Електронний журнал «Ефективна економіка» включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України № 975 від 11.07.2019). Спеціальності – 051, 071, 072, 073, 075, 076, 292.
Ефективна економіка. 2026. № 4.
ISSN 2307-2105

DOI: http://doi.org/10.32702/2307-2105.2026.4.199

УДК [005.934:004.056.5]:339.5

В. А. Фєтісов,

аспірант кафедри європейської економіки і бізнесу,

Київський національний економічний університет імені Вадима Гетьмана

ORCID ID: https://orcid.org/0009-0009-2859-3032

РИЗИКИ ЦИФРОВОГО СЕРЕДОВИЩА В МІЖНАРОДНОМУ АУТСОРСИНГУ: ІНСТИТУЦІЙНО-ПРАВОВИЙ АСПЕКТ

V. Fietisov,

Postgraduate Student, Department of European Economics and Business,

Vadym Hetman Kyiv National University of Economics

DIGITAL ENVIRONMENT RISKS IN INTERNATIONAL OUTSOURCING: INSTITUTIONAL AND LEGAL ASPECT

У статті досліджено природу та класифікацію ризиків цифрового середовища, що виникають у процесі міжнародного аутсорсингу в умовах глобалізації та євроінтеграції України. Проаналізовано специфіку транскордонних ризиків у сферах кібербезпеки, захисту персональних даних та правової відповідальності в умовах різних юрисдикцій. Особливу увагу приділено правовому середовищу України, зокрема чинному Закону «Про захист персональних даних», проекту його нового закону №8153, а також

механізму «Дія.City» як спеціального правового простору для IT-компаній. Систематизовано міжнародні правові рамки — GDPR, ISO/IEC 27001, NIS2 Directive, DORA — та обґрунтовано необхідність їх імплементації в Україні. Встановлено, що український ринок IT-аутсорсингу, попри значний потенціал, характеризується інституційними прогалинами у сфері управління цифровими ризиками. Запропоновано рекомендації щодо формування комплексної системи ризик-менеджменту для українських підприємств, що залучають зовнішніх постачальників IT-послуг.

The article explores the nature and classification of digital environment risks arising in the context of international outsourcing under conditions of globalisation and Ukraine's European integration. The specifics of cross-border risks in the fields of cybersecurity, personal data protection, and legal liability across multiple jurisdictions are analysed. Special attention is paid to Ukraine's legal environment, particularly the existing Law "On Personal Data Protection," the draft new law No. 8153, and the "Diia.City" mechanism as a special legal and tax framework for IT companies operating in Ukraine. International legal frameworks — the General Data Protection Regulation (GDPR), ISO/IEC 27001, the NIS2 Directive, and the Digital Operational Resilience Act (DORA) — are systematised from the perspective of their applicability to outsourcing relationships, and the necessity of their implementation in Ukraine is substantiated within the context of EU accession obligations. The study finds that the domestic IT outsourcing market, despite its significant potential and the presence of seventeen Ukrainian companies in the global outsourcing rankings in 2023, is characterised by considerable institutional gaps in digital risk management. The article identifies Ukraine's specific vulnerabilities in the context of the ongoing armed conflict and intensified cyber warfare, noting that the number of registered cyber incidents in Ukraine grew by 62.5 percent in 2023 alone, a significant share of which targeted IT service providers and their foreign clients. The research demonstrates that an effective risk management system for cross-border outsourcing must integrate

three levels: technical standards such as DSTU ISO/IEC 27005:2023 and ITIL frameworks; contractual mechanisms including detailed service level agreements and data processing agreements; and institutional measures encompassing the adoption of updated data protection legislation and harmonisation with EU digital acquis. Practical recommendations are proposed for Ukrainian enterprises engaging external IT service providers, as well as for policymakers shaping national digital and cybersecurity strategy.

