Siroshtan, O. & Vasyliev, O. (2026). Military conflict as a risk factor for the IT sector: a systematisation of threats and mitigation strategies. Management and Entrepreneurship: Trends of Development, 3(37), 413-429. https://doi.org/10.26661/2522-1566/2026-3/37-29

## МЕНЕДЖМЕНТ

**ОТРИМАНО:**
13 Серпня 2026
**ПРИЙНЯТО:**
28 Вересня 2026
**ВИПУСК:**
20 Жовтня 2026

CC BY 4.0

**УДК 338.242:004.9:355.01**

**DOI 10.26661/2522-1566/2026-3/37-29**

# ВІЙСЬКОВИЙ КОНФЛІКТ ЯК ЧИННИК РИЗИКУ ДЛЯ IT-СЕКТОРУ: СИСТЕМАТИЗАЦІЯ ЗАГРОЗ І СТРАТЕГІЙ МІНІМІЗАЦІЇ

**Сіроштан О. О.***
*кафедра управління та адміністрування*
*Харківський національний університет імені В. Н. Каразіна, ННІ «Каразінська школа бізнесу»*
*м. Харків, Україна*
*ORCID 0009-0003-5148-4770*

**Васильєв О. В.**
*д.е.н., професор*
*кафедра управління та адміністрування*
*Харківський національний університет імені В. Н. Каразіна, ННІ «Каразінська школа бізнесу»*
*м. Харків, Україна*
*ORCID 0000-0003-1819-6761*

** Email автора для листування: alexanderr.seroshtan@gmail.com*

**Анотація.** Мета. Систематизувати задокументовані загрози, які військовий конфлікт створює для IT-компаній, і побудувати матрицю «група загроз – стратегія мінімізації – очікуваний ефект – межа дієвості» з явним позначенням доказового статусу кожного рядка. Дизайн, методологія, підхід. Роботу виконано як кабінетний аналіз документованих свідчень із подальшою якісною систематизацією. Джерельну базу дібрано цілеспрямовано з верифікованих за DOI або URL записів; у побудові результатів використано чотири доказові групи: галузеві релізи IT Ukraine Association з даними Національного банку України, рецензовані українські та міжнародні публікації, вендорський звіт про кіберзагрози та конференційні матеріали. Для кожного рядка матриці запроваджено шкалу доказового статусу, а обмеження прочитання джерел зафіксовано явно. Результати. Обґрунтовано критерій класифікації за ураженим активом IT-компанії та виокремлено шість груп загроз воєнного часу: персонал; обчислювальна та енергетична інфраструктура; дані й IT-периметр; фінансові потоки; правовий і регуляторний статус; клієнтські відносини. Кожній групі зіставлено стратегію мінімізації, очікуваний ефект і межу дієвості, за якою стратегія перестає працювати, а доказову опору рядка позначено окремо. Показано, що стратегії діють комплементарно: відмова однієї ланки не компенсується посиленням сусідньої. Оригінальність, цінність. Загрози воєнного часу для IT-сектору зведено не в перелік заходів, а в матрицю з явними межами дієвості та доказовим статусом кожного рядка. Специфіку воєнного чинника автор пов'язує не з переліком груп, а з профілем їх одночасної активації, який знімає ефект внутрішньофірмової диверсифікації. Матриця придатна для попереднього діагностування ризикової експозиції IT-компанії та потребує емпіричної перевірки.

**Ключові слова***:* управління ризиками, військовий конфлікт, IT-сектор, класифікація загроз, стратегії мінімізації, межа дієвості стратегії, безперервність діяльності.

**JEL класифікація:** D81, L86, M10.

eISSN 2522-1566
ISSUE 3 (37), 2026

## ПОСТАНОВКА ПРОБЛЕМИ

Воєнний стан змінює не окремі параметри господарської діяльності, а сам склад загроз, з якими стикається підприємство. У фаховій періодиці відповідне проблемне поле вже сформоване: трансформацію загроз економічній безпеці підприємства під час воєнного стану винесено в самостійний предмет аналізу з виробленням рекомендацій [1], а ризики та економічну безпеку підприємств розглядають також у прив'язці до процесу відновлення України [2]. Перехід від констатації нових загроз до управлінського рішення, однак, потребує впорядкування: загрози мають бути згруповані за ознакою, яка одразу вказує на адресата захисного заходу.

Емпіричний вимір воєнного ризику на регіональному рівні дають оцінки, побудовані на інтегрованих даних про інтенсивність, тривалість і добову структуру повітряних тривог, атаки на об'єкти інфраструктури та міжрегіональні релокації бізнесу за період серпень 2024 – серпень 2025 [3]. У цьому дослідженні за даними про простій торговельних центрів зафіксовано, що в окремих прифронтових областях магазини втрачають до 50 % свого операційного часу, тоді як у західних регіонах відповідний показник не перевищує 1 %; що релокації не зводяться до простої міграції зі сходу на захід, а прифронтові й високоризикові області – Харківська, Дніпропетровська, Запорізька – одночасно перебувають у зоні підвищеної небезпеки та активного припливу бізнесу; що пошкодження житлової, енергетичної, медичної та освітньої інфраструктури накладається на зони активної релокації, утворюючи асиметричні профілі ризику [3].

Для ІТ-сектору наслідки воєнного чинника простежуються на рівні галузевих агрегатів. Аналіз динаміки українського ІТ-ринку за 2020–2024 рр. фіксує зростання експорту ІТ-послуг із 5,03 млрд дол. США у 2020 р. до рекордних 7,34 млрд у 2022 р. з подальшим скороченням до 6,45 млрд у 2024 р., а також зрушення на ринку праці – зменшення частки молодших спеціалістів і зростання ролі гіг-контрактів; попри це ІТ зберіг статус найбільшого експортера послуг, а серед нових тенденцій названо розвиток продуктових компаній і появу сектору військових технологій [4]. За даними Національного банку України, наведеними в галузевому релізі, експорт ІТ-послуг у 2024 р. становив 6,4 млрд дол. США, що на 4,3 % менше за показник 2023 р., із розподілом за країнами-замовниками [5]; обидві оцінки узгоджуються за напрямом динаміки й різняться в межах округлення. Отже, документально зафіксованими є принаймні два канали впливу воєнного чинника на ресурсну базу галузі: зрушення у структурі зайнятості та кваліфікаційному складі виконавців [4] і пошкодження інфраструктури разом із втратою операційного часу й вимушеною зміною локації в регіональному розрізі [3]. Поширення цієї логіки на решту активів ІТ-компанії – дані та транскордонні контракти – приймається в цій статті як вихідна аналітична передумова, а не як емпірично встановлений факт, і саме в такому статусі використовується далі.

Опрацьовані записи корпусу різняться за глибиною доступу: для рецензованих публікацій [1; 2] прочитано назви, для [3; 4] – авторські анотації, для галузевого релізу [5] – повний текст. У межах прочитаного загрози воєнного часу або трансформуються й перелічуються як самостійний предмет аналізу, або вимірюються кількісно в регіональному розрізі, або відображаються через галузеву динаміку експорту й ринку праці, проте ніде не зіставляються з конкретним заходом реагування, його очікуваним ефектом і умовами, за яких цей захід перестає діяти. Саме на цьому зрізі формулюється прикладне завдання: керівництву ІТ-компанії потрібен компактний інструмент, який пов'язував би структуру загроз воєнного часу зі структурою відповіді на них і з межами дієвості кожної відповіді.

Об'єктом дослідження є управління ризиками ІТ-компаній та їхніх проєктних портфелів в умовах дестабілізованого зовнішнього середовища; предметом – склад, структура та профіль взаємної пов'язаності груп загроз, що їх породжує військовий конфлікт, і відповідні їм стратегії мінімізації з межами дієвості. Завдання статті: обґрунтувати критерій класифікації

загроз воєнного часу за ураженим активом IT-компанії; побудувати на цій основі класифікацію, спираючись на верифіковані галузеві, статистичні та рецензовані джерела; зіставити кожній групі загроз стратегію мінімізації, очікуваний ефект і межу дієвості у вигляді матриці; визначити умови застосовності отриманого інструмента та напрями його емпіричної перевірки.

## АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Перша група релевантних публікацій зіставляє нормативні рамки управління ризиком. П. Ржегачек систематизує стандарти ризик-менеджменту, застосовні в управлінні проєктами: він зводить у таблицю визначення ризику, прийняті в PMI (PMBOK), PRINCE2, IPMA та ISO/IEC, і викладає шість процесів управління ризиком за п’ятим виданням PMBOK [7]. А. Портуґал Діаш зіставляє COSO ERM 2017 та ISO 31000:2009 як альтернативні настанови з управління ризиком і розглядає, як вибір між ними позначається на результативності аудиту [8, с. 73–82]. С. Галайці зі співавторами розводять управління безперервністю діяльності, операційну стійкість та організаційну стійкість, спираючись на визначення ISO 22301 у редакції 2019 року й шукаючи спільні риси, відмінності та можливий синтез цих понять [9]. Предметом зіставлення в цих працях виступає рамка управління ризиком – послідовність дій організації щодо ризику; ознак диференціації самого типу зовнішнього збурення в розглянутих текстах не сформульовано.

Друга група праць підходить до питання з протилежного боку – від властивостей самої події. Серед розглянутих публікацій найдетальніше опрацьовано пандемічний випадок. Д. Іванов, моделюючи вплив епідемічних спалахів на глобальні ланцюги постачання на прикладі COVID-19, виокремлює три ознаки, якими епідемія відрізняється від інших дизрупційних ризиків: тривале існування збурення з непередбачуваним нарощуванням масштабу; одночасне поширення ефекту доміно в ланцюзі постачання й самого епідемічного процесу в популяції; одночасні збурення в постачанні, попиті та логістичній інфраструктурі [6]. На противагу цьому землетрус чи вибух на заводі створюють негайний і локалізований вплив, тоді як епідемічний спалах починається з малого, швидко нарощує масштаб і розсіюється багатьма географічними регіонами [6]. Отже, рецензована література вже має аналітичний словник для опису збурення, яке активує кілька каналів ураження водночас; цей словник сформовано на пандемічному, а не на воєнному матеріалі.

Третю лінію становлять праці про геополітичну дизрупцію та збройний конфлікт. С. Роско зі співавторами досліджують управління невизначеністю ланцюга постачання, породженою геополітичними дизрупціями, на матеріалі фармацевтичної галузі та Brexit і трактують геополітичну дизрупцію як окремий клас зовнішньої невизначеності, способи пом’якшення якої залежать від розміру фірми [11]. Дж. С. Срай зі співавторами на досвіді російсько-української війни вводять поняття від’єднання активів ланцюга постачання від території конфлікту та простежують короткострокові, середньострокові й довгострокові шляхи реконфігурації [10]. Л. Мадурейра зі співавторами, аналізуючи поведінку транснаціональних мереж швидкого харчування під час російсько-українського конфлікту, описують адаптацію маркетингових, ланцюгових, соціально-відповідальних та інвестиційних рішень; за даними реферату, наявні рамки міжнародного розвитку бізнесу потребують геополітичної розвідки в режимі реального часу [12]. Об’єктом цих праць є матеріальні ланцюги постачання та роздрібні мережі, а не компанії, чиї активи мають переважно нематеріальний і кадровий характер.

Українська література воєнного періоду розробляє тему безперервності діяльності прямо. У. Ситайло розмежовує стійкість і безперервність бізнесу за підходом до реагування на виклики, класифікує загрози за чотирма категоріями – антропогенні, технологічні, біологічні та стихійні лиха – і оцінює вразливість України за Індексом крихких держав та

INFORM Risk [13]. Критерієм цієї класифікації виступає походження загрози, а вимірювання вразливості ведеться на рівні країни.

Зіставлення розглянутих текстів дає змогу сформулювати таке узагальнення. По-перше, порівняння нормативних рамок [7; 8; 9] розгортається довкола того, як організація має діяти з ризиком, тоді як розрізнення збурень, що активують кілька груп загроз водночас, у цих працях не є предметом аналізу. По-друге, ознаки такої одночасної активації та взаємної пов'язаності наслідків детально виписано на пандемічному матеріалі [6], тоді як щодо збройного конфлікту опрацьовані праці фіксують передусім територіальну реконфігурацію активів і потребу постійного геополітичного моніторингу [10; 11; 12]. Саме на цьому тлі доцільно розглядати воєнне збурення не як поодинокий операційний збій, а як тривалий стан середовища, що одночасно вражає різнорідні активи компанії. По-третє, класифікація загроз воєнного часу, наведена в [13], побудована за походженням загрози та доповнена страновим вимірюванням вразливості, а не переліком уражених активів окремої компанії. Відповідно, у розглянутих джерелах не виявлено інструмента, який зіставляв би групу загроз воєнного часу для IT-компанії з конкретною стратегією мінімізації, очікуваним ефектом і межею дієвості цієї стратегії. Саме на заповнення цієї прогалини спрямовано подальший виклад.

## ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ ТА ПОСТАНОВКА ЗАВДАННЯ

Мета статті – систематизувати задокументовані загрози, які військовий конфлікт створює для IT-компаній, і звести їх у матрицю «група загроз – стратегія мінімізації – очікуваний ефект – межа дієвості». Для кожного рядка матриці окремо позначено доказовий статус за чотирирівневою шкалою: пряме підтвердження галузевими даними, пряме емпіричне підтвердження якісного типу, непряме підтвердження або авторське аналітичне припущення. У запропонованому форматі захід прив'язано одночасно до групи загроз, на яку він спрямований, і до умов, за яких він перестає давати очікуваний ефект.

Критерієм класифікації обрано уражений актив IT-компанії – персонал, обчислювальна та енергетична інфраструктура, дані й IT-периметр, фінансові потоки, правовий і регуляторний статус, клієнтські відносини. Вибір саме цієї основи зумовлений відмінністю в точці прикладання управлінського рішення. Класифікації за походженням загрози – як-от поділ на антропогенні (випадкові та навмисні), технологічні, біологічні та стихійні лиха, застосований у дослідженні безперервності бізнесу в Україні [13], – групують події за джерелом їх виникнення. Натомість реагування компанія будує навколо конкретного активу, який потрібно утримати, захистити або перемістити. Дослідження реконфігурації ланцюгів постачання під час російсько-української війни описує відчеплення (unhooking) активів ланцюга постачання від території та відповідні траєкторії перебудови в коротко-, середньо- і довгостроковому горизонтах [10]. Цей результат узгоджується з активо-орієнтованою оптикою, хоча активи, про які в ньому йдеться, належать ланцюгу постачання, а не переліку критичних активів IT-компанії.

Специфіку воєнного чинника, за гіпотезою цієї статті, несе не сам перелік груп: жодна з них окремо не є унікальною для воєнного контексту. Вирізняльним є профіль одночасної активації та взаємної пов'язаності груп, за якого внутрішньофірмова диверсифікація втрачає ефект, а стратегії мінімізації доводиться застосовувати комплементарним набором. Це припущення сформульоване автором і перевіряється далі, а не запозичене з розглянутих джерел. Орієнтиром для його постановки слугує дослідження того, як фірми різного розміру формують стратегії пристосування до зовнішнього середовища, зруйнованого геополітичною подією (багатонаціональні компанії – планування за найгіршим сценарієм, великі фірми та підприємства малого й середнього бізнесу – стратегія «wait-and-see»), і як вони далі застосовують реактивні та проактивні стратегії пом'якшення ризиків ланцюга постачання [11].

