, що може призвести до істотного скорочення іноземних клієнтів. - Неефективна регулятивна політика та високий рівень корупції, що пригнічують розвиток приватного бізнесу. - Економічна нестабільність внаслідок значної інфляції та зростання державного боргу, які посилюють ризики щодо вільного доступу до передових технологій вітчизняним компаніям, що мають обмежені грошові ресурси.

Джерело: складено автором

Розглянемо більш детально виклики для економічної безпеки ІТ-галузі України з позиції глобалізації:

1. Втрата інтелектуального потенціалу. Низький рівень життя в Україні порівняно з іншими країнами світу (в першу чергу ЄС та США) нівелювався для працівників у сфері інформаційних технологій відносно високою оплатою праці порівняно з локальними цінами на продукти харчування та послуги. В умовах війни істотно зросли ціни на усі товари та послуги, а за певними категоріями продуктів вартість перевищила аналоги в інших країнах світу. Посилилась небезпека для життя та здоров'я внаслідок атак населених пунктів та знищення інфраструктури в усіх регіонах країни. В результаті відзначається релокація працівників ІТ-сфери в інші країни з метою отримання кращих умов праці та безпеки. Слід зазначити, що у передвоєнний період значна кількість програмістів і тестувальників чоловічої статі були переведені в іноземні офіси компаній, що також негативно вплинуло на розвиток ринку інформаційних технологій в Україні. Високий рівень привабливості ІТ-сфери в Україні дає можливість певним чином компенсувати вплив досвідчених працівників новими кадрами, проте відбувається втрата частини інтелектуального потенціалу країни, що в підсумку призводить до недоотримання податкових надходжень і не дозволяє певною мірою реалізувати потенціал економічного зростання.

Система вищої освіти в умовах війни та кризових явищ в економіці змушена реалізовувати реформи з метою оптимізації використання наявних грошових ресурсів. Порівняно з багатьма освітніми програмами, для майбутніх фахівців в ІТ-сфері у 2025 р. заплановано виділити відносно багато бюджетних місць на бакалавраті (у 2024 р. для ЗВО: 122 «Комп'ютерні науки» – 3841 місце; 121 «Інженерія програмного забезпечення» – 2400 місць; 123 «Комп'ютерна інженерія» – 1402 місця), проте окреслені обсяги не відповідають потребам ринку та не дозволяють повною мірою реалізувати потенціал майбутньої висококваліфікованої робочої сили (спеціальності, яким держава виділила найбільше бюджетних місць у 2024 р.). Фактор війни та безкоштовні бакалаврські програми у сфері інформаційних технологій в країнах ЄС стимулюють значну кількість потенційних абітурієнтів виїжджати з України.

2. Залежність від зовнішніх ринків і кон'юнктури. Інтеграція України у глобальний економічний простір упродовж останніх десятиліть призвела до істотної залежності країни

від зовнішніх ринків. Значна кількість товарів та послуг імпортується в Україну у зв'язку з відсутністю якісних вітчизняних аналогів. У минулому лідерами серед національних виробників електроніки та комп'ютерної техніки були львівський завод «Електрон», київський завод «Радіоприлад» та харківський приладобудівний завод ім. Шевченка. На цьому етапі розвитку апаратне забезпечення переважно експортується з Китаю (плати, мікросіпи, датчики, процесори тощо), а в Україні здійснюється часткове/повне збирання необхідного електронного та комп'ютерного обладнання. Відповідно, вітчизняні розробники програмного забезпечення повинні враховувати у своїй діяльності імпортозалежність національної економічної системи від іноземного апаратного забезпечення.

Специфіка розвитку глобального ринку споживчої електроніки, особливо сучасних гаджетів (смартфони, ноутбуки, планшети, розумні годинники) впливає на українських розробників з позиції якості наявного попиту та рівня конкуренції. Споживачі масових цифрових продуктів в першу чергу будуть звертати увагу на якісні характеристики, що відкриває перед українськими інноваційними компаніями значні перспективи. До вдалих прикладів слід віднести Grammarly – AI-помічник з написання та редагування текстів, GitLab – популярна DevOps-платформа, Ring – цифрові рішення у сфері безпеки (Dedicated Software Development Teams in Ukraine). Поряд з цим, на ринку промислового обладнання можуть діяти специфічні неринкові закони щодо можливості виробників програмного забезпечення вигравати контракти на основі конкурентних переваг. У США при розробці програмного забезпечення для державних та оборонних потреб уряд надає перевагу співпраці з Palantir та Microsoft (Palantir and Microsoft Partner). Отже, для українських ІТ-компаній на ринку США наявний доступ лише у некритичні сектори економіки.