Ключові слова: *міжнародний аутсорсинг, ризики, кібербезпека, захист персональних даних, євроінтеграція, Дія.City, інституційно-правове регулювання, цифрове середовище, IT-послуги, інформаційні технології.*

Keywords: *international outsourcing, risks, cybersecurity, personal data protection, European integration, Diia.City, institutional and legal regulation, digital environment, IT services, information technology.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Україна посідає провідне місце на глобальному ринку IT-аутсорсингу. У 2023 році сімнадцять українських IT-аутсорсингових компаній потрапили до рейтингу найбільших аутсорсингових компаній світу [1]. За даними Lviv IT Cluster, обсяг IT-експорту у 2022 році становив близько 7,3 млрд дол. США, проте у 2023–2024 роках спостерігається певне уповільнення через вплив повномасштабного збройного конфлікту [2]. Незважаючи на це, ринок демонструє адаптивність: понад 140 CEO компаній планували відкривати нові офіси в Україні, а попит на IT-фахівців зберігається з боку міжнародних замовників.

Разом з тим стрімка цифровізація та транскордонний характер аутсорсингових операцій породжують якісно нові ризики — ризики цифрового середовища, що виходять за межі окремих юрисдикцій. Кіберінцидент у постачальника IT-послуг може спричинити витік персональних даних клієнтів, порушуючи вимоги відразу кількох правових

систем. В умовах активного кіберпротистояння, яке супроводжує збройний конфлікт, ця проблема набуває для України особливої гостроти: лише у 2022 році Україна відбила понад 1,5 млн. кібератак на об'єкти енергетичної галузі [3], і значна частина атак була спрямована саме на інфраструктуру IT-компаній та їх клієнтів за кордоном.

Актуальність дослідження зумовлена тим, що українські підприємства, або залучають зовнішніх постачальників IT-послуг, або самі–виступають постачальниками для іноземних замовників, і досить часто не мають сформованих інституційно-правових механізмів управління цифровими ризиками у транскордонному контексті. Прогрес у сфері євроінтеграції вимагає гармонізації українського законодавства з вимогами ЄС — і це завдання безпосередньо стосується регулювання ризиків цифрового аутсорсингу.

Аналіз останніх досліджень і публікацій. Проблематика ризиків у сфері IT-аутсорсингу активно досліджується в українській науковій літературі. Полякова Ю. В., Шайда О. Є., Миронова М. І. та Крутяк М. Б. та ін. науковці і спеціалісти аналізують переваги та ризики міжнародного IT-аутсорсингу для України, зокрема виокремлюють ризики витоку конфіденційної інформації та складність забезпечення відповідності міжнародним стандартам безпеки [4]. Конопленко А., Ковальов Б., Цапковатий Р. та Веньянь Л. тощо досліджують фактори конкурентоспроможності ринку IT-аутсорсингу в Україні та вказують на те, що безпеці й конфіденційності даних приділятиметься дедалі більша увага з боку міжнародних замовників [1].

У правовому контексті важливим є дослідження вітчизняного науковця Головацького Н.Т., яке присвячене порівняльному аналізу GDPR[1] та законодавства про захист персональних даних різних юрисдикцій, включно з

[1] GDPR (General Data Protection Regulation - Загальний регламент про захист даних) - нормативно-правовий акт ЄС (Регламент 2016/679), що з 2018 року встановлює єдині стандарти збору, зберігання, обробки та транскордонної передачі персональних даних, визначає права суб'єктів даних і обов'язки їх обробників, передбачаючи штрафи до 20 млн євро за порушення.

Україною. Погоджуємося з автором, що Україна знаходиться на шляху до повної гармонізації з європейськими стандартами, що є обов'язковою умовою для зміцнення правового захисту в сфері цифрового аутсорсингу [5]. Питання захисту персональних даних в умовах воєнного стану та необхідності адаптації до GDPR детально розглядаються у дослідженнях Михайлик А.С., яка виявляє ключову прогалину: чинне законодавство України не забезпечує належного рівня захисту персональних даних відповідно до оновлених міжнародно-правових стандартів [6].

Проблематика кібербезпеки у контексті правового регулювання критичної інфраструктури досліджують Ковалів М., Скриньковський Р. та Єсімов С. та ін., які систематизують нормативно-правову базу кібербезпеки України та обґрунтовують необхідність її синхронізації з директивами ЄС [7]. Дудко П.М. аналізує сучасні тенденції розвитку ІТ-аутсорсингу у світі та доходить висновку, що модель «цифрового резонансу», яка враховує рівень правового захисту інтелектуальної власності та цифрові навички робочої сили, є вирішальним чинником при виборі країни-постачальника аутсорсингових послуг [8].

