

DOI: <https://doi.org/10.32782/2524-0072/D2026-86-180>

УДК 334.72:658:004.771:330.131.7

РИЗИКИ ТА СТІЙКІСТЬ ВІРТУАЛЬНИХ КОМПАНІЙ У ЦИФРОВІЙ ЕКОНОМІЦІ: ВИКЛИКИ ДЛЯ УКРАЇНСЬКОГО БІЗНЕСУ

RISKS AND RESILIENCE OF VIRTUAL COMPANIES IN THE DIGITAL ECONOMY: CHALLENGES FOR UKRAINIAN BUSINESS

Булкот Оксана Вікторівнакандидат економічних наук, доцент,
Київський національний університет імені Тараса Шевченка
ORCID: <https://orcid.org/0000-0002-6311-1459>**Петрієв Денис Андрійович**аспірант 2го року навчання,
Київський національний університет імені Тараса Шевченка
ORCID: <https://orcid.org/0009-0006-2397-1741>**Bulkot Oksana, Petriiev Denys**

Taras Shevchenko National University of Kyiv

Стаття присвячена дослідженню ризиків та стійкості віртуальних компаній в умовах цифрової економіки з урахуванням специфіки українського бізнес-середовища. Проаналізовано сутність та ключові характеристики віртуальних компаній як організаційної форми, що набуває дедалі більшого поширення в умовах глобальної цифровізації. На основі методів аналізу і синтезу, класифікації та системного підходу систематизовано чотири основні групи ризиків: кіберзагрози, операційні, правові та управлінські ризики. Визначено особливості функціонування українського бізнесу в цифровому середовищі в умовах воєнного часу, зокрема досліджено феномен стійкості вітчизняного IT-сектору. Запропоновано практичні рекомендації щодо підвищення стійкості віртуальних компаній, що становить практичну цінність для українських підприємців та менеджерів у процесі цифрової трансформації бізнесу.

Ключові слова: віртуальна компанія, цифрова економіка, ризики, стійкість бізнесу, цифрова трансформація, українські підприємства, національна економічна система.

The rapid expansion of the digital economy has fundamentally transformed the nature of business organization, giving rise to a new type of enterprise – the virtual company – which operates without traditional physical infrastructure, relying instead on digital platforms, cloud technologies, and geographically distributed teams. For Ukraine, whose IT sector has demonstrated remarkable resilience during the full-scale war and whose businesses have been forced to accelerate digital transformation under extreme conditions, understanding the risks and resilience mechanisms of virtual companies is of particular practical importance. The purpose of this article is to systematize the key risks associated with virtual companies in the digital economy, analyze the specific challenges facing Ukrainian business, and develop practical recommendations for strengthening resilience. The research employs general scientific methods including analysis and synthesis, classification, comparative analysis, and a systemic approach to the study of economic phenomena. The article examines the theoretical foundations of the concept of virtual companies, tracing its evolution from early network organization theory to contemporary digital platform models. A comprehensive classification of risks is developed, encompassing cybersecurity threats, operational risks related to distributed team management, legal and regulatory risks arising from cross-border activity, and strategic risks linked to dependency on digital infrastructure. The Ukrainian context is analyzed through the lens of wartime conditions, which have simultaneously accelerated digitalization and introduced new vulnerabilities. Evidence is presented showing that Ukrainian IT companies generated USD 7.35 billion in computer services exports in 2022, demonstrating the sector's capacity for resilience, while also facing unprecedented infrastructure disruption, talent migration, and geopolitical uncertainty. The article concludes with a set of practical recommendations for Ukrainian businesses seeking to strengthen the resilience of virtual organizational structures, including investment in cybersecurity, diversification of digital infrastructure, development of adaptive governance models, and engagement with the Diia.City legal framework.

Keywords: virtual company, digital economy, risks, business resilience, digital transformation, Ukrainian enterprises, national economic system.



