МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
«КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

Кваліфікаційна наукова
праця на правах рукопису

МИРОНЧЕНКО ДМИТРО ВОЛОДИМИРОВИЧ

УДК 339.9:334.7.009.12:004.056(043.5)

ДИСЕРТАЦІЯ
ВПЛИВ ГЛОБАЛЬНИХ КІБЕРЗАГРОЗ НА МІЖНАРОДНУ КОНКУРЕНТОСПРОМОЖНІСТЬ І ЕКОНОМІЧНУ БЕЗПЕКУ КРАЇН

Спеціальність: 292 «Міжнародні економічні відносини»
Галузь знань: 29 «Міжнародні відносини»

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.
_____ Д.В.Мирончeнко

Науковий керівник: Сидоренко Катерина Вікторівна, кандидат економічних наук, доцент, доцент кафедри міжнародних економічних відносин

Київ – 2026

АНОТАЦІЯ

Миронченко Д.В. Вплив глобальних кіберзагроз на міжнародну конкурентоспроможність і економічну безпеку країн. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії зі спеціальності 292 – Міжнародні економічні відносини галузі знань 29 – Міжнародні відносини. Державний університет «Київський авіаційний інститут», Київ, 2026.

У дисертаційній роботі здійснено теоретичне узагальнення й запропоновано нове розв'язання наукового завдання – обґрунтування теоретико-методичних засад та розроблення науково-практичних рекомендацій щодо підвищення міжнародної конкурентоспроможності й економічної безпеки країн в умовах зростання сучасних глобальних кіберзагроз, з урахуванням інституційних механізмів кіберстійкості, кібергігієни та етичного виміру управління цифровими ризиками. Доведено, що у цифровій економіці кіберризики набувають ознак економіко-інституційного шоку, який впливає на макроекономічну стабільність, стійкість критичної інфраструктури, якість ланцюгів створення доданої вартості та умов міжнародного контрактування через канали довіри й транзакційних витрат.

На основі систематизації наукових поглядів на еволюцію економічної безпеки обґрунтовано її сучасну багатовимірність, у межах якої цифрова інфраструктура, дані та довіра виступають ключовими ресурсами конкурентоспроможності. Розкрито теоретичні рамки інноваційних кластерів як інструменту формування міжнародних конкурентних переваг, показано роль державної політики у розвитку кластерних екосистем та їх інтеграції у глобальні ланцюги вартості. Сформовано аналітичне підґрунтя для переходу до основного вектора дослідження – оцінювання впливу кіберзагроз на міжнародну конкурентоспроможність і

економічну безпеку країн через інституційну конвергенцію, кіберстійкість і стандартизацію «мінімальних контролів» у державному та приватному секторах.

Обґрунтовано, що інституційні системи кібербезпеки впродовж останнього десятиліття еволюціонують від логіки «захисту периметра» до парадигми кіберстійкості та Zero Trust, а рекомендаційні підходи дедалі частіше замінюються юридично зобов'язувальними вимогами до управління уразливостями, сегментації, журналювання та інцидент-репортингу. Розкрито економічну роль кібергігієни як «мікрофундаменту» міжнародної довіри, що знижує інформаційну асиметрію між контрагентами й здешевлює транскордонне контрактування. Показано значення публічно-приватних механізмів (CERT/CSIRT, ISAC/ISAO, SOC (див. дод. А)) та безпеки ланцюгів постачання (SBOM, SSDF, договірні SLA на виправлення уразливостей) як чинників, що прямо конвертуються у конкурентні переваги через зменшення каскадних ризиків та підвищення передбачуваності для інвесторів і партнерів.

Розроблено концептуальну модель переходу «від кіберризику до конкурентоспроможності через довіру та стійкість», а також запропоновано інтегральний інструментарій оцінювання впливу кіберзагроз на економіку – рамку CCSI (Composite Cybersecurity Impact), що агрегує чотири ключові виміри: SWIR (severity-weighted інциденти), ASURF (див. дод. А) (поверхня атаки), RESIL (кіберстійкість) та ETS (етика/довіра). Доведено, що етичний компонент у моделі виступає не декларативним елементом, а методологічним медіатором і модератором, який підсилює ефект кіберстійкості на міжнародну конкурентоспроможність через формування «премії довіри» (прозорість, приватність-by-design, підзвітність, недискримінаційність алгоритмів, постінцидентні розбори). Запропоновано науковий підхід до операціоналізації латентних конструкцій через систему показників (інтенсивність та суворість інцидентів, цифровізація й залежність від cloud/SaaS/IoT, метрики MTTD/MTTR,

DR/BCP-спроможності, прозорість інцидентів і етичні індикатори), а також описано методи нормалізації та інтегрування (AHP/Delphi для ваг, PCA/SEM для верифікації структури індексу.

В межах дослідження здійснено прикладне застосування запропонованої логіки до України. Обґрунтовано, що в умовах тривалих шоків війни та високої інтенсивності гібридних загроз ключовою є трансформація безпекової парадигми в напрямі управління стійкістю складних систем і підтримання безперервності критичних послуг. Показано багатовимірну роль IT-сектору України як мультиплікатора кіберстійкості та елементу «економіки довіри» через кадровий потенціал, експорт кіберпослуг, розвиток кластерних екосистем, поширення мінімальних контролів у малі та середні підприємства та поглиблення державно-приватної взаємодії. Обґрунтовано науково-практичні рекомендації для державної політики мінімізації впливу глобальних кіберзагроз на економіку України, зокрема через інституціоналізацію прозорості, впровадження вимог до постачальників (SBOM/SSDF, SLA на CVE), масштабування Zero Trust у держсекторі, регулярні DR/BCP-тести, підтримку керованих сервісів безпеки для підприємництва, анти-DDoS/route-guard для критичних мереж та стандартизовані «мікропакети» контролів для пріоритетних секторів.

Наукова новизна одержаних результатів полягає в обґрунтуванні та інтеграції етико-довірчого виміру у модель впливу кіберзагроз на міжнародну конкурентоспроможність і економічну безпеку країн, а практичне значення – у можливості застосування рамки CCSI як аналітичного інструментарію для пріоритизації державних інтервенцій, моніторингу прогресу та підвищення передбачуваності національної економіки для міжнародних партнерів.

Ключові слова: міжнародна конкурентоспроможність, економічна безпека, глобалізація, глобальні кіберзагрози, кіберстійкість, Zero Trust, цифровий суверенітет, цифрова трансфорація, економіка довіри, критична інфраструктура,

ланцюги постачання, supply chain security, SBOM, SSDF, кластери інновацій, ТНК, цифрова економіка, діджиталізація, інституційна політика, інцидент-репортинг (24/72), CERT/CSIRT, ISAC/ISAO, етичне управління, ethics-by-design, privacy-by-design, DPIA, AI impact assessment (AIA), GDPR, NIS2, AI Act, ISO/IEC 27001, SOC 2, NIST CSF, SSPM, DLP, захист даних, інформаційна безпека, сертифікація, сигнали якості, кіберстрахування, каузальна ідентифікація, інтегральні індекси, CCSI, моделювання, big data analytics, оцінювання ризиків, ransomware, phishing, IoT, IIoT, OT, ICS, TMaaS, хмарні SaaS, хмарні платформи, макроекономічна стабільність, смарт-спеціалізація, DR/BCP, RTO/RPO, MTTD/MTTR, венчурний капітал, інноваційна політика.

ABSTRACT

Myronchenko D.V. The Impact of Global Cyber Threats on International Competitiveness and Economic Security of Countries. – Qualification scientific work as a manuscript.

Dissertation for the degree of Doctor of Philosophy in specialty 292 – International Economic Relations, field of knowledge 29 – International Relations. State University "Kyiv Aviation Institute", Kyiv, 2026.

In the dissertation, a theoretical generalization and a new solution to a scientific problem are provided - substantiating the theoretical and methodological foundations and developing scientific and practical recommendations for strengthening countries' international competitiveness and economic security amid the growing impact of contemporary global cyber threats, taking into account institutional mechanisms of cyber resilience, cyber hygiene, and the ethical dimension of digital risk governance. It is demonstrated that in a digital economy cyber risks increasingly take the form of an economic and institutional shock affecting macroeconomic stability, the resilience of critical infrastructure, the quality of value-added chains, and the conditions of cross-border contracting through the channels of trust and transaction costs.

Based on a systematization of scholarly views on the evolution of economic security, its contemporary multidimensional nature is substantiated, within which digital infrastructure, data, and trust become key resources of competitiveness. The theoretical framework of innovation clusters as an instrument for building international competitive advantages is clarified, the role of public policy in developing cluster ecosystems and integrating them into global value chains is explained, and an analytical basis is established for the main trajectory of the study – assessing how cyber threats affect international competitiveness and economic security through institutional convergence,

cyber resilience, and the standardization of minimum controls across the public and private sectors.

It is argued that institutional cybersecurity systems have evolved over the last decade from a perimeter-defense logic to a cyber-resilience and Zero Trust paradigm, while guidance-based approaches are increasingly replaced by legally binding requirements for vulnerability management, segmentation, logging, and incident reporting. The economic role of cyber hygiene as a micro-foundation of international trust is explained - reducing information asymmetry between counterparties and lowering the cost of cross-border contracting. The importance of public-private mechanisms (CERT/CSIRT, ISAC/ISAO, SOC) and supply-chain security (SBOM, SSDF, contractual SLAs for vulnerability remediation) is demonstrated as factors that convert directly into competitive advantages by limiting cascading risks and increasing predictability for investors and partners.

A conceptual model linking cyber risk to competitiveness through trust and resilience is developed, and an integral assessment toolkit is proposed – the CCSI (Composite Cybersecurity Impact) framework – aggregating four key dimensions: SWIR (severity-weighted incidents), ASURF (attack surface), RESIL (cyber resilience), and ETS (ethics/trust). It is shown that the ethical component functions not as a declarative element but as a methodological mediator and moderator that strengthens the effect of cyber resilience on international competitiveness by forming a trust premium (transparency, privacy-by-design, accountability, non-discrimination of algorithms, post-incident reviews). A scientific approach to operationalizing latent constructs is proposed through a system of indicators (incident intensity and severity; digitalization and dependence on cloud/SaaS/IoT; MTTD/MTTR metrics; DR/BCP capabilities; incident transparency; and ethical indicators), as well as methods for normalization and integration (AHP/Delphi for weights, PCA/SEM for validating the index structure).

The proposed logic is applied to Ukraine. It is substantiated that under prolonged wartime shocks and high-intensity hybrid threats, the key priority is the transformation of the security paradigm toward managing the resilience of complex systems and ensuring continuity of critical services. The multidimensional role of Ukraine's IT sector is highlighted as a multiplier of cyber resilience and an element of the trust economy through human capital, cybersecurity service exports, cluster ecosystem development, diffusion of minimum controls among SMEs, and stronger public-private interaction. Scientific and practical recommendations for public policy are substantiated to minimize the impact of global cyber threats on Ukraine's economy, including institutionalizing transparency; introducing supplier requirements (SBOM/SSDF, CVE SLAs); scaling Zero Trust in the public sector; conducting regular DR/BCP tests; supporting managed security services for SMEs; deploying anti-DDoS/route-guard protections for critical networks; and implementing standardized sectoral micro-packages of controls for priority domains.

The scientific novelty of the results lies in substantiating and integrating the ethical-and-trust dimension into a model of how cyber threats affect international competitiveness and economic security of countries, and the practical value lies in the applicability of the CCSI framework as an analytical tool for prioritizing public interventions, monitoring progress, and increasing the predictability of the national economy for international partners.

Keywords: international competitiveness, economic security, globalization, global cyber threats, cyber resilience, Zero Trust, digital sovereignty, trust economy, critical infrastructure, supply chains, supply chain security, SBOM, SSDF, innovation clusters, TNCs, digital economy, digital transformation, digitalization, institutional policy, incident reporting (24/72), CERT/CSIRT, ISAC/ISAO, ethical governance, ethics-by-design, privacy-by-design, DPIA, AI impact assessment (AIA), GDPR, NIS2, AI Act, ISO/IEC 27001, SOC 2, NIST CSF, SSPM, DLP, data protection, information

security, certification, quality signals, cyber insurance, causal identification, composite indices, CCSI, modelling, big data analytics, risk assessment, ransomware, phishing, IoT, IIoT, OT, ICS, TMaaS, cloud SaaS, cloud platforms, macroeconomic stability, smart specialization, DR/BCP, RTO/RPO, MTTD/MTTR, Colonial Pipeline, venture capital, innovation policy.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях категорії «Б»:

1. Myronchenko D., Sydorenko K. Role of the IT-sector of Ukraine in the global cyber security system. *Економічний простір*. 2023. №186. С. 13-17. DOI: 10.32782/2224-6282/186-2 (0,95 д.а., особисто автора 0,85 д.а. – обґрунтовано роль IT-сектору в системі забезпечення глобальної кібербезпеки).
2. Myronchenko D. Ethical aspects of cyber security in the global economy and international relations.. С. 133-140. DOI: 10.33111/vz_kneu.40.25.03.02.012.018.
3. Myronchenko D. Securing Digital Frontier: Cyber Hygiene in the Global Economy. *Актуальні проблеми економіки*. 2025. Вип. 12. №294. С. 151-159. DOI: 10.32752/1993-6788-2025-1-294-151-159.