Водночас в українській науці залишається недостатньо дослідженим питання комплексного управління саме цифровими ризиками в транскордонному аутсорсингу — у поєднанні правових, технічних та інституційних інструментів із урахуванням специфіки України як країни-кандидата на вступ до ЄС та активного учасника кіберпростору в умовах збройного конфлікту.

Формулювання цілей статті (постановка завдання). Метою статті є систематизація ризиків цифрового середовища в міжнародному аутсорсингу з акцентом на специфіці України та розробка науково обґрунтованих пропозицій щодо формування інституційно-правового механізму їх мінімізації на основі аналізу чинних міжнародних й українських правових рамок.

Для досягнення мети поставлено такі завдання: охарактеризувати основні типи цифрових ризиків у транскордонному аутсорсингу; проаналізувати чинні правові інструменти регулювання, зокрема в контексті євроінтеграційних зобов'язань України; виявити регуляторні прогалини в українському законодавстві; запропонувати рекомендації щодо вдосконалення системи управління такими ризиками.

Виклад основного матеріалу дослідження. Під ризиками цифрового середовища в міжнародному аутсорсингу розуміємо ймовірні негативні події або умови, пов'язані з використанням інформаційних технологій, що можуть спричинити фінансові, репутаційні або правові збитки учасникам аутсорсингових відносин у транскордонному контексті. Такі ризики поділяються на кілька ключових типів, що різняться за природою та правовими інструментами реагування.

Кіберінциденти є найбільш поширеним та матеріально значущим видом цифрових ризиків. Для України ця загроза є особливо актуальною. Кількість зареєстрованих в Україні кіберінцидентів у 2023 році зросла на 62,5% порівняно з попереднім роком [3]. Частина з них безпосередньо стосувалася IT-компаній, що надають аутсорсингові послуги іноземним замовникам. Атаки на ланцюги постачання програмного забезпечення перетворилися на системну загрозу: зловмисники цілеспрямовано атакують аутсорсерів як «точку входу» до інфраструктури кінцевого замовника.

У правовому вимірі кібербезпека регулюється на двох рівнях (рис.1).

На національному рівні основу становить Закон України «Про основні засади забезпечення кібербезпеки України» та Стратегія кібербезпеки України, план реалізації якої на 2023–2024 роки затверджено Розпорядженням КМУ №1163-р від 19.12.2023 р. [9]. На міжнародному рівні ключовою є Директива NIS2 (ЄС, 2022), яку Україна зобов'язана імплементувати в процесі вступу до ЄС: вона поширює вимоги кібербезпеки

безпосередньо на постачальників ІТ-послуг та запроваджує персональну відповідальність керівників організацій за недотримання стандартів.

Рис.1. Рівні регулювання кібербезпеки

Джерело: розроблено автором самостійно

На національному рівні основу становить Закон України «Про основні засади забезпечення кібербезпеки України» та Стратегія кібербезпеки України, план реалізації якої на 2023–2024 роки затверджено Розпорядженням КМУ №1163-р від 19.12.2023 р. [9]. На міжнародному рівні ключовою є Директива NIS2 (ЄС, 2022), яку Україна зобов'язана імплементувати в процесі вступу до ЄС: вона поширює вимоги кібербезпеки безпосередньо на постачальників ІТ-послуг та запроваджує персональну відповідальність керівників організацій за недотримання стандартів.

Захист персональних даних є другим за значущістю виміром цифрових ризиків в аутсорсингу. Будь-який аусторсинговий бізнес, що обробляє персональні дані клієнтів ЄС, підпадає під повний обсяг вимог GDPR незалежно від свого місцезнаходження. Це безпосередньо стосується більшості українських ІТ-компаній, що надають послуги замовникам із країн Євросоюзу. Ключовими інструментами відповідності є укладення угод про обробку даних (DPA- Data Processing Agreement), проведення оцінки впливу

на захист даних (Data Protection Impact Assessment) та застосування стандартних договірних застережень (SCC- Standard Contractual Clauses) при передачі даних за межі ЄС.