Постановка проблеми. Стрімкий розвиток цифрових технологій докорінно змінює архітектуру сучасного бізнесу. Поява та масове поширення хмарних обчислень, платформних рішень та інструментів дистанційної співпраці створили умови для виникнення принципово нової організаційної форми – віртуальної компанії. На відміну від традиційних підприємств, віртуальні компанії функціонують без сталої фізичної інфраструктури, залучаючи географічно розподілені команди та цифрові платформи як основний виробничий ресурс.

Питання дослідження ризиків та стійкості таких компаній набуває особливої актуальності в умовах глобальних криз – пандемії COVID-19, геополітичних потрясінь та воєнних конфліктів. Для України, де бізнес вимушений функціонувати в умовах повномасштабної війни, розуміння механізмів ідентифікації та впливу ризиків разом із посиленням стійкості віртуальних компаній є не лише теоретичним питанням, а й нагальною практичною потребою. Вітчизняний IT-сектор, що зберіг та навіть наростив обсяги експорту під час війни, став переконливим свідченням того, що цифрові організаційні форми здатні демонструвати виняткову стійкість у кризових умовах. Водночас виклики, що постають перед українським бізнесом у сучасному цифровому середовищі, залишаються недостатньо систематизованими в науковій літературі.

Аналіз останніх досліджень і публікацій.

Теоретичні засади організації віртуальних підприємств закладено ще в роботах 1990-х років. Концепцію «віртуальної організації» розвивали дослідники мережевих форм бізнесу, зокрема M. Alawamleh та K. Popplewell, які визначали її як гнучку мережу незалежних суб'єктів, пов'язаних інформаційними технологіями з метою спільного використання навичок, знань та доступу до ресурсів [13]. З розвитком цифрових технологій ця концепція зазнала суттєвої еволюції.

Сучасні дослідники зосереджують увагу на взаємозв'язку між цифровою трансформацією та стійкістю підприємств. Зокрема, C. Li та Y. Wang встановили, що цифрова трансформація здатна суттєво підвищити стійкість підприємств за умови розвиненої мережевої інфраструктури та ефективної системи захисту інтелектуальної власності [2]. Водночас дослідники наголошують на неоднозначності цього взаємозв'язку: мікрохарактеристики підприємств та макросередовищні фактори, зокрема стадія життєвого циклу та рівень конкуренції в галузі, по-різному впли-

вають на ефект підвищення стійкості від цифрових перетворень [3].

Важливим внеском у дослідження проблем кібербезпеки став систематизований огляд кіберризиків дистанційної роботи, проведений M. Nizamuddin на основі 20 рецензованих досліджень за період 2010–2024 років. Встановлено, що людський чинник є домінуючим вектором ризику, посиленням недостатнім навчанням персоналу та розмитістю меж між особистим і професійним простором [4]. Дослідники глобальних форм віртуальної праці F.J. Froese, T. Blay, C.V. Gibson, M.A. Shaffer та J. Benitez проаналізували 346 профільних статей за 1990–2023 роки, виділивши ключові теми: управління розподіленими командами, культурне різноманіття та залежність від цифрових інструментів [5].

В сучасних умовах господарювання українських підприємств особливого значення набувають дослідження цифрової трансформації релокованого бізнесу в умовах війни. Є. Поліщук, Ю. Гернего та В. Горбов встановили, що цифрова зрілість компаній стала вирішальним фактором їхньої адаптивності до кризових умов [1]. Дослідження Організації економічного співробітництва та розвитку (ОЕСР) підтверджує, що цифрові технології не лише підвищують продуктивність підприємств, а й забезпечують стійкість і сприяють економічному відновленню в умовах воєнного часу, хоча малий та середній бізнес ще не повною мірою реалізує потенціал цифровізації [8].

Виділення невирішених раніше частин загальної проблеми. Попри значну увагу науковців до окремих аспектів функціонування віртуальних компаній, у науковій літературі бракує комплексного підходу до систематизації ризиків такого типу компаній з урахуванням специфіки українського бізнес-середовища, зокрема в умовах воєнного часу. Залишаються недостатньо дослідженими механізми забезпечення стійкості вітчизняних підприємств, що функціонують у цифровому форматі, та практичні рекомендації щодо їх адаптації до наявних викликів.