Важливими зовнішніми факторами впливу на діяльність українських інноваційних компаній є політико-правові та економічні чинники. Залежно від ситуації в окремій країні світу та у глобальному економічному середовищі формується попит на програмне забезпечення від іноземних розробників. Перегрів ринку ІТ в США у 2022–2023 рр. у постпандемічний період призвів до скорочення більше 60 тис. працівників у таких компаніях, як Amazon, Google, Meta, Microsoft (Tech employees..., 2025, March 19). Кризові явища на ІТ-ринку та скорочення попиту відобразилось на доходах усіх учасників, включаючи українські компанії-розробники. Введені Д. Трампом тарифи на рівні 10 % для України не призвели до значних втрат у вітчизняній ІТ-індустрії, а деякі експерти бачать потенційні можливості для українських технологічних компаній внаслідок більш жорсткої тарифної політики США відносно інших країн світу, які активно продавали програмне забезпечення на американському ринку. На початок 2025 р. основними конкурентами для українських розробників програмного забезпечення у світі є фахівці з Індії, Польщі, Філіппін та В'єтнаму (9 best countries..., 2025, March 7). Кризові ситуації в економіці або зміна політико-правового вектора можуть істотно збільшити ризики втрати конкурентоспроможності українських компаній на ринку США. На цьому етапі розвитку представлений сценарій є малоімовірним, проте доцільно реалізовувати комплекс заходів щодо диверсифікації потенційних ризиків. В Європі Україна відноситься до лідерів на ринку розробки програмного забезпечення, проте виникає потреба у постійному дотриманні високих стандартів якості цифрових продуктів – Загальний регламент про захист даних (GDPR).

3. Загрози кібербезпеці та втраті цифрового суверенітету. Війна в Україні та геополітична напруга істотно посилюють вразливість вітчизняного ІТ-сектору. Кібератаки стали ефективною зброєю у контексті гібридної війни, оскільки дозволяють завдавати значної шкоди обороноздатності країни та окремим видам економічної діяльності. Основні форми кібератак реалізуються таким чином: DDoS-атаки, атаки на критичну інфраструктуру, фішинг і соціальна інженерія, шкідливе програмне забезпечення, шпигунство та витік даних. Внаслідок кібератак ІТ-компанії в Україні можуть зазнати як прямих, так і опосередкованих збитків:

- Фінансові втрати. Подолання наслідків кібератак та компенсація моральних і матеріальних збитків клієнтів вимагає від ІТ-компаній виділення значних грошових ресурсів. Так, 12 грудня 2023 р. Київстар зазнав кібератаки, внаслідок якої відбувся збій мобільного зв'язку та Інтернету у мільйонів абонентів. На подолання негативних наслідків мобільному оператору знадобилось витратити близько 10 % річного виторгу (близько 3,6 млрд грн) (Kyivstar Completes Preliminary Assessment). Впродовж війни в Україні фінансових втрат на постійній основі зазнають багато компаній, а в сфері цифрових технологій можна виділити Monobank, Triacom, Kim та ін.

- Втрата клієнтів і ділової репутації. В глобальному середовищі існує велика кількість компаній, які працюють на ринку ІТ, поряд з корпораціями також функціонують середні та малі суб'єкти підприємницької діяльності. Високий рівень конкуренції у глобальному середовищі передбачає постійне вдосконалення якості надання послуг відповідно до існуючих викликів. Недоліки у роботі вітчизняних компаній на ринку інформаційних технологій особливо можуть посилюватись в умовах війни, що призводить до репутаційних втрат і переорієнтації замовників на іноземних розробників цифрових рішень. Відновлення ділової репутації – складний процес, що вимагає значних фінансових ресурсів та часу.

