УДК 339.9 doi: 10.20998/2519-4461.2024.1.82

І.М. ПОСОХОВ, В.Д. ПОНОМАРЬОВ

РИЗИКИ УКРАЇНСЬКИХ ІТ-КОМПАНІЙ В УМОВАХ ІНТЕГРАЦІЇ ДО ЄВРОПЕЙСЬКОГО СОЮЗУ ТА АНАЛІЗ ЗМІН У СФЕРІ УКРАЇНСЬКИХ ІТ-ТЕХНОЛОГІЙ

Розглянуто ризики вітчизняних ІТ-компаній в умовах інтеграції до Європейського Союзу та аналіз проведено аналіз змін вітчизняних компаній. Досліджено розвиток вітчизняних ІТ-компаній в умовах нестабільності та воєнних конфліктів. Проведено аналіз ризиків, з якими стикаються українські ІТ-компанії в сучасних умовах, враховуючи економічну, політичну, інноваційну та геополітичну обстановку. Проаналізовано динаміку та зміни, що відбулися в сфері українських інформаційних технологій, ураховуючи останні тренди та інновації. Визначено основні ризики, з якими стикаються українські ІТ-компанії, зокрема, в контексті політичних, економічних змін, змін в законодавстві, конкуренції на ринку, кадрового забезпечення тощо. Виконано порівняльний аналіз ризиків для українських та міжнародних ІТ-компаній в умовах війни. Виокремлено основні ризики, із якими зіштовхуються міжнародні компанії ІТ-компаній, особливо в умовах активного використання кіберпростору та поширення геополітичних турбуленцій: кадровий потенціал та кібербезпека: важливою ареною впливу стає кадровий потенціал. Загроза для безпеки та стабільності може спричинити відтік кваліфікованих кадрів, що може вплинути на розвиток та конкурентоспроможність ІТ-компаній, посилення кібербезпеки стає стратегічно важливим завданням; економічні ризики та фінансова стійкість: економічна нестабільність, зокрема у зв'язку із військовим конфліктом, може призвести до зменшення попиту на ІТ послуги та збільшення витрат на кіберзахист, ІТ компанії повинні враховувати ці ризики при формуванні своїх бізнес-стратегій; міжнародні відносини та імідж: зміни в міжнародних відносинах та імідж ІТ-компаній можуть визначати їхню можливість розширення на міжнародні ринки та співпрацю з партнерами, ретельне вивчення політичного та економічного контексту є важливим елементом стратегічного управління; гнучкість та спроможність до адаптації: ІТ-компанії повинні проявляти гнучкість та спроможність адаптуватися до швидкозмінюваних умов, зміни в бізнес-стратегіях, акцент на інновації та гнучкі форми організації робочого процесу допомогають компаніям впоратися з нестабільністю; соціальна відповідальність та сприяння миру: ІТ-компанії виявиють свою соціальну відповідальність через участь у гуманітарних програмах та сприяння мирним ініціативам; це може сприяти підтримці громадськості та зміцненню позитивного іміджу компаній.

Ключові слова: ризик; міжнародні відносини; Європейський Союз; інтеграція; міжнародні ринки; ІТ-компанії; ІТ-технології

I.M. POSOKHOV, V.D. PONOMAREV

RISKS OF UKRAINIAN IT COMPANIES IN THE CONDITIONS OF INTEGRATION INTO THE EUROPEAN UNION AND ANALYSIS OF CHANGES IN THE SPHERE OF UKRAINIAN IT TECHNOLOGIES

The risks of domestic IT companies in the conditions of integration into the European Union were considered and the analysis of changes in domestic companies was carried out. The development of domestic IT companies in the conditions of instability and military conflicts is studied. An analysis of the risks faced by Ukrainian IT companies in modern conditions was carried out, taking into account the economic, political, innovative and geopolitical situation. The dynamics and changes that took place in the field of Ukrainian information technologies were analyzed, taking into account the latest trends and innovations. The main risks faced by Ukrainian IT companies are identified, in particular, in the context of political, economic changes, changes in legislation, market competition, personnel support, etc. A comparative analysis of risks for Ukrainian and international IT companies in war conditions was performed. The main risks faced by international IT companies are highlighted, especially in the conditions of active use of cyberspace and the spread of geopolitical turbulence: personnel potential and cyber security: personnel potential becomes an important arena of influence. A threat to security and stability can cause an outflow of qualified personnel, which can affect the development and competitiveness of IT companies, strengthening cyber security becomes a strategically important task; economic risks and financial stability: economic instability, in particular in connection with a military conflict, can lead to a decrease in the demand for IT services and an increase in the costs of cyber protection, IT companies should take these risks into account when forming their business strategies; international relations and image: changes in international relations and the image of IT companies can determine their ability to expand to international markets and cooperate with partners, careful study of the political and economic context is an important element of strategic management; flexibility and ability to adapt: IT companies must show flexibility and ability to adapt to rapidly changing conditions, changes in business strategies, emphasis on innovation and flexible forms of work process organization help companies to cope with instability; social responsibility and promotion of peace: IT companies demonstrate their social responsibility through participation in humanitarian programs and promotion of peace initiatives; it can contribute to public support and strengthen the positive image of companies.