Прикладна деталізація описаного профілю для IT-сектору та зіставлення його з межами дієвості кожної стратегії і становлять завдання подальшого викладу.

## МЕТОДОЛОГІЯ

Дослідження виконано як кабінетний аналіз документованих свідчень із подальшою якісною систематизацією. Джерельну базу сформовано цілеспрямованим добором. Умовою включення запису до бази були дві обов'язкові ознаки: верифікована доступність запису за DOI або URL на момент підготовки статті та тематична належність до воєнного чинника ризику для IT-компаній або до суміжних умов їхньої діяльності – енергетичної інфраструктури, кіберсередовища, регіональної економіки, ринку праці. Окремою, третьою умовою – уже не включення до бази, а залучення запису до побудови рядків матриці – була наявність у прочитаному тексті атрибутованого числового показника, описаного методу збору даних або зафіксованої управлінської практики. Записи, що відповідають двом першим умовам, але не третій, використано лише як свідчення існування відповідного наукового обговорення.

Фактично використаний у «Результатах» корпус складається з чотирьох доказових груп. Перша – галузеві релізи IT Ukraine Association, що відтворюють дані Національного банку України про експорт IT-послуг: 6,7 млрд дол. США у 2023 р. з падінням на 8,5 % проти 2022 р. [16] та 6,4 млрд дол. США у 2024 р. з падінням на 4,3 % проти 2023 р. і країновою розбивкою [5]. Сюди ж віднесено сторінку асоціації з компанійними відсотковими значеннями 2022 р. щодо релокації, адаптації та частки працівників у складі Сил оборони [17]. Друга – публікації в журналах із заявленою процедурою рецензування: українські дослідження воєнних ризиків і регіональної стійкості [3] та динаміки IT-ринку 2020–2024 рр. [4], а також міжнародне дослідження управління кібератаками воєнного часу, побудоване на 19 напівструктурованих інтерв'ю, проведених з травня 2023 р. до травня 2024 р. [14]. Третя – вендорський звіт про трансформацію кіберзагроз, який подає зростання фішингових кампаній російських урядово підтримуваних акторів проти користувачів в Україні у 2022 р. на 250 % відносно базового 2020 р. і понад 300 % проти користувачів у країнах НАТО за той самий період [15]; ці значення стосуються саме окресленого кола акторів, а не фішингового ландшафту загалом. Четверта – конференційні матеріали, з яких залучено відтворені галузеві показники ринку праці та експорту [18]; їхню вагу в доказовій частині свідомо знижено порівняно з журнальними публікаціями. Поза цими чотирма групами перебуває п'ята, недоказова: матеріали міжнародної конференції CyCon (IEEE) [19; 20] та індексна сторінка аналітичної серії асоціації [21], які не використано для жодного твердження по суті.

Для рядків матриці запроваджено чотирирівневу шкалу доказового статусу. Рівень «пряме підтвердження галузевими даними» присвоєно твердженням, під якими стоїть прочитаний показник із зазначеним джерелом даних, роком і предметом вимірювання: це показники експорту IT-послуг за даними НБУ [5; 16] та кількісні оцінки кібератак із вендорської телеметрії [15]. Рівень «пряме емпіричне підтвердження якісного типу» виокремлено для результатів інтерв'ю [14]: дослідження дає тематичні узагальнення, а не вимірюваний показник, а його респондентами є представники українських органів публічної влади – керівники місцевого самоврядування та фахівці з кібербезпеки, – а не працівники IT-компаній, тому його висновки переносяться на корпоративний сектор лише як опис середовища. Рівень «непряме підтвердження» присвоєно твердженням, що спираються на показники суміжного об'єкта – регіональної економіки, енергетичної інфраструктури, ринку праці – і переносяться на IT-компанії як зовнішню умову їхньої діяльності [3; 18], а також на самозвітні компанійні значення без описаної процедури вибірки [17]. Рівень «аналітичне припущення» позначає авторське узагальнення, що логічно випливає із зіставлення джерел, але не має власного числового підтвердження; такі рядки позначено в матриці окремо, і на них не будується жодного кількісного висновку.

Обмеження прочитання зафіксовано явно. Для матеріалів конференції CyCon [19; 20] встановлено лише реєстраційні метадані – назви, авторів, видавця, сторінки й майданчик публікації. Повних текстів не відкрито, тому з них не виведено жодного показника, жодної моделі та жодної кількості стадій. Ці записи засвідчують лише те, що проблематика кіберстійкості критичної інфраструктури та хмарної міграції в Україні є предметом обговорення на профільному міжнародному майданчику. Індексна сторінка аналітичної серії асоціації [21] підтверджує існування й назви відповідних звітів, але не є джерелом цифр: текстів окремих звітів не відкрито. Публікацію про динаміку IT-ринку [4] прочитано на рівні анотації на сторінці видавця, тому з неї взято лише наведені в самій анотації річні обсяги експорту та якісні характеристики ринку праці, без деталізації за сегментами ринку й без відтворення розрахунків. Сторінка асоціації за 2022 р. [17] не наводить обсягу вибірки та методу польового збору, тому її значення подано як звітні дані галузевого об'єднання, а не як результат репрезентативного опитування.

Із зазначених обмежень випливає й правило формулювання, прийняте в статті: жодне твердження про відсутність певних положень у документах, доступ до повних текстів яких обмежено, не робиться; узагальнення щодо трактування конфліктного ризику подано як авторські й відмежовано від цитованого змісту. Метод має три власні обмеження, які враховано при інтерпретації результатів: корпус не є вичерпним і зміщений у бік української емпірики періоду 2022–2025 рр.; переважна частина показників має агрегований галузевий, а не фірмовий рівень, що унеможливлює кількісне оцінювання ефекту окремого заходу; панельних спостережень за одними й тими самими компаніями в динаміці серед прочитаних джерел не виявлено, тому межі дієвості стратегій встановлюються аналітично і потребують подальшої емпіричної перевірки.

## ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Класифікацію воєнних загроз побудовано за ознакою ураженого активу IT-компанії, що дає шість груп: персонал; обчислювальна та енергетична інфраструктура; дані й IT-периметр; фінансові потоки; правовий і регуляторний статус; клієнтські відносини. Активом тут вважається ресурс або відношення, втрата якого зупиняє виконання зобов'язань перед замовником, тому дві останні групи є активами не в обліковому значенні цього слова. Групи розмежовано за точкою прикладання управлінського рішення, а не за причиною ураження, тож вони не є причинно незалежними, а перелік не претендує на вичерпність. Обраний критерій відрізняється від тих, за якими згруповано ризики в суміжних дослідженнях: у праці, присвяченій ризикам та економічній безпеці підприємств у процесі відновлення України, ризики поділено за їх природою на воєнні, енергетичні, логістичні, кадрові та кібернетичні [2], а трансформацію загроз економічній безпеці підприємства в умовах воєнного стану описано через пошкодження інфраструктури, розрив ланцюгів постачання, зростання ринкової невизначеності та мобілізацію персоналу [1]. Запропонований поділ не заперечує цих переліків і частково з ними перетинається, проте впорядковує загрози за об'єктом ураження, а не за походженням, і тим самим дозволяє зіставити кожну групу зі стратегією та межею її дієвості. Для прозорості доказової бази до кожної групи застосовано описану в методології чотирирівневу шкалу: пряме підтвердження галузевими даними – числові показники галузевих або офіційних джерел, прочитані в їх тексті; пряме емпіричне підтвердження якісного типу – результати інтерв'ю без вимірюваного показника; непряме підтвердження – фіксація явища в рецензованій літературі без деталізації саме для IT-сектору; аналітичне припущення – узагальнення авторів, яке з наявних даних випливає логічно, але окремо не виміряне.