- Ризики втрати цифрового суверенітету. В умовах війни в Україні існують істотні ризики щодо знищення даних у реєстрах або викрадення приватних даних з метою здійснення протиправних дій. У 2022 р. відбулось переміщення певних баз даних органів державного управління з України до Польщі, також відзначено міграцію цінних реєстрів до інших країн (Ukraine has begun moving..., 2022, June 14). У сфері бізнесу доцільно звернути увагу на співпрацю між Приватбанком та AWS, в результаті було перенесено 270 застосунків і 4 петабайти клієнтських даних на закордонні сервери з метою забезпечення безпеки (Migrating from on premises..., 2024). Співпраця з міжнародними компаніями є позитивною, оскільки сприяє трансферу технологій та забезпеченню високого рівня якості продукції вітчизняних компаній. Поряд з цим, існують потенційні ризики втрати даних або цифрового суверенітету на мікро- та макрорівнях.

- Витік комерційних даних. Важливим елементом конкурентоспроможності компаній виступають комерційні таємниці, за рахунок яких можливо забезпечити переваги порівняно з іншими учасниками ринку. Специфіка діяльності ІТ-компаній передбачає зберігання інноваційних рішень у цифровому вигляді (код, алгоритми, патентні розробки) та пропонування споживачам інноваційних продуктів на постійній основі з метою задоволення наявного попиту. Одним із резонансних прикладів у 2025 р. є звинувачення OpenAI китайського розробника DeepSeek у несанкціонованому використанні моделей американської компанії для навчання своєї системи (OpenAI). В цифрову епоху викрадення комерційних даних в Україні та інших країнах світу відбувається на постійній основі, чому сприяла інтеграція національних цифрових систем на рівні органів державного управління та окремих суб'єктів підприємницької діяльності до глобального простору.

Висновки

Отже, в умовах глобалізації спостерігається комплексний вплив системи чинників на економічну безпеку ІТ-галузі України, в результаті виникають нові можливості для якісних трансформацій та значні виклики, які спричинені військовими діями. ІТ-сектор залишається ключовим драйвером економічного зростання України, забезпечуючи 3,4 % ВВП за рахунок експорту інноваційних послуг у 2024 р. та демонструючи прогнозоване зростання доходів до 4,95 млрд дол. до 2030 р. Військові дії у поєднанні з динамічністю подій на зовнішніх ринках та наявними кіберзагрозами спричиняють суттєві ризики для сталого розвитку галузі. До основних висновків можна віднести такі:

1. Зростання ІТ-сектору в умовах глобалізації. ІТ-компанії з України активно інтегруються у глобальний ринок, в першу чергу йдеться про співпрацю на умовах

аутсорсингу (80 % вітчизняних суб'єктів підприємницької діяльності взаємодіють із клієнтами зі США, ЄС та Канади), що стимулює економічне зростання країни та залучення інвестицій. Такі компанії, як ЕРАМ демонструють успішне впровадження інноваційних технологій (ІІІ, блокчейн), посилюючи конкурентоспроможність України на міжнародному ринку.

2. Втрата інтелектуального потенціалу. Військові дії та істотне зниження рівня життя населення порівняно з багатьма країнами світу стимулювали відплив висококваліфікованої робочої сили, зокрема у сфері ІТ, за кордон, в результаті загострюються проблеми втрати інтелектуального капіталу та недоотримання податкових надходжень. Система освіти потребує подальшої трансформації та запровадження нових моделей стимулювання абітурієнтів вступати на навчання за ІТ-спеціальностями, які користуються високим попитом на національному та міжнародному ринках праці.

3. Залежність від зовнішніх ринків. Недостатній рівень розвитку високотехнологічних виробництв призвів до імпортозалежності апаратного забезпечення в Україні та негативно впливає на окремі діяльності в ІТ-галузі. Періодичні кризові явища на глобальному ринку також створюють вразливість для українських компаній. Розвиток українських продуктових компаній (наприклад Grammarly, GitLab) дозволяє певним чином нівелювати негативні чинники зовнішніх ринків.

4. Кіберзагрози та цифровий суверенітет. Кібератаки спричиняють значні фінансові та репутаційні втрати вітчизняних компаній, а рівень кіберзагроз істотно зріс під час війни в Україні. Перенесення даних на іноземні сервери вирішує проблему пошкодження та втрати цінних даних, проте відзначається суттєве зростання ризиків втрати цифрового суверенітету. Для України загалом і національної ІТ-галузі зокрема формування сучасних систем кібербезпеки є важливим стратегічним напрямом діяльності.