Keywords: risk; international relations; European Union; integration; international markets; IT companies; IT technologies

Вступ. У XXI столітті інформаційні технології (ІТ) визначають ключову роль у глобальному економічному та соціальному розвитку. Україна, яка стала важливим гравцем на світовому ІТ ринку, стикається із завданням забезпечення сталого функціонування свого технологічного сектору в умовах нестабільності та воєнних конфліктів. Одним із ключових аспектів цієї проблематики є ризики, які ІТ компанії в Україні можуть зазнавати в періоди воєнного стану.

Аналіз стану питання. В умовах сучасного світового господарства, глобалізації економіки та інтеграції України до Європейського Союзу підвищується актуальність дослідження ризиків вітчизнаних ІТ-компаній та аналіз змін у ссфері вітчизняних ІТ-технологій.

Аналіз основних досягнень і літератури.

Фундаментальні засади теорії ризику були розглянуто в наукових дослідженях А. Матвійчука, В. Вітлінського, Г. Великоіваненко, Н. Скопенко. С. Смеричевського. Дослідження ризиків вітчизнаних ІТ-компаній опубліковано в працях Ю. Грицюка, І. Нечаєвої, О. Лаговської. Останні дослідження та публікації в галузі українських ІТ-компаній виокремлюють декілька ключових тенденцій та ризиків: Вплив геополітичних подій: згідно з дослідженням, проведеним Українським Інститутом Інформаційних Технологій, зростаюча напруга на сході країни має потенціал вплинути на діяльність ІТ-

компаній. Ризики включають обмеження в міжнародних торгівельних операціях та втрату іноземних інвестицій. Законодавчі та регуляторні зміни: за даними статті в журналі "IT-Тренди України", нові податкові та правові норми можуть змінити оподаткування IT-підприємств та створити додатковий адміністративний та фінансовий обтяження. Кадрові виклики: конкуренція за IT-фахівців росте, що призводить до зростання витрат на заробітну плату та ризику втрати ключових талантів.

Технологічні інновації: останні дослідження Gartner вказують на те, що українські IT-компанії активно впроваджують інновації в області штучного інтелекту та блокчейну, що може вплинути на їх конкурентоспроможність та ризики в цих сегментах ринку. Водночас в сучасних умовах європейської інтеграції України потребує подальшої розробки проблематика дослідження ризиків вітчизнаних IT-компаній та аналіз змін у ссфері вітчизняних IT-технологій.

Мета роботи. Метою дослідження є вивчення та аналіз ризиків, з якими стикаються українські IT-компанії в сучасних умовах, враховуючи економічну, політичну, інноваційну та геополітичну обстановку. Крім того, стаття має на меті розглянути та проаналізувати динаміку та зміни, що відбулися в сфері українських інформаційних технологій, ураховуючи останні тренди та інновації. Основні завдання цієї роботи включають визначення та аналіз основних ризиків, з якими стикаються українські IT-компанії, зокрема, в контексті політичних, економічних змін, змін в законодавстві, конкуренції на ринку, кадрового забезпечення тощо.

Викладення основного матеріалу дослідження.

Ризики IT-компаній:

1. Політичні та геополітичні ризики:

1.1 Зміни в урядовій політиці: В умовах воєнного конфлікту влада може зазнавати значних змін. Це може включати перехід до тимчасового уряду, введення воєнного стану або інших форм політичного контролю. Для IT-компаній це означає нестабільність в законодавстві, можливість суттєвих змін у регулюючих політиках, включаючи податкові та економічні аспекти.

1.2 Націоналізація та конфіскація майна: У воєнних умовах можливе рішення влади націоналізувати або конфісковувати певні види майна для потреб оборони чи економічного відновлення. Це може вплинути на власність, інтелектуальну власність та інші активи IT-компаній, порушуючи їх бізнес-модель та стратегії розвитку.

1.3 Обмеження експорту-імпорту: геополітичні конфлікти можуть викликати введення обмежень на зовнішньоекономічні операції. Це може обмежити можливості IT-компаній працювати з іноземними клієнтами, постачальниками та інвесторами, що призводить до складнішого доступу до іноземних ринків.