Група 1, персонал, має пряме числове підтвердження. За опублікованими IT Ukraine Association показниками 2022 р., 70,8 % IT-компаній здійснили незаплановану релокацію, 16,7

% перемістилися повністю або частково за кордон, водночас 81,5 % компаній, що релокувалися за кордон, заявили про намір повернутися після скасування воєнного стану; 70 % компаній мали фахівців, які служать у Збройних Силах, причому в 43 % компаній це до 5 % штату, а в 25 % – від 5 до 15 % [17]. Публікація не зазначає обсягу вибірки та методу збору даних, тому ці значення використано як задекларовані галузевим об'єднанням, а не як результат репрезентативного опитування. Кадровий чинник підтверджено й з боку наслідків: скорочення експорту ІТ-послуг у 2023 р. асоціація пояснювала, зокрема, дефіцитом висококваліфікованих фахівців [16]. Якісні зрушення на ринку праці фіксує й аналіз ІТ-ринку 2020–2024 рр. – зменшення частки молодших спеціалістів і зростання ролі гіг-контрактів [4]. Релокацію як інструмент адаптації підприємництва в умовах економічної нестабільності описано в рецензованій літературі поряд із реструктуризацією, диверсифікацією та цифровізацією [23]; це підтвердження непряме, оскільки стосується підприємництва загалом, а не ІТ-сектору окремо.

Група 2, обчислювальна та енергетична інфраструктура, підтверджена прямо, але на рівні регіональної економіки, а не окремих ІТ-компаній. Оцінювання воєнних ризиків за серпень 2024 – серпень 2025 рр. виконано на релокаційних даних Opendatabot, обліку простою торговельних центрів, записах ACLED про удари по інфраструктурі та динаміці повітряних тривог; за цими вимірюваннями в окремих прифронтових областях магазини втрачають до 50 % свого операційного часу, тоді як у західних регіонах простій падає нижче 1 %, а переміщення бізнесу не зводиться до схеми «схід – захід»: регіони з підвищеною безпековою загрозою водночас є зонами активної релокаційної активності [3]. Показник простою стосується роздрібної торгівлі, тому в цій роботі він використовується як проксі-індикатор регіональної експозиції до воєнного ризику, а не як вимірювання втрат ІТ-сектору. Пошкодження інфраструктури як самостійну загрозу економічній безпеці підприємства зафіксовано й у [1]. Для енергетичної складової нормативну відповідь запропоновано в дослідженні енергетичної стійкості та бізнес-життєздатності: адаптивну стратегію побудовано на автономності, адаптивності та стійкості й розгорнуто в чотири послідовні етапи [25]; ця стратегія емпірично не перевірена, тому її статус тут – нормативна рекомендація. Тематику переходу від кінетичного руйнування до хмарної міграції як способу побудови стійкої інфраструктури в Україні винесено в назву доповіді CyCon [19]; повний текст у межах цього дослідження не опрацьовано, тому за нею фіксується лише предметна віднесеність, без запозичення результатів.

Група 3, дані й ІТ-периметр, підтверджена прямо за зовнішніми вимірюваннями. Звіт про трансформацію кіберзагроз унаслідок війни фіксує зростання фішингу, спонсорованого державними структурами РФ, проти користувачів в Україні у 2022 р. на 250 % відносно базового 2020 р. і більш ніж на 300 % проти користувачів у країнах НАТО [15]. Управлінський бік цієї загрози досліджено у кейсі України в Public Administration Review, побудованому на 19 напівструктурованих інтерв'ю, проведених у травні 2023 – травні 2024 рр. [14]. Кібернетичні ризики присутні й у розглянутому галузевому угрупованні [2]. Істотно, що ця група загроз безпосередньо змикається з групою 2: кібернетичний і кінетичний вплив спрямовані на ту саму енергетичну й комунікаційну основу, від якої залежить безперервність розробки.

Група 4, фінансові потоки, має найповніше числове підтвердження. Експорт ІТ-послуг України зріс із 5,03 млрд дол. США у 2020 р. до пікових 7,34 млрд у 2022 р. (за даними НБУ – 7,322 млрд, див. табл. 3), а у 2024 р. становив 6,45 млрд [4]. Перше воєнне скорочення зафіксовано за підсумками 2023 р. – 6,7 млрд дол. США, що на 8,5 % менше за 2022 р., з одночасним зниженням частки ІТ у загальному експорті послуг [16]; обсяг і темп цього скорочення відтворено також у матеріалах конференції, де частку ІТ подано як понад 40 % експорту послуг України [18], однак це збірник доповідей, а не рецензований журнал, що знижує його доказову вагу. За 2024 р. асоціація, спираючись на дані Національного банку України, наводить 6,4 млрд дол. США – на 4,3 % менше за 2023 р. [5]; розбіжність із наведеним

у [4] значенням 6,45 млрд лежить у межах округлення й не змінює напряму динаміки. Ці ряди підтверджують не разовий шок, а багаторічну низхідну траєкторію доходу за умов, коли решта груп загроз лишаються активними.

Група 5, правовий і регуляторний статус, підтверджена прямо в частині мобілізаційного регулювання. Відправною точкою цього режиму стало ухвалення 4 листопада 2022 р. законопроєкту № 7687 про бронювання військовозобов'язаних на підприємствах, визнаних критично важливими [22]; подальші зміни порядку бронювання перебувають поза межами опрацьованого корпусу. Правовий аналіз бронювання ІТ-фахівців фіксує прогалини чинного порядку – передусім відсутність механізму обліку осіб, які працюють за гіг-контрактами, – і пропонує електронну реєстрацію даних про зайнятість та прискорений порядок для роботодавців-резидентів Дія Сіті [24]. Регуляторний вимір має й транскордонний бік: правову складність ділових поїздок асоціація прямо назвала серед причин скорочення експорту 2023 р. [16]. Отже, ця група загроз впливає не лише на утримання персоналу, а й на здатність компанії підтримувати присутність на зовнішніх ринках.

Група 6, клієнтські відносини, підтверджена непрямо. Прямих опитувань замовників у доступному корпусі не опрацьовано; наявні дані дають лише структуру попиту. Розподіл експорту 2024 р. показує високу концентрацію за країнами, при цьому динаміка за окремими ринками різноспрямована: зниження надходжень з одних юрисдикцій супроводжується зростанням з інших [5]. Різноспрямованість динаміки за країнами свідчить, що клієнтський ризик не є однорідним за ринками. Загальну рамку дає зафіксоване в літературі зростання ринкової невизначеності як складова трансформації загроз воєнного часу [1]. Висновок про репутаційний та контрактний тиск на українського постачальника як самостійну групу загроз лишається аналітичним припущенням авторів.

Зіставлення груп загроз зі стратегіями мінімізації зведено в табл. 1. Стовпці матриці фіксують чотири елементи: групу загроз, стратегію мінімізації, очікуваний ефект і межу дієвості, тобто умову, за якої стратегія перестає давати цей ефект. Останній стовпець є ключовим для управлінського застосування: саме він відрізняє матрицю від антикризових переліків заходів. Формулювання стовпців «очікуваний ефект» і «межа дієвості» мають, за прийнятою шкалою, статус аналітичного узагальнення авторів: у джерелах, текст яких опрацьовано, результативність окремого заходу в ІТ-компанії не вимірювалася. Доказовий статус прямого підтвердження стосується наявності самої загрози та факту нормативного закріплення стратегії там, де таке закріплення зафіксовано.