5. Перспективи післявоєнного відновлення. Глобалізація характеризується вільним рухом капіталу, який за умови створення сприятливого інвестиційного клімату після війни може бути залучений у достатніх обсягах для проведення якісних трансформацій інфраструктури та усіх видів економічної діяльності. За сприятливих умов вдасться досягти істотного зростання ІТ-сфери та посилення конкурентоспроможності вітчизняних компаній з розробки програмного забезпечення. Державна підтримка, спрямована на стимулювання ІТ-ринку та вдосконалення регуляторної політики, може забезпечити стійкість галузі в довгостроковій перспективі.

Таким чином, економічна безпека ІТ-галузі України залежить від здатності адаптуватися до глобальних викликів, формування стратегій протидії комплексу потенційних ризиків та стимулювання розвитку інноваційних продуктів. В сучасних умовах динамічних змін у глобальному економічному середовищі важливо забезпечити збереження та розвиток людського капіталу в Україні з урахуванням процесів цифровізації.

Подяки

Немає.

Конфлікт інтересів

Немає.

Список використаних джерел / References

- Васильченко, Л. С., Якушев, О. В., & Литвин, С. В. (2020). Веб-сайт підприємства як ефективний інструмент маркетингових комунікацій в мережі Інтернет. *Вісник Херсонського національного технічного університету*, 1(72). 2, 19–24. doi: 10.35546/kntu2078-4481.2020.1.2.2
- Новицька, О. В. (2014). Особливості підтримки малого та середнього бізнесу в системі сучасного регіонального менеджменту. *Збірник наукових праць Черкаського державного технологічного університету. Серія: Економічні науки*, 37(II), 62–169.

- Новицька, О. В. (2015). Інструменти стимулювання малого та середнього бізнесу в контексті регіонального розвитку. *Збірник наукових праць Черкаського державного технологічного університету. Серія: Економічні науки*, 39(II), 143–149.
- Спеціальності, яким держава виділила найбільше бюджетних місць у 2024 році. (2024, Липень, 12). Взято з <https://www.education.ua/news/2024/07/12/spetsialnosti-yakym-derzhava-vydilyla-naibilshe-biudzhethnykh-mists-u-2024-rotsi/>
- Які українські ІТ-компанії заробляють найбільше. (2025, Березень, 21). Взято з <https://speka.media/yaki-ukrayinski-it-kompaniyi-zaroblyayut-naibilse-vm5qzn>
- Якушев, О. В. (2023). Розробка дорожньої карти активізації розвитку підприємств ІТ-сфери в регіонах України. *Економіка і організація управління*, 131–142. doi: 10.31558/2307-2318.2023.1.13
- 9 best countries to outsource software development in 2025. (2025, March 7). Retrieved from <https://kaynes.com/9-best-countries-to-outsource-software-development/>
- Anand, K., Duley, C., & Gai, P. (2022). Cybersecurity and financial stability (Deutsche Bundesbank Discussion Paper No. 08/2022). Deutsche Bundesbank. doi: 10.2139/ssrn.4073158
- Dedicated software development teams in Ukraine: A comprehensive overview. (2024, December 24). Retrieved from <https://www.michele.com.ua/en/dedicated-software-development-teams-in-ukraine/#:~:text=Grammarly%20%2D%20grammarly.com%20Grammarly%2C%20a%20leading%20AI%2Dpowered,the%20innovative%20potential%20of%20Ukrainian%20tech%20talent.>
- EPAM: Головний офіс в Україні. (б.д.). Взято з <https://careers.epam.ua/company/contact>
- Havryliuk, O., Yakushev, O., Petchenko, M., Zachosova, N., Bielialov, T., & Kozlovskaya, S. (2023). Cyber security and artificial intelligence in the context of ensuring business security in wartime. *Financial and credit activity problems of theory and practice*, 6(53), 451–459. doi: 10.55643/fcaptp.6.53.2023.4130
- Ilyash, O., Smoliar, L., Lupak, R., Duliaba, N., Dzhadan, I., Kohut, M., & Radov, D. (2021). Multidimensional analysis and forecasting the relationship between indicators of industrial-technological development and the level of economic security. *Eastern-European Journal of Enterprise Technologies*, 5(13), 113. doi: 10.15587/1729-4061.2021.243262
- IT Services – Ukraine. (2025). Retrieved from <https://www.statista.com/outlook/tmo/it-services/ukraine>
- Kalinin, O., Gonchar, V., Abliazova, N., Filipishyna, L., et al. (2024). Enhancing economic security through digital transformation in investment processes: Theoretical perspectives and methodological approaches integrating environmental sustainability. *Natural and Engineering Sciences*, 9(1), 26–45. doi: 10.28978/nesciences.1469858
- Kianpour, M., Kowalski, S. J., & Øverby, H. (2021). Systematically understanding cybersecurity economics: A survey. *Sustainability*, 13(24), 13677. doi: 10.3390/su132413677
- Kyivstar completes preliminary assessment of the financial impact of the cyberattack. (2024, January 18). Retrieved from <https://www.veon.com/newsroom/press-releases/kyivstar-completes-preliminary-assessment-of-the-financial-impact-of-the-cyberattack>
- Matyskevicius, Y., Simanaviciene, Z., Belova, I., Fen, K., & Skljarić, Y. (2021). Blockchain impact on economic security. *Independent journal of management & production*, 12(3), s019-s040. doi: 10.14807/ijmp.v12i3.1493
- McCaffrey, C., & Poitiers, N. (2024). Instruments of economic security (No. 12/2024). *Bruegel Working Paper*. Retrieved from <https://www.econstor.eu/bitstream/10419/301006/1/1895455219.pdf>
- Migrating from on premises to AWS in less than 43 days with PrivatBank. (2024). Retrieved from <https://aws.amazon.com/solutions/case-studies/privatbank/>
- Mishchuk, I., Riabiykina, Y., Ushenko, N., Hamova, O., Tkachenko, S., & Yastremska, N. (2022). Intellectual capital as a factor forming economic security of enterprises in Society 5.0. *WSEAS Transactions on Business and Economics*, 19, 269–277. doi: 10.37394/23207.2022.19.25
- Onyshchenko, S. V., Masliy, O. A., & Buriak, A. A. (2023). Threats and risks of ecological and economic security of Ukraine in the conditions of war. In *17th International Conference Monitoring of Geological Processes and Ecological Condition of the Environment* (Vol. 2023, No. 1, pp. 1–5). *European Association of Geoscientists & Engineers*. doi: 10.3997/2214-4609.2023520072
- OpenAI ‘reviewing’ allegations that its AI models were used to make DeepSeek. (2025, January 29). Retrieved from <https://www.theguardian.com/technology/2025/jan/29/openai-chatgpt-deepseek-china-us-ai-models>
- Palantir and Microsoft partner to deliver enhanced analytics and AI services to classified networks for critical national security operations. (2024, August 8). Retrieved from