1.4 Негативний вплив на ринкові можливості: Геополітичні нестабільності можуть створити негативний образ країни на світовій арені. Це може вплинути на відносини з потенційними інвесторами та клієнтами, обмежуючи можливості залучення нових проєктів та партнерств.

1.5 Негативний вплив на репутацію IT-компаній: Сучасне IT підприємство в значній мірі покладається на свою репутацію та відносини з клієнтами. Воєнний конфлікт може призвести до змін у сприйнятті бізнесу та вплинути на довіру клієнтів, що може мати великі наслідки для IT-компаній. Ретельний аналіз цих політичних та геополітичних ризиків дозволяє IT-компаніям планувати стратегії реагування та ризик-менеджменту в умовах воєнного конфлікту.

2. Кібербезпека та інформаційна війна:

2.1 Збільшення кількості кібератак: У воєнних умовах збільшується ймовірність кібератак на IT-інфраструктуру. Атаки можуть бути спрямовані на викрадення конфіденційної інформації, блокування доступу до систем або завдання інших шкідливих наслідків. Це створює загрозу для безпеки даних та неперервності бізнесу.

2.2 Розширення спектру загроз: Військовий конфлікт може спричинити розширення спектру кіберзагроз. Це може включати як краудсорсинг кібератак, так і спроби дестабілізації критичних інфраструктурних об'єктів. IT-компанії повинні бути готові до нових та вдосконалених методів кіберзагроз.

2.3 Втрати конфіденційної інформації: Інформаційна війна може призвести до витоку конфіденційної інформації, такої як технічні розробки, корпоративні секрети та інтелектуальна власність. Це може зашкодити конкурентоспроможності компаній та вплинути на їхню ринкову позицію.

2.4 Поширення дезінформації: У військових конфліктах інформаційні кампанії можуть бути спрямовані на поширення дезінформації та створення негативного образу IT-компаній. Це може викликати втрату довіри як від клієнтів, так і від інвесторів.

2.5 Безперервність бізнесу та реагування на інциденти: IT-компанії повинні бути готові до збільшення інтенсивності кібератак та вміти ефективно реагувати на інциденти. Навички кібербезпеки, планування реагування та відновлення стають визначальними для забезпечення неперервності бізнесу в умовах кіберзагроз.

Аналіз цих аспектів дозволяє IT-компаніям визначити критичні області для підвищення кібербезпеки та розробки стратегій вразливості для неперервного функціонування в умовах інформаційних конфліктів.

3. Економічні ризики та фінансова нестабільність:

3.1 Зменшення попиту на IT-послуги: В умовах воєнного конфлікту споживачі та компанії можуть зменшити свої витрати на IT послуги. Це може вплинути на прибутковість та обсяги робіт для IT компаній, зокрема тих, які мають клієнтів або проекти у зоні конфлікту.

3.2 Збільшення витрат на кіберзахист: Умови воєнного конфлікту зазвичай призводять до зростання кількості та складності кіберзагроз. IT-компанії змушені інвестувати в підвищення рівня кібербезпеки для захисту власних даних, інтелектуальної власності та інфраструктури.

3.3 Вплив на курс національної валюти та інфляцію: Економічні турбуленції, пов'язані з воєнним конфліктом, можуть призвести до змін валютних курсів та збільшення інфляції. Це може вплинути на вартість обладнання, програмного забезпечення та інших ресурсів, що використовують ІТ компанії.

3.4 Зниження рівня інвестицій та підвищення кредитного ризику: Економічна нестабільність в умовах воєнного конфлікту може призвести до зниження рівня інвестицій та доступу до кредитів для ІТ-компаній. Це може ускладнити фінансове планування, інноваційні проекти та розвиток нових напрямків бізнесу.

3.5 Фінансова вразливість малих та середніх підприємств: Малі та середні ІТ-компанії можуть бути особливо вразливими у воєнних умовах через обмежені фінансові резерви та меншу здатність адаптуватися до економічних трускавок. Дослідження фінансової стійкості цих компаній є ключовим аспектом аналізу.

3.6 Вплив на заощадження та пенсійні фонди: Економічна нестабільність може вплинути на заробітні плати та стабільність фінансових інструментів, таких як пенсійні фонди та інвестиційні портфелі. Це може вплинути на фінансове благополуччя працівників та можливості компаній забезпечити соціальні вигоди.

Аналіз фінансових ризиків та економічної нестабільності дозволяє ІТ-компаніям адаптувати свої стратегії, управління ресурсами та фінансове планування для забезпечення стійкості в умовах економічних викликів війни.

4. Зміни в міжнародних відносинах та співпраці:

4.1 Обмеження міжнародних партнерств: Умови воєнного конфлікту можуть призвести до обмежень у міжнародних відносинах та партнерствах. Зміни в політичній сфері та стосунках з іншими країнами можуть вплинути на можливості ІТ компаній для співпраці та входження до міжнародних ринків.