Наукові публікації в монографічних виданнях:

1. Myronchenko D., Sydorenko K. Digital vulnerability of transport infrastructure in the context of global crises. *The International Sustainable Transportation Symposium (ISTRAS'25). National Aviation Academy of Azerbaijan.* 2025. P. 23. ISBN: 978-9952-582-08-6. DOI: 10.71108/istras.2025 *(Scopus)* (0,5 д.а., особисто автора 0,25 д.а. – обґрунтовано цифрову вразливість критичної інфраструктури в контексті глобальних криз).

Наукові праці, які додатково відображають наукові результати дисертації:

1. Myronchenko D. Cybersecurity as a Factor of Stabilization of the Global Economy. *Fundamental Shifts in Geo-Economic Systems Of The World:* A Collection of International Scientific Works. Kyiv, 2023. P. 193-197. URL: http://ief.org.ua/wp-content/uploads/2023/06/Fundamental-shifts_.pdf.
2. Myronchenko D. Ensuring national and economic security through effective

cybersecurity measures. *Національні економічні стратегії розвитку в глобальному середовищі:* тези доп. XIV міжнар. наук.-практ. конф. (м. Київ, 11 травня 2023 р.). К., 2023. С. 27-30. URL: https://drive.google.com/file/d/18gwybyPV5UPbae1rcWR-PDiZwne8bbxe/view.

3. Мирончeнко Д. Вплив цифрової трансформації на стратегії міжнародних стартапів. *XVII Міжнародна науково-практична конференція «B2B MARKETING» з нагоди 125-річного ювілею КПІ ім. Ігоря Сікорського*. К., 2023. С. 172-173. URL: http://b2b-marketing.fmm.kpi.ua/proc/issue/view/17528/10197.

4. Мирончeнко Д. Вплив цифрової трансформації на стратегії міжнародних стартапів. *B2B MARKETING» з нагоди 125-річного ювілею КПІ ім. Ігоря Сікорського:* тези доп. XVII міжнар. наук.-практ. конф. (м. Київ, 14-15 грудня 2023 р.). К., 2023. С. 172-173.

5. Myronchenko D. Enhancing international economic relations through cyber hygiene practices. *Соціально-економічні виклики та можливості глобалізації:* тези доп. міжнар. наук.-практ. конф. (м. Одеса, 5 березня 2024 р.). Одеса, 2024. С. 49-52. URL: https://researcheurope.org/wp-content/uploads/2024/03/re-05.03.2024.pdf.

6. Myronchenko D. Cyber Hygiene and the Future of International Economics. *Importance of Soft Skills for Life and Scientific Success:* A Collection of Scientific Works of 3rd International Scientific and Practical Internet Conference (Dnipro, March 7-8, 2024). Dnipro, 2024. P. 20-21. URL: http://www.wayscience.com/wp-content/uploads/2024/03/Conference-Proceedings-March-7-8-2024.pdf.

7. Myronchenko D. Ethical considerations in cybersecurity within the global economy. *Розвиток науки та освіти в умовах глобалізації:* тези доп. III міжнар. наук.-практ. конф. (м. Чернігів, 2 серпня 2024 р.). Чернігів, 2024. С. 136-139. URL: https://researcheurope.org/wp-content/uploads/2024/08/re-02.08.24.pdf.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ABAC – керування доступом на основі атрибутів (англ. – Attribute-Based Access Control)

AHP – метод аналізу ієрархій (англ. – Analytic Hierarchy Process)

AIA – оцінка впливу систем ШІ (англ. – AI Impact Assessment)

API – інтерфейс прикладного програмування (англ. – Application Programming Interface)

ASURF – індекс «поверхні атаки» (англ. – Attack Surface)

BCP – планування безперервності бізнесу (англ. – Business Continuity Planning)

BGP – протокол маршрутизації між автономними системами (англ. – Border Gateway Protocol)

BYOD – використання працівниками власних пристроїв (англ. – Bring Your Own Device)

CCPA – каліфорнійський закон про приватність (англ. – California Consumer Privacy Act)

CCSI – інтегральний індекс впливу кібербезпеки (англ. – Composite Cybersecurity Impact)

CCSI-UA – інтегральний індекс для України (англ. – Composite Cybersecurity Impact for Ukraine)

CERT – команда реагування на комп’ютерні інциденти (англ. – Computer Emergency Response Team)

CERT-UA – урядова команда реагування України (англ. – Computer Emergency Response Team for Ukraine)

CI/CD – безперервна інтеграція/доставка (англ. – Continuous Integration / Continuous Delivery)

CISA – агентство США з кібербезпеки (англ. – Cybersecurity and Infrastructure Security Agency)

CVE – реєстр відомих вразливостей (англ. – Common Vulnerabilities and Exposures)

DDoS – розподілена атака на відмову в обслуговуванні (англ. – Distributed Denial of Service)

DFIR – цифрова криміналістика та реагування (англ. – Digital Forensics and Incident Response)

DLP – запобігання втраті даних (англ. – Data Loss Prevention)

DNS – система доменних імен (англ. – Domain Name System)

DNSSEC – розширення безпеки DNS (англ. – DNS Security Extensions)

DPIA – оцінка впливу на захист даних (англ. – Data Protection Impact Assessment)

DR – відновлення після інцидентів/катастроф (англ. – Disaster Recovery)

EDR – виявлення й реагування на кінцевих пристроях (англ. – Endpoint Detection and Response)

EG/T – етичне врядування / довіра (англ. – Ethical Governance / Trust)

ENISA – агентство ЄС з кібербезпеки (англ. – European Union Agency for Cybersecurity)

ERP – планування ресурсів підприємства (англ. – Enterprise Resource Planning)

ЕБ – економічна безпека (англ. – Economic Security)

ETS – індекс етики/довіри (англ. – Ethics/Trust Score)

ЄС – Європейський Союз (англ. – European Union)

FAT – справедливість, підзвітність, прозорість (англ. – Fairness, Accountability, Transparency)

FE – модель фіксованих ефектів у панельних даних (англ. – Fixed Effects)

GCT – загроза/експозиція; інтенсивність і складність атак (англ. – Threat/Exposure)

GDPR – Загальний регламент захисту даних ЄС (англ. – General Data Protection Regulation)

GRC – врядування, ризики, відповідність (англ. – Governance, Risk, Compliance)

H1/H2 – перше/друге півріччя (англ. – Half-year 1 / Half-year 2)

IA – оцінка впливу; загальний термін (англ. – Impact Assessment)

МКС – міжнародна конкурентоспроможність (англ. – International Competitiveness)

ICS – промислові системи керування (англ. – Industrial Control Systems)

IIoT – промисловий інтернет речей (англ. – Industrial Internet of Things)

IOC(s) – індикатори компрометації (англ. – Indicators of Compromise)

IoT – інтернет речей (англ. – Internet of Things)

ISAC/ISAO – центри/організації обміну інформацією (англ. – Information Sharing and Analysis Center/Organization)

ISO 27001 – міжнародний стандарт системи управління інформаційною безпекою

IT – інформаційні технології

KMS – сервіс керування ключами (англ. – Key Management Service)

МСП - малі та середні підприємства

MDR – кероване виявлення й реагування (англ. – Managed Detection and Response)

MES – система управління виробництвом (англ. – Manufacturing Execution System)

MFA – багатофакторна автентифікація (англ. – Multi-Factor Authentication)

МКС – міжнародна конкурентоспроможність (див. IC)

MTTD – середній час до виявлення (англ. – Mean Time to Detect)

MTTR – середній час реагування/відновлення (англ. – Mean Time to Respond/Recover)

NIS2 – Directive (EU) 2022/2555 – директива ЄС щодо кіберстійкості мереж і систем

NIST – Національний інститут стандартів і технологій (англ. – National Institute of Standards and Technology)

NTP/PTP – протоколи синхронізації часу (англ. – Network/Precision Time Protocol)

OAuth – протокол авторизації (англ. – Open Authorization)

OT – операційні технології (англ. – Operational Technology)

PCA – аналіз головних компонент (англ. – Principal Component Analysis)

PLC – програмований логічний контролер (англ. – Programmable Logic Controller)

Purdue model – модель зонування/рівнів для сегментації OT/ICS

RBAC – керування доступом на основі ролей (англ. – Role-Based Access Control)

RESIL (CR) – індекс/параметр кіберстійкості (англ. – Cyber Resilience)

RPO – допустима втрата даних у часі (англ. – Recovery Point Objective)

RTO – допустимий час відновлення (англ. – Recovery Time Objective)

SaaS – програмне забезпечення як сервіс(англ. – Software as a Service)

SBOM – перелік компонентів ПЗ (англ. – Software Bill of Materials)

SCADA – диспетчерське керування та збір даних (англ. – Supervisory Control and Data Acquisition)

SecEng – інженерія безпеки (англ. – Security Engineering)

SEM – моделювання структурними рівняннями (англ. – Structural Equation Modeling)

SIEM – керування подіями та інцидентами безпеки(англ. – Security Information and Event Management)

SLA – угода про рівень сервісу (англ. – Service Level Agreement)

SOC – центр операцій безпеки (англ. – Security Operations Center)

SOC 2 – стандарт/рамка аудиту контролів сервісних організацій (AICPA)

SOAR – оркестрація/автоматизація реагування (англ. – Security Orchestration, Automation and Response)

Spearphishing – цільовий фішинг

SSDF – рамка безпечної розробки ПЗ (англ. – Secure Software Development Framework)

STIX/TAXII – стандарти обміну кіберзагрозовою інформацією

SWIR – індекс інцидентів із вагами суворості (англ. – Severity-Weighted Incident Rate)

TOS – термінальна операційна система в портах (англ. – Terminal Operating System)

TTP(s) – тактики, техніки, процедури (англ. – Tactics, Techniques, and Procedures)

UEBA – аналітика поведінки користувачів/сутностей (англ. – User and Entity Behavior Analytics)

VPN – віртуальна приватна мережа (англ. – Virtual Private Network)

XDR – розширене виявлення й реагування(англ. – Extended Detection and Response)

Zero Trust – модель «нульової довіри» (перевірка кожного запиту/контексту доступу)

ВСТУП

Актуальність теми. Сучасний етап розвитку міжнародних економічних відносин характеризується одночасним поглибленням цифровізації та зростанням геоекономічної турбулентності, що радикально підвищує роль кібербезпеки як фактору міжнародної конкурентоспроможності та економічної безпеки країн. Глобальні ланцюги вартості, транснаціональні платформи, хмарні SaaS-екосистеми та API-економіка істотно знизили бар'єри для транскордонної торгівлі й інновацій, однак паралельно збільшили "площу атаки" на критичні бізнес-процеси, фінансову інфраструктуру, логістику та державні цифрові сервіси. В таких умовах кіберінциденти перетворюються з локальних технічних збоїв на макроекономічні шоки: вони здатні запускати каскадні ефекти простоїв, порушувати контрактну дисципліну, підвищувати страхові премії та вартість капіталу, а також знижувати довіру контрагентів на міжнародних ринках.

Для України зазначена проблематика набуває особливого значення з огляду на поєднання трьох чинників. По-перше, країна функціонує в середовищі тривалої гібридної війни, де кібератаки мають системний, високочастотний і транскордонний характер, спрямований насамперед на критичну інфраструктуру та державні інституції. По-друге, українська економіка в значній мірі спирається на цифрові сервіси та IT-сектор як джерело експорту й компетенцій, що одночасно підсилює потенціал розвитку і підвищує вимоги до стійкості. По-третє, курс на європейську інтеграцію й нормативну конвергенцію у сфері кібербезпеки та захисту даних (зокрема у логіці NIS2/AI-регулювання та вимог до безпеки ланцюгів постачання) робить питання вимірюваної кіберстійкості та "економіки довіри" практичним інструментом конкурентної боротьби на зовнішніх ринках, а не суто комплаєнс-вимогою.