Формулювання цілей статті (постановка завдання). Метою статті є систематизація ключових ризиків, що постають перед віртуальними компаніями в умовах цифрової економіки, аналіз специфічних викликів для українського бізнесу та розроблення практичних рекомендацій щодо підвищення стійкості підприємств, що функціонують у цифровому форматі.

Виклад основного матеріалу дослідження. Поняття «віртуальна компанія» охоплює широкий спектр організаційних форм, що об'єднані кількома ключовими ознаками: відсутністю або мінімальністю фізичної інфраструктури, функціонуванням переважно у цифровому середовищі, географічним розподілом учасників та залежністю від інформаційно-комунікаційних технологій як основного виробничого ресурсу. В сучасній літературі термін «віртуальна компанія» часто вживається паралельно з поняттями «цифрова організація», «розподілена компанія» та «онлайн-підприємство», хоча між ними існують певні концептуальні відмінності [13].

Ключовими характеристиками віртуальних компаній є: гнучкість організаційної структури та здатність до швидкої реконфігурації; широке використання хмарних технологій та цифрових платформ; дистанційна організація праці та асинхронна комунікація; транскордонна діяльність, що виходить за межі традиційних юрисдикційних обмежень; висока залежність від цифрової інфраструктури та кіберзахисту [5].

Сучасна цифрова економіка створює сприятливі умови для розвитку віртуальних компаній. Пандемія COVID-19 значно прискорила перехід до дистанційних форм організації праці, а геополітичні потрясіння, у тому числі повномасштабна війна в Україні, продемонстрували як переваги, так і вразливості цієї організаційної форми [1; 12].

На основі аналізу наукової літератури та практики функціонування вітчизняного біз-

несу можна виокремити чотири основні групи ризиків, що властиві віртуальним компаніям (табл. 1).

Кіберризика є одними з найбільш актуальних для віртуальних компаній. Систематичний огляд досліджень з кібербезпеки дистанційної роботи засвідчує, що людський чинник залишається провідним вектором атак: фішинг, соціальна інженерія, використання незахищених мереж є найпоширенішими загрозами [4]. Для України ця проблема посилюється активністю державних хакерських груп, що здійснюють цілеспрямовані атаки на підприємства та критичну інфраструктуру.

Операційні ризики пов'язані зі складністю управління розподіленими командами. Дослідники глобальних форм віртуальної праці встановили, що ефективність таких команд суттєво залежить від якості цифрових інструментів комунікації, чіткості розподілу ролей та лідерських компетенцій керівників [5]. В українських реаліях операційні ризики набувають додаткового виміру через перебої в електропостачанні, вимушену релокацію персоналу та масову еміграцію кваліфікованих фахівців.

Правові та регуляторні ризики обумовлені транскордонним характером діяльності більшості віртуальних компаній. Функціонування в кількох юрисдикціях одночасно породжує складні питання щодо вибору застосовного права, захисту персональних даних відповідно до GDPR та регулювання трудових відносин з дистанційними працівниками різних країн. Для українських компаній, що активно

Таблиця 1

Класифікація ризиків віртуальних компаній у цифровій економіці

Група ризиків	Основні прояви	Особливості прояву в Україні
Кіберризика	Фішинг, соціальна інженерія, витік даних, несанкціонований доступ через незахищені мережі, атаки на хмарну інфраструктуру	Посилені атаки з боку державних хакерських груп; вразливість через масовий перехід на дистанційний формат у 2022 р.
Операційні ризики	Порушення комунікації між розподіленими командами, відсутність контролю якості, залежність від цифрових платформ, часові зони	Перебої електропостачання, вимушена релокація співробітників, втрата кадрів через еміграцію
Правові та регуляторні ризики	Транскордонна діяльність в різних юрисдикціях, захист персональних даних (GDPR), невизначеність трудового законодавства	Правова невизначеність воєнного часу; адаптація до вимог ЄС у рамках євроінтеграції
Управлінські ризики	Складність формування корпоративної культури, довіри та ідентифікації працівників з компанією, ризики координації	Психологічний тиск воєнного часу на персонал; управлінські виклики при роботі з релокованими командами

Джерело: сформовано авторами на основі [3; 4; 5; 7; 13]

інтегруються в ринок ЄС, ці питання набувають особливої актуальності [8].

