

15. ISO. (2018). *ISO 14064-1:2018 — Greenhouse gases — Part 1: Specification with guidance at the organization level for quantification and reporting of greenhouse gas emissions and removals*. Geneva: International Organization for Standardization. ISO
16. ISO. (2018). *ISO 14067:2018 — Greenhouse gases — Carbon footprint of products — Requirements and guidelines*. Geneva: International Organization for Standardization. ISO
17. European Commission (DG ENV). (2021). *Commission Recommendation (EU) 2021/2279 on the use of Environmental Footprint methods (PEF/OEF)*. Brussels: European Commission. EnvironmentEPLCA
18. Keohane, R. O., & Victor, D. G. (2011). The Regime Complex for Climate Change. *Perspectives on Politics*, 9(1), 7–23. JSTOR
19. Nordhaus, W. D. (2015). Climate Clubs: Overcoming Free-Riding in International Climate Policy. *American Economic Review*, 105(4), 1339–1370. Американська економічна асоціація [ycsg.yale.edu](http://ycsg.yale.edu)
20. ERCST. (2022). *Reflection Note on Carbon Contracts for Difference (CCfD): State of Play and Design Questions*. Brussels: European Roundtable on Climate Change and Sustainable Transition. [ercst.org](http://ercst.org)
21. European Investment Bank. (2020). *EIB Group Climate Bank Roadmap 2021–2025*. Luxembourg: EIB. [eib.org+1](http://eib.org+1)
22. World Bank Group. (2021). *Climate Change Action Plan 2021–2025: Supporting Green, Resilient, and Inclusive Development*. Washington, DC: World Bank. World Bank
23. International Labour Organization. (2015). *Guidelines for a Just Transition towards Environmentally Sustainable Economies and Societies for All*. Geneva: ILO. International Labour Organization
24. European Commission. (2020–2025). *Just Transition Mechanism (JTM) — policy pages & factsheets*. Brussels: European Commission.

DOI 10.33111/vz\_kneu.40.25.03.12.081.087

**УДК 339.9**

**Миронченко Дмитро Володимирович**

здобувач третього (освітньо-наукового) рівня вищої освіти,  
Державне некомерційне підприємство «Державний університет «Київський авіаційний інститут»

e-mail: 8286196@stud.kai.edu.ua

ORCID: <https://orcid.org/0000-0002-9422-961X>

## **ЕТИЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ У СВІТОВІЙ ЕКОНОМІЦІ ТА МІЖНАРОДНИХ ВІДНОСИНАХ**

**Myronchenko Dmytro**

PhD student,

State Non-Profit Enterprise «State University «Kyiv Aviation Institute»

e-mail: 8286196@stud.kai.edu.ua

ORCID: <https://orcid.org/0000-0002-9422-961X>

## **ETHICAL ASPECTS OF CYBERSECURITY IN THE GLOBAL ECONOMY AND INTERNATIONAL RELATIONS**

**Анотація.** У статті розглянуто етичні аспекти забезпечення кібербезпеки у глобальній економіці та міжнародних відносинах. Виокремлено ключові етичні виклики, такі як захист приватності користувачів, корпоративні ризики безпеки та дилеми

у використанні даних, визначаючи їх вплив на економічну стабільність та міжнародні відносини. Актуальність дослідження полягає в необхідності адаптації світових практик забезпечення кібербезпеки та підтримки міжнародної економічної співпраці України, що сприятиме підвищенню довіри інвесторів і створенню більш безпечного середовища для функціонування міжнародних бізнес-процесів. Методологічною основою дослідження стали сучасні теорії міжнародних економічних відносин, концепції глобальної цифровізації економіки, наукові підходи до етики у сфері кібербезпеки. Використано як загальнонаукові, так і спеціальні методи наукового пізнання — порівняльний аналіз, системний підхід, метод структурно-логічного аналізу, контент-аналіз міжнародних нормативно-правових актів, стратегій та аналітичних звітів. Інформаційною основою дослідження слугують наукові праці та монографічні видання українських й іноземних вчених, дані міжнародних організацій та аналітичні звіти провідних компаній з кібербезпеки. Результати дослідження можуть бути використані для наукового обґрунтування та практичної реалізації стратегій з підвищення рівня захисту даних, удосконалення етичних стандартів у сфері цифрової безпеки, зниження корпоративних ризиків, а також для сприяння формуванню сталих міжнародних економічних зв'язків. Практичне значення отриманих результатів полягає у можливості застосування їх у процесі розробки національних стратегій кібербезпеки та міжнародних угод.