- <https://news.microsoft.com/source/2024/08/08/palantir-and-microsoft-partner-to-deliver-enhanced-analytics-and-ai-services-to-classified-networks-for-critical-national-security-operations/>
- Shmatkovska, T., Britchenko, I., Voitovych, S., Lošonczy, P., Lorvi, I., Kulyk, I., & Begun, S. (2022). Modern information and communication technologies in the digital economy in the system of economic security of the enterprises. *Journal of Interdisciplinary Research* (12/01-XXVII), 153–156. Retrieved from <https://philpapers.org/archive/SHMMIA.pdf>
- Spivakovskyy, S., Kochubei, O., Shebanina, O., Sokhatska, O., Yaroshenko, I., & Nych, T. (2021). The impact of digital transformation on the economic security of Ukraine. *Studies of Applied Economics*, 39(5). doi: 10.25115/eea.v39i5.5040
- Tech employees are getting the message: Playtime's over. (2025, March 19). Retrieved from <https://www.businessinsider.com/tech-industry-amazon-microsoft-meta-google-companies-intensity-hardcore-2025-3#:~:text=By%20the%20end%20of%202022,drip%20across%20the%20industry%20since>
- Ukraine has begun moving sensitive data outside its borders. (2022, June 14). Retrieved from <https://www.wsj.com/articles/ukraine-has-begun-moving-sensitive-data-outside-its-borders-11655199002>
- Ukrainian IT industry paid more than \$1 billion in taxes in 2024 - IT Ukraine Association research. (2025, March 24). Retrieved from <https://en.ain.ua/2025/03/24/ukrainian-it-industry-paid-more-than-1-billion-in-taxes-in-2024/>
- Yakushev, O., Moisieienko, L., Yakusheva, O., Prodanova, L., Plaksiuk, O., & Chepurda, L. (2024). Socio-economic sustainability of the tourism sector enterprises in the context of the covid-19 pandemic: Global and Ukrainian dimensions. *Financial & Credit Activity: Problems of Theory & Practice*, 5(58). 484–499. doi: <https://doi.org/10.55643/fcaptp.5.58.2024.4377>