Управлінські ризики пов'язані зі специфікою формування корпоративної ідентичності та організаційної культури у віртуальному середовищі. Дослідження підтверджують, що організаційна ідентифікація є ключовим механізмом координації і контролю у віртуальних організаціях, оскільки вона мотивує працівників приймати цілі організації як власні [13]. В умовах воєнного часу психологічний тиск на персонал додатково ускладнює управлінські завдання.

Українські підприємства, що функціонують у цифровому форматі, продемонстрували виняткову стійкість в умовах повномасштабного вторгнення. Показово, що за підсумками 2022 року обсяг експорту комп'ютерних послуг вітчизняного ІТ-сектору склав 7,35 млрд дол. США, що на 5,8% перевищило показник попереднього року, перетворивши галузь на єдиний повноцінний функціонуючий експортний сектор країни в умовах воєнного стану [12].

Ключовими факторами цієї стійкості стали: по-перше, вже наявна цифрова інфраструктура, що дозволила оперативно перейти до повністю дистанційного формату роботи; по-друге, гнучкість організаційних структур, що уможливила швидку релокацію як всередині країни, так і за кордон; по-третє, диверсифікація клієнтської бази та географія надання послуг, що зменшила залежність від внутрішнього ринку [11].

Важливим інструментом підтримки цифрового бізнесу в Україні став правовий режим Дія.Сіті, запроваджений у 2022 році. Станом на сьогодні до цього режиму приєдналося понад 1 560 компаній, що отримали сприятливе правове середовище та знижене податкове навантаження, а також можливість узгодити свою діяльність із міжнародними правовими стандартами, що суттєво підвищило привабливість для іноземних інвесторів [10].

Водночас дослідження ОЕСР фіксує, що малий та середній бізнес ще не повністю реалізував потенціал цифровізації. Серед ключових перешкод – брак обізнаності, нестача цифрових навичок, галузева специфіка та фінансові обмеження [8]. Моніторинг цифрової трансформації в Україні засвідчив зростання проникнення інтернету з 62% у 2019 році до 78% у 2023 році та 42-відсоткове збільшення кількості користувачів застосунку «Дія» за цей же період, що свідчить про прискорення цифровізації загалом [9].

Окремого дослідницького інтересу заслуговує феномен «цифрової стійкості» українських організацій. Аналіз 40 інтерв'ю з українськими менеджерами засвідчив, що цифрова трансформація в умовах воєнного часу відбувається не планово, а стихійно — як реакція на необхідність забезпечення виживання бізнесу. При цьому ключовими інструментами стали соціальні мережі та месенджери, що забезпечили безперервність комунікації та підтримку морального духу команд [7].

Висновки. Проведений аналіз дозволяє сформулювати такі висновки та практичні рекомендації для українського бізнесу.

По-перше, віртуальні компанії є організаційною формою, що органічно відповідає викликам цифрової економіки та кризових умов, однак несе з собою специфічний комплекс ризиків – кіберризиків, операційні, правові та управлінські, – що потребують системного управління.

По-друге, українські підприємства, особливо в ІТ-секторі, продемонстрували значний потенціал стійкості, однак ця стійкість значною мірою виникла як стихійна реакція на кризу, а не як результат цілеспрямованої стратегії. Формування проактивних моделей управління ризиками є ключовим завданням для підвищення довгострокової конкурентоспроможності.

По-третє, на основі здійсненого дослідження пропонується комплекс практичних рекомендацій для українських підприємств: інвестиції в кібербезпеку як пріоритетний напрям, включаючи багатофакторну аутентифікацію, шифрування даних та регулярне навчання персоналу [4]; диверсифікація цифрової інфраструктури для уникнення єдиної точки відмови, включаючи використання кількох хмарних провайдерів та інтернет-каналів; розвиток адаптивних моделей корпоративного управління, орієнтованих на формування організаційної ідентичності та довіри у дистанційному середовищі [3]; використання правового режиму Дія.Сіті для мінімізації регуляторних ризиків та підвищення привабливості для міжнародних партнерів [10]; розроблення стратегій утримання та залучення талантів в умовах конкуренції на міжнародному ринку праці.