У світовій економічній думці конкурентоспроможність дедалі частіше пояснюється не ресурсами як такими, а здатністю економіки генерувати інновації та підтримувати інституційну якість взаємодії. Особливості підвищення глобальної конкурентоспроможності країн в контексті інноваційного розвитку розглядали такі науковці, як Н.Горбаль, Н.Зарицька, О.Іващенко, Ф.Кастелаччі, М.Корж, Ю.Костинець, Ж.А.Мена, І.Набок, Ю.Орловська, О.Плотніков, Л.Побоченко, М.Портер, А.Прокоп'єва, А.Румянцев, К.Сидоренко, А.Туль-Кшищук, К.Шваб, Т.Циганкова, Б.Р.Чабовскі, А.Шлапак, О.Яценко, П.Янковскі та інші. Питання управління ризиками та впливу кіберзагроз на економічну безпеку країн, перш за все з позицій творчого руйнування, досліджували вчені М.Вілсон, Ю.Вдовиченко, Н.Грущинська, А.Кіа, О.Кравченко, Ф.Кремер, М.Лещенко, Дж.Льюїс, М.Маллінз, З.Пічкурова, Ф.Сашвальд, М.Фортманн, Дж.Хеш, П.Шеремета, Б.Ші, Й.Шумпетер, І.Штулер та інші. Інституційний аспект забезпечення економічної безпеки та кіберстійкості національних економік започаткований і знайшов подальшого розвитку в наукових працях таких дослідників, як А.Баррікелло, О.Борчерт, Б.Дюпон, В.Дячек, Е.Гомес дос Сантос, А.Котт, І.Лінков, Е.Маттесон, Р.С.Морано, Д.Норт, С.Роуз, К.Скарфоун, В.Харроп та інші.

Водночас, попри наявність глибоких і ґрунтовних наукових напрацювань різних років, у науковій літературі залишається недостатньо опрацьованим цілісний механізм, який зв’язує інтенсивність глобальних кіберзагроз із показниками міжнародної конкурентоспроможності та економічної безпеки країн через канали довіри, прозорості та відновлюваності критичних функцій. Бракує комплексних інтегральних підходів, які одночасно враховують: (а) загрозову експозицію та “площу атаки” (включно з ризиками ланцюгів постачання й залежністю від SaaS/API-провайдерів), (б) вимірювану кіберстійкість (MTTD/MTTR, DR/BCP, RTO/RPO, Zero Trust), (в) етичний вимір як економічний модератор довіри (privacy-by-design, прозорість інцидентів, недискримінаційність

алгоритмів), та (г) макроекономічні наслідки – від стійкості критичної інфраструктури до конкурентних позицій у міжнародній торгівлі та інвестиціях. Особливої конкретизації потребує застосування таких рамок до України з урахуванням її реалій: гібридних загроз, ролі ІТ-сектору як мультиплікатора стійкості, а також необхідності перетворити практики кібергігієни та управління ланцюгами постачання на національний стандарт "керованого ризику".

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження виконано в межах науково-дослідних робіт Державного університету «Київський авіаційний інститут»: держбюджетної науково-дослідної теми «Міжнародний рух капіталу в умовах зовнішньої збройної агресії проти України та повоєнної відбудови» (номер державної реєстрації №12-2024/15.01.01, період виконання – 02.01.2024 - 31.12.2025 рр.), в межах якої автором здійснено науковий пошук, спрямований на розробку теоретико-методичних положень та практичних рекомендацій щодо нівелювання глобальних кіберзагроз економічній безпеці та міжнародній конкурентоспроможності країн, а також «Теоретичні та практичні аспекти модифікації системи міжнародних економічних відносин в умовах багатополярності розвитку світового господарства» (номер державної реєстрації №118-2022/15.01.01, період виконання – 01.01.2022 – 30.12.2023 рр.), в рамках якої дисертантом були розроблені концептуальні положення та практичні рекомендації щодо розвитку міжнародних економічних відносин в контексті забезпечення кібергігієни.

Тема дисертації відповідає освітньої-науковій програмі «Міжнародні економічні відносини» за спеціальністю 292 «Міжнародні економічні відносини» галузі знань 29 «Міжнародні відносини» в КАІ (зокрема, ОК1.3.1, ОК1.3.2, ОК1.3.3, ОК1.3.4, ОК1.3.5).

Мета і завдання дослідження. Метою дисертаційного дослідження є обґрунтування механізмів та інструментів нівелювання впливу глобальних

кіберзагроз на міжнародну конкурентоспроможність та економічну безпеку країн на основі комплексного узагальнення і вдосконалення теоретико-методичних засад і розроблення інтегральної аналітичної моделі оцінювання впливу сучасних кіберзагроз в умовах цифрової трансформації.

Для досягнення визначеної мети було поставлено та вирішено такі завдання:

- охарактеризувати генезис концепцій економічної безпеки країн;
- розкрити особливості забезпечення глобальної конкурентоспроможності країн;
- дослідити сутність та систематизувати глобальні кіберзагрози;
- узагальнити основні тенденції розвитку інституційного забезпечення економічної безпеки країн в контексті зменшення впливу глобальних кіберзагроз;
- здійснити комплексний аналіз сучасного стану економічної безпеки України;
- ідентифікувати безпекове середовище та актуальні кіберзагрози національним інтересам України;
- обґрунтувати концептуальні підходи до оцінювання глобальних кіберзагроз міжнародній конкурентоспроможності та економічній безпеці країн;
- оцінити вплив кібернетичних загроз національним інтересам України;
- розробити систему пріоритетних механізмів та запропонувати інструменти підвищення ефективності заходів держави щодо мінімізації впливу глобальних кіберзагроз на економіку України.

Об'єктом дослідження є процеси формування та підвищення міжнародної конкурентоспроможності і економічної безпеки країн.

Предметом дослідження є сукупність методологічних і прикладних аспектів запобігання та мінімізації впливу глобальних кіберзагроз на міжнародну конкурентоспроможність і економічну безпеку країн.

Методи дослідження. Для досягнення мети та розв'язання завдань дисертаційної роботи використано комплекс загальнонаукових і спеціальних методів дослідження міжнародних економічних відносин та економічної безпеки в умовах цифрової глобалізації. Методологічну основу становлять: історико-логічний та інституційний підходи (для аналізу еволюції парадигм кібербезпеки від «периметра» до кіберстійкості, Zero Trust і governance-моделей; обґрунтування ролі інституційних механізмів – інцидент-репортингу, вимог до постачальників, стандартизації базових контролів – у формуванні довіри та підвищенні конкурентоспроможності); описово-аналітичний метод і контент-аналіз (під час систематизації сучасних загроз, класифікації каналів впливу кібератак на міжнародну конкурентоспроможність та економічну безпеку країн, а також інтерпретації концептів «економіка довіри», «етика-by-design», «кібергігієна», «кіберстійкість», «цифровий суверенітет»); методи аналізу й синтезу (для формування концептуальної рамки «кіберризик → стійкість/етика → довіра → конкурентоспроможність», інтеграції технічних, інституційних і економічних аспектів, а також для побудови узагальненої логіки державної політики і державно-приватної взаємодії CERT↔ISAC↔SOC). Застосовано системно-структурний і системно-динамічний аналіз (при розгляді критичної інфраструктури та транспортно-логістичних коридорів як кіберфізичних систем із каскадними ризиками; оцінюванні взаємозалежностей між енергетикою, телекомом, фінансами, е-сервісами та логістикою); порівняльний аналіз і метод кейс-стаді (для зіставлення моделей державної політики і механізмів інституційної кіберстійкості в різних юрисдикціях; аналізу прикладів інцидентів і «ланцюгових» ефектів, зокрема у supply chain, фінансах, транспорті та цифрових платформах, а також для узагальнення практик прозорості й репутаційних наслідків). Для формування набору індикаторів та їх агрегування використано методи економіко-статистичного аналізу та індексного моделювання (операціоналізація

латентних конструкцій SWIR/ASURF/RESIL/ETS; нормування показників; побудова інтегрального індексу CCSI та інтерпретація шкали впливу), а також методи багатовимірного аналізу даних (PCA/факторний аналіз – для перевірки структури показників і зменшення розмірності; кореляційний аналіз – для первинної перевірки зв'язків між змінними). Для аналізу впливів і відокремлення причинно-наслідкових ефектів використано економетричні методи панельного аналізу (моделі з фіксованими ефектами; робастні оцінки стандартних похибок; event study та різниця-різниць для оцінювання ефектів регуляторних змін і великих інцидентів), а також структурне моделювання (SEM) для тестування медіаційно-модераційної ролі етичного виміру та довіри у зв'язку між кіберризиком, стійкістю та конкурентоспроможністю. Додатково застосовано сценарне моделювання та аналіз чутливості (оцінювання еластичностей міжнародної конкурентоспроможності й економічної безпеки до змін RESIL/ETS/SWIR/ASURF (див. дод. А); формування дорожньої карти політики 2025-2027 та панелі KPI).

Інформаційною основою дисертаційного дослідження є монографічні видання та наукові публікації переважно зарубіжних авторів з проблем підвищення міжнародної конкурентоспроможності, забезпечення економічної безпеки, інституційної економіки, цифрової трансформації та економіки кіберризиків. Ключовий масив емпіричних даних і аналітики сформовано на основі міжнародних звітів, оглядів і інформаційно-аналітичних матеріалів профільних організацій та компаній кібербезпекового ринку, зокрема регулярних threat reports/incident reports, аналітики щодо рансомверу, supply chain security, DLP , хмарної безпеки, SSPM, Zero Trust і кіберстійкості, а також галузевих бенчмарків витрат, втрат і практик управління інцидентами. Нормативно-методичну базу становлять міжнародні та європейські акти і стандарти у сфері кібербезпеки та захисту даних (GDPR, NIS2, AI Act), а також загальновизнані стандарти і фреймворки (ISO/IEC 27001, SOC 2,

NIST CSF), що використовуються для операціоналізації вимог до контролів, прозорості та підзвітності. Для верифікації національного контексту України й побудови прикладних зрізів використано офіційні матеріали національних інституцій реагування та кіберзахисту (зокрема звіти CERT-UA/Держспецзв'язку), а також відкриті статистичні й аналітичні дані щодо експорту IT-послуг, розвитку цифрової економіки та динаміки кіберінцидентів. Додатковими джерелами виступають відкриті міжнародні бази даних, професійні публікації, кейс-матеріали та публічні звіти організацій, що описують наслідки резонансних кіберінцидентів і практики управління ризиками у критичних секторах.

Наукова новизна одержаних результатів полягає у розробленні цілісної системи теоретико-методичних і науково-практичних положень щодо виявлення та нівелювання сучасних глобальних кіберзагроз економічній безпеці країн та їх міжнародній конкурентоспроможності. Здобуті автором особисто нові наукові положення, які виносяться на захист, полягають у наступному:

вперше:

- розроблено концептуально-методологічну рамку CCSI (Composite Cybersecurity Impact) для інтегральної оцінки впливу кіберзагроз на міжнародну конкурентоспроможність і економічну безпеку країн, що поєднує чотири виміри – SWIR (severity-weighted інциденти), ASURF (поверхня атаки), RESIL (кіберстійкість) та ETS (етика/довіра), при чому етичний вимір інтегрований у модель як економічно значущий модератор і медіатор, де privacy-by-design, прозорість інцидентів, підзвітність і недискримінаційність алгоритмів розглядаються як детермінанти зниження транзакційних витрат, підвищення якості контрактування та кредитування і формування «премії за передбачуваність» на зовнішніх ринках, що дозволяє вимірювати «чистий» ефект впливу кіберризиків на ключові вузли національних інтересів через механізми експозиції, стійкості та довіри;

удосконалено:

- науково-прикладні аспекти інтегральної оцінки впливу кіберзагроз на національні інтереси країни (енергетика, зв'язок, фінанси, державні е-сервіси, транспортно-логістичні коридори) на основі поєднання показників загрозової інтенсивності, цифрової залежності, стійкості, прозорості та етичного управління даними, що забезпечує можливість ранжування дефіцитів спроможностей і визначення пріоритетів інтервенцій;

- теоретико-методичні положення оцінювання взаємозв'язку кіберризику та міжнародної конкурентоспроможності шляхом конкретизації причинно-наслідкового ланцюга «загроза/експозиція → (через стійкість і етико-довірче управління) → довіра контрагентів → умови контрактування/фінансування → міжнародна конкурентоспроможність та економічна безпека», що дозволяє операціоналізувати довіру як економічну змінну;

набули подальшого розвитку:

- методичний підхід до обґрунтування державних механізмів мінімізації впливу кіберзагроз на економіку країн через поєднання регуляторних, договірних і організаційних інструментів (SBOM/SSDF у закупівлях, вимоги до інцидент-репортингу, Zero Trust у держсекторі, DR/BCP-тестування, підтримка керованих сервісів безпеки для бізнесу), що переводять безпеку зі сфери «реакції» у сферу вимірюваної економічної політики;

- теоретичне обґрунтування ролі кібергігієни як мікроінституційної основи міжнародної довіри, що зменшує інформаційну асиметрію між контрагентами та знижує трансакційні витрати у транскордонних угодах, формуючи додаткові конкурентні переваги суб'єктів із вищою дисципліною контролів;

- методичні засади аналізу кіберстійкості як характеристики економічної безпеки через акцент на «процедурних здатностях відновлення» (перевірювані

DR/BCP-режими, контроль RTO/RPO, регулярні навчання та плейбуки реагування), що дозволяє пояснювати відмінності макроекономічних наслідків інцидентів між країнами і секторами економіки.