Стан українського законодавства у цій сфері є недостатнім. Головацький Н.Т. констатує, що Україна знаходиться на шляху до гармонізації з GDPR, однак цей процес ще не завершено [5]. Михайлик А.С. прямо зазначає, що «головна проблема у сфері захисту персональних даних в Україні полягає у відсутності законодавчих актів, які б забезпечували належний рівень захисту персональних даних відповідно до оновлених міжнародно-правових стандартів» [6]. Реагуванням на цю прогалину є розроблений Проект Закону №8153 від 25.10.2022 р., який передбачає суттєве наближення українського законодавства до вимог GDPR, зокрема в частині транскордонної передачі даних, прав суб'єктів даних та відповідальності обробників.

Окремим позитивним прикладом інституційного реагування є механізм «Дія.City» — спеціальний правовий та податковий простір для IT-компаній в Україні, запроваджений у лютому 2022 року. Незважаючи на запуск буквально за два тижні до початку повномасштабного вторгнення, станом на середину 2023 року його перевагами вже користувалися близько 600 компаній [10]. «Дія.City» формує зрозуміле правове середовище для міжнародних аутсорсингових операцій, що є важливим чинником довіри з боку іноземних замовників. Проте механізм наразі не містить спеціальних положень щодо управління цифровими ризиками та розподілу відповідальності у транскордонних аутсорсингових угодах — ця прогалина потребує усунення.

Юрисдикційна неузгодженість є однією з найбільш складних проблем у транскордонному аутсорсингу. Коли замовник знаходиться в Німеччині, розробка ведеться в Україні, а сервери розміщені в Нідерландах, виникає питання: право якої держави застосовується у разі спору? Стандартні договірні підходи передбачають вибір права (choice of law clause) та вибір

юрисдикції, проте їх ефективність обмежена у випадках порушення GDPR, де застосування регламенту є обов'язковим незалежно від договірних домовленостей.

ITIL[2] та стандарт ISO/IEC 27001 [3]набувають дедалі більшого значення як квазіюридичні інструменти в аутсорсингових договорах. Будучи добровільними технічними стандартами, їх положення про управління інцидентами та безперервністю послуг все частіше включаються у договірні SLA (Service Level Agreement) як обов'язкові умови. ДСТУ ISO/IEC 27005:2023, що набув чинності в Україні, містить настанови з керування ризиками інформаційної безпеки, що є безпосередньо застосовними до аутсорсингових відносин [7]. З 2025 року набуває повного застосування Регламент DORA (Digital Operational Resilience Act), що встановлює обов'язкові вимоги до цифрової стійкості фінансових установ ЄС та їх ІКТ-постачальників, включно з реєстрацією та аудитом. Це безпосередньо стосується українських ІТ-компаній, що обслуговують фінансовий сектор ЄС.

Дослідники виокремлюють специфічні ризики, що виникають у зв'язку зі збройним конфліктом. За даними дослідження «IT Research Ukraine 2023», заступник міністра цифрової трансформації Олександр Борняков зазначає, що чим довше триває війна, тим більше проєктів міжнародні замовники ставлять на паузу. Це формує новий тип ризику — ризик операційної переривності, пов'язаний із форс-мажорними обставинами воєнного характеру. Ефективна система ризик-менеджменту має передбачати плани забезпечення безперервності бізнесу з урахуванням сценаріїв, специфічних для умов збройного конфлікту.

[2] ITIL (Information Technology Infrastructure Library - Бібліотека інфраструктури інформаційних технологій) - звіт найкращих практик управління ІТ-послугами, що регламентує процеси їх планування, надання, підтримки та безперервності.

[3] ISO/IEC 27001 — міжнародний стандарт управління інформаційною безпекою, що встановлює вимоги до побудови, впровадження та підтримки системи захисту інформаційних активів організації.

Висновки та перспективи подальших розвідок у даному напрямі. Проведене дослідження дозволяє сформулювати низку науково обґрунтованих висновків. По-перше, Україна є активним учасником глобального ринку IT-аутсорсингу, проте її правове середовище у сфері управління цифровими ризиками в транскордонних аутсорсингових відносинах залишається недостатньо розвиненим. Чинний Закон «Про захист персональних даних» не відповідає стандартам GDPR, а механізм «Дія.City», попри свій потенціал, не містить спеціальних положень щодо розподілу відповідальності за цифрові ризики.

