УДК 339.9:004.946.5.056
DOI: https://doi.org/10.32782/2413-9971/2024-53-2

Заяць Д.Ф.
студентка магістратури
Волинського національного університету імені Лесі Українки
Кицюк І.В.
кандидат економічних наук, доцент,
доцент кафедри міжнародних економічних відносин
та управління проєктами
Волинського національного університету імені Лесі Українки

Zaiats Diana
Master's Student
Lesya Ukrainka Volyn National University
Kytsyuk Iryna
PhD in Economics, Associate Professor,
Associate Professor of International Economic Relations
and the Project Management Department
Lesya Ukrainka Volyn National University

РОЛЬ КІБЕРБЕЗПЕКИ В МІЖНАРОДНИХ ЕКОНОМІЧНИХ ВІДНОСИНАХ

Анотація. *У статті досліджується роль кібербезпеки в міжнародних економічних відносинах. Акцентується увага на зростаючій важливості цифрової інфраструктури для глобальної економіки, що створює нові ризики, пов'язані з кіберзлочинністю, промисловим шпигунством, кібератаками на критичні об'єкти та порушеннями конфіденційності даних. Аналізуються міжнародні ініціативи та політики у сфері кібербезпеки, спрямовані на запобігання відповідним загрозам і формування стійкої економічної системи. Окрему увагу приділено взаємозв'язку кіберзахисту з економічними інтересами держав, транснаціональних корпорацій і міжнародних організацій. Як підсумок наголошується, що забезпечення кібербезпеки є не лише технологічним, але й стратегічним завданням, здатним вплинути на стабільність і розвиток міжнародної економіки в умовах цифрової трансформації.*

Ключові слова: *кібербезпека, міжнародні економічні відносини, кібератаки, кіберзагрози, глобальна економіка, захист даних, цифровізація, інновації, геополітика.*

Вступ та постановка проблеми. Цифровізація глобальної економіки спричинила сприятливі масштабні трансформації у міжнародних економічних відносинах, проте водночас виявила «слабкі місця», пов’язані з кіберзагрозами. Кібератаки на критичну інфраструктуру, викрадення конфіденційних даних, промислове шпигунство та економічний саботаж стали реальними викликами, які впливають не лише на окремі держави, а й на глобальну економічну стабільність в цілому. Ця проблема є особливо актуальною в умовах посилення міждержавної конкуренції, залежності від цифрових технологій та ескалації геополітичної напруги.

Ключовою науковою проблемою є визначення впливу кіберзагроз на міжнародну економіку, а також розробка ефективних механізмів їхньої нейтралізації. На практичному рівні завдання полягає у створенні дієвих політик і міжнародних стандартів у сфері кібербезпеки, які забезпечуватимуть стійкість цифрової інфраструктури, захист даних і безпеку транскордонних економічних операцій.

Наукове значення проблеми полягає в дослідженні взаємозв’язку кібербезпеки з ключовими аспектами міжнародних економічних відносин, зокрема глобальними ланцюгами поставок, фінансовими ринками, інноваційними технологіями та економічною дипломатією. Також важливо проаналізувати нові форми загроз, такі як економічний кібертероризм і використання кіберзброї у міжнародній конкуренції.

Аналіз останніх досліджень і публікацій. Питанням кібербезпеки як виклику для міжнародних економічних відносин присвячено праці таких вчених, як Андерсон Р. [6], Келло Л. [7], Шнайєр Б. [10]. Аспекти впливу кібератак на економічну стабільність і глобальні ланцюги постачання висвітлено у роботах Андерсона Р. [6]. Проблеми геополітичних кіберзагроз і їх впливу на економічну конкуренцію між державами розглядаються у дослідженнях Келло Л. [7], а також у звітах таких міжнародних організацій, як UNCTAD [16] і ITU [15]. У контексті дослідження також використовуються праці міжнародної корпорації у сфері аудиторських та консалтингових послуг Делойт Інсайтс [14].

Міжнародні ініціативи у сфері кібербезпеки, такі як роль публічно-приватного партнерства та впровадження міжнародних стандартів, аналізуються у роботах Всесвітнього економічного форуму [17]

і ITU [15]. Інноваційні підходи до забезпечення кіберзахисту за допомогою штучного інтелекту, блокчейну та інших технологій висвітлено у звітах Cisco [13].