Практичне значення полягає у тому, що сформульовані в дисертаційному дослідженні теоретичні положення, науково-практичні рекомендації та висновки можуть бути використані для вдосконалення підходів до забезпечення кіберстійкості, захисту SaaS-даних, управління ризиками цифрових середовищ, а також підвищення рівня відповідності сучасним вимогам у сфері інформаційної безпеки та комплаєнсу. Наукові розробки, висновки і практичні рекомендації дослідження були впроваджені в діяльність: міжнародної компанії Spin.AI (Каліфорнія, США) – застосовано науково-практичні рекомендації щодо оцінювання кіберризиків у хмарних і SaaS-середовищах, удосконалення механізмів забезпечення безперервності бізнес-процесів, зниження наслідків ransomware-інцидентів, а також підвищення ефективності політик захисту даних і комплаєнсу в умовах цифрової трансформації (довідка від 10.03.2026); ТОВ «Промислово-технологічний парк «КИЇВЩИНА» – впроваджено наукові положення, висновки та рекомендації автора, що стосуються оцінювання впливу кіберзагроз на економічну стійкість, мінімізації ризиків у цифровому середовищі, а також удосконалення підходів до управління ризиками та забезпечення інформаційної безпеки в умовах цифровізації (довідка №04.04-26 від 27.04.2026).

Окремі положення результатів дослідження використано в навчальному процесі при підготовці фахівців за спеціальністю 292 «Міжнародні економічні відносини» освітньо-професійних програм «Міжнародні економічні відносини» та «Міжнародний бізнес» першого (бакалаврського) та другого (магістерського) рівнів вищої освіти з дисциплін «Міжнародне конкурентне управління», «Міжнародний менеджмент і маркетинг», «Менеджмент зовнішньоекономічної діяльності підприємства» та «Транснаціоналізація світової економіки та менеджмент

персоналу в міжнародних корпораціях» (акт від 04.05.2026).

Особистий внесок здобувача. Дисертація є завершеним, самостійно виконаним дослідженням. Одержані у процесі дослідження наукові результати, які характеризуються науковою новизною і виносяться на захист, були отримані дисертантом особисто. З наукових праць, які були опубліковані у співавторстві з іншими науковцями, у дисертації використані лише ті ідеї та розробки, які отримані особисто здобувачем.

Публікації. Основні положення та результати дисертаційного дослідження опубліковано дисертантом самостійно та у співавторстві в 11 наукових працях, із них: 3 – у періодичних наукових виданнях, що включені до переліку фахових видань України; 1 – у монографічному виданні, що зареєстроване у міжнародній наукометричній базі Scopus; 7 – у матеріалах науково-практичних конференцій.

Апробація результатів дисертації. Основні положення і результати дисертаційного дослідження оприлюднено та обговорено на 7 міжнародних і всеукраїнських науково-практичних конференціях, зокрема: міжнародній науковій конференції «Fundamental shifts in geo-economic system of the world» (м. Київ, 2023); XIV міжнародній науково-практичній конференції «Національні економічні стратегії розвитку в глобальному середовищі» (м. Київ, 2023); XVII міжнародній науково-практичній конференції «B2B Marketing» з нагоди 125-річного ювілею КПІ ім. Ігоря Сікорського (м. Київ, 2023); науково-практичній конференції «Творчий внесок професора Антона Філіпенка у навчально-науковий процес економічних спеціальностей вищих навчальних закладів України» (м. Київ, 2023); міжнародній науково-практичній конференції «Соціально-економічні виклики та можливості глобалізації» (Eastern European Center for Scientific Research, 2024); III міжнародній науково-практичній інтернет-конференції «Importance of Soft Skills for Life and Scientific Success» (м. Чернігів, 2024); III міжнародній науково-практичній конференції «Розвиток науки та освіти в умовах глобалізації» (м. Дніпро, 2024).

Структура та обсяг дисертації. Дисертація складається з анотації, вступу, трьох розділів основної частини, висновків, списку використаних джерел і додатків. Повний обсяг дисертації становить 224 сторінок друкованого тексту. Дисертація містить 4 таблиці, 21 рисунків, 6 додатків. Список використаних джерел налічує 181 найменування.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ МІЖНАРОДНОЇ КОНКУРЕНТОСПРОМОЖНОСТІ ТА ЕКОНОМІЧНОЇ БЕЗПЕКИ КРАЇН

1.1. Генезис концепцій економічної безпеки країн

Поняття економічної безпеки бере свій початок із періодів, коли держави почали усвідомлювати взаємозалежність між добробутом суспільства та здатністю країни захищати власні ресурси від зовнішніх і внутрішніх загроз. Уже в епоху раннього капіталізму, коли відбувалося становлення світової системи господарювання, питання контролю над потоками товарів і ресурсів розглядалося не лише як елемент економічного розвитку, а й як інструмент забезпечення політичної та військової стабільності. У XVII–XVIII століттях меркантилізм сформував основу для трактування економічної безпеки. Згідно з його принципами, головною умовою могутності держави вважався активний торговельний баланс і накопичення дорогоцінних металів. Економічна безпека (ЕБ) ототожнювалася з обмеженням імпорту, стимулюванням експорту та контролем за колоніями, а держава виступала активним гравцем, що застосовував протекціоністські заходи для захисту внутрішнього ринку. Таким чином, безпека мала суто матеріальний характер, зводячись до кількісних показників золота, срібла та стратегічних товарів.

У XIX столітті, з розвитком класичної політичної економії, відбулася трансформація поглядів на економічну безпеку: її почали пов’язувати не лише з накопиченням ресурсів, а й з ефективністю використання факторів виробництва та вигодами вільної торгівлі. А. Сміт підкреслював суспільний ефект ринкової взаємодії, зазначаючи, що індивід, переслідуючи власний інтерес, «is led by an

invisible hand to promote an end which was no part of his intention» [“ведений невидимою рукою сприяти меті, що не була частиною його намірів”] (Smith, 1776). Цей підхід логічно підтримав Д. Рікардо у теорії порівняльних переваг: навіть якщо країна може виробляти товар дешевше всередині, торгівля може бути вигідною, адже «Though she could make the cloth with the labour of 90 men, she would import it … because it would be advantageous … to employ her capital in the production of wine» [“хоч вона могла б виробляти сукно працею 90 людей, вона імпортувала б його…, бо вигідніше спрямувати капітал у виробництво вина”] (Ricardo, 1817). Отже, зміцнення економічної безпеки можливе не лише через ізоляцію, а й через спеціалізацію та інтеграцію у світове господарство. Водночас у періоди воєн і криз зростає інтерес до протекціонізму, що підтверджує діалектичний характер еволюції концепції: від відкритості до замикання національних економік. Зокрема, Ф. Ліст наголошував на пріоритеті довгострокових спроможностей держави, стверджуючи: «The power of producing wealth is therefore infinitely more important than wealth itself» [“спроможність виробляти багатство незрівнянно важливіша за саме багатство”] (List, 1841).

На початку XX століття взаємозв’язок між економічними та військово-політичними аспектами посилився. Саме в міжвоєнний період з’явилися перші спроби визначити економічну безпеку як окрему категорію, коли держави прагнули мінімізувати наслідки світових воєн і Великої депресії. Показовою є позиція Ф. Д. Рузвельта, який наголошував, що «No one can guarantee this country against the dangers of future depressions but we can reduce these dangers» [“ніхто не може гарантувати захист від майбутніх депресій, але ці ризики можна зменшити”] (Roosevelt, 1935). У цей період також розвивалися механізми колективної безпеки на міжнародному рівні: наприклад, Ліга Націй розглядалася як перша міждержавна структура, створена «to promote international cooperation and to achieve international

peace and security» [“для розвитку міжнародного співробітництва та досягнення міжнародного миру й безпеки”] (United Nations Office at Geneva, n.d.).

Поступово поняття безпеки виходить за межі фінансових балансів і починає охоплювати стійкість до криз, контроль над стратегічними ресурсами та розвиток національної промисловості. Після Другої світової війни ЕБ стає складовою міжнародних інституційних підходів: вона закріплюється у засадничих документах ООН, зокрема через тезу про необхідність «to employ international machinery for the promotion of the economic and social advancement of all peoples» [“використовувати міжнародні механізми для економічного і соціального поступу всіх народів”] (United Nations, 1945). У межах Бреттон-Вудської системи роль економічної стабільності додатково інституціоналізується: МВФ визначає серед своїх цілей «to promote international monetary cooperation» та сприяти «the expansion and balanced growth of international trade» [“міжнародній валютній співпраці” та “збалансованому зростанню міжнародної торгівлі”] (IMF, n.d.), а Світовий банк (IBRD) орієнтує ресурси на «projects for development and projects for reconstruction» [“проєкти розвитку та відбудови”] (IBRD, 1965). Надалі ця логіка була закріплена і в діяльності ОЕСР, яка визначає своєю метою сприяння політикам для досягнення «the highest sustainable economic growth and employment and a rising standard of living» [“найвищого сталого економічного зростання, зайнятості та підвищення рівня життя”] (OECD, n.d.).

У другій половині XX століття концепція економічної безпеки значно розширюється, набуваючи багатофакторного характеру. Поява кейнсіанських і неокейнсіанських ідей зумовила наголос на ролі держави у стабілізації економіки та підтриманні повної зайнятості. Джон Мейнард Кейнс доводив, що ключова проблема ринкової економіки полягає у нездатності гарантувати повну зайнятість, підкреслюючи: «The outstanding faults of the economic society in which we live are its failure to provide for full employment…». Саме тому державне втручання почало

трактуватися не лише як інструмент економічної політики, а як умова економічної безпеки, адже, за Кейнсом, у межах laissez-faire «the avoidance of wide fluctuations in employment may… prove impossible». Відповідно, підтримання стабільності та керованості інвестиційної активності отримало безпековий зміст: «the duty of ordering the current volume of investment cannot safely be left in private hands» (Keynes, 1936). Забезпечення економічної стабільності розглядалося як основа запобігання соціальним потрясінням і політичній нестабільності, що стало теоретичним підґрунтям для практик державного регулювання, соціальних програм та інституційних реформ.

Не менш важливою в еволюції концепції стала неоліберальна школа, яка у другій половині XX століття акцентувала увагу на економічній відкритості, конкуренції та глобалізації. Її представники обґрунтовували, що безпека в сучасному світі ґрунтується не стільки на контролі держави, скільки на спроможності економіки адаптуватися через ринкові стимули та інновації. Зокрема Мілтон Фрідман підкреслював подвійне значення економічних свобод, зазначаючи, що «economic freedom is also an indispensable means toward the achievement of political freedom» (Friedman, n.d.). Паралельно Фрідріх Гаєк попереджав про ризики заміщення конкуренції директивним плануванням, підкреслюючи: «planning and competition can be combined only by planning for competition, not by planning against competition» (Hayek, n.d.). У цей період загострилися дискусії щодо меж державного втручання – чи здатний вільний ринок захистити країну від структурних криз, енергетичних шоків чи фінансових потрясінь.

Показовим прикладом стала нафтова криза 1970-х років, коли країни-імпортери опинилися у вразливому становищі, що засвідчило стратегічну важливість диверсифікації ресурсів і формування механізмів колективної відповіді на ризики. Цей підхід закріпився в міжнародних інституційних рішеннях: держави-учасники заклали принципи реагування на шоки постачання, декларуючи

намір діяти спільно задля подолання нафтових криз через формування резервів та обмеження попиту: «take common effective measures to meet oil supply emergencies… restraining demand and allocating available oil… on an equitable basis» (IEA, 1974). Унаслідок кризи енергетична безпека стала однією з ключових складових ширшої економічної безпеки та предметом довгострокових стратегій країн-імпортерів (IEA, 1974).

Паралельно розвиваються концепції структурної залежності та світ-системного аналізу, які розглядають економічну безпеку крізь призму нерівності між центром і периферією світової економіки. Представники цих підходів, зокрема І. Валлерстайн, обґрунтовували, що ядро і периферія є не «стадіями розвитку», а структурним відношенням у межах глобального поділу праці: «Core-periphery is a relational concept» [«ядро–периферія є відносним (реляційним) поняттям»] (Wallerstein, n.d.). Більше того, внаслідок цього обміну формується системна асиметрія: «there is a constant flow of surplus-value… to the producers of core-like products» [«існує постійний потік додаткової вартості… до виробників “ядрових” продуктів»] (Wallerstein, n.d.). У межах теорії залежності А. Г. Франк ще радикальніше пов’язував уразливість периферії з історичним розвитком капіталізму, підкреслюючи: «Underdevelopment… was and still is generated by… the development of capitalism itself» [«недорозвиненість… зароджувалась і досі породжується… самим розвитком капіталізму»] (Frank, n.d.). Це підштовхнуло до розуміння економічної безпеки як здатності країн формувати власні моделі розвитку, зміцнювати інститути та контролювати стратегічні ресурси, зокрема технологічні.