По-друге, умови збройного конфлікту та кіберпротистояння додають до традиційного переліку цифрових ризиків специфічну складову — ризики воєнного та гібридного характеру, що потребують окремих механізмів реагування як у договірній, так і в інституційній площинах. Зростання кількості кіберінцидентів на 62,5% у 2023 році свідчить про те, що ця загроза є системною.

По-третє, З огляду на викладене, пропонуються такі практичні рекомендації щодо вдосконалення системи управління цифровими ризиками в міжнародному аутсорсингу. По-перше, українським підприємствам, що виступають постачальниками IT-послуг, доцільно пройти сертифікацію за стандартом ISO/IEC 27001 та впровадити ITIL-практики управління інцидентами — це суттєво підвищить довіру з боку іноземних замовників і знизить ризик розірвання контрактів через кіберінциденти. По-друге, у всіх транскордонних аутсорсингових договорах необхідно передбачати окремі розділи щодо розподілу відповідальності за витік даних, порядку повідомлення про інциденти та механізмів виходу з договірних відносин відповідно до вимог DORA. По-третє, на рівні державної політики пріоритетним завданням є якнайшвидше прийняття нової редакції Закону про захист персональних даних (№8153) та внесення змін до умов «Дія.City» в частині регулювання цифрових ризиків — це забезпечить правову

визначеність для учасників ринку та наблизить Україну до виконання вимог цифрового acquis ЄС.

Перспективами подальших досліджень є емпіричний аналіз практики управління цифровими ризиками на українських підприємствах, що залучають зовнішніх IT-постачальників або самі виступають аутсорсерами, а також розробка методичного інструментарію оцінки відповідності їх договірних практик вимогам GDPR і майбутнього Закону України про захист персональних даних.

Література

1. Конопленко А., Ковальов Б., Цапковатий Р., Веньянь Л. Фактори економічної конкурентоспроможності ринку IT аутсорсингу в Україні. *Цифрова економіка та економічна безпека.* 2024. № 3(12). С. 126–132.

2. *IT Research Ukraine 2023: адаптивність та стійкість під час війни* / Lviv IT Cluster. Львів, 2024. 110 с. URL: https://itcluster.lviv.ua/wp-content/uploads/lana-downloads/2024/03/it-research-ukraine-2023-extended-ua.pdf (дата звернення: 01.03.2026).

3. Поліковська Ю. Кількість зареєстрованих в Україні кіберінцидентів у 2023 році зросла на 62,5%. *Detector Media.* 2024. 12 січ. URL: https://ms.detector.media/internet/post/33956/ (дата звернення: 15.03.2025).

4. Полякова Ю. В., Шайда О. Є., Миронова М. І., Крутяк М. Б. Міжнародний IT-аутсорсинг: перспективи для України. *Підприємництво і торгівля.* 2023. № 38. С. 54–61. DOI: https://doi.org/10.32782/2522-1256-2023-38-07.

5. Головацький Н. Т. Правове регулювання захисту персональних даних: GDPR та законодавство США, Канади й України. *Науковий вісник УжНУ. Серія «Право».* 2024. Том 4. № 86. С. 44–50.

6. Михайлик А. С. До питання нормативно-правового регулювання захисту персональних даних. *Науковий вісник УжНУ. Серія «Право».* 2022. Том 1. № 73. С. 84–89.

7. Ковалів М., Скриньковський Р., Назар Ю., Єсімов С. Правове забезпечення кібербезпеки критичної інформаційної інфраструктури України. *Traektoriâ Nauki = Path of Science.* 2021. Vol. 7. No. 4. С. 2011–2018. DOI: https://doi.org/10.22178/pos.69-12.

8. Дудко П. М. Сучасні світові тенденції розвитку IT-аутсорсингу. *Вісник Київського національного університету технологій та дизайну.* 2022. № 3. С. 45–53.