**Ключові слова:** економічна безпека, ризики, кіберзагрози, цифровізація, інформатизація, міжнародні економічні відносини, міжнародна співпраця.

**Abstract.** The article examines the ethical aspects of ensuring cybersecurity in the global economy and international relations. Key ethical challenges are identified, such as protecting user privacy, corporate security risks, and dilemmas in data use, determining their impact on economic stability and international relations. The relevance of the study lies in the need to adapt global practices for ensuring cybersecurity and supporting international economic cooperation in Ukraine, which will help increase investor confidence and create a safer environment for the functioning of international business processes. The methodological basis of the study was modern theories of international economic relations, concepts of global digitalization of the economy, and scientific approaches to ethics in the field of cybersecurity. Both general scientific and special methods of scientific knowledge were used — comparative analysis, systems approach, method of structural-logical analysis, content analysis of international regulatory legal acts, strategies, and analytical reports. The information basis of the study is scientific works and monographic publications of Ukrainian and foreign scientists, data from international organizations and analytical reports of leading cybersecurity companies. The results of the study can be used for scientific substantiation and practical implementation of strategies to increase the level of data protection, improve ethical standards in the field of digital security, reduce corporate risks, as well as to promote the formation of sustainable international economic ties. The practical significance of the results obtained lies in the possibility of their application in the process of developing national cybersecurity strategies and international agreements.

**Keywords:** economic security, risks, cyber threats, digitalization, informatization, international economic relations, international cooperation.

JEL codes: F02, F52, O33.

**Постановка проблеми.** На сьогоднішній день етичні аспекти кібербезпеки є одним з ключових чинників стабільності міжнародних економічних відносин. Зростання обсягів даних і поширення кіберзагроз формують дилеми захисту приватності, корпоративної відповідальності та справедливого використання інформації. Порушення етичних стандартів веде до фінансових витрат і втрати довіри між державами та партнерами. В таких умовах для України набуває особливого значення впровадження світових практик кіберзахисту, що сприятиме інтеграції у міжнародний економічний простір, підвищенню довіри інвесторів і розвитку співпраці.

**Аналіз останніх досліджень і публікацій.** Функціонування економічної системи в умовах інформаційної безпеки привертає все більшу увагу науковців. Так,

Г. Маркус, професор Нью-Йоркського університету, досліджує етичні аспекти використання ІІІ та піднімає питання відповідальності за алгоритмічні рішення, що впливають на суспільство. [1; 2]. Б. Шнайер та Е. Коул заклали основи сучасних теорій кібербезпеки, розробили інструменти протидії загрозам і сформували міжнародні рамки безпеки, що охоплюють моніторинг на глобальному рівні [3; 4]. Українські вчені О. Дерев'янка та Ю. Щиголь досліджують міжнародну кібербезпеку. Науковець О. Дерев'янка акцентує увагу на зростанні кібератак і їхньому впливі на критичну інфраструктуру та інформаційні ресурси, а також на викликах для ЄС [5]. Ю. Щиголь досліджує особливості регулювання кібербезпеки в міжнародних секторах економіки та загрози національним інтересам [6]. Вчений Р. Андерсон підкреслює значення кібербезпеки для міжнародної торгівлі та економічної стабільності. Дж. Спаффорд, професор Університету Пердью, заснував центр освіти та досліджень інформаційної безпеки (CERIAS) і зробив вагомий внесок у розвиток прикладної кіберкриміналістики та розробки захисних інструментів [7]. Дж. Спаффорд обґрунтовує інструменти з відкритим кодом, як от Tripwire [8].

**Виділення невирішених раніше частин загальної проблеми.** Попри значні наукові напрацювання, відкритими залишаються питання балансу між конфіденційністю та державним моніторингом, запобігання дискримінації даних у торгівлі й фінансах, дотримання етичних принципів.

**Метою** статті є обґрунтування науково-практичних рекомендацій щодо вирішення етичних проблем забезпечення кібербезпеки у міжнародних економічних відносинах.

**Методика дослідження.** Теоретико-методологічною основою дослідження є сучасні теорії міжнародних економічних відносин, концепції глобальної цифровізації економіки, наукові підходи до етики у сфері кібербезпеки. Основні методи дослідження включають порівняльний аналіз (для виявлення відмінностей і подібностей у міжнародних практиках кібербезпеки), системний підхід (для дослідження взаємозв'язку між етичними аспектами кіберзагроз та економічною стабільністю), метод структурно-логічного аналізу (для визначення ключових етичних проблем кібербезпеки та їх впливу на міжнародні відносини), контент-аналіз міжнародних нормативно-правових актів, стратегій та звітів з кібербезпеки.