Юридичні аспекти, включаючи питання міжнародного регулювання та етики кібербезпеки, досліджуються у працях Шнайєра Б. [10], а також у роботах Бендіка М., Портера Г. [11]. Разом з тим, слід зазначити, що залишаються недостатньо вивченими аспекти впливу кіберзагроз на формування довгострокових економічних стратегій держав і транснаціональних корпорацій, а також питання координації міжнародної співпраці у цій сфері.

Формулювання цілей статті (постановка завдання). Основне завдання статті полягає у дослідженні напрямів забезпечення кібербезпеки у контексті міжнародних економічних відносин для мінімізації ризиків кібератак, захисту цифрової інфраструктури та зміцнення економічної стабільності на глобальному рівні.

Результати дослідження. Кіберагресія є зростаючою загрозою для міжнародної безпеки та глобальної стабільності. Хоча національні політики, спрямовані на стримування кіберагресії, можуть дати певні результати у короткостроковій перспективі, їхня ефективність у довгостроковій перспективі викликає сумніви. Національні стратегії кіберстримування несуть ризик постійної гонки озброєнь у кіберпросторі та циклу ескалації між потенційними кібер-супротивниками. Дипломатія, хоч і може дати менші результати в короткостроковій перспективі, є більш дієвою в довгостроковій.

Цифрова трансформація, зокрема питання кібербезпеки, є одним із найважливіших викликів для сучасного міжнародного бізнесу. Сьогоднішні компанії зберігають великі обсяги конфіденційних даних і клієнтської інформації в електронних системах. Зростання кількості кібератак та порушень безпеки даних ставить під загрозу діяльність міжнародних компаній, що зумовлює необхідність пошуку ефективних засобів захисту цієї інформації.

Кібербезпека передбачає захист ключових інтересів особи, суспільства та держави у сфері використання кіберпростору. Це включає підтримку стабільного розвитку інформаційного суспільства і цифрового середовища, а також вчасне виявлення, попередження та нейтралізацію як існуючих, так і потенційних загроз.

Кіберзахист, у свою чергу, являє собою комплекс організаційних, правових, інженерних та технічних заходів, зокрема криптографічних методів і технічного захисту даних, який спрямований на запобігання кіберінцидентам. Він також охоплює виявлення та протидію кібератакам, усунення їх наслідків і відновлення стабільності та надійності функціонування комунікаційних і технологічних систем. У свою чергу, Законом України «Про основні засади забезпечення кібербезпеки України», поняття «кібербезпеки» трактує наступним чином: «кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [1].

Важливість кібербезпеки зумовлена тим, що цифрова економіка значною мірою залежить від обробки, передачі та зберігання великих обсягів даних, що створює нові виклики для захисту конфіденційності, цілісності та доступності інформації. Таким чином, кібербезпека набуває критичного значення для забезпечення стабільності та безпеки сучасного інформаційного середовища в умовах цифрової економіки.

Цифрова економіка відкриває безмежні можливості для підвищення ефективності, зручності та впровадження інновацій у бізнесі та державному секторі. Вона дозволяє підприємствам швидше реагувати на ринкові зміни, пропонувати нові послуги та автоматизувати процеси. Проте, разом із цими перевагами зростають і ризики, пов'язані з кібербезпекою. Кількість кібератак збільшується, а хакери стають дедалі винахідливішими, агресивніше використовуючи прогалини в захисті цифрових систем. Кіберзлочинці швидко освоюють нові технології, тому підходи до кібербезпеки повинні бути не лише захищеними, але й динамічними, постійно адаптуючись до змінних загроз.

Забезпечення кібербезпеки в умовах цифрової економіки потребує всебічного, комплексного підходу. Насамперед, необхідно вдосконалювати технічні засоби захисту. Це включає впровадження інноваційних систем інтелектуального аналізу для виявлення аномалій у мережевому трафіку, шифрування даних на різних етапах їх обробки, а також запровадження сучасних систем ідентифікації та багатофакторної аутентифікації для обмеження доступу до чутливих даних.

Однак технічний захист – це лише частина стратегії. Не менш важливою є робота з персоналом. Розвиток культури кібербезпеки всередині організацій допомагає запобігти людським помилкам, які можуть спричинити серйозні витоки інформації. Регулярні тренінги, симуляції кібератак і підвищення обізнаності працівників щодо сучасних кіберзагроз формують навички та знання, необхідні для підтримки безпеки.