4.2 Скасування торгових угод та угод про співпрацю: Економічна нестабільність та політичні напруги можуть призвести до скасування торгових угод та угод про співпрацю між країнами. Це може вплинути на витрати та можливості для ІТ компаній експортувати свої товари та послуги на міжнародні ринки.

4.3 Зміна міжнародної репутації країни: Військові конфлікти можуть впливати на репутацію країни в міжнародних відносинах. Це може стати причиною негативного ставлення до продукції та послуг, створених у цій країні. Для ІТ компаній це може означати втрату підтримки та довіри з боку зарубіжних клієнтів.

4.4 Погіршення доступу до міжнародних ресурсів: Міжнародні санкції та обмеження можуть ускладнити доступ до міжнародних ресурсів, таких як фінансування, технології та інші необхідні ресурси для ІТ-компаній. Це може вплинути на їхню конкурентоспроможність та рівень інновацій.

4.5 Відкриття нових ринків та можливостей: Незважаючи на негативні аспекти, військові конфлікти можуть відкривати нові ринки та можливості для співпраці. ІТ-компанії можуть знайти нові сфери застосування своїх рішень та послуг в умовах змін в міжнародних відносинах.

Аналіз міжнародних відносин та можливих змін у співпраці дозволяє ІТ-компаніям адаптуватися до нових реалій та шукати інноваційні способи розвитку у складних геополітичних умовах.

5. Втрати кадрів та відсутність фахівців:

5.1 Масовий відтік кваліфікованих кадрів: Умови воєнного конфлікту можуть викликати масовий відтік кваліфікованих ІТ-фахівців через загрозу для їхньої безпеки, нестабільність та неспокій. Це може стати серйозним викликом для ІТ-компаній, особливо для тих, які сильно залежать від талановитих професіоналів.

5.2 Втрати досвіду та експертизи: Велика кількість відходжень може призвести до втрати досвіду та експертизи в компанії. Це може вплинути на рівень якості розробок, технічну підтримку та інші аспекти діяльності компанії.

5.3 Конкуренція за таланти та збільшення витрат на зарплати: Зменшення кількості доступних спеціалістів може призвести до зростання конкуренції за таланти в ІТ секторі. Це може викликати збільшення витрат на зарплати та пакети соціальних вигод для збереження та залучення кваліфікованих кадрів.

5.4 Стратегії утримання талантів: Розробка та впровадження стратегій утримання талантів стає критичним завданням у воєнних умовах. ІТ компанії повинні вивчати найкращі практики, що дозволяють зберегти та мотивувати свій персонал.

5.5 Співпраця з освітніми установами та розвиток ІТ-галузі: Стимулювання співпраці з освітніми установами та участь в програмах розвитку ІТ-галузі може допомогти забезпечити доступ до нового покоління кваліфікованих спеціалістів та зменшити негативний вплив втрат кадрів.

5.6 Гнучкість та адаптивність компаній: Гнучкість та адаптивність ІТ-компаній у реагуванні на втрати кадрів можуть визначити їхню успішність у важких умовах. Розробка гнучких моделей роботи, децентралізованих команд та стратегій перепідготовки персоналу стають критичними аспектами. Аналіз ризиків втрат кадрів та розробка стратегій утримання талантів є важливим завданням для забезпечення стабільності та продовження розвитку ІТ-компаній в умовах воєнного конфлікту.

Порівняння з Міжнародними Компаніями. Порівняння ризиків для українських та міжнародних ІТ-компаній в умовах війни вимагає аналізу їхнього географічного положення, розміру, ринкової диверсифікації та інших факторів.

1. Географічне положення:

– Українські ІТ-компанії: Знаходячись в Україні, ІТ-компанії піддаються більшому геополітичному ризику через повномасштабне вторгнення. Це може призвести до обмежень у веденні бізнесу та втрати іноземних інвестицій.

– Міжнародні ІТ-компанії: Міжнародні компанії, розташовані в стабільних регіонах, зазвичай не мають таких геополітичних ризиків та можуть

зосередитися на розвитку своїх проектів без зайвих обмежень.

2. Розмір і ресурси:

– Українські IT-компанії: Більшість українських IT-компаній є меншими за міжнародні корпорації та можуть мати обмежені ресурси для реагування на ризики та забезпечення стабільності.

– Міжнародні IT-компанії: Міжнародні корпорації зазвичай мають значно більший обсяг ресурсів, фінансовий потенціал та доступ до різних джерел фінансування, що дає їм можливість ефективно впоратися з ризиками та зберегти стабільність діяльності.