Для групи «персонал» стратегією є бронювання критично важливих фахівців у поєднанні з географічним розосередженням команд і релокацією [22; 24; 23; 17]; очікуваний ефект – утримання ключових компетенцій і збереження виробничої спроможності підрозділів. Межа дієвості визначається тим, що бронювання не поширюється рівномірно на всі форми зайнятості, зокрема на гіг-контракти, і залежить від статусу підприємства як критично важливого [24; 22]; щодо релокації за кордон сама асоціація фіксує намір повернутися у 81,5 % компаній, що перемістилися за межі країни [17], тож ризик неповернення персоналу є тут аналітичним припущенням авторів, а не задокументованим фактом. Для групи «інфраструктура» пряму опору в опрацьованих джерелах має лише автономне енергозабезпечення: адаптивну стратегію на засадах автономності, адаптивності та стійкості з розгортанням у чотири етапи сформульовано в [25] як нормативну, емпірично не перевірену рекомендацію. Розподілену архітектуру обчислень додано до цього рядка як аналітичну пропозицію авторів – у [25] вона не розглядається. Очікуваний ефект – скорочення простою під час знеструмлень і обстрілів. Межею є вичерпання автономності за тривалих і повторюваних відключень та прив'язка резервування до конкретної локації, безпекова експозиція якої в прифронтових областях суттєво вища, що засвідчують регіональні контрасти простою та релокаційної активності [3]. Для групи «дані й ІТ-периметр» кратне зростання фішингових кампаній, зафіксоване в [15], та управлінські труднощі протидії кібератакам,

задокументовані в кейсі українських органів влади, серед яких недостатня підготовка та чинник людської поведінки [14], обґрунтовують стратегію кіберстійкості периметра й навчання працівників; ефект – зниження успішності масових кампаній. Межа дієвості полягає в тому, що навчання й посилення периметра знижують частку успішних спроб, але не їх кількість, тож за зростання інтенсивності атак, задокументованого в [15], залишковий ризик зростає навіть за незмінної частки успішних проникнень; припущення про перенесення тиску на зовнішні залежності компанії, які вона не контролює, є аналітичним узагальненням авторів і в опрацьованому тексті звіту підтвердження не має.

Для групи «фінансові потоки» опрацьовані джерела прямо підтверджують саму загрозу – багаторічне скорочення експорту [16; 5] – і структуру попиту за країнами, у якій динаміка 2024 р. різноспрямована [5]. Диверсифікацію ринків і валютних надходжень виведено авторами з цієї структури як аналітичну пропозицію: у розглянутих релізах асоціації вона не рекомендована й не задокументована як застосована практика; причинами скорочення 2023 р. асоціація називає правову складність ділових поїздок і дефіцит фахівців [16], а щодо 2024 р. характеризує падіння як поступове й очікує стабілізації з 2025 р. [5]. Відповідно очікуваний ефект цього рядка – компенсація падіння в одному сегменті зростанням в інших – і межа його дієвості – концентрація портфеля на одному ринку, за якої перерозподіл не встигає спрацювати в межах бюджетного року, тоді як сукупний обсяг усе одно скорочується [5; 4], – мають статус авторського узагальнення. Для групи «правовий і регуляторний статус» стратегія – набуття та підтримання статусу критично важливого підприємства й резидентства Дія Сіті, а також формалізація процедур бронювання [22; 24]; ефект – передбачуваність кадрового режиму. Межа – залежність від змін законодавства та від неврегульованих категорій зайнятості [24]. Рядок «клієнтські відносини» подано як аналітичну пропозицію авторів: договірні гарантії безперервності, прозорість повідомлення про безпекові інциденти та юрисдикційна диверсифікація виводяться з логіки попередніх груп, а не з опрацьованих джерел; емпіричну опору має лише географія попиту, зокрема різноспрямована динаміка експорту за країнами у 2024 р. [5]. Відповідно очікуваний ефект і межу дієвості для цього рядка сформульовано аналітично: підтвердження в корпусі вони не мають і потребують окремої перевірки.

Комплементарність стратегій випливає зі структури самої матриці. Бронювання утримує фахівця в країні, але не забезпечує йому робоче місце під час знеструмлення; автономне енергозабезпечення дає електрику, але не захищає периметр від фішингових кампаній, інтенсивність яких зросла в рази [15]; кіберстійкість периметра, своєю чергою, не відновлює замовлення, втрачені через правову складність ділових поїздок [16]. Кожна стратегія закриває лише свою групу загроз і має власну, незалежну від інших межу. Тому набір стратегій діє як система: відмова однієї ланки не компенсується посиленням сусідньої, а навпаки, відкриває канал, через який реалізується вся пов’язана група.

Профіль одночасної активації пояснює, чому внутрішньофірмова диверсифікація втрачає ефект. Опрацьовані дані вказують, що групи загроз реалізуються не послідовно, а в межах одного проміжку часу: на 2022–2024 рр. припадають масова релокація та відтік персоналу до Збройних Сил [17], кратне зростання кібератак [15], пошкодження інфраструктури з регіонально диференційованою експозицією бізнесу [3], скорочення експорту два роки поспіль [16; 5] і зміни мобілізаційного регулювання [22; 24]. Це не спільне вимірювання: кожен показник отримано окремим джерелом для свого об’єкта, тож ідеться про збіг періодів, а не про доведену одночасність на рівні окремої компанії. За таких умов перенесення ресурсів між напрямами всередині компанії не зменшує сукупного ризику, бо джерело збурення спільне й компанії непідконтрольне. Це і є та властивість воєнного чинника, яку запропонована матриця робить операційною: управлінське рішення приймається не щодо окремої ризик-події, а щодо набору стратегій із явно зазначеними межами, за якими кожна з них перестає працювати.

Географію попиту, різноспрямована динаміка якої лежить в основі цього спостереження, унаочнює рис. 1.

Галузеві показники релокації та участі фахівців в обороні, на які спирається цей рядок матриці, зведено в табл. 2.

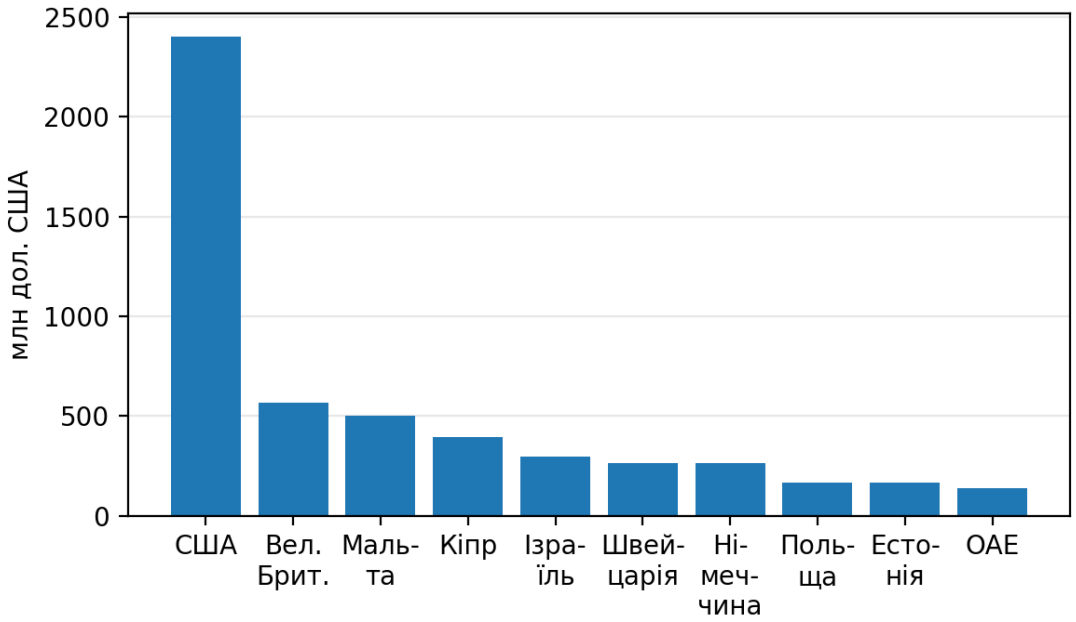



*Рис. 1 Географічна структура експорту IT-послуг України у 2024 р. за десятьма найбільшими країнами-замовниками, млн дол. США (за даними Національного банку України)*