Загрози в кіберпросторі визначаються двома ключовими факторами: наявністю наміру діяти проти цілі та здатністю реалізувати цей намір. Якщо можливість атакувати існує, але відсутній намір її використати, загроза, фактично, стає малоймовірною. Мотивація кіберзлочинців може значно варіюватися – від випадкових атак до політичної активності та державного шпигунства [12].

Державне шпигунство є лише однією з численних загроз у сфері кібербезпеки. Критична важливість кібербезпеки для міжнародного бізнесу проявляється у випадках, коли корпоративні мережі стають мішенню кібератак, зокрема фішингових кампаній,

витоків даних, зламу облікових записів користувачів і адміністраторів. Окрім цього, діяльність, пов'язана з віртуальним шпигунством, зокрема крадіжкою інтелектуальної власності та конфіденційної інформації, також створює серйозні ризики для компаній. Такі інциденти не лише підривають стабільність і довіру до бізнесу, але й можуть завдати значних фінансових збитків, що ще більше підкреслює важливість забезпечення кіберзахисту в глобальному масштабі.

Вразливість цифрової інфраструктури різних галузей створює ризики, що можуть призвести до фінансових втрат, збоїв у роботі систем і навіть до глобальних економічних криз. Для ілюстрації цього питання доцільно розглянути специфіку кіберзагроз і заходи захисту в ключових секторах економіки, що представлені в таблиці 1.

Вдосконалення правової та регуляторної бази має критичне значення для ефективного реагування на кіберзагрози. Законодавство повинно залишатися гнучким, щоб відповідати на нові технологічні виклики та кіберзагрози. Водночас розвиток міжнародних стандартів і посилення співпраці між країнами створюють можливості для обміну інформацією та об'єднання зусиль у протидії кіберзлочинності.

Підвищення рівня кіберграмотності суспільства також є вагомим елементом кібербезпеки. Інформування громадськості про потенційні загрози, навчання базових навичок кібербезпеки та популяризація принципів самозахисту в інтернеті здатні значно знизити ризики кібератак та шахрайства.

Таким чином, для забезпечення кібербезпеки в цифровій економіці потрібен комплексний підхід, що охоплює технічні, правові та освітні заходи. Тільки взаємодія між державою, бізнесом та громадськістю може гарантувати надійний захист від кіберзагроз і підтримку стабільності в цифровій економіці.

У вересні 2017 року, коли компанія Equifax, одна з найбільших агенцій кредитних рейтингів у США, оголосила про масштабний витік даних, який вплинув на понад 147 мільйонів клієнтів. Внаслідок цієї кібератаки були викрадені важливі особисті дані, включаючи номери соціального страхування, дати народження, адреси та в деяких випадках навіть номери водійських посвідчень і дані про кредитні картки. Хакери отримали доступ до системи Equifax через вразливість у веб-додатку, яку компанія не встигла вчасно усунути, хоча про цю вразливість було відомо заздалегідь. Компанія зазнала значних фінансових збитків, сплатила штрафи та зіштовхнулася з багатьма колективними позовами. Збитки для репутації також були суттєвими, оскільки витік даних значно підірвав довіру клієнтів до Equifax як до агенції, що має забезпечувати захист їхньої фінансової інформації [9].

Однак, кібератаки більше не є локальними подіями – вони мають глобальні наслідки, які можуть впливати на держави, корпорації та мільйони людей. Фінансові втрати від кіберзлочинності щорічно обчислюються сотнями мільярдів доларів, тоді як наслідки порушень у критичній інфраструктурі, таких як енергетика чи транспорт, можуть дестабілізувати регіони і навіть цілі економіки. Прикладом є масштабні атаки на фінансові установи, що паралізують банківські системи, або втручання у промислові об'єкти, які можуть спричинити екологічні катастрофи.