У цей самий час посилюється інтерес до концепції національної безпеки, яка дедалі більше включає економічний вимір. Дослідники міжнародної політичної економії показували, що економічна стійкість є базою державної сили: наприклад, Р. Гілпін визначав міжнародний розподіл сили через сукупність «military, economic,

and technological capabilities of states» [«військових, економічних і технологічних спроможностей держав»] (Gilpin, 1981). На цьому тлі зростає роль міжнародних організацій – від ООН і МВФ до СОТ та регіональних інтеграційних блоків – у формуванні механізмів колективної економічної безпеки. Показово, що в преамбулі Марракеської угоди (СОТ) прямо закріплено орієнтир на політики, спрямовані на «raising standards of living, ensuring full employment… and expanding the production of and trade in goods and services» [«підвищення рівня життя, забезпечення повної зайнятості… та розширення виробництва і торгівлі товарами й послугами»] (WTO, 1994). Проте водночас держави продовжують вдаватися до протекціонізму у стратегічних галузях, що підтверджує: ЕБ зберігає національний вимір навіть у добу глобалізації.

Наприкінці XX століття концепція економічної безпеки виходить за межі класичних економічних показників і починає інтегрувати нові параметри: соціальну стабільність, технологічний розвиток, екологічну стійкість і, зрештою, інформаційні та кібернетичні фактори. Розвиток цифрової економіки створив нові виклики, коли ЕБ почала прямо залежати від захисту інформаційних систем, даних і критичної інфраструктури. Зокрема, у документах ОЕСР наголошується на необхідності зниження цифрових ризиків без шкоди для відкритості цифрового середовища: «reduce… digital security risk… without unnecessarily restricting the flow of technologies, communications and data» [«зменшувати цифрові ризики… не обмежуючи без потреби потоки технологій, комунікацій і даних»] (OECD, 2015). Додатково підкреслюється, що критично важливі види діяльності дедалі частіше стають цілями атак: «critical activities have been increasingly exposed to digital security threats» [«критичні види діяльності стають дедалі більш підданими цифровим загрозам»] (OECD, 2021). Таким чином, класичні теорії сформували фундамент для розуміння економічної безпеки як багатовимірного явища, де

поєднуються економічні, політичні, соціальні й технологічні компоненти, а держава виступає координатором адаптації до глобальних викликів.

У другій половині XX століття відбувається суттєва модернізація підходів до економічної безпеки, що була зумовлена трансформацією світового порядку після Другої світової війни, холодною війною та глобальною економічною інтеграцією. ЕБ перестає розглядатися лише крізь призму фінансової стабільності чи захисту національних ресурсів, набуваючи багатовимірного характеру, який поєднує політичні, технологічні, енергетичні та соціальні фактори. Поступово формується уявлення про те, що безпека держави не може бути забезпечена винятково за рахунок власних ресурсів, а вимагає участі у міжнародних інституційних механізмах і колективних формах співпраці. Саме в цей період ЕБ остаточно виходить за межі вузького національного трактування і стає предметом глобального регулювання.

У контексті післявоєнної відбудови та Бреттон-Вудської системи особливого значення набули інститути міжнародного економічного регулювання. Створення Міжнародного валютного фонду, Світового банку та подальший розвиток інституцій багатосторонньої співпраці закріпили економічну безпеку як складову міжнародної координації. Зокрема, МВФ прямо фіксує ціль підтримання валютної стабільності: «To promote exchange stability, to maintain orderly exchange arrangements…» [«сприяти стабільності обмінних курсів і підтримувати впорядковані валютні режими…»] (IMF, n.d.). Паралельно Світовий банк (IBRD) визначає використання ресурсів на користь держав-членів із балансом між відбудовою і розвитком: «…projects for development and projects for reconstruction alike» [«…проєкти розвитку та проєкти відбудови однаково»] (IBRD, 1965). Вперше було закладено механізми колективної відповідальності за фінансову стабільність, валютну конвертованість та інвестиційні потоки, а інституційний

вимір економічної безпеки посилив роль наддержавних структур у забезпеченні стійкості системи.

Водночас доба холодної війни внесла у розуміння економічної безпеки виразний геополітичний вимір. Змагання між США та СРСР відбувалося не лише на політичному чи військовому рівні, а й у площині контролю над технологіями, стратегічними ресурсами та світовими ринками. Показовим є формування систем експортного контролю стратегічних технологій: у документах ОЕСР зазначалося, що COCOM було створено у 1950 р. «to respond to the threat of the Cold War by preventing the sale of arms, and controlling the export of strategic products» [«щоб відповісти на загрозу холодної війни шляхом запобігання продажу озброєнь і контролю експорту стратегічних продуктів»] (OECD, n.d.). Обмеження експорту високотехнологічних товарів, формування стратегічних резервів енергоресурсів і розвиток військово-промислових комплексів стали інструментами економічної безпеки, які визначали розстановку сил у міжнародних відносинах. В епоху ядерного протистояння економічна стійкість визначалася не лише здатністю до виробництва озброєння, а й спроможністю підтримувати внутрішню соціально-економічну стабільність у довготривалій конфронтації.

Особливого значення набув енергетичний аспект економічної безпеки, кульмінацією якого стала нафтова криза 1970-х років. Вона продемонструвала, що залежність від зовнішніх постачальників енергоносіїв здатна паралізувати навіть найрозвиненіші економіки. У відповідь держави-учасники Міжнародної енергетичної програми задекларували готовність діяти спільно, будучи «DETERMINED to take common effective measures to meet oil supply emergencies…» [«сповнені рішучості вжити спільних ефективних заходів для реагування на надзвичайні ситуації з постачанням нафти…»] (IEA, 1974). Пізніше в межах механізмів IEA закріплюється обов’язок тримати запаси нафти щонайменше на 90 днів імпорту, що стало практичним інструментом зниження енергетичної

вразливості. Таким чином, у структурі економічної безпеки виокремився енергетичний компонент, який згодом трансформувався у комплексну систему енергетичної безпеки.

Паралельно посилюється значення фінансової стабільності як ключового фактора безпеки. Розвиток світових фінансових ринків і лібералізація капітальних потоків у 1980–1990-х роках створили нові виклики: валютні кризи, боргові пастки, спекулятивні атаки на національні валюти. У наукових підходах підкреслювалося, що валютні потрясіння можуть набувати навіть характеру очікувань, тобто «balance-of-payments crises can also be purely self-fulfilling events» [«кризи платіжного балансу можуть бути суто самоздійснюваними подіями»] (Obstfeld, 1984). Це виявило уразливість держав перед глобальним фінансовим капіталом і стимулювало пошук механізмів регіонального та міжнародного фінансового захисту.

Наприкінці XX століття модернізація концепції економічної безпеки завершується переходом до багаторівневих і міждисциплінарних підходів. Під економічною безпекою починають розуміти не лише захист від загроз, а й здатність держави та суспільства до адаптації, інновацій і розвитку. Поширюється поняття стійкості (resilience), яке К. Голлінг визначав як властивість системи, що є «a measure of the persistence of systems and of their ability to absorb change and disturbance» [«мірою здатності систем зберігатися та поглинати зміни й збурення»] (Holling, 1973). Одночасно у фокусі опиняється конкурентоспроможність як здатність до оновлення: М. Портер підкреслював, що «a nation’s competitiveness depends on the capacity of its industry to innovate and upgrade» [«конкурентоспроможність країни залежить від здатності її промисловості інноваційно розвиватися та модернізуватися»] (Porter, 1990). Таким чином, модернізація другої половини XX століття стала фундаментом для подальшого

розширення концепції у XXI столітті, коли цифровізація, інформаційна економіка та кіберзагрози почали визначати нові параметри економічної безпеки.

У XXI столітті ЕБ набула принципово нового виміру, що безпосередньо пов'язаний із цифровою трансформацією глобальної економіки. Якщо в попередні десятиліття ключовими аспектами безпеки залишалися енергетика, фінанси та стратегічні ресурси, то нині дедалі більшого значення набуває кіберпростір. Саме в цифровому середовищі концентруються критично важливі економічні процеси – від роботи банківської системи та біржових торгів до логістичних операцій, управління транспортом і функціонування інфраструктури. У результаті традиційні загрози – шпигунство, саботаж, незаконне втручання у фінансові чи торговельні відносини – трансформуються у форму кіберзагроз, що здатні паралізувати цілі галузі економіки та створити масштабні соціальні наслідки.

Особливістю сучасного цифрового виміру є те, що ЕБ тепер безпосередньо залежить від стійкості інформаційних систем, мережевих інфраструктур і технологій обробки даних. У цьому контексті ключовою категорією стає кіберстійкість: NIST визначає кіберрезильєнтність як «the ability to anticipate, withstand, recover from, and adapt to adverse conditions…» [«здатність передбачати, витримувати, відновлюватися та адаптуватися…»] (NIST, n.d.). Хакерські атаки на фінансові інститути, збої в роботі платіжних систем, витоки персональних і комерційних даних демонструють, що навіть найрозвиненіші економіки залишаються вразливими перед новими викликами. Таким чином, національна ЕБ у XXI столітті дедалі більше ототожнюється з кіберстійкістю, а цифрова інфраструктура набуває статусу критично важливого ресурсу.

Важливим фактором є також глобалізація цифрових платформ, які формують нову архітектуру міжнародних економічних відносин. Транснаціональні корпорації фактично виступають не лише ринковими гравцями, а інфраструктурними акторами, від яких залежить функціонування інформаційних і фінансових потоків у

масштабах усього світу. Це породжує нові виклики для економічної безпеки держав, адже залежність від іноземних цифрових сервісів може стати інструментом економічного тиску або політичного впливу. Питання цифрового суверенітету сьогодні дедалі частіше постає як категорія економічної безпеки: у документах Європейського парламенту зазначено, що «digital sovereignty refers to Europe's ability to act independently in the digital world» [«цифровий суверенітет означає здатність Європи діяти незалежно в цифровому світі»] (European Parliament, 2020).

У сучасних концепціях економічної безпеки з'являються нові ключові категорії: resilience (стійкість), cyber resilience (кіберстійкість), trust economy (економіка довіри). Поняття стійкості означає здатність економічної системи не лише протидіяти загрозам, а й швидко відновлюватися після кризових подій, зберігаючи основні функції та продовжуючи розвиток. Кіберстійкість передбачає не лише технічний захист, а й інституційну та соціальну готовність реагувати на кіберінциденти – через співпрацю, обмін інформацією та спільні стандарти. Зростає й роль "економіки довіри", де довіра стає критичним активом: у глобальних дискусіях прямо підкреслюється теза «Trust is the new currency…» [«довіра – це нова валюта…»] (World Economic Forum, 2025).

Цифровий вимір трансформує підходи до класичних категорій економічної безпеки. Енергетична безпека тепер тісно пов'язана з кіберзахистом енергетичних мереж і «розумних» систем управління. Фінансова безпека потребує захисту електронних платежів та інфраструктур цифрових транзакцій. Продовольча й транспортна безпека залежать від стійкості логістичних платформ та управління ланцюгами постачання. У зв'язку з цим в європейських підходах з'являються практики "кібер-стрес тестування", а ENISA визначає кіберстрес-тест як «a targeted assessment… ability to withstand and recover… ensuring the provision of critical services» [«цільову оцінку… здатності витримувати та відновлюватися… забезпечуючи критичні послуги»] (ENISA, 2025). Таким чином, цифровізація

зробила економічну безпеку міжсекторальною категорією, у якій загрози перетинають одразу кілька сфер і поширюються з високою швидкістю.

Не менш важливим є й міжнародний вимір цифрової економічної безпеки. Оскільки кіберзагрози не визнають державних кордонів, колективна безпека у кіберпросторі стала необхідною умовою стабільності глобальної економіки. НАТО, зокрема, акцентує необхідність бути «as safe and resilient in the digital world as we are in the physical one» [«настільки ж захищеними і стійкими у цифровому світі, як і в фізичному»] (NATO, 2021). Одночасно ОЕСР підкреслює, що країни мають знижувати цифрові ризики, не перетворюючи безпеку на бар'єр для розвитку: «…without unnecessarily restricting the flow of technologies, communications and data» [«…не обмежуючи без потреби потоки технологій, комунікацій і даних»] (OECD, 2015). Такі підходи відображають інтеграцію цифрового виміру в саму основу економічної дипломатії – через стандарти, норми та положення про дані й кібербезпеку.

У підсумку цифровий вимір економічної безпеки відображає глобальну трансформацію: від матеріальних ресурсів і фізичного контролю – до управління інформаційними потоками та забезпечення стійкості цифрової інфраструктури. Сьогодні ЕБ не може бути гарантована без потужного кіберзахисту, міжнародної кооперації та розвитку цифрового суверенітету. Саме тому цифрова складова поступово стає ключовою у стратегіях держав і корпорацій, а ЕБ набуває нового, комплексного значення, де інформація, довіра та технології стають стратегічними ресурсами.