*Таблиця 1*

*Матриця «група загроз – стратегія мінімізації – очікуваний ефект – межа дієвості» для IT-компанії в умовах військового конфлікту, із зазначенням доказового статусу кожного рядка*

| Група загроз (уражений актив) | Стратегія мінімізації | Очікуваний ефект | Межа дієвості | Доказовий статус рядка |
|---|---|---|---|---|
| **1** | 2 | 3 | 4 | 5 |
| 1. Персонал | Бронювання критично важливих фахівців; географічне розосередження команд і релокація [22; 24; 23] | Утримання ключових компетенцій і збереження виробничої спроможності підрозділів | Бронювання не охоплює рівномірно всі форми зайнятості, зокрема гіг-контракти, і залежить від статусу підприємства як критично важливого [24; 22] | Пряме підтвердження загрози галузевими даними [17] і нормативного закріплення стратегії [22]; ефект і межа – аналітичне узагальнення авторів |
| 2. Обчислювальна та енергетична інфраструктура | Автономне енергозабезпечення за схемою «автономність – адаптивність – стійкість», розгорнутою в чотири етапи [25]; розподілена | Скорочення простою під час знеструмлень і обстрілів | Вичерпання автономності за тривалих і повторюваних відключень; прив'язка резервування до локації, безпекова експозиція якої в | Непряме підтвердження загрози (регіональні виміри простою та релокації [3]); стратегія – нормативна, емпірично не перевірена рекомендація [25] |

| | | | | |
|---|---|---|---|---|
| | архітектура обчислень – пропозиція авторів | | прифронтових областях суттєво вища [3] | |
| 3. Дані й IT-периметр | Кіберстійкість периметра та навчання працівників [14; 15] | Зниження успішності масових фішингових кампаній | Навчання й захист периметра знижують частку успішних спроб, але не їх кількість: за зростання фішингу російських урядово підтримуваних акторів проти користувачів в Україні на 250 % у 2022 р. до базового 2020 р. залишковий ризик зростає [15] | Пряме підтвердження вендорською телеметрією [15]; пряме емпіричне підтвердження якісного типу за 19 напівструктурованими інтерв'ю [14] |
| 4. Фінансові потоки | Диверсифікація ринків і валютних надходжень – аналітична пропозиція авторів, виведена зі структури попиту за країнами [5] | Компенсація падіння в одному сегменті зростанням в інших | Концентрація портфеля на одному ринку, за якої перерозподіл не встигає спрацювати в межах бюджетного року, тоді як сукупний обсяг усе одно скорочується [5; 4] | Пряме підтвердження загрози: −8,5 % експорту у 2023 р. [16] і −4,3 % у 2024 р. [5]; стратегія, ефект і межа – аналітичне припущення |
| 5. Правовий і регуляторний статус | Набуття та підтримання статусу критично важливого підприємства й резидентства Дія Сіті; формалізація процедур бронювання [22; 24] | Передбачуваність кадрового режиму та умов транскордонної присутності | Залежність від змін законодавства та від неврегульованих категорій зайнятості [24] | Пряме підтвердження: ухвалення законопроєкту № 7687 від 04.11.2022 [22] і правовий аналіз прогалин порядку бронювання [24] |
| 6. Клієнтські відносини | Договірні гарантії безперервності, прозоре повідомлення про безпекові інциденти, юрисдикційна диверсифікація – пропозиція авторів | Утримання довіри замовника за передбачуваного інформування про безпекові інциденти; у корпусі не підтверджено | Договірні гарантії не діють, коли перерву кваліфіковано як форс-мажор; юрисдикційна диверсифікація не допомагає, якщо місце фактичного виконання робіт не змінюється | Аналітичне припущення авторів; емпірична опора – лише різноспрямована динаміка експорту за країнами у 2024 р. [5] та зафіксоване зростання ринкової невизначеності [1] |

*Таблиця 2*

*Кадрові та релокаційні показники ІТ-компаній України за галузевим обстеженням 2022 р., % (обсяг вибірки та метод польового збору в публікації не зазначено)*

| Показник | Значення, % | База обчислення |
|---|---|---|
| Здійснили незаплановану релокацію | 70,8 | усі опитані компанії |
| Здійснили повну або часткову релокацію за кордон | 16,7 | усі опитані компанії |
| Планують повернути бізнес в Україну | 81,5 | компанії, що релокувалися за кордон |
| Мають фахівців, які служать у Збройних Силах України | 70,0 | усі опитані компанії |
| Частка фахівців у Збройних Силах – до 5 % штату | 43,0 | усі опитані компанії |
| Частка фахівців у Збройних Силах – від 5 % до 15 % штату | 25,0 | усі опитані компанії |

*Таблиця 3*

*Параметри першого воєнного скорочення експорту ІТ-послуг України: 2023 р. проти 2022 р. (за даними Національного банку України)*

| Показник | Значення |
|---|---|
| Експорт ІТ-послуг, 2022 р. | 7,322 млрд дол. США |
| Експорт ІТ-послуг, 2023 р. | 6,7 млрд дол. США |
| Абсолютне скорочення 2023 р. до 2022 р. | −622 млн дол. США |
| Відносне скорочення 2023 р. до 2022 р. | −8,5 % |
| Частка ІТ в експорті послуг, 2022 р. | 45,3 % |
| Частка ІТ в експорті послуг, 2023 р. | 42 % |
| Експорт у грудні 2023 р. | 611 млн дол. США (+8,3 %) |

## ВИСНОВКИ

Проведене дослідження дало змогу звести задокументовані загрози воєнного часу для ІТ-компаній не в перелік, а в матрицю «група загроз – стратегія мінімізації – очікуваний ефект – межа дієвості», у якій доказовий статус кожного рядка зазначено явно. Матриця придатна до застосування за трьох умов: компанія зберігає операційну присутність у зоні дії конфлікту або залежність від її ресурсів; вона управляє портфелем проєктів із транскордонними зобов'язаннями; безпекове середовище трактується як постійний, а не разовий чинник планування. Поза цими умовами рядки матриці зберігають радше діагностичне, ніж приписове значення, оскільки специфіку воєнного чинника несе не склад груп, а профіль їх одночасної активації.

Результат обмежений трьома обставинами. Перша – проєктний характер частини зіставлених стратегій. Так, адаптивну стратегію енергетичної стійкості, на яку спирається рядок «інфраструктура», побудовано методом концептуального моделювання й на емпіричному матеріалі не перевірено [25], тому відповідні очікувані ефекти мають у матриці статус аналітичного припущення, а не виміряної величини. Друга обставина – нерівномірність доказової бази: рядки, забезпечені галузевими опитуваннями та офіційною статистикою, і

рядки з непрямим підтвердженням не є взаємозамінними за надійністю, тому матриця має читатися разом із зазначеним для кожного рядка доказовим статусом. Третя – українська прив'язка вибірки: усі прямі підтвердження походять з одного конфліктного контексту, і перенесення висновків на інші юрисдикції потребує окремого обґрунтування.

Окремо слід зважати на термінологічну межу. Стійкість і безперервність діяльності різняться за підходом до реагування на виклики [13], тож стратегії матриці не варто ототожнювати з плануванням безперервності бізнесу: матриця фіксує реакції на визначені групи загроз, а не повний управлінський контур цього планування.