3. Ринкова диверсифікація:

– Українські IT-компанії: Багато українських IT-компаній можуть бути залежними від обмеженого кола клієнтів та ринків через внутрішні обставини та обмеження географічного розташування.

– Міжнародні IT-компанії: Міжнародні корпорації мають можливість розширювати свою клієнтську базу на різних ринках і галузях, що дозволяє їм зменшити ризики, пов'язані з конкретними обставинами або індустріями.

4. Партнерські відносини і стратегії управління ризиками:

– Українські IT-компанії: Відсутність досвіду та обмежені можливості можуть ускладнити розробку ефективних стратегій управління ризиками та відсутність доступу до страхових ринків.

– Міжнародні IT-компанії: Міжнародні корпорації часто мають більше досвіду у роботі з ризиками, розвинуті плани бізнес-контингенту та можуть легше залучати страхувальників для зменшення фінансових ризиків.

Статистика та Аналіз Даних.

1. Кібератаки.

Протягом 2022 року Україна стикнулася з 7000 кібератак на інформаційну інфраструктуру. За минулий рік в Україні було зареєстровано у 2,8 раза більше кіберінцидентів, ніж у 2021-му.

З 24 лютого і до кінця 2022 року урядова команда реагування на комп'ютерні надзвичайні події CERT-UA опрацювала 2194 кіберінциденти. З них 120 стосувалися фінансового сектору, 156 – комерційних організацій та 92 – сектору телекомунікацій і розробки програмного забезпечення.

Україна – друга серед найбільш атакованих країн світу після США, каже технічний директор IT-компанії UNITY-BARS, що розробляє ПЗ для фінансових установ, Олег Музика. У 2022 році кібератак побільшало у 3,5 рази порівняно з 2021-м – на фінансовий сектор України припадає 5% усіх атак, на IT-галузь – 10%, констатують у UNITY-BARS.

2. Кадрові зміни на IT ринку.

За даними українського сайту з пошуку роботи для спеціалістів у сфері IT Djinni, кількість вакансій за рік знизилася майже вдвічі, тим часом кількість претендентів навпаки – у два рази зросла. Це вказує на те, що ринок кандидата тепер стає ринком роботодавця, а пропозиція відчутно перевищує попит.

Хвиля звільнень, що розпочалася наприкінці 2022 року у світовій IT-індустрії, набирає обертів: за перші три місяці 2023 року без роботи залишилось 139 тисяч працівників. Навіть такі гіганти ринку, як Google, Microsoft, Meta, Amazon, Twitter, Apple звільняють своїх працівників.

Компанії продовжуватимуть оптимізовувати свої витрати. Наприклад, компанія Meta, яка вже звільнила 11 000 працівників у листопаді 2022 року, має намір звільнити ще 10 000 спеціалістів та закрити 5 000 додаткових вакансій до кінця 2023 року.

При вивченні досвіду зарубіжних країн у стимулюванні розвитку інформаційних технологій під час воєнних конфліктів, важливо розглянути приклад Ізраїлю. Ізраїль, часто визнаний "Країною стартапів", активно спрямовує зусилля на розвиток інтелектуального потенціалу та технологічних досягнень, незважаючи на обмежені ресурси та військові конфлікти.

Військова сфера Ізраїлю сприяє технологічному розвитку країни через спеціалізовані підрозділи, зосереджені на розвідці та кібербезпеці.

Ізраїль вкладає 5,44% ВВП у наукові дослідження, що відзначається порівняно з 0,41% в Україні та 1,39% в Польщі.

Війна заохочує Україну розвивати новий напрямок в інформаційних технологіях - військово-технологічну сферу.

Особливо успішно розвиваються безпілотні літальні апарати (БПЛА). Деякі розробки вже впроваджені та застосовуються на полі бою, а інші очікують на розгляд. Проект "Армія дронів" є яскравим прикладом цього напрямку. Для його втілення держава виділила 20 мільярдів гривень на закупівлю вітчизняних апаратів.

Очевидно, що напрямок військово-технологічних розробок стане пріоритетним для України в найближчі роки.

Аналіз змін у сфері IT. Підсумовуючи десять місяців 2022 року, інформаційна технологійна галузь внесла $6 млрд української економіки через експорт та показала 10% зростання порівняно з попереднім роком. Ці результати стали можливими завдяки успішній реалізації стратегій бізнес-контингенту, своєчасній релокації команд та розвитку розробницьких центрів як в Україні, так і за кордоном.

IT справедливо вважається однією з ключових галузей української економіки, яка стрімко розвивається кожен рік. За останні шість років частка комп'ютерних послуг у ВВП зросла з 1,8% до 3,5%, а в експорті послуг – з 13,4% до 37,8%.

У сфері ІКТ налічується 289 000 фахівців, що складає 1,9% від загальної кількості зайнятих осіб.