9. Про затвердження плану заходів на 2023–2024 роки з реалізації Стратегії кібербезпеки України: Розпорядження Кабінету Міністрів України від 19.12.2023 № 1163-р. URL: https://zakon.rada.gov.ua/go/1163-2023-р (дата звернення: 20.03.2026).

10. Борняков О. Євроінтеграція України: перспективи для IT-сектору та стартап-індустрії. *Forbes Ukraine.* 2023. 29 серп. URL: https://forbes.ua/innovations/efekt-tsifrovoi-sinergii (дата звернення: 25.03.2026).

11. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union and repealing Directive (EU) 2016/1148 (NIS2 Directive). Official Journal of the European Union. L 333. 27.12.2022. P. 80–152.

12. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (DORA). Official Journal of the European Union. L 333. 27.12.2022. P. 1–79.

References

1. Konoplenko, A. Kovalov, B. Tsapkovatyi, R. and Veniany, L. (2024), “Factors of economic competitiveness of the IT outsourcing market in Ukraine”, *Tsyfrova ekonomika ta ekonomichna bezpeka,* vol. 3, no. 12, pp. 126–132.

2. Lviv IT Cluster (2024), *IT Research Ukraine 2023: Adaptyvnist ta stiikist pid chas viiny* [IT Research Ukraine 2023: Adaptability and resilience during war],

Lviv IT Cluster, Lviv, Ukraine, Available at: https://itcluster.lviv.ua/wp-content/uploads/lana-downloads/2024/03/it-research-ukraine-2023-extended-ua.pdf (accessed 1 March 2026).

3. Polikovska, Yu. (2024), “The number of registered cyber incidents in Ukraine grew by 62.5% in 2023”, *Detector Media,* Available at: https://ms.detector.media/internet/post/33956/ (accessed 15 March 2026).

4. Poliakova, Yu. V., Shaida, O. Ye., Myronova, M. I. and Krutiak, M. B. (2023), “International IT outsourcing: prospects for Ukraine”, *Pidpryiemnytstvo i torhivlia,* vol. 38, pp. 54–61. DOI: https://doi.org/10.32782/2522-1256-2023-38-07.

5. Holovatskyi, N. T. (2024), “Legal regulation of personal data protection: GDPR and the legislation of the USA, Canada and Ukraine”, *Naukovyi visnyk UzhNU. Seriia "Pravo",* Vol. 4, No. 86, pp. 44–50.

6. Mykhailyk, A. S. (2022), “On the issue of regulatory and legal regulation of personal data protection”, *Naukovyi visnyk UzhNU. Seriia "Pravo",* Vol. 1, No. 73, pp. 84–89.

7. Kovaliv, M., Skrynikovskyi, R., Nazar, Yu. and Yesimov, S. (2021), “Legal provision of cybersecurity of critical information infrastructure of Ukraine”, *Traektoriia Nauki,* Vol. 7, No. 4, pp. 2011–2018. DOI: https://doi.org/10.22178/pos.69-12.

8. Dudko, P. M. (2022), “Modern global trends in IT outsourcing development”, *Visnyk KNUTD,* vol. 3, pp. 45–53.

9. Cabinet of Ministers of Ukraine (2023), Resolution "On the approval of the action plan for 2023–2024 for the implementation of the Cybersecurity Strategy of Ukraine", available at: https://zakon.rada.gov.ua/go/1163-2023-p (Accessed 20 March 2026).

10. Bornikov, O. (2023), “European integration of Ukraine: prospects for the IT sector and startup industry”, *Forbes Ukraine,* Available at: https://forbes.ua/innovations/efekt-tsifrovoi-sinergii (accessed 25 March 2026).

11. European Parliament and Council (2022), Directive (EU) 2022/2555 "On measures for a high common level of cybersecurity across the Union (NIS2 Directive)", *Official Journal of the European Union,* L 333, 27 December.

12. European Parliament and Council (2022), Regulation (EU) 2022/2554 "On digital operational resilience for the financial sector (DORA)", *Official Journal of the European Union,* L 333, 27 December.

Отримано редакцією журналу / Received: 13.04.26

Прорецензовано / Revised: 20.04.26

Дата публікації / Published: 23.04.26