Таблиця 1

Аналіз заходів кібербезпеки у ключових секторах економіки

Сектор економіки	Типи вразливостей	Основні заходи захисту	Потенційні втрати від атак
Фінансовий	– Фішинг – Шкідливе ПЗ – Атаки на банкомати	– Впровадження багатофакторної автентифікації – Регулярне оновлення ПЗ – Навчання персоналу	– Фінансові втрати – Втрата довіри клієнтів – Юридичні наслідки
Енергетичний	– Атаки на SCADA-системи – DDoS-атаки – Впровадження шкідливого ПЗ	– Сегментація мережі – Моніторинг аномалій – Резервне копіювання систем	– Перебої в енергопостачанні – Економічні збитки – Загроза національній безпеці
Транспортний	– Втручання в навігаційні системи – Атаки на системи управління трафіком – Крадіжка даних пасажирів	– Шифрування даних – Контроль доступу – Оновлення систем безпеки	– Затримки та збої в перевезеннях – Фінансові втрати – Порушення логістичних ланцюгів
Охорона здоров'я	– Викрадення медичних даних – Атаки на медичне обладнання – Шкідливе ПЗ	– Захист електронних медичних записів – Контроль доступу до обладнання – Навчання персоналу	– Порушення роботи медичних закладів – Втрата конфіденційності пацієнтів – Юридичні наслідки
Виробничий	– Атаки на промислові контролери – Шпигунство – Впровадження шкідливого ПЗ	– Сегментація мережі – Моніторинг аномалій – Захист інтелектуальної власності	– Зупинка виробництва – Втрата конкурентних переваг – Фінансові збитки

Джерело: складено за [1–5]

Висновки. Таким чином, загроза кібербезпеки – це стратегічна проблема, що вимагає комплексного підходу. Держави і міжнародні організації повинні об'єднати свої зусилля для створення ефективних механізмів захисту. У цьому контексті особливої ваги набуває міжнародне співробітництво. Необхідно розробляти глобальні стандарти у сфері кібербезпеки, які будуть обов'язковими для всіх учасників міжнародного економічного процесу. Це дозволить мінімізувати ризики кібератак і створити стійку цифрову екосистему.

Однак міжнародна співпраця стикається з низкою перешкод. Геополітична напруга, що часто виявляється у кіберпросторі, ускладнює досягнення глобального консенсусу. Країни, які використовують кіберзброю як інструмент у своїх стратегіях, створюють додаткові ризики для міжнародної стабільності. Водночас цифровий розрив між розвиненими країнами та країнами, що розвиваються, ставить під загрозу глобальні ініціативи у сфері кібербезпеки.

Для вирішення цих проблем необхідно діяти у кількох напрямах. Перш за все, держави повинні зосередитися на захисті критичної інфраструктури, оскільки її вразливість має наймасштабніші наслідки. Інноваційні технології, такі як штучний інтелект і блокчейн, можуть стати потужними інструментами у забезпеченні кіберзахисту, однак їх впровадження потребує ретельного регулювання.

Освіта також відіграє важливу роль у зміцненні кібербезпеки. Глобальне суспільство має підвищити рівень обізнаності про загрози, пов'язані з кіберзлочинністю, і навчити людей основам кібергігієни. Особлива увага має бути приділена підготовці кадрів, які зможуть ефективно реагувати на виклики цифрової епохи.

Не менш важливим є надання підтримки країнам, що розвиваються, у зміцненні їх кіберстійкості. Розвинені держави та міжнародні організації повинні надавати технічну, фінансову та експертну допомогу, щоб зменшити цифровий розрив і забезпечити глобальну економічну стабільність.

Кібербезпека – це не лише технічне завдання, а й питання глобального значення, що визначає майбутнє міжнародних економічних відносин. Лише через об'єднання зусиль усіх учасників міжнародної спільноти можливо створити безпечне цифрове середовище, яке сприятиме економічному розвитку, інноваціям та стабільності. Тому вирішення цього виклику має бути пріоритетом як на національному, так і на міжнародному рівні.