Зокрема, IT-галузь орієнтована на експорт, і за останні шість років обсяг експорту комп'ютерних послуг зрос на 26,8% в середньому щорічно, досягнувши у 2021 році $6,9 млрд, що перевищило прогноз на $0,1 млрд.

Статистика щодо кількості IT-компаній в Україні різниться. За даними Держстату, у 2021 році активні юридичні особи з IT-КВЕДами налічували 8800. Однак розрахунки порталу Tech Ecosystem показують, що на

початку грудня 2022 року активних ІТ-компаній оцінюється в 2400, при тому, що експерти вказують на 1800-2000 активних учасників ринку праці. У 2022 році на ІТ-спеціальності вступила рекордна кількість студентів, а саме 329 000, з яких уже на початку року працювали в галузі.

Технології все більше проникають в різні галузі, допомагаючи автоматизувати виробничі процеси, збільшити продуктивність та підвищити ефективність бізнесу. Понад 21% українських компаній у 2021 році вже використовували послуги ІТ-фахівців, а близько 15% залучали експертів ззовні.

Вплив повномасштабної війни став випробуванням для усієї економіки України. Однак, ІТ-галузь є винятком, збільшивши обсяг експорту в порівнянні з попереднім роком. Компанії активно переглядають мотиваційні пакети для своїх працівників та контрактників, не зважаючи на виклики війни. Дослідження винагород в ІТ-галузі від Korn Ferry у 2022 році вказує на кілька ключових тенденцій, зокрема плани більшості ІТ-компаній збільшувати бюджети на компенсації, варіації рівня заробітної плати залежно від позиції та регіонального розподілу, а також вплив специфіки роботи галузі на залучення ФОП ІТ-компаніями.

Незважаючи на ускладнення в умовах війни, ІТ-галузь продовжує вносити свій внесок у податкову систему, а деякі компанії планують підтримати державу, сплачуючи податки наперед. Кількість платників податків зросла на 7,5% до листопада 2022 року в порівнянні з попереднім роком.

З початком війни багато ІТ-компаній активно підтримують Збройні сили України, перераховуючи кошти на благодійні фонди та надаючи підтримку бійцям. Більше половини планували відкривати нові офіси та філії у 2022 році, але лише чверть це вдалося через негативні наслідки вторгнення. 70,8% компаній провели непланову релокацію, а 25% з них повністю.

Повномасштабне вторгнення викликало нові виклики для ІТ-галузі, такі як обмеження виїзду фахівців за кордон та проблеми із електропостачанням. У разі масових ракетних ударів по об’єктах енергетичної інфраструктури з 10 жовтня 2022 року виникли проблеми з електропостачанням, що вимагало від галузі введення нових антикризових заходів. ІТ-галузь виявилася адаптивною, зазнаючи впливу війни. За опитуванням, 34,3% компаній успішно пристосувались до нових реалій, а понад 43% очікують зростання обсягів бізнесу у 2022 році.

Головним викликом для ІТ-фахівців стала релокація через війну. З них 64% були змушені переїхати, але 24% вже повернулися на свої старі місця проживання. Із зростанням ролі віддаленої роботи, 71,5% компаній відзначили, що більше 75% їхніх працівників працюють віддалено.

Бойові дії та окупація призвели до зміни стратегій ІТ-бізнесу. Частина компаній розглядає відкриття нових офісів, інші провели непланову релокацію через нестабільні умови. Тим не менше, 81,5% компаній, що релокувалися, планують повертати бізнес до України, і 5,6% вже знаходяться в процесі цього.

Прогнозування майбутнього української ІТ-галузі зазнало корекцій через воєнні події. Обсяг експорту ІТ-послуг у 2022 році прогнозується на рівні $7,1 млрд, нижче від очікувань, але все ще перевищує показники минулого року. Вплив війни на економіку виявився значно меншим, ніж прогнозували, але атаки на енергетичну систему призвели до повернення до попередніх економічних прогнозів.

Опитування проведено в жовтні та листопаді 2022 року серед 147 ІТ-компаній, що виявили високу адаптивність та готовність до змін у складних умовах війни.

Переосмислення Бізнес-стратегій: Сучасні умови можуть змусити ІТ компанії переглянути свої бізнес-стратегії. Це може включати перегляд ринкових стратегій, зміни в інвестиційних планах та акцент на стійкості та гнучкості в умовах неспокійності.

Вплив воєнного конфлікту та сучасних геополітичних умов на ІТ компанії визначається рядом факторів, включаючи їх місце розташування, ринкові сегменти, готовність до кіберзагроз, та ефективність управління ризиками. Індивідуальний підхід та гнучкі стратегії допомагають компаніям адаптуватися та забезпечити сталість у викликливих умовах.