**Виклад основного матеріалу.** Баланс між конфіденційністю та національною безпекою є ключовим викликом сучасної кібербезпеки. Зростання цифрових технологій змушує уряди захищати громадян від кіберзагроз, уникаючи порушення прав людини. Протистояння посилюється після терактів 11 вересня 2001 року, коли США ухвалили USA PATRIOT Act [9], що розширив державний доступ до персональних даних і викликав критику за обмеження приватності. Подібні тенденції спостерігалися в Україні, хоча підходи до моніторингу відрізняються.

Сучасні технології — ІІІ, розпізнавання облич, великі дані та ІоТ — розширили можливості держав у моніторингу та протидії кіберзлочинності й тероризму. Водночас правозахисники критикують такі практики як загрозу праву на приватність. Наприклад:

- в США пріоритет надано безпеці — програми на кшталт PRISM показали, що масовий збір даних став інструментом державного нагляду, викликавши суспільне обурення;
- ЄС зробив пріоритетом захист даних — регламент GDPR (General Data Protection Regulation, або «Загальний регламент про захист даних») (2018)

встановив жорсткі правила й штрафи, забезпечивши високий рівень конфіденційності, але ускладнивши державний моніторинг кіберзагроз;

- в Китаї домінує суворий контроль — система соціального кредиту з ШІ та розпізнаванням облич підтримує порядок, але порушує питання прав людини;

- в Україні баланс безпеки й конфіденційності загострився через війну з росією. З 2014 року держава посилює кіберзахист, застосовуючи системи моніторингу та аналізу даних в реальному часі. Такі заходи мають на меті захист національної безпеки проте правозахисники критикують відсутність належного нагляду й ризик зловживань;

- в Росії домінує жорсткий державний контроль — «Пакет Яровой» та система СОПМ передбачають масштабний моніторинг інтернет-активності, що посилює ризики масового нагляду.

Жорсткий контроль над конфіденційністю впливає й на бізнес. Так, компанії Facebook та Google несуть значні витрати на відповідність GDPR, що знижує їхню конкурентоспроможність через урівнювання можливостей.

В Україні ж посилення кібербезпеки підвищило довіру партнерів та інвестиційну привабливість.

Таблиця 1

**ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА ПІДХОДІВ ДО БАЛАНСУВАННЯ ІНТЕРЕСІВ  
У РІЗНИХ КРАЇНАХ**

| Країна  | Підхід до національної безпеки                                                                                                             | Підхід до конфіденційності                                                                                |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| США     | Широкий державний моніторинг та програми збору даних (наприклад, PRISM). Пріоритет безпеки                                                 | Після терактів 2001 року використання даних без достатнього нагляду                                       |
| ЄС      | Суворий нагляд за безпекою в межах вимог GDPR. Прагнення до прозорості                                                                     | Основний акцент на захист персональних даних                                                              |
| Китай   | Тотальний державний контроль, використання технологій для моніторингу та соціального кредиту                                               | Обмежена конфіденційність, відсутність прав на приватність в умовах державного контролю                   |
| Україна | Посилення кібербезпеки у відповідь на конфлікт з Росією. Використання системи «СОТА» для перехоплення комунікацій та аналізу великих даних | Зростаюча стурбованість щодо порушення прав людини внаслідок надмірного моніторингу без належного нагляду |
| Росія   | Жорсткий контроль за інтернетом та комунікаціями, системи моніторингу (СОПМ)                                                               | Акцент на державний контроль. Закони на зразок «Ярової пакету»                                            |

Джерело: розроблено автором

Прозорість державного моніторингу передбачає право громадян знати, як обробляються їх дані. Це забезпечується незалежним наглядом — омбудсменами чи радами з участю громадськості та експертів, які проводять аудит і публікують звіти. Важливим завданням є створення міжнародних стандартів кібербезпеки й конфіденційності під егідою ООН чи ЄС, що встановлять правила зберігання, обміну даними та прозорості програм моніторингу. Діалог між державою та суспільством є ключем до балансу безпеки й конфіденційності: регулярні

обговорення й звіти за участю науковців, урядовців, бізнесу та правозахисних органів підвищують довіру та знижують напругу. Заходи кіберзахисту мають гарантувати дотримання прав людини — приватності, свободи слова та доступу до інформації, що потребує чітких законів для обмеження моніторингу й захисту від зловживань. Необхідно інвестувати в технології захисту — шифрування, анонімізацію, блокчейн і квантові рішення, що поєднують конфіденційність із безпекою. Водночас міжнародна співпраця через обмін інформацією, узгодження стандартів та спільну протидію інцидентам підвищує ефективність глобальної кібербезпеки, захищає дані й знижує ризики для громадян та бізнесу.