Список використаних джерел*:*

1. Деркач М. 10 трендів кібербезпеки у 2024 році, до яких треба готуватися вже зараз. *PaySpace Magazine:* веб-сайт. URL: https://psm7.com/uk/analytics/10-trendov-kiberbezopasnosti-v-2024-godu-k-kotorym-nado-gotovitsya-uzhe-sejchas.html (дата звернення: 09.09.2024).
2. Мельник О. П'ять порад. Як захистити бізнес від кіберзагроз. *VKP:* веб-сайт. URL: http://surl.li/kyvucq (дата звернення: 11.09.2024).
3. Донич Д. Кібербезпека: актуальні загрози та методи захисту. *Lemon School:* веб-сайт. URL: https://lemon.school/blog/kiberbezpeka-aktualni-zagrozy-ta-metody-zahystu (дата звернення: 09.09.2024).
4. Боянжи В. Основні тенденції у кібербезпеці на 2024 рік: які виклики стоять перед бізнесом. *ISPP:* веб-сайт. URL: https://www.issp.ua/post/main-cybersecurity-trends-in-2024 (дата звернення: 10.09.2024).
5. Отейр Н. Топ-10 кіберзагроз для малого бізнесу: Як захистити свою компанію у глобальній мережі. *Introserv:* веб-сайт. URL: http://surl.li/prjhsn (дата звернення: 10.09.2024).
6. Андерсон Р. On Fibonacci Keystream Generators. Fast Software Encryption 1994, 346–352. URL: https://link.springer.com/chapter/10.1007/3-540-60590-8_26 (дата звернення: 09.09.2024).
7. Келло Л. The Virtual Weapon and International. *Academia:* веб-сайт. URL: https://www.academia.edu/61597942/The_Virtual_Weapon_and_International_Order(дата звернення: 09.09.2024).
8. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. Zakon Rada*:* веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 10.09.2024).
9. Паливода Н. Хакери зламали дані про 143 млн кредитних карток американців. *Mind:* веб-сайт. URL: https://mind.ua/news/20176389-hakeri-zlamali-dani-pro-143-mln-kreditnih-kartok-amerikanciv (дата звернення: 11.09.2024).
10. Шнайєр Б. *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World.* W.W. Norton & Company, 2018. URL: https://www.schneier.com/books/click_here/ (дата звернення: 09.09.2024).
11. Bendiek A., Porter H. "European Cybersecurity Policy." *SWP Research Paper*, 2021. URL: https://www.swp-berlin.org/10.18449/2021RP03/ (дата звернення: 09.09.2024).
12. Петерсен К. Challenges of Public-Private Partnerships in: A practice of loyalty. ResearchGate*:* веб-сайт. URL http://surl.li/lweyqs (дата звернення: 10.09.2024).
13. San Joce. Annual Cybersecurity Report 2018. *Cisco:* веб-сайт. URL: http://surl.li/ddqwpk (дата звернення: 11.09.2024).
14. Deloitte Insights. Cybersecurity: The Changing Role of Audit Committee and Board. 2021. URL: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cybersecurity-the-changing-role.pdf (дата звернення: 09.09.2024).
15. ITU. Global Cybersecurity Index 2021. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (дата звернення: 10.09.2024).
16. UNCTAD. Data protection regulations and international data flows: Implications for trade and development. 2022. URL: https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf (дата звернення: 09.09.2024).
17. World Economic Forum. The Global Risks Report 2023. URL: https://www.weforum.org/reports/global-risks-report-2023 (дата звернення: 09.09.2024).

References:

1. Derkach M. 10 trendiv kiberbezpeky u 2024 rotsi, do yakykh treba hotuvatysia vzhe zaraz [10 Cybersecurity Trends for 2024 to Prepare for Right Now]. Available at: https://psm7.com/uk/analytics/10-trendov-kiberbezopasnosti-v-2024-godu-k-kotorym-nado-gotovitsya-uzhe-sejchas.html (accessed September 9, 2024).
2. Melnyk O. 5 porad. Yak zakhystyty biznes vid kiberzahroz [5 Common Cybersecurity Threats – and How to Protect Your Business]. Available at: http://surl.li/kyvucq (accessed September 11, 2024).
3. Donych D. Kiberbezpeka: aktualni zahrozy ta metody zakhystu [Cybersecurity: Current Threats and Protection Methods]. Available at: https://lemon.school/blog/kiberbezpeka-aktualni-zagrozy-ta-metody-zahystu (accessed September 9, 2024).
4. Boianzhy V. Osnovni tendentsii u kiberbezpetsi na 2024 rik: yaki vyklyky stoiat pered biznesom [Main Cybersecurity Trends for 2024: Business Challenges]. Available at: https://www.issp.ua/post/main-cybersecurity-trends-in-2024 (accessed September 10, 2024).
5. Oteir N. Top-10 kiberzahroz dlia maloho biznesu: Yak zakhystyty svoiu kompaniiu u hlobalnii merezhi [Top 10 Cybersecurity Threats for Small Businesses: How to Protect Your Company in the Global Network]. Available at: http://surl.li/prjhsn (accessed September 10, 2024).
6. Anderson R. (1994). On Fibonacci Keystream Generators. Fast Software Encryption, 346–352. Available at: https://link.springer.com/chapter/10.1007/3-540-60590-8_26 (accessed September 9, 2024).
7. Kello L. (2017) *The Virtual Weapon and International.* Yale University Press. Available at: https://www.academia.edu/61597942/The_Virtual_Weapon_and_International_Order (accessed September 9, 2024).
8. On the Basic Principles of Cybersecurity in Ukraine: Law of Ukraine dated October 5, 2017. Available at: https://zakon.rada.gov.ua/laws/show/2163-19#Text (accessed September 10, 2024).
9. Palyvoda N. Khakery zlamaly dani pro 143 mln kredytnykh kartok amerykantsiv [Hackers Stole Personal and Financial Data of 143 Million Americans]. Available at: https://espreso.tv/news/2017/09/08/khakery_vykraly_osobysti_i_finansovi_dani_143_mln_amerykanciv (accessed September 11, 2024).
10. Schneier B. (2018) *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World.* W.W. Norton & Company. Available at: https://www.schneier.com/books/click_here/ (accessed September 9, 2024).
11. Bendiek A., Porter H. (2021) European Cybersecurity Policy. *SWP Research Paper*. Available at: https://www.swp-berlin.org/10.18449/2021RP03/ (accessed September 9, 2024).
12. Petersen K. Challenges of Public-Private Partnerships in: A practice of loyalty. Available at: http://surl.li/lweyqs (accessed September 10, 2024).
13. San Joce (2018) Annual Cybersecurity Report. *Cisco:* веб-сайт. Available at: http://surl.li/ddqwpk (accessed September 11, 2024).
14. Deloitte Insights (2018) Cybersecurity: The Changing Role of Audit Committee and Board. Available at: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cybersecurity-the-changing-role.pdf (accessed September 9, 2024).
15. ITU (2021) Global Cybersecurity Index. Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (accessed September 10, 2024).
16. UNCTAD (2022) Cybersecurity and Data Protection: Implications for Developing Countries. Available at: https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf (accessed September 9, 2024).
17. World Economic Forum (2023) The Global Risks Report. Available at: https://www.weforum.org/reports/global-risks-report-2023 (accessed September 9, 2024).

THE ROLE OF CYBERSECURITY IN INTERNATIONAL ECONOMIC RELATIONS

Summary. *This article explores cybersecurity as a critical challenge for contemporary international economic relations. The increasing reliance of the global economy on digital infrastructure has introduced significant vulnerabilities, including cyberattacks, data breaches, industrial espionage, and threats to critical infrastructure. These challenges have profound implications for states, multinational corporations, and international organizations, reshaping the dynamics of economic interdependence and competition on a global scale. The research highlights the growing sophistication of cyber threats and their potential to disrupt economic stability. The article examines specific case studies of cyber incidents that have had far-reaching economic and political consequences, demonstrating how malicious actors exploit the interconnected nature of digital systems. Furthermore, it delves into the geopolitical dimensions of cybersecurity, emphasizing the role of cyber operations in statecraft, economic sabotage, and competitive advantage in international markets. Special attention is paid to international cooperation and the development of global cybersecurity frameworks. The study evaluates existing policies and agreements, such as the Budapest Convention and efforts by organizations like the United Nations and the World Economic Forum, aimed at promoting a unified approach to addressing cyber risks. However, it also addresses the challenges posed by geopolitical rivalries, which often hinder collective action and foster fragmentation in the global governance of cybersecurity. The article also explores the implications of cybersecurity for economic policies and strategies. It underscores the need for countries to balance openness in trade and technology with the imperatives of national security and data sovereignty. Emerging technologies such as artificial intelligence, blockchain, and quantum computing are identified as both opportunities and vulnerabilities in*

this context. The study concludes that cybersecurity is not merely a technical issue but a strategic imperative that profoundly influences the future of international economic relations. Addressing cyber threats requires a holistic approach that integrates technological innovation, regulatory frameworks, and multilateral cooperation. Only through coordinated efforts can the international community mitigate risks, foster economic resilience, and ensure sustainable growth in the digital age. This article contributes to the broader discourse on the intersection of cybersecurity and global economics, offering insights into the strategies necessary to navigate the complex challenges of a rapidly evolving digital landscape.

Keywords: *cybersecurity, international economic relations, cyberattacks, cyberthreats, global economy, data protection, digitalization, innovations, geopolitics.*