Перспективи подальших досліджень пов'язані з розробкою кількісних методик оцінювання рівня ризиків та стійкості конкретних підприємств, що функціонують у цифровому форматі, а також з вивченням впливу євроінтеграційних процесів на регуляторне середовище для віртуальних компаній в Україні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Поліщук Є., Гернего Ю., Горбов В. Цифрова трансформація релокованого бізнесу / *Економіка України*. 2025. № 5 (762). URL: <https://nasu-periodicals.org.ua/index.php/economyukr/article/view/2025-05-4> (дата звернення: 10.04.2026)
2. Li C., Wang Y. Digital technology innovation and corporate resilience / *ScienceDirect*. 2024. URL: <https://www.sciencedirect.com/science/article/abs/pii/S1044028324001145> (дата звернення: 10.04.2026)
3. Li C., Wang Y. Digital transformation and enterprise resilience: Enabling or burdening? / *PLOS ONE*. 2024. URL: <https://pmc.ncbi.nlm.nih.gov/articles/PMC11259276/> (дата звернення: 10.04.2026)
4. Nizamuddin M. Investigating the cybersecurity risks of remote work: a systematic literature review of organizational vulnerabilities and mitigation strategies / *International Journal of Information Security*. 2025. URL: <https://link.springer.com/article/10.1007/s10207-025-01095-z> (дата звернення: 10.04.2026)
5. Froese F.J., Blay T., Gibson C.B., Shaffer M.A., Benitez J. Global virtual work: a review, integrative framework, and future research opportunities / *Journal of International Business Studies*. 2025. URL: <https://link.springer.com/article/10.1057/s41267-025-00775-1> (дата звернення: 10.04.2026)
6. Віртуальне підприємство як ефективна форма організації бізнесу / *Економіка та довкілля*. 2025. URL: <https://www.econa.org.ua/index.php/econa/article/download/6478/6565657751> (дата звернення: 10.04.2026)
7. Lindström N.B., Razmerita L., Prokopenko S., Popovich N. Building Digital Resilience in Major Shocks: How Ukrainian Organizations Enact Digital Transformation in Times of War / *ResearchGate*. 2024. URL: <https://www.researchgate.net/publication/380531626> (дата звернення: 10.04.2026)
8. OECD. Enhancing Resilience by Boosting Digital Business Transformation in Ukraine / *OECD Publishing*. 2023. URL: https://www.oecd.org/en/publications/enhancing-resilience-by-boosting-digital-business-transformation-in-ukraine_4b13b0bb-en.html (дата звернення: 10.04.2026)
9. Digital transformation as a tool for creating an inclusive economy in Ukraine during wartime / *Problems and Perspectives in Management*. 2024. URL: <https://www.businessperspectives.org/index.php/journals/problems-and-perspectives-in-management/issue-461> (дата звернення: 10.04.2026)
10. Ukraine's IT Powerhouse: Innovation Without Limits / Ministry of Digital Transformation of Ukraine. 2024. URL: <https://digitalstate.gov.ua/news/it-outsourcing/ukraines-it-powerhouse-innovation-without-limits> (дата звернення: 10.04.2026)
11. Цифрова економіка в Україні: стратегічні виклики, можливості зростання та трансформація / *Вчені записки Університету «КРОК»*. URL: <https://snku.krok.edu.ua/index.php/vcheni-zapiski-universitetu-krok/article/view/1145> (дата звернення: 10.04.2026)
12. Digital Tiger: the Power of Ukrainian IT — 2023 / IT Ukraine Association. 2024. URL: <https://itukraine.org.ua/en/digital-tiger-the-power-of-ukrainian-it-2023/> (дата звернення: 10.04.2026)
13. Alawamleh M., Popplewell K. Understanding virtual organisation to identify possible risks / *Int. J. Management and Network Economics*. 2011. Vol. 2, No. 1. URL: https://www.researchgate.net/publication/264837030_Understanding_virtual_organisation_to_identify_possible_risks (дата звернення: 10.04.2026)