Таким чином, баланс між конфіденційністю та безпекою потребує не лише законодавчих і технологічних рішень, а й участі громадянського суспільства, міжнародної співпраці та підзвітності держави. Лише комплексний підхід дозволяє захистити права громадян і забезпечити безпеку у цифровому світі.

У міжнародній торгівлі дані стали ключовим інструментом ухвалення рішень, однак їхнє неналежне використання, відсутність перевірок можуть призвести до того, що алгоритми можуть стати упередженими, оскільки базуються на історичних даних, що відображають соціальну чи економічну нерівність.

Найбільший ризик дискримінації проявляється у кредитуванні, де використання історичних даних відтворює расові й етнічні упередження, що позбавляє окремі групи населення доступу до кредитів або погіршує умови кредитування. Подібні практики спостерігаються у страхуванні, де соціально-економічний статус впливає на розмір виплат чи відмову у полісі. У сфері персоналізованої реклами це виражається в обмеженні пропозицій для певних категорій клієнтів за віком, статтю чи культурною ознакою, що формує бар'єри до рівного доступу.

Досить великий ризик дискримінації у міжнародних фінансових операціях де алгоритми програм та ШІ можуть дискримінувати, автоматично виключаючи групи населення за расою, національністю чи соціально-економічним статусом.

Таблиця 2

#### КЛАСИФІКАЦІЯ ДИСКРИМІНАЦІЙНИХ ПРАКТИК У ФІНАНСОВИХ ОПЕРАЦІЯХ

| Параметр                   | Дискримінаційний фактор         | Наслідки                                     |
|----------------------------|---------------------------------|----------------------------------------------|
| Оцінка кредитоспроможності | Гендер, раса або національність | Відмова у кредитуванні або гірші умови       |
| Страхові поліси            | Соціально-економічний статус    | Вищі премії або відмова у страхуванні        |
| Персоналізована реклама    | Гендер, раса або національність | Обмежений доступ до пропозицій або вищі ціни |

Джерело: розроблено автором

Можемо побачити як використання ШІ або алгоритмів в оцінці кредитоспроможності призводить до того, що представники певних гендерних, етнічних і расових груп отримують відмову в кредитуванні, обмежується доступ до певних товарів і послуг або призводить до встановлення вищих цін.

Законодавчі ініціативи відіграють ключову роль у запобіганні дискримінації при використанні даних. Прикладом є GDPR, що встановив суворі вимоги до обробки персональних даних та гарантував права громадян на конфіденційність і захист від упередженості. Регламент забороняє обробку даних без згоди користувача й вимагає, щоб автоматизовані рішення мали можливість перегляду. Це зобов'язує компанії поєднувати алгоритми з контролем людини, що мінімізує ризики дискримінаційних практик у міжнародній торгівлі та фінансах.

Приклади успішного впровадження GDPR у боротьбі з дискримінацією:

1. Запобігання дискримінації в оцінці кредитоспроможності. До GDPR кредитні алгоритми часто дискримінували окремі групи. Регламент зобов'язав фінансові установи забезпечити прозорість, людський нагляд і аудит рішень, що зменшило упередженість.

2. Застосування GDPR у рекламних технологіях. GDPR змусив компанії змінити таргетинг: компанії на кшталт Google і Facebook обмежили використання чутливих даних, запровадили антидискримінаційні політики, аудит і незалежний моніторинг.

3. Вплив GDPR на глобальні компанії. GDPR поширився й на глобальні корпорації, що працюють з даними громадян ЄС. Він змусив їх переглянути обробку даних, підвищити прозорість і став моделлю для інших країн, сприяючи уніфікації стандартів та міжнародній співпраці.

Етичне використання даних спирається на наступні принципи: прозорість, справедливість, відповідальність і підзвітність. Прозорість означає зрозуміле інформування про збір і використання даних та алгоритмів, що впливають на рішення, що підвищує довіру суспільства. Справедливість передбачає уникнення відтворення соціальних, економічних чи расових нерівностей в алгоритмах і гарантування рівних можливостей. Відповідальність і підзвітність зобов'язують компанії, уряди та розробників захищати персональні дані й створювати механізми для оскарження рішень. Незалежний аудит і відкриті системи моніторингу допомагають зменшити ризики зловживань та забезпечити справедливе використання інформації.