У другій половині XX – на початку XXI століття концепція економічної безпеки почала все активніше включати в себе не лише матеріальні чи фінансові аспекти, а й нематеріальні чинники, пов'язані з довірою, прозорістю та соціальною відповідальністю. Глобалізація, зростання ролі цифрових технологій та поява кіберпростору як нового виміру міжнародних відносин зумовили розширення

дискурсу економічної безпеки до етичного виміру. Якщо раніше ЕБ трактувалася переважно як здатність держави забезпечувати стійкість до зовнішніх шоків, захищати ресурси та підтримувати конкурентоспроможність, то сьогодні дедалі більшого значення набувають етичні аспекти – насамперед у сфері даних і цифрових прав. Зокрема, регуляторні підходи ЄС виходять із того, що «The protection of natural persons in relation to the processing of personal data is a fundamental right» [«захист осіб у зв'язку з обробкою персональних даних є фундаментальним правом»], а сама обробка має бути зорієнтована на суспільне благо: «The processing of personal data should be designed to serve mankind» [«обробка персональних даних має бути спрямована на служіння людству»] (GDPR, 2016). Такий підхід переводить питання захисту персональних даних, недискримінації та підзвітності алгоритмів у площину економічної безпеки, оскільки довіра до цифрових сервісів стає умовою стабільності цифрових ринків.

В умовах розвитку інформаційного суспільства та економіки знань ЕБ неможлива без інтеграції принципів цифрової етики. На перший план виходить регулювання потоків даних і баланс між інноваціями та захистом прав людини, а також уникнення зловживань монопольним становищем платформ, які контролюють значну частину глобальної цифрової інфраструктури. У цьому контексті міжнародні принципи відповідального використання технологій роблять акцент на прозорості: ОЕСР зазначає, що «AI Actors should commit to transparency and responsible disclosure regarding AI systems» [«учасники мають забезпечувати прозорість і відповідальне розкриття інформації щодо AI-систем»] (OECD, n.d.). Паралельно формується підхід до транскордонних потоків даних як до економічного ресурсу, що потребує "довіроорієнтованого" управління: ініціатива DFFT «aims to promote the free flow of data while ensuring trust in privacy, security…» [«прагне підтримувати вільний рух даних, водночас забезпечуючи довіру щодо приватності та безпеки…»] (OECD, n.d.).

Етичний вимір також прямо впливає на міжнародну конкурентоспроможність: країни, які впроваджують високі стандарти прозорості й захисту даних (зокрема ЄС через GDPR), здобувають довіру споживачів і підвищують передбачуваність правил гри для бізнесу. У ширшій рамці відповідальності бізнесу ОЕСР підкреслює, що «Responsible business conduct can enable the creation of a level playing field across global markets» [«відповідальна ділова поведінка може забезпечити рівні умови на глобальних ринках»] (OECD, 2023), а глобальний стандарт ООН фіксує базовий імператив: «Business enterprises should respect human rights» [«підприємства мають поважати права людини»] (OHCHR, 2011). У такий спосіб довіра, прозорість і корпоративна відповідальність перестають бути "додатком" до економічної політики й стають елементом її безпекової архітектури. Додатково інституційні рішення ЄС прямо пов'язують довіру та економічну ефективність цифрових ринків: Data Governance Act «provides a framework to enhance trust in voluntary data sharing for the benefit of businesses and citizens» [«створює рамку для посилення довіри до добровільного обміну даними на користь бізнесу та громадян»] (European Commission, n.d.).

Нами встановлено, що сучасна ЕБ виходить за межі традиційних моделей державного контролю і вимагає вироблення глобальних стандартів, що враховують не лише технічні, а й морально-правові параметри. Слід наголосити на необхідності розуміння кіберпростору як простору не тільки економічної діяльності, але й простору соціальної взаємодії, де відсутність етичних засад породжує довгострокові загрози (Мирончeнко, 2024).

Водночас необхідно зазначити, що традиційні моделі безпеки застарівають. Вони орієнтовані переважно на протидію зовнішнім загрозам (економічний шантаж, санкційний тиск, енергетична залежність). У цифровій економіці значну частку ризиків формують внутрішні фактори – корупція в управлінні даними, неетичне використання технологій, зловживання владними чи корпоративними

повноваженнями (Мирончeнко, 2024). Саме тому ЕБ у XXI столітті повинна доповнюватися етичними регуляторами, які формують межі допустимого використання цифрових інструментів.

Етика є елементом цифрової стійкості. Ігнорування етичного виміру призводить до зниження здатності суспільства долати кризи. Там, де відсутня культура захисту приватності або панує толерантність до маніпуляцій, виникає ефект «кризи довіри». Дане твердження узгоджується з підходом ЄС, де захист даних визначено як базове право: «The protection of natural persons… is a fundamental right» [«захист осіб… є фундаментальним правом»], а обробка даних має бути спрямована на суспільне благо: «should be designed to serve mankind» [«має бути спрямована на служіння людству»] (GDPR, 2016). Відповідно, порушення приватності та підзвітності алгоритмів стає не лише юридичним, а й економічним ризиком – через падіння довіри, репутаційні втрати і зменшення вартості активів.

Акцентуємо увагу, що довіра у XXI столітті набуває економічного виміру, подібно до капіталу чи праці: фінансові ринки, електронні платежі та логістика глобальних ланцюгів постачання функціонують настільки ефективно, наскільки високим є рівень довіри до надійності цифрових механізмів (Мирончeнко, 2024). Таку логіку підсилюють міжнародні дискусії, де прямо формулюється теза «Trust is the new currency…» [«довіра – це нова валюта…»] (World Economic Forum, 2025). Якщо порушується баланс між інноваціями та правами користувачів, довіра руйнується, а ЕБ втрачає фундамент.

Досвід ЄС показав, що захист приватності є не лише правом людини, але перш за все інструментом конкурентоспроможності через формування високого стандарту довіри до цифрових послуг (GDPR, 2016). У результаті країни, що впроваджують жорсткі стандарти прозорості та захисту даних, отримують стратегічні переваги у глобальних економічних відносинах.

Кейс Cambridge Analytica продемонстрував, що витоки/зловживання даними здатні конвертуватися у прямі фінансові втрати та регуляторні санкції: FTC зафіксувала рекордне стягнення з Facebook – «The $5 billion penalty… is the largest ever imposed… for violating consumers' privacy» [«штраф $5 млрд… є найбільшим… за порушення приватності споживачів»] (FTC, 2019). Подібні інциденти трансформують довіру у економічний параметр: за повідомленням CBS, після скандалу акції Facebook падали більш ніж на 24%, що означало приблизно 134 млрд дол. США втрати ринкової вартості (CBS News, 2018). Для Uber ризики проявилися через регуляторний тиск та примус до посилення захисту даних: FTC підкреслювала, що компанія погодилася на комплексну програму приватності через обвинувачення у «deceptive privacy and data security claims» [«оманливих твердженнях щодо приватності та безпеки даних»] (FTC, 2017). Таким чином, нехтування етичним виміром веде до економічної вразливості – через втрату довіри, падіння капіталізації, штрафи та довгострокові репутаційні наслідки.

У вітчизняних умовах питання етики кібербезпеки має додатковий вимір – взаємодія держави та громадян у воєнний час. Використання моніторингових інструментів і збір даних задля національної безпеки потребує чітких етичних рамок, інакше ризик падіння довіри до інститутів може підірвати економічну стійкість (Мирончeнко, 2024). При цьому міжнародні стандарти прямо вимагають безпекових запобіжників: Конвенція Ради Європи №108 визначає, що «Appropriate security measures shall be taken for the protection of personal data…» [«мають бути вжиті належні заходи безпеки для захисту персональних даних…»] (Council of Europe, 1981). Це означає, що навіть за умов кризи ЕБ має спиратися на легітимність і довіру, які неможливі без етичних і правових гарантій.

Таким чином, у дослідженнях обґрунтовується, що ЕБ неможлива без етики, оскільки саме етичні стандарти виступають бар'єром проти зловживань і підґрунтям для довгострокового економічного розвитку. Якщо класичні концепції

безпеки розглядали її через призму матеріальних ресурсів, то сучасні підходи демонструють: ресурс довіри, справедливості та прозорості має не меншу, а часто й більшу вагу у глобальній економіці (Мирончeнко, 2024).

Етичні категорії у сфері кібербезпеки – конфіденційність, недискримінація, прозорість, відповідальність – стають ключовими складовими забезпечення міжнародної конкурентоспроможності. Зокрема, підхід “ethics by design” передбачає вбудовування етичних вимог у процес створення технологій: у керівних матеріалах Єврокомісії зазначено, що «Ethics by Design maps its guidelines onto the steps in each individual methodology» [«Ethics by Design накладає етичні настанови на етапи кожної методології розробки»] (European Commission, 2021). Компанії, які впроваджують “ethics by design”, отримують вищу лояльність клієнтів і партнерів, що трансформується в економічні переваги. Водночас держави, які нехтують етичними стандартами, ризикують опинитися в умовах цифрової ізоляції – через обмеження доступу до ринків та технологій у разі невідповідності міжнародним нормам (GDPR, 2016).

Одним із найяскравіших прикладів інтеграції етики у сферу економічної безпеки став Загальний регламент захисту даних (GDPR), прийнятий ЄС у 2016 році. Даний юридичний акт став символом формування нової культури цифрової етики, де права людини ставляться вище за економічні інтереси корпорацій. У GDPR прямо підкреслюється гуманістичний принцип: «The processing of personal data should be designed to serve mankind» [«обробка персональних даних має бути спрямована на служіння людству»]. GDPR суттєво змінив глобальні стандарти обробки даних, змусивши навіть американські та азійські компанії адаптуватися до європейських правил. Таким чином, етичні принципи отримали інституційну силу, безпосередньо вплинувши на конкурентоспроможність держав і бізнесів.

Іншим показовим прикладом є скандал з Cambridge Analytica (2018), коли стало відомо про використання персональних даних користувачів Facebook для

політичних маніпуляцій. Дана подія продемонструвала, що ігнорування етичних норм у сфері кібербезпеки призводить до глобальних криз довіри, політичної дестабілізації та економічних збитків для корпорацій. Після розслідування FTC у США було накладено рекордні санкції, і регулятор прямо зафіксував: «The $5 billion penalty… is the largest ever imposed… for violating consumers' privacy» [«штраф у $5 млрд… є найбільшим… за порушення приватності споживачів»] (FTC, 2019). Отже, нехтування етичним виміром даних перетворюється на вимірюваний економічний ризик – через штрафи, падіння капіталізації та регуляторне посилення норм у сфері privacy та accountability (U.S. Department of Justice, 2019).

Особливу увагу слід приділити практиці Китаю, де через систему соціального рейтингу (Social Credit System) використовується масовий збір та аналіз даних для оцінки поведінки громадян. Дослідники підкреслюють, що система означає «парадигмальний зсув» та «aims for a comprehensive and uniform social rating based on penalty and award mechanisms» [«прагне комплексного та уніфікованого соціального рейтингу на основі механізмів покарань і заохочень»]. З одного боку, це подається як інноваційний механізм підтримання соціальної стабільності; з іншого – викликає серйозні етичні сумніви, оскільки створює ризики тотального контролю, дискримінації та обмеження індивідуальних свобод. Такий кейс показує, що нехтування етичним виміром у кіберполітиці може формально посилювати керованість системи, але водночас підривати міжнародну довіру та спричиняти довгострокові репутаційні й економічні наслідки (Mac Síthigh & Siems, 2019).

У корпоративному середовищі варто відзначити зусилля Microsoft, Google, OpenAI щодо створення та публікації принципів відповідального використання ШІ. Microsoft формулює шість базових принципів Responsible AI: fairness, reliability and safety, privacy and security, inclusiveness, transparency, accountability (Microsoft, n.d.).

Google у своїх AI Principles окремо підкреслює антидискримінаційний фокус, зокрема принцип: «Avoid creating or reinforcing unfair bias» [«уникати створення або посилення несправедливої упередженості»] (Google, n.d.). OpenAI у Charter фіксує етичний пріоритет запобігання шкоді: «…avoid enabling uses of AI or AGI that harm humanity or unduly concentrate power» [«…уникати сприяння застосуванням ШІ, що шкодять людству або надмірно концентрують владу»] (OpenAI, n.d.).

Такий підхід має не лише репутаційне значення, але й стратегічно впливає на глобальну конкурентоспроможність: компанії, які першими впроваджують етичні стандарти, стають лідерами у встановленні нових ринкових правил і забезпечують основу для “економіки довіри”, де довіра стає критичним активом цифрового середовища (рис. 1.1).