Висновки. На сучасному етапі воєнний конфлікт та геополітичні події впливають на діяльність ІТ-компаній, особливо в умовах активного використання кіберпростору та поширення геополітичних турбуленцій. Розглядаючи різні аспекти впливу, можна зробити кілька ключових висновків.

1. Кадровий потенціал та кібербезпека: Важливою ареною впливу стає кадровий потенціал. Загроза для безпеки та стабільності може спричинити відтік кваліфікованих кадрів, що може вплинути на розвиток та конкурентоспроможність ІТ компаній. Посилення кібербезпеки стає стратегічно важливим завданням.

2. Економічні ризики та фінансова стійкість: Економічна нестабільність, зокрема у зв'язку із військовим конфліктом, може призвести до зменшення попиту на ІТ послуги та збільшення витрат на кіберзахист. ІТ компанії повинні враховувати ці ризики при формуванні своїх бізнес-стратегій.

3. Міжнародні відносини та імідж: Зміни в міжнародних відносинах та імідж ІТ компаній можуть визначати їхню можливість розширення на міжнародні ринки та співпрацю з партнерами. Ретельне вивчення політичного та економічного контексту є важливим елементом стратегічного управління.

4. Гнучкість та спроможність до адаптації: ІТ-компанії повинні проявляти гнучкість та спроможність адаптуватися до швидкозмінюваних умов. Зміни в бізнес-стратегіях, акцент на інновації та гнучкі форми організації робочого процесу можуть допомогти компаніям впоратися з нестабільністю.

5. Соціальна відповідальність та сприяння миру: ІТ-компанії можуть виявити свою соціальну відповідальність через участь у гуманітарних програмах та сприяння мирним ініціативам. Це може сприяти підтримці громадськості та зміцненню позитивного іміджу компаній.

Загальною тенденцією є необхідність адаптації до нових умов та розробка стратегій, що враховують ризики та можливості.

ІТ компанії, які будуть готові до викликів, зможуть ефективно керувати ризиками та забезпечити сталість своєї діяльності в умовах нестабільності.

Список літератури

1. Державна податкова служба. Надходження податків і зборів. URL: https://tax.gov.ua/diyalnist-/pokazniki-roboti/nadhodjennya-podatkiv-i-zboriv--obovyaz/nadhodjennya-podatkiv-i-zboriv/ (дата звернення: 08.10.2023).
2. Довгань Л.Є., Малик І.П. Тенденції та проблеми розвитку сфери інформаційних технологій в Україні: кадрові аспекти. *Економічний Вісник НТУ «КПІ».* 2017. № 14. С. 437-443.
3. Львівський ІТ-кластер. Дослідження ІТ ринку в 2022 році. URL: https://itcluster.lviv.ua/projects/it-research/ (дата звернення: 06.10.2023).
4. Назаренко І.Л., Ткаченко Ю.В. Стан і перспективи розвитку ІТ сфери в Україні в період війни. *Вісник економіки транспорту і промисловості.* 2023. № 81-82. С. 59-67.
5. Національний Банк України. Статистика зовнішнього сектору. URL: https://bank.gov.ua/ua/statistic/sector-external#1 (дата звернення: 06.10.2023).
6. Журавльов О.В. Статистичне дослідження ринку ІТ-послуг в Україні. *Статистика та економіка, аналіз*. 2018. № 4. С. 25-33.
7. Ситник О.Ю., & Дубровський С.С. (2022). Особливості розвитку ринку інформаційних технологій в Україні. *Економічні горизонти*, № 3(21), 72–82.
8. Тарасова К.І. Ринок інформаційно-комунікаційних технологій у системі національного господарства. *Інфраструктура ринку*. 2018. № 16. С. 46-51.
9. Тернова І.А. Роль ІТ-сектора України у розвитку зовнішньоекономічної діяльності. *Соціальна економіка*. 2016. Вип. 51.1. С. 69–76.
10. Djinni Analytics. Year in review: Ukrainian tech job market in 2022. URL: https://djinni.substack.com/p/year-in-review-ukrainian-tech-job (date of application: 08.10.2023)
11. Ринок праці під час війни: 13% айтівців без роботи, ще половина боїться її втратити. URL: https://dou.ua/lenta/articles/job-market-during-war-part-1/ (дата звернення: 08.10.2023)
12. IT association of Ukraine. Research "Do IT like Ukraine". URL: https://itukraine.org.ua/files/reports/2022/DoITLikeUkraine2022.pdf (date of application: 08.10.2023)
13. Reuters.Ukrainian minister vows more drones for strikes on Russian warships. URL: https://www.reuters.com/world/europe/ukrainian-minister-vows-more-drone-strikes-russian-ships-2023-09-16/ (date of application: 08.10.2023)