Насьогодні етичність використання даних стає пріоритетом на міжнародному рівні. ЄС у межах GDPR розробляє стандарти «Fair AI», що передбачають тестування алгоритмів на упередженість і запровадження механізмів прозорості й підзвітності з жорсткими санкціями за порушення.

У США IBM впровадила програму «AI Ethics Framework», що інтегрує принципи справедливості, прозорості та відповідальності. Її інструмент AI Fairness 360 дозволяє виявляти й виправляти упередженість у сферах кредитування, страхування та HR, забезпечуючи рівне ставлення до клієнтів.

Канада запровадила політику обов'язкової оцінки впливу на конфіденційність та стандарти прозорості перед впровадженням нових технологій, що використовують персональні дані, які зобов'язують компанії розкривати принципи роботи алгоритмів [11].

Японія у межах «Роботичної стратегії» впроваджує стандарти етичного використання III та робототехніки, засновані на справедливості, прозорості й відповідальності. Вони спрямовані на запобігання упередженню та соціальній ізоляції груп населення [12].

Попри активну розробку етичних стандартів, їх дотримання залишається проблемою через різні підходи країн. Необхідними є міжнародні механізми моніторингу та оцінки впливу алгоритмів. У майбутньому стандарти, особливо у сфері

ШІ, розвиватимуться, а співпраця й інноваційні рішення, такі як AI Fairness 360 чи канадські оцінки впливу на конфіденційність, можуть стати основою глобальних правил, що гарантують рівність і недискримінаційність.

В умовах війни Україна активно розвиває кіберзахист із використанням ШІ та прагне впроваджувати етичні стандарти на рівні західних країн. У співпраці з міжнародними організаціями ухвалюються регуляторні акти для етичного застосування ШІ у військовій та цивільній сферах. Прикладами є «Національна стратегія цифрової трансформації до 2025 року», що включає етичне використання ШІ в державних послугах, зокрема платформі «Дія» [13], а також Закон «Про захист персональних даних». Україна впроваджує кібербезпекові протоколи, що базуються на міжнародних етичних стандартах [14]. Співпрацюючи з Європейським агентством з оборони, Україна розробляє стандарти для використання ШІ у військових цілях [15].

**Висновки.** У ході дослідження встановлено, що кібербезпека у сучасних умовах є не лише технічним, а й етичним викликом, який безпосередньо впливає на стабільність світової економіки та розвиток міжнародних відносин. Визначено, що головними етичними проблемами у сфері цифрової безпеки виступають: захист приватності особистих та корпоративних даних, відповідальність бізнесу за безпечне зберігання інформації, а також етичні дилеми, пов'язані з використанням великих масивів даних у глобальній економіці.

Результати аналізу свідчать про необхідність формування міжнародних стандартів етичної поведінки у сфері кібербезпеки, що забезпечить баланс між технологічним прогресом, економічними інтересами та правами користувачів. Важливою умовою зміцнення глобальної цифрової довіри є розвиток партнерства між державами, міжнародними організаціями та бізнесом, спрямованого на протидію кіберзагрозам.

Практичне значення дослідження полягає у можливості використання його результатів для вдосконалення національних і міжнародних стратегій кіберзахисту, зниження корпоративних ризиків, підвищення інвестиційної привабливості країн та підтримки сталого економічного розвитку. Для України впровадження світових етичних практик у сфері кібербезпеки створює додаткові можливості інтеграції у глобальний економічний простір і посилення міжнародної співпраці.

### **Література**

1. Marcus G. I went for a walk with Gary Marcus, AI's loudest critic // MIT Technology Review. — 2024. — February 20. — URL: <https://www.technologyreview.com/2024/02/20/1088701/i-went-for-a-walk-with-gary-marcus-ais-loudest-critic/>
2. New York University Stern School of Business. Fubon Center for Technology, Business and Innovation: 2022–2023 events. — URL: <https://www.stern.nyu.edu/experience-stern/about/departments-centers-initiatives/centers-of-research/fubon-center-technology-business-and-innovation/fubon-center-technology-business-and-innovation-events/2022-2023-events-2-1>
3. Schneier B. Data and Goliath: The hidden battles to collect your data and control your world. — New York: W. W. Norton & Company, 2015. — URL: [https://ciberativismoeguerra.wordpress.com/wp-content/uploads/2017/09/bruce-schneier-data-and-goliath\\_-2015.pdf](https://ciberativismoeguerra.wordpress.com/wp-content/uploads/2017/09/bruce-schneier-data-and-goliath_-2015.pdf)
4. Cole E. Network Security Bible. — Hoboken, NJ: Wiley, 2009. — URL: [https://www.academia.edu/12085040/Network\\_Security\\_Bible](https://www.academia.edu/12085040/Network_Security_Bible)