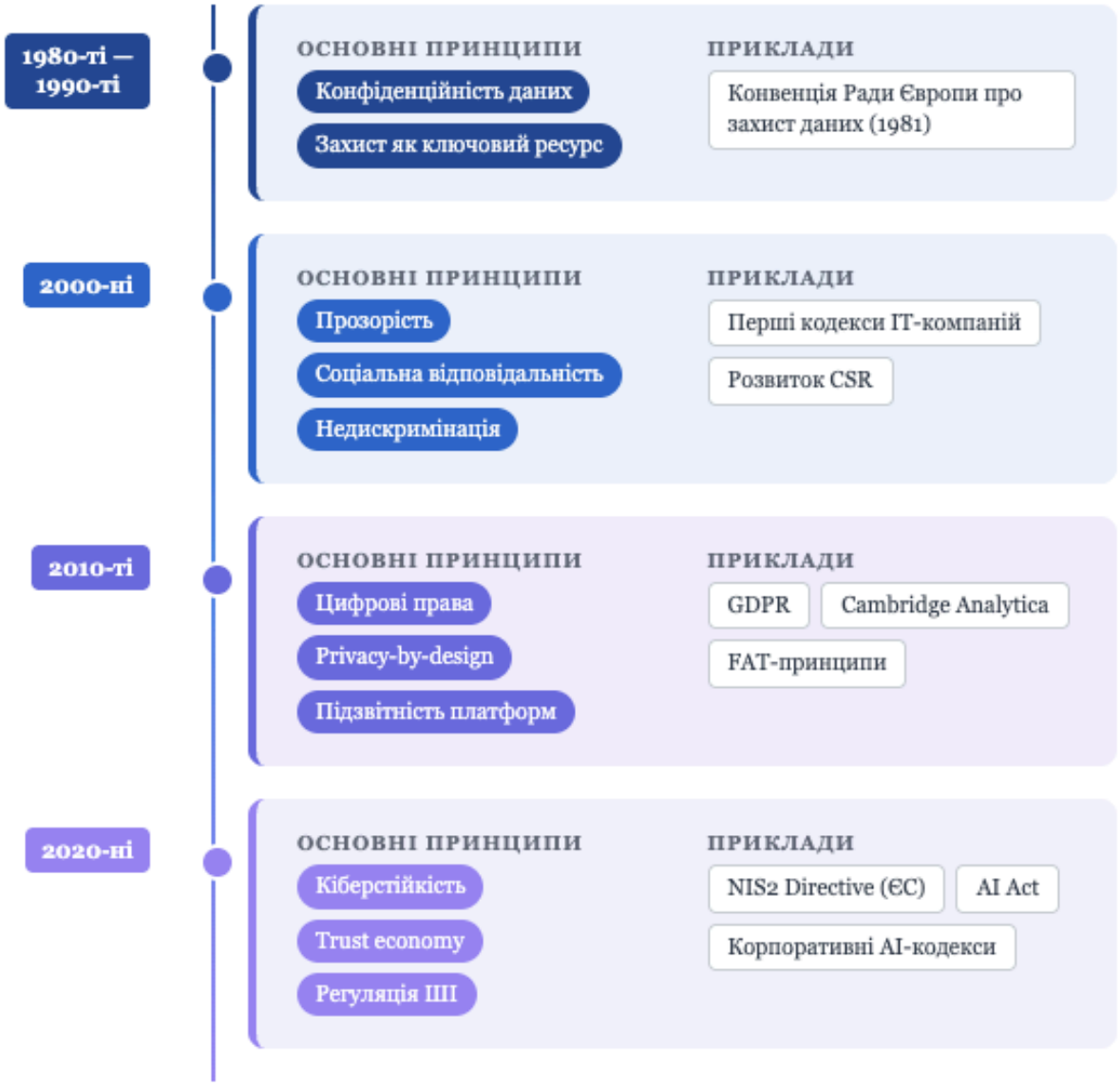

Рис. 1.1. Еволюція етичних принципів у цифровому просторі

Джерело: розроблено автором.

Така еволюція демонструє поступовий перехід від вузького трактування етичних вимог (лише захист приватності) до комплексного підходу, де етика стає основою цифрової довіри й фактором економічної стійкості.

Еволюція уявлень про економічну безпеку відображає загальний розвиток світової економіки та міжнародних відносин. Від первісних ідей фізичного захисту ресурсів до сучасних багатовимірних концепцій, що інтегрують цифровий та етичний виміри, пройдено кілька ключових етапів. Кожен з них формував нове розуміння сутності безпеки відповідно до історичного контексту, наявних викликів та рівня розвитку технологій.

На ранніх етапах домінував матеріальний підхід: ЕБ ототожнювалась із захистом національного багатства у вигляді золота, срібла, територій та стратегічних ресурсів. У добу меркантилізму головною метою було збереження позитивного торговельного балансу, а головним інструментом – протекціоністська політика. Логіка безпеки полягала у створенні своєрідних «економічних укріплень» навколо національної економіки: у працях Т. Мана прямо наголошувалося, що «…to sell more to strangers yearly than we consume of theirs in value» [«продавати іноземцям щороку більше, ніж споживаємо їхніх товарів за вартістю»] (Mun, n.d.).

З розвитком класичної політичної економії в центр уваги переходить не накопичення, а ефективність використання ресурсів. У працях А. Сміта, Д. Рікардо та Ф. Ліста ЕБ дедалі більше поєднується з категоріями продуктивності, національної конкурентоспроможності та спеціалізації. Зокрема, підхід А. Сміта до економічної взаємодії акцентував загальний ефект ринкових стимулів: «is led by an invisible hand…» [«ведений невидимою рукою…»] (Smith, 1776). Д. Рікардо розвинув цю логіку в теорії порівняльних переваг, показавши, що інтеграція може бути вигідною навіть за різної продуктивності (Ricardo, 1817). Водночас Ф. Ліст наголошував на пріоритеті довгострокових спроможностей держави, зазначаючи: «The power of producing wealth… more important than wealth itself» [«спроможність виробляти багатство важливіша за саме багатство»] (List, 1841). Тут формується принципова дилема: чи варто відкривати ринки для світової торгівлі, ризикуючи залежністю, чи захищати внутрішнє виробництво від зовнішньої конкуренції.

XX століття стало періодом інституціоналізації економічної безпеки. Після світових воєн та Великої депресії вона перетворилася на предмет глобальної політики: створення ООН, МВФ, Світового банку та розвиток багатосторонньої співпраці заклали механізми колективної стабільності. У цей час акцент робився на стійкості до фінансових криз та впорядкуванні міжнародних правил: МВФ прямо визначає мету «to promote exchange stability» [«сприяти валютній стабільності»] (IMF, n.d.), а інститути розвитку орієнтувалися на відбудову та модернізацію економік (IBRD, 1965). В умовах Холодної війни безпека набуває чіткого геополітичного виміру: технології, ресурси та інновації стають полем боротьби за глобальний вплив, що проявлялося і через системи експортного контролю стратегічних товарів. Окремо посилюється енергетичний компонент після шоку 1970-х років: держави були «DETERMINED to take common effective measures to meet oil supply emergencies…» [«сповнені рішучості діяти спільно для реагування на надзвичайні ситуації з постачанням нафти…»], що закріпило енергетичну стійкість як частину економічної безпеки (IEA, 1974).

З кінця XX – початку XXI століття ЕБ дедалі більше розглядається у багатовимірному контексті. Вона включає фінансову стабільність, продовольчу безпеку, енергетичну незалежність, екологічну стійкість та інформаційний захист. Найбільшою трансформацією став перехід у цифровий вимір: у добу глобалізації критично важливими стали кіберстійкість, захист даних та технологічний суверенітет. NIST визначає кіберрезильєнтність як «the ability to anticipate, withstand, recover from, and adapt…» [«здатність передбачати, витримувати, відновлюватися та адаптуватися…»] (NIST, n.d.). Питання довіри до цифрових платформ, прозорості алгоритмів та етики використання штучного інтелекту також перетворилися на складову економічної безпеки. Такий підхід підсилює логіку “економіки довіри”, де довіра стає стратегічним активом цифрових ринків.

Таким чином, на сьогодні концепція економічної безпеки інтегрує як класичні елементи (контроль над ресурсами, захист ринків), так і нові – цифрову інфраструктуру, етичні стандарти та технологічну інноваційність. Якщо у XVII–XIX ст. економічна безпека визначала передусім «фізичний захист ресурсів» і торгові бар'єри (Mun, n.d.), то у XXI ст. вона вже трактується як здатність держави та суспільства зберігати конкурентоспроможність у цифровій економіці, де ключовими ресурсами стають знання, дані, довіра та інновації.

1.2. Особливості забезпечення глобальної конкурентоспроможності країн

Інноваційні кластери як сучасна форма організації економічного розвитку є ключовим інструментом підвищення глобальної конкурентоспроможності країн. Під інноваційними кластерами розуміють географічно та інституційно пов'язані мережі підприємств, університетів, науково-дослідних центрів, інвесторів і державних структур, що функціонують у взаємодії задля створення і впровадження нових технологій. Класичне визначення М. Портера підкреслює саме просторову й мережеву природу цього явища: «Clusters are geographic concentrations of interconnected companies and institutions in a particular field» [«кластери є географічними концентраціями взаємопов'язаних компаній та інституцій у певній сфері»] (Porter, 1998). Їхньою особливістю є висока концентрація інтелектуального капіталу, науково-технічного потенціалу та підприємницької активності, що формує середовище швидкої комерціалізації інновацій і доступу на глобальні ринки (OECD, 2009).

Нами встановлено, що міжнародний бізнес у XXI столітті дедалі частіше інтегрується в такі кластери, оскільки вони дають можливість не лише локально тестувати та розгортати технології, а й швидко масштабувати рішення на міжнародні ринки (Мирончeнко, 2024). Слід підкреслити, що кластери виконують

функцію «каталізатора» глобалізації: вони поєднують транснаціональні корпорації з локальними стартапами, сприяють залученню венчурного капіталу та відкривають доступ до міжнародних наукових мереж. Такий підхід забезпечує подвійний ефект – з одного боку, країна отримує інструмент підвищення конкурентоспроможності, з іншого – міжнародні компанії здобувають стратегічні переваги, використовуючи інноваційний потенціал регіонів [(Мирончeнко, 2024); (Sachwald, 2013)].

Особливістю інноваційних кластерів є їхня здатність акумулювати глобальні ресурси знань і капіталу в межах локального простору. Нами встановлено, що саме тут формується «точка входу» міжнародного бізнесу в економіку країни. Наприклад, співпраця університетів і стартапів з міжнародними корпораціями у сфері біотехнологій чи фінтеху дозволяє прискорювати цикл «ідея → продукт → ринок» і зменшувати ризики виходу на глобальну арену, оскільки доступ до міжнародних R&D-мереж та партнерств скорочує часові лаги інновацій. У цьому сенсі інноваційні кластери стають не лише економічним, а перш за все безпековим чинником: країни, що інтегрують свої компанії в глобальні ланцюги створення вартості через кластери, є менш вразливими до зовнішніх шоків та економічних криз завдяки диверсифікації партнерів, технологій і джерел фінансування.

Важливим елементом у формуванні конкурентоспроможності є наявність кластерних стратегій на рівні держави. Досвід провідних країн демонструє, що саме державна підтримка інноваційних кластерів – через податкові стимули, державні замовлення, інвестиції в R&D та створення технопарків – створює базу для їх інтеграції в міжнародний бізнес-простір. Європейська комісія підкреслює, що кластери – це «groups of firms, related economic actors, and institutions located near each other…» [«групи компаній, пов’язаних економічних акторів та інституцій, розташованих поруч…»] – які досягають масштабу для розвитку спеціалізованих навичок, ресурсів і постачальників (European Commission, n.d.). Слід наголосити,

що стратегія кластеризації стає частиною національної конкурентної політики, оскільки дозволяє поєднувати локальні переваги (географія, ресурси, людський капітал) із глобальними потребами ринку.

Забезпечення глобальної конкурентоспроможності через кластери має кілька ключових особливостей:

1. Інноваційна спеціалізація. Кластери концентрують ресурси в певних сферах, створюючи ефект критичної маси, що дозволяє країнам займати нішеве лідерство у глобальній економіці.

2. Міжнародна інтеграція. Кластери виступають «воротами» для корпорацій та інвесторів, сприяючи включенню країни у глобальні ланцюги доданої вартості та міжнародні мережі досліджень і розробок.

3. Зменшення вразливості. Завдяки диверсифікації партнерів і технологій кластери підвищують стійкість економік до глобальних шоків (зокрема енергетичних чи фінансових).

4. Підвищення довіри. Кластери формують «економіку довіри» через взаємодію бізнесу, науки та держави на основі інституційних правил, прозорих процедур і стандартів відповідальної кооперації.

Таким чином, інноваційні кластери слід розглядати як стратегічні інструменти забезпечення глобальної конкурентоспроможності країн. Адже вони поєднують національні інтереси з міжнародними тенденціями, створюючи нові можливості для інтеграції у глобальну економіку. Необхідно підкреслити, що міжнародний бізнес в інноваційних кластерах виступає «містком» між локальними економіками й глобальними ринками, що визначає майбутні контури світової економічної безпеки.