References (transliterated)

1. Derzhavna podatkova sluzhba. Nadxodzhennya podatkiv i zboriv. URL: https://tax.gov.ua/diyalnist-/pokazniki-roboti/nadhodjennya-podatkiv-i-zboriv--obovyaz/nadhodjennya-podatkiv-i-zboriv/ (date of application: 08.10.2023).
2. Dovgan` L.Ye., Maly`k I.P. Tendenciyi ta problemy` rozvy`tku sfery` informacijny`x texnologij v Ukrayini: kadrovi aspekty` [Dovgan L.E., Malik I.P. Trends and problems of the development of information technologies in Ukraine: personnel aspects]. *Ekonomichny`j Visny`k NTU «KPI»* [Economic Bulletin of NTU "KPI"]. 2017. Vol. 14. pp. 437-443.
3. L`vivs`ky`j IT-klaster. Doslidzhennya IT ry`nku v 2022 roci. URL: https://itcluster.lviv.ua/projects/it-research/ (date of application: 06.10.2023).
4. Nazarenko I.L., Tkachenko Yu.V. Stan i perspekty`vy` rozvy`tku IT sfery` v Ukrayini v period vijny` [Nazarenko I.L., Tkachenko Yu.V. The state and prospects of the development of the IT sector in Ukraine during the war]. *Visny`k ekonomiky` transportu i promy`slovosti* [Bulletin of the economy of transport and industry]. 2023. Vol. 81-82. pp. 59-67.
5. Nacional`ny`j Bank Ukrayiny`. Staty`sty`ka zovnishn`ogo sektoru. URL: https://bank.gov.ua/ua/statistic/sector-external#1 (date of application: 06.10.2023).
6. Zhuravl`ov O.V.. Staty`sty`chne doslidzhennya ry`nku IT-poslug v Ukrayini [Zhuravlev O.V. Statistical study of the IT services market in Ukraine]. *Staty`sty`ka ta ekonomika, analiz* [Statistics and economics, analysis]. 2018. Vol. 4. pp. 25-33.
7. Sy`tny`k, O.Yu., & Dubrovs`ky`j, S.S. (2022). Osobly`vosti rozvy`tku ry`nku informacijny`x texnologij v Ukrayini [Sytnyk, O. Yu., & Dubrovskyi, S. S. Peculiarities of the development of the information technology market in Ukraine]. *Ekonomichni gory`zonty`* [Economic horizons]. Vol. 3(21), pp. 72–82.
8. Tarasova K.I. Ry`nok informacijno-komunikacijny`x texnologij u sy`stemi nacional`nogo gospodarstva [Tarasova K. I. The market of information and communication technologies in the system of the national economy]. Infrastruktura ry`nku [Market infrastructure]. 2018. Vol. 16. pp. 46-51.
9. Ternova I.A. Rol` IT-sektora Ukrayiny` u rozvy`tku zovnishn`oekonomichnoyi diyal`nosti [Ternova I.A. The role of the IT sector of Ukraine in the development of foreign economic activity]. Social`na ekonomika [Social economy]. 2016. issue 51.1. pp. 69–76.
10. Djinni Analytics. Year in review: Ukrainian tech job market in 2022. URL: https://djinni.substack.com/p/year-in-review-ukrainian-tech-job (date of application: 08.10.2023).
11. The labor market during the war: 13% of Haitians are without work, another half are afraid of losing it. URL: https://dou.ua/lenta/articles/job-market-during-war-part-1/ (date of application: 08.10.2023)
12. IT association of Ukraine. Research "Do IT like Ukraine". URL: https://itukraine.org.ua/files/reports/2022/DoITLikeUkraine2022.pdf (date of application: 08.10.2023).
13. Reuters.Ukrainian minister vows more drones for strikes on Russian warships. URL: https://www.reuters.com/world/europe/ukrainian-minister-vows-more-drone-strikes-russian-ships-2023-09-16/ (date of application: 08.10.2023).

Надійшла (received) 13.02.2024

Відомості про авторів / About the Authors

***Посохов Ігор Михайлович* (*Posokhov Igor*)** – доктор економічних наук, професор, професор кафедри економіки бізнесу і міжнародних економічних відносин, Національний технічний університет «Харківський політехнічний інститут»; м. Харків,Україна; ORCID: https://orcid.org/0000-0001-9668-642X;e-mail: posokhov7@gmail.com

Пономарьов Владислав (Ponomarov Vladyslav) – аспірант кафедри економіки бізнесу і міжнародних економічних відносин, Національний технічний університет «Харківський політехнічний інститут»; м. Харків, Україна; ORCID: https://orcid.org/0000-0001-8742-5615; e-mail: vladyslav.ponomarov@emmb.khpi.edu.ua