5. CNBC. Oleh Derevianko. — 2017. — September 7. — URL: <https://www.cnb.com/2017/09/07/oleh-derevianko.html>
6. Sakellariadis J., Miller M. Ukraine gears up for new phase of cyber war with Russia // Politico. — 2022. — July 14. — URL: <https://www.politico.com/news/magazine/2022/07/14/russia-cyberattacks-ukraine-cybersecurity-00045486>
7. The College at Brockport. Securing a place in cyberspace. — 2022. — April 20. — URL: <https://www.brockport.edu/live/news/5208-securing-a-place-in-cyberspace>
8. Purdue University. Spaf's narrations: Stories from the trenches. — URL: <https://spaf.cerias.purdue.edu/narrate.html>
9. Congress.gov. USA PATRIOT Act. — 2001. — URL: <https://www.congress.gov/bill/107th-congress/house-bill/3162>
10. European Commission. Ethics guidelines for trustworthy AI. — 2019. — URL: <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>
11. IBM. AI Ethics Framework. — URL: <https://www.ibm.com/watson/ai-ethics/>
12. Ministry of Economy, Trade and Industry (METI), Japan. Robot Strategy. — 2015. — URL: [https://www.meti.go.jp/english/policy/mono\\_info\\_service/robot\\_industry/index.html](https://www.meti.go.jp/english/policy/mono_info_service/robot_industry/index.html)
13. Міністерство цифрової трансформації України. Національна стратегія цифрової трансформації до 2025 року. — 2020. — URL: <https://plan2.dii.gov.ua> [In Ukrainian]
14. NATO. NATO Cyber Defence Trust Fund. — 2020. — URL: [https://www.nato.int/cps/en/natohq/topics\\_78170.htm](https://www.nato.int/cps/en/natohq/topics_78170.htm)
15. European Defence Agency. European Defence Agency (EDA). — URL: <https://eda.europa.eu/>
16. Миронченко Д. Вплив цифрової трансформації на стратегії міжнародних етапів // Збірник наукових праць XVII Міжнародної науково-практичної конференції «B2B Marketing» з нагоди 125-річчя КПП ім. Ігоря Сікорського: Збірник тез. — Київ: КПП ім. Ігоря Сікорського, 2023. — С. 172–173. — URL: <http://b2b-marketing.fmm.kpi.ua/proc/issue/view/17528/10197> [In Ukrainian]
17. Миронченко Д. Міжнародний бізнес в інноваційних кластерах // Збірник наукових праць «Творчий внесок професора Антона Філіпенка у навчально-науковий процес економічних спеціальностей вищих навчальних закладів України»: Збірник тез. — Київ: Київський національний університет імені Тараса Шевченка, 2023. — С. 172–173. [In Ukrainian]
18. Myronchenko D. Ensuring national and economic security through effective cybersecurity measures // XIV міжнародна науково-практична конференція «Національні економічні стратегії розвитку в глобальному середовищі»: Збірник тез. — Київ: НАУ, 2023. — С. 27–30. — URL: <https://drive.google.com/file/d/18gwybyPV5UPbae1rcWR-PDiZwne8bbxe/view>
19. Myronchenko D., Sydorenko K. Role of the IT-sector of Ukraine in the global cyber security system // Економічний простір. — 2023. — № 186. — URL: <http://www.prostir.pdaba.dp.ua/index.php/journal/issue/archive>

## References

1. Marcus, G. (2024, February 20). I went for a walk with Gary Marcus, AI's loudest critic. *MIT Technology Review*. <https://www.technologyreview.com/2024/02/20/1088701/i-went-for-a-walk-with-gary-marcus-ais-loudest-critic/>
2. New York University Stern School of Business. (2023). *Fubon Center for Technology, Business and Innovation: 2022–2023 events*. <https://www.stern.nyu.edu/experience-stern/about/departments-centers-initiatives/centers-of-research/fubon-center-technology-business-and-innovation/fubon-center-technology-business-and-innovation-events/2022-2023-events-2-1>