Напрями емпіричної перевірки випливають із цих обмежень. Перший – панельне обстеження ІТ-компаній, яке дало б змогу зіставити задекларовані та фактично застосовані стратегії й перевести очікувані ефекти з аналітичного статусу у вимірюваний. Другий – перенесення схеми на інші сектори, для яких управлінські реакції в межах цього ж конфлікту вже досліджено: реконфігурацію й від'єднання ланцюгів постачання від території конфлікту в російсько-українській війні [10] та стратегії міжнародного розвитку і конкурентної розвідки транснаціональних компаній у зоні цього конфлікту на матеріалі індустрії швидкого харчування [12]; перевірка на інших конфліктних контекстах становить окреме завдання, яке потребує власної емпіричної бази. Третій – зіставлення внутрішньофірмових оцінок ураженості із зовнішніми індексами, які вже застосовувалися для оцінювання вразливості України, зокрема з Індексом крихких держав (Fragile States Index) та Індексом INFORM Risk [13]. Така перевірка дозволить уточнити межі дієвості кожного рядка, не розширюючи при цьому переліку самих стратегій.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Файфер С. М. Трансформація загроз економічній безпеці підприємства під час воєнного стану: аналіз та рекомендації. Інвестиції: практика та досвід. 2024. С. 145–150. DOI: 10.32702/2306-6814.2024.21.145

2. Бобиль В. В., Лоскутова Г. А. Ризики та економічна безпека підприємств у процесі відновлення України. Інвестиції: практика та досвід. 2025. С. 52–57. DOI: 10.32702/2306-6814.2025.24.52

3. Кабанова М., Мельничук В., Семенченко Н. Wartime risks and regional economic resilience in Ukraine: air raids, infrastructure attacks and business relocation. Сталий розвиток економіки. 2025. С. 155–163. DOI: 10.32782/2308-1988/2025-57-21

4. Мазур Н., Чухрай Н. Динаміка ІТ-ринку України: аналіз за 2020–2024 роки. Grail of Science. 2025. С. 189–197. DOI: 10.36074/grail-of-science.20.06.2025.020

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: 19.09.2026).

6. Ivanov D. Predicting the impacts of epidemic outbreaks on global supply chains: A simulation-based analysis on the coronavirus outbreak (COVID-19/SARS-CoV-2) case. Transportation Research Part E: Logistics and Transportation Review. 2020. P. 101922. DOI: 10.1016/j.tre.2020.101922

7. Rehacek P. Risk management standards for project management. International Journal of Advanced and Applied Sciences. 2017. P. 1–13. DOI: 10.21833/ijaas.2017.06.001

8. Dias A. P. A more effective audit after COSO ERM 2017 or after ISO 31000:2009? Perspectiva Empresarial. 2017. P. 73–82. DOI: 10.16967/rpe.v4n2a8

9. Galaitsi S. E., Pinigina E., Keisler J. M., Pescaroli G., Keenan J. M., Linkov I. Business continuity management, operational resilience, and organizational resilience: commonalities, distinctions, and synthesis. International Journal of Disaster Risk Science. 2023. P. 713–721. DOI: 10.1007/s13753-023-00494-x

10. Srai J. S., Graham G., Van Hoek R., Joglekar N., Lorentz H. Impact pathways: unhooking supply chains from conflict zones – reconfiguration and fragmentation lessons from the Ukraine-Russia war. International Journal of Operations & Production Management. 2023. P. 289–301. DOI: 10.1108/IJOPM-08-2022-0529

11. Roscoe S., Skipworth H., Aktas E., Habib F. Managing supply chain uncertainty arising from geopolitical disruptions: evidence from the pharmaceutical industry and Brexit. International Journal of Operations & Production Management. 2020. P. 1499–1529. DOI: 10.1108/IJOPM-10-2019-0668

12. Madureira L., Sergeenko I., Zaimeko S. Competitive intelligence and international business development strategies for multinational enterprises in conflict zones: a study of the fast-food industry during the Russia-Ukraine conflict. Journal of Intelligence Studies in Business. 2023. P. 10–32. DOI: 10.37380/jisib.v13si1.1133

13. Ситайло У. Безперервність бізнесу в Україні: виклики та можливості в умовах війни. Економіка та суспільство. 2024. DOI: 10.32782/2524-0072/2024-62-22

14. Fyshchuk I., Noesgaard M. S., Nielsen J. A. Managing cyberattacks in wartime: the case of Ukraine. Public Administration Review. 2025. P. 619–627. DOI: 10.1111/puar.13895

15. Google Threat Analysis Group, Mandiant, Google Trust & Safety. Fog of war: how the Ukraine conflict transformed the cyber threat landscape. Google, 2023. 27 pp. URL: https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf (дата звернення: 19.09.2026).

16. IT Ukraine Association. In 2023, Ukrainian IT services export faced its first decline in years. 2024. URL: https://itukraine.org.ua/en/in-2023-ukrainian-it-services-export-faced-its-first-decline-in-years/ (дата звернення: 19.09.2026).

17. IT Ukraine Association. Do IT like Ukraine research: tech industry is growing despite the war. 2022. URL: https://itukraine.org.ua/en/do-it-like-ukraine-research-tech-industry-is-growing-despite-the-war/ (дата звернення: 19.09.2026).

18. Акулов О. Ринок праці ІТ-сектору України в умовах воєнного стану та його вплив на національну економіки. Матеріали конференцій МЦНД. 2024. С. 23–26. DOI: 10.62731/mcnd-25.10.2024.001

19. Kulyk S., Zubok V., Mishyna N., Davydiuk A. From kinetic destruction to cybersecurity: building resilient infrastructure through cloud migration in Ukraine. 2026 18th International Conference on Cyber Conflict (CyCon). IEEE, 2026. P. 281–304. DOI: 10.23919/cycon70911.2026.11609429

20. Davydiuk A., Zubok V. Analytical review of the resilience of Ukraine's critical energy infrastructure to cyber threats in times of war. 2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon). IEEE, 2023. P. 121–139. DOI: 10.23919/cycon58705.2023.10181813

21. IT Ukraine Association. Research. 2026. URL: https://itukraine.org.ua/en/research/ (дата звернення: 19.09.2026).

22. IT Ukraine Association. The law on the reservation of IT professionals has been adopted! 2022. URL: https://itukraine.org.ua/en/the-law-on-the-reservation-of-it-professionals-has-been-adopted/ (дата звернення: 19.09.2026).

23. Малярчук О. Релокація бізнесу як інструмент адаптації суб'єктів підприємництва в умовах економічної нестабільності. Економіка та суспільство. 2025. DOI: 10.32782/2524-0072/2025-82-90

24. Сапітон Д. В. Щодо питання бронювання ІТ-фахівців на період мобілізації та на воєнний час. Збірник наукових праць ХНПУ імені Г. С. Сковороди «Право». 2024. С. 149–159. DOI: 10.34142/23121661.2024.39.18

25. Зарічна Н. З., Маркович І. Б. Енергетична стійкість та бізнес-життєздатність: стратегії адаптації підприємств України в умовах війни та дефіциту енергоресурсів. Науковий вісник

Siroshtan, O. & Vasyliev, O. (2026). Military conflict as a risk factor for the IT sector: a systematisation of threats and mitigation strategies. Management and Entrepreneurship: Trends of Development, 3(37), 413-429. https://doi.org/10.26661/2522-1566/2026-3/37-29

Полтавського університету економіки і торгівлі. Серія «Економічні науки». 2026. С. 29–31. DOI: 10.37734/2409-6873-2026-1-3

**REFERENCES**

Faifer, S. M. (2024). Transformatsiia zahroz ekonomichnii bezpetsi pidpryiemstva pid chas voiennoho stanu: analiz ta rekomendatsii. Investytsii: praktyka ta dosvid, 145–150. https://doi.org/10.32702/2306-6814.2024.21.145

Bobyl, V. V., & Loskutova, H. A. (2025). Ryzyky ta ekonomichna bezpeka pidpryiemstv u protsesi vidnovlennia Ukrainy. Investytsii: praktyka ta dosvid, 52–57. https://doi.org/10.32702/2306-6814.2025.24.52