REFERENCES:

1. Polishchuk Y., Herneho Y., Horbov V. Tsyfrova transformatsiia relokovannoho biznesu [Digital transformation of relocated business]. (2025). *Ekonomika Ukrainy*, 5(762). Retrieved from <https://nasu-periodicals.org.ua/index.php/economyukr/article/view/2025-05-4> (accessed April 10, 2026)
2. Li C., Wang Y. Digital technology innovation and corporate resilience. (2024). *ScienceDirect*. Retrieved from <https://www.sciencedirect.com/science/article/abs/pii/S1044028324001145> (accessed April 10, 2026)
3. Li C., Wang Y. Digital transformation and enterprise resilience: Enabling or burdening? (2024). *PLOS ONE*. Retrieved from <https://pmc.ncbi.nlm.nih.gov/articles/PMC11259276/> (accessed April 10, 2026)
4. Nizamuddin M. Investigating the cybersecurity risks of remote work: a systematic literature review of organizational vulnerabilities and mitigation strategies. (2025). *International Journal of Information Security*. <https://doi.org/10.1007/s10207-025-01095-z> (accessed April 10, 2026)
5. Froese F.J., Blay T., Gibson C.B., Shaffer M.A., Benitez J. Global virtual work: a review, integrative framework, and future research opportunities. (2025). *Journal of International Business Studies*. <https://doi.org/10.1057/s41267-025-00775-1> (accessed April 10, 2026)
6. Virtualne pidpriemstvo yak efektyvna forma orhanizatsii biznesu [Virtual enterprise as an effective form of business organization]. (2025). *Ekonomika ta dovkillia*. Retrieved from <https://www.econa.org.ua/index.php/econa/article/download/6478/6565657751> (accessed April 10, 2026)

7. Lindström N.B., Razmerita L., Prokopenko S., Popovich N. Building Digital Resilience in Major Shocks: How Ukrainian Organizations Enact Digital Transformation in Times of War. (2024). *Proceedings of the 57th Annual Hawaii International Conference on System Sciences (HICSS 2024)*. Retrieved from <https://www.researchgate.net/publication/380531626> (accessed April 10, 2026)
8. OECD. (2023). Enhancing Resilience by Boosting Digital Business Transformation in Ukraine. *OECD Publishing*. <https://doi.org/10.1787/4b13b0bb-en> (accessed April 10, 2026)
9. Digital transformation as a tool for creating an inclusive economy in Ukraine during wartime. (2024). *Problems and Perspectives in Management*. Retrieved from <https://www.businessperspectives.org/index.php/journals/problems-and-perspectives-in-management/issue-461> (accessed April 10, 2026)
10. Ministry of Digital Transformation of Ukraine. (2024). Ukraine's IT Powerhouse: Innovation Without Limits. Retrieved from <https://digitalstate.gov.ua/news/it-outsourcing/ukraines-it-powerhouse-innovation-without-limits> (accessed April 10, 2026)
11. Tsyfrova ekonomika v Ukraini: stratehichni vyklyky, mozhlyvosti zrostantia ta transformatsiia [Digital economy in Ukraine: strategic challenges, growth opportunities and transformation]. *Vcheni zapysky Universytetu «KROK»*. Retrieved from <https://snku.krok.edu.ua/index.php/vcheni-zapiski-universitetu-krok/article/view/1145> (accessed April 10, 2026)
12. IT Ukraine Association. (2024). Digital Tiger: the Power of Ukrainian IT — 2023. Retrieved from <https://itukraine.org.ua/en/digital-tiger-the-power-of-ukrainian-it-2023/> (accessed April 10, 2026)
13. Alawamleh M., Popplewell K. Understanding virtual organisation to identify possible risks. (2011). *Int. J. Management and Network Economics*, Vol. 2, No. 1, pp. 75–92. Retrieved from https://www.researchgate.net/publication/264837030_Understanding_virtual_organisation_to_identify_possible_risks (accessed April 10, 2026)

Дата надходження статті: 20.04.2026

Дата прийняття статті: 12.05.2026

Дата публікації статті: 26.05.2026