Kabanova, M., Melnychuk, V., & Semenchenko, N. (2025). Wartime risks and regional economic resilience in Ukraine: Air raids, infrastructure attacks and business relocation. Stalyi rozvytok ekonomiky, 155–163. https://doi.org/10.32782/2308-1988/2025-57-21

Mazur, N., & Chukhrai, N. (2025). Dynamika IT-rynku Ukrainy: analiz za 2020–2024 roky. Grail of Science, 189–197. https://doi.org/10.36074/grail-of-science.20.06.2025.020

IT Ukraine Association. (2025). Ukraine's IT exports declined by over 4% in 2024. What's next? https://itukraine.org.ua/en/ukraine-s-it-exports-declined-by-over-4-in-2024-what-next/

Ivanov, D. (2020). Predicting the impacts of epidemic outbreaks on global supply chains: A simulation-based analysis on the coronavirus outbreak (COVID-19/SARS-CoV-2) case. Transportation Research Part E: Logistics and Transportation Review, 101922. https://doi.org/10.1016/j.tre.2020.101922

Rehacek, P. (2017). Risk management standards for project management. International Journal of Advanced and Applied Sciences, 1–13. https://doi.org/10.21833/ijaas.2017.06.001

Dias, A. P. (2017). A more effective audit after COSO ERM 2017 or after ISO 31000:2009? Perspectiva Empresarial, 73–82. https://doi.org/10.16967/rpe.v4n2a8

Galaitsi, S. E., Pinigina, E., Keisler, J. M., Pescaroli, G., Keenan, J. M., & Linkov, I. (2023). Business continuity management, operational resilience, and organizational resilience: Commonalities, distinctions, and synthesis. International Journal of Disaster Risk Science, 713–721. https://doi.org/10.1007/s13753-023-00494-x

Srai, J. S., Graham, G., Van Hoek, R., Joglekar, N., & Lorentz, H. (2023). Impact pathways: Unhooking supply chains from conflict zones – reconfiguration and fragmentation lessons from the Ukraine-Russia war. International Journal of Operations & Production Management, 289–301. https://doi.org/10.1108/IJOPM-08-2022-0529

Roscoe, S., Skipworth, H., Aktas, E., & Habib, F. (2020). Managing supply chain uncertainty arising from geopolitical disruptions: Evidence from the pharmaceutical industry and Brexit. International Journal of Operations & Production Management, 1499–1529. https://doi.org/10.1108/IJOPM-10-2019-0668

Madureira, L., Sergeenko, I., & Zaimeko, S. (2023). Competitive intelligence and international business development strategies for multinational enterprises in conflict zones: A study of the fast-food industry during the Russia-Ukraine conflict. Journal of Intelligence Studies in Business, 10–32. https://doi.org/10.37380/jisib.v13si1.1133

Sytailo, U. (2024). Bezperervnist biznesu v Ukraini: vyklyky ta mozhlyvosti v umovakh viiny. Ekonomika ta suspilstvo. https://doi.org/10.32782/2524-0072/2024-62-22

Fyshchuk, I., Noesgaard, M. S., & Nielsen, J. A. (2025). Managing cyberattacks in wartime: The case of Ukraine. Public Administration Review, 619–627. https://doi.org/10.1111/puar.13895

Google Threat Analysis Group, Mandiant, & Google Trust & Safety. (2023). Fog of war: How the Ukraine conflict transformed the cyber threat landscape (27 pp.). Google. https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf

IT Ukraine Association. (2024). In 2023, Ukrainian IT services export faced its first decline in years. https://itukraine.org.ua/en/in-2023-ukrainian-it-services-export-faced-its-first-decline-in-years/

IT Ukraine Association. (2022). Do IT like Ukraine research: Tech industry is growing despite the war. https://itukraine.org.ua/en/do-it-like-ukraine-research-tech-industry-is-growing-despite-the-war/

Akulov, O. (2024). Rynok pratsi IT-sektoru Ukrainy v umovakh voiennoho stanu ta yoho vplyv na natsionalnu ekonomiky. Materialy konferentsii MTsND, 23–26. https://doi.org/10.62731/mcnd-25.10.2024.001

Kulyk, S., Zubok, V., Mishyna, N., & Davydiuk, A. (2026). From kinetic destruction to cybersecurity: Building resilient infrastructure through cloud migration in Ukraine. In 2026 18th International Conference on Cyber Conflict (CyCon) (pp. 281–304). IEEE. https://doi.org/10.23919/cycon70911.2026.11609429

Davydiuk, A., & Zubok, V. (2023). Analytical review of the resilience of Ukraine's critical energy infrastructure to cyber threats in times of war. In 2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon) (pp. 121–139). IEEE. https://doi.org/10.23919/cycon58705.2023.10181813

IT Ukraine Association. (2026). Research. https://itukraine.org.ua/en/research/

IT Ukraine Association. (2022). The law on the reservation of IT professionals has been adopted! https://itukraine.org.ua/en/the-law-on-the-reservation-of-it-professionals-has-been-adopted/

Maliarchuk, O. (2025). Relokatsiia biznesu yak instrument adaptatsii subiektiv pidpryiemnytstva v umovakh ekonomichnoi nestabilnosti. Ekonomika ta suspilstvo. https://doi.org/10.32782/2524-0072/2025-82-90

Sapiton, D. V. (2024). Shchodo pytannia broniuvannia IT-fakhivtsiv na period mobilizatsii ta na voiennyi chas. Zbirnyk naukovykh prats KhNPU imeni H. S. Skovorody «Pravo», 149–159. https://doi.org/10.34142/23121661.2024.39.18

Zarichna, N. Z., & Markovych, I. B. (2026). Enerhetychna stiikist ta biznes-zhyttiezdatnist: stratehii adaptatsii pidpryiemstv Ukrainy v umovakh viiny ta defitsytu enerhoresursiv. Naukovyi visnyk Poltavskoho universytetu ekonomiky i torhivli. Seriia «Ekonomichni nauky», 29–31. https://doi.org/10.37734/2409-6873-2026-1-3

## MILITARY CONFLICT AS A RISK FACTOR FOR THE IT SECTOR: A SYSTEMATISATION OF THREATS AND MITIGATION STRATEGIES

**Oleksandr Siroshtan**
*V. N. Karazin Kharkiv National University, Karazin Business School, Department of Management and Administration*

**Oleksii Vasyliev**
*V. N. Karazin Kharkiv National University, Karazin Business School, Department of Management and Administration*

Purpose. To systematise documented threats that military conflict creates for IT companies and to build a «threat group – mitigation strategy – expected effect – limit of effectiveness» matrix with the evidentiary status stated explicitly. Design/methodology/approach. A desk analysis of documented evidence with subsequent qualitative systematisation. The source base was selected purposively from records verified by DOI or URL: association releases carrying National Bank of Ukraine data, peer-reviewed Ukrainian and international publications, and a vendor cyber-threat report. A four-level scale of evidentiary status was introduced for each matrix row, and the limits of what was actually read are recorded explicitly. Findings. The classification criterion – the affected asset of an IT company – is substantiated, and six groups of wartime threats are identified: personnel; computing and energy infrastructure; data and the IT perimeter; financial flows; legal and regulatory status; client relations. Each group is matched with a mitigation strategy, an expected effect and the

limit beyond which it ceases to work, with the evidentiary basis marked separately. The strategies act complementarily: the failure of one link is not compensated by reinforcing its neighbour. Originality/value. Wartime threats are brought together not as a list of measures but as a matrix with explicit limits of effectiveness and an evidentiary status for each row. The specificity of the wartime factor is attributed not to the list of groups but to the profile of their simultaneous activation, which removes the effect of intra-firm diversification. The matrix suits a preliminary diagnosis and requires empirical validation.

**Keywords:** risk management, military conflict, IT sector, threat classification, mitigation strategies, limit of strategy effectiveness, business continuity.