Теорія міжнародної конкурентоспроможності тривалий час перебувала у фокусі провідних економістів, а кластери стали одним із ключових елементів пояснення стійкості країн у глобальній економіці. Серед класичних підходів

важливе місце посідає концепція Майкла Портера, який у моделі «діаманта конкурентних переваг» довів, що конкурентоспроможність держави визначається не стільки ресурсами, скільки продуктивністю та інноваційністю. Показово, що Портер прямо формулює: «The only meaningful concept of competitiveness at the national level is national productivity» [«єдиним змістовним поняттям конкурентоспроможності на національному рівні є національна продуктивність»] (Porter, 1990). У даному контексті інноваційні кластери розглядаються як концентровані зони взаємодії бізнесу, науки та держави, де конкуренція та кооперація одночасно створюють стійкі переваги на глобальному рівні. Таким чином, конкурентоспроможність країни формується не стільки через накопичення ресурсів, скільки через здатність до інноваційної взаємодії та швидкого оновлення економічної структури.

Ще одним теоретичним орієнтиром виступають ідеї Йозефа Шумпетера, який наголошував на ролі підприємництва та «творчого руйнування» як рушія економічного розвитку. Вчений підкреслював фундаментальність цього механізму, зазначаючи: «This process of Creative Destruction is the essential fact about capitalism» [«цей процес творчого руйнування є сутнісним фактом капіталізму»] (Schumpeter, 1942). Саме в кластерному середовищі «творче руйнування» відбувається особливо інтенсивно: старі технології швидко витісняються новими, а стартапи та підприємці стають каталізаторами глобальних зрушень. У цьому сенсі кластери виконують функцію локомотива постійного оновлення, що дозволяє країнам залишатися конкурентоспроможними навіть за умов високої турбулентності світової економіки.

Важливим у сучасному дискурсі є також підхід інституціональної економіки, який розглядає кластери як результат ефективної взаємодії формальних (законодавство, державна політика, міжнародні угоди) і неформальних (мережі довіри, ділова культура, етичні стандарти) інститутів. Д. Норт визначає інститути

як «the rules of the game in a society» [«правила гри в суспільстві»] і водночас як «humanly devised constraints that shape human interaction» [«людьми створені обмеження, що формують взаємодію»] (North, 1990). У контексті кластерів це означає, що конкурентні переваги формуються не лише через технології, а й через якість правил кооперації – прозорість, довіру, підзвітність і низький рівень опортунізму. Тут проявляється інтеграція етичного виміру економічної безпеки: країни, які формують кластери на засадах довіри та прозорості, мають вищі шанси утримувати глобальні позиції, ніж ті, де переважають корупційні практики або слабкі правові механізми.

Валлерстайн наголошував, що «ядро–периферія» є системним відношенням: «Core-periphery is a relational concept» [«ядро–периферія є реляційним (відносним) поняттям»](Wallerstein, n.d.). Це дозволяє трактувати високотехнологічні кластери як інструменти закріплення технологічної переваги центру, тоді як периферійні країни можуть потрапляти у залежність через імпорт технологій і ноу-хау. Отже, кластеризація має подвійний характер: з одного боку, вона підсилює конкурентоспроможність лідерів, з іншого – потенційно поглиблює глобальну економічну нерівність.

Узагальнюючи, можна сказати, що інноваційні кластери стали не лише економічною, а й теоретичною категорією, через яку пояснюється перехід від класичних ресурсних моделей конкурентоспроможності до моделей, де домінують знання, інновації та етика співпраці. Дане твердження дозволяє інтегрувати дослідження міжнародного бізнесу в кластерах у ширший контекст глобальної економічної безпеки, де ключовими стають інституційна якість, технологічна незалежність і спроможність до адаптації.

Державна політика розвитку інноваційних кластерів є чинником глобальної конкурентоспроможності. Розвиток інноваційних кластерів не є виключно стихійним процесом, що формується навколо університетів чи технологічних

компаній. У більшості випадків успіх кластерів напряму пов’язаний із цілеспрямованою політикою держав, які виступають каталізаторами створення інноваційних екосистем. Така політика поєднує інституційні стимули, інвестиції в наукову інфраструктуру, податкові пільги для стартапів та програми міжнародної кооперації. Вона дозволяє країнам інтегрувати свої кластери у глобальні ланцюги вартості, що підсилює їхню конкурентоспроможність на світовому рівні.

Класичним прикладом є Силіконова долина у Каліфорнії, яка стала глобальним символом інноваційної економіки. Її успіх неможливо пояснити лише приватною ініціативою – ключову роль відігравали державні замовлення у сфері оборони, розвиток інноваційних програм та підтримка фундаментальних досліджень через спеціалізовані агентства. Показовим є підхід DARPA, де сама місія сформульована як стратегічне завдання: «The DARPA mission is to create and prevent technological surprise for our national security» [«місія DARPA – створювати та запобігати технологічному сюрпризу для національної безпеки»] (DARPA, n.d.). Саме за рахунок поєднання інноваційного фінансування, наукового потенціалу університетів та венчурного капіталу виникає ефект «інноваційного магніту»: кластери притягують таланти, інвестиції та транснаціональні корпорації, забезпечуючи США лідерство у високих технологіях та цифрових платформах.

ЄС застосовує модель, орієнтовану на мережеву взаємодію та регіональну диверсифікацію. Політика Smart Specialisation (S3) прямо визначається як «place-based approach» [«підхід, заснований на територіальних (регіональних) особливостях»], що «builds on the assets and resources available on the territory» [«спирається на активи й ресурси, доступні на конкретній території»] (European Commission, n.d.). Це означає, що регіони визначають власні конкурентні ніші (біотехнології, зелена енергетика, креативні індустрії) і формують навколо них кластерні екосистеми. Додатково Horizon Europe виступає фінансовою опорою інтеграції інновацій: Єврокомісія підкреслює, що «Horizon Europe is the EU’s key

funding programme for research and innovation» [«Horizon Europe є ключовою програмою ЄС з фінансування досліджень та інновацій»]. Завдяки цьому ЄС інтегрує регіональні кластери у спільний інноваційний простір, посилюючи конкурентні переваги через кооперацію, стандартизацію та транскордонні проєкти (European Commission, n.d.).

У країнах Східної Азії розвиток кластерів тісно пов'язаний із національними стратегіями модернізації. Сінгапур сформував біомедичні та фінтех-екосистеми завдяки централізованим інвестиціям у наукові парки та інфраструктуру підтримки інновацій. Зокрема, Biopolis визначається як один із ключових проєктів, що «supports the biomedical industry as Singapore's engine of economic growth» [«підтримує біомедичну індустрію як рушій економічного зростання Сінгапуру»] (JTC Singapore, n.d.).

Південна Корея демонструє іншу модель, де важливе місце посідає взаємодія держави з великими промисловими групами (chaebol). В аналітичних оглядах підкреслюється, що chaebol історично «relied on close cooperation with the government… subsidies, loans, and tax incentives» [«спиралися на тісну співпрацю з урядом… субсидії, кредити та податкові стимули»] (Council on Foreign Relations. n.d). Така модель підкреслює роль держави як координатора, який спрямовує ресурси у ключові напрями технологічної модернізації (зокрема напівпровідники, AI, цифрову інфраструктуру), забезпечуючи інтеграцію в глобальні ринки високих технологій.

Для України політика розвитку інноваційних кластерів залишається відносно новим, але стратегічно важливим напрямом. Досвід українських IT-кластерів у Львові, Харкові та Києві демонструє, що навіть у кризових умовах кластерні мережі можуть виступати драйверами конкурентоспроможності. Показовим є приклад Lviv IT Cluster, який визначає свою місію як спільний розвиток індустрії «together with representatives of government and education» [«разом із

представниками уряду та освіти»], а стратегічною ціллю – трансформацію України у «world-class innovative… technological center» [«інноваційний технологічний центр світового рівня»] (Lviv IT Cluster, n.d.).

Водночас для сталого розвитку потрібна системна державна підтримка: податкові стимули, інтеграція з європейськими інноваційними мережами, доступ до венчурного капіталу та захист інтелектуальної власності. Важливим ресурсом можуть стати європейські програми. Зокрема, Digital Europe Programme визначається ЄС як інструмент, що «focused on bringing digital technology to businesses, citizens and public administrations» [«зосереджений на впровадженні цифрових технологій для бізнесу, громадян і державного сектору»]. Участь України в таких ініціативах (поряд із Horizon Europe) може посилити включення українських кластерів у глобальні ланцюги інновацій та підвищити технологічну конкурентоспроможність.

Таким чином, державна політика відіграє подвійну роль: вона створює базові умови для формування інноваційних кластерів і водночас задає напрям інтеграції цих кластерів у міжнародну економіку. В умовах цифрової глобалізації країни, що сформували ефективні механізми підтримки кластерів, отримують стратегічну перевагу у змаганні за глобальну конкурентоспроможність через інновації, кооперацію та розвиток інституцій довіри (рис. 1.2).

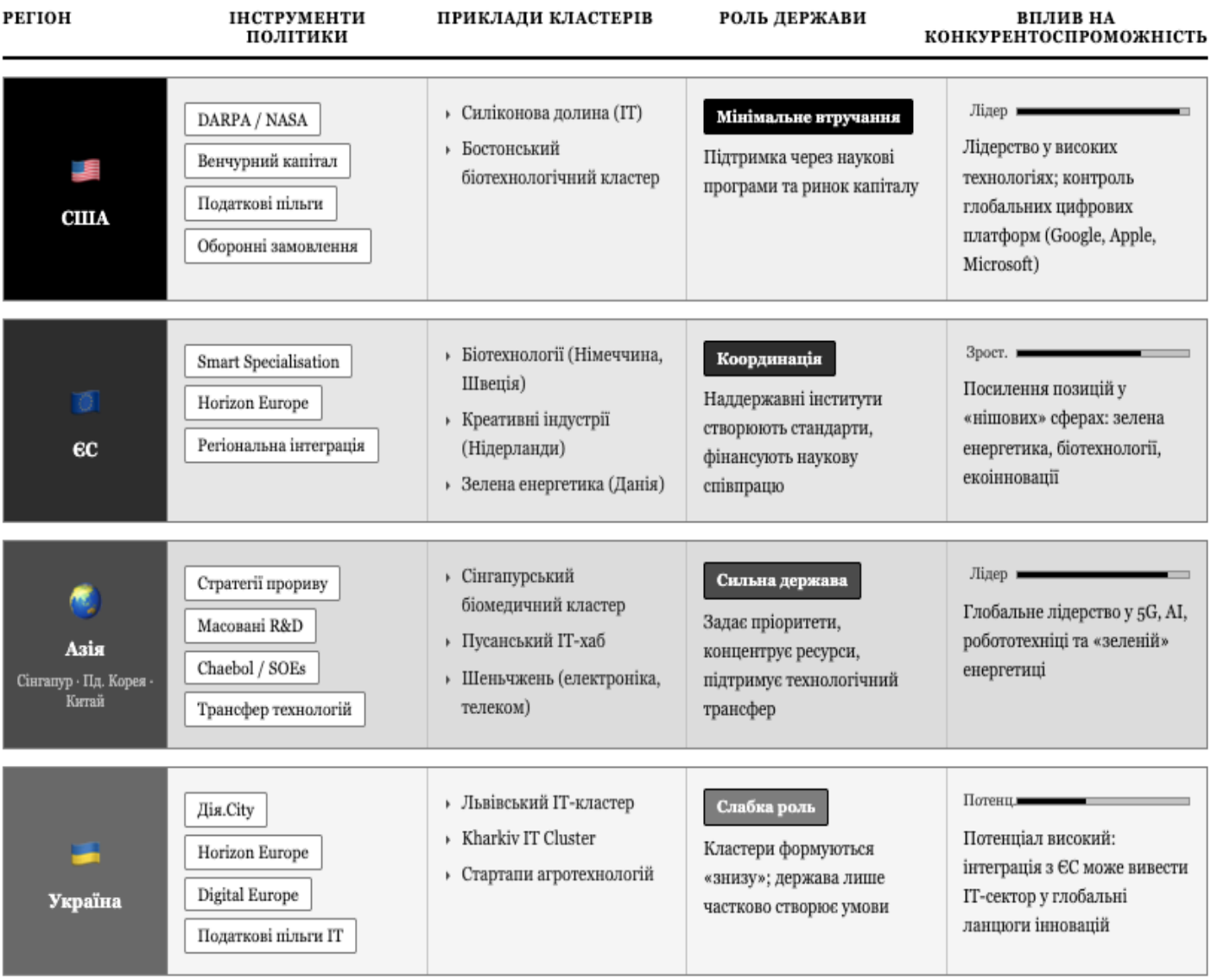

Рис. 1.2. Порівняльний аналіз інноваційної кластерної політики

Джерело: складено автором на основі порівняльного аналізу кластерних стратегій

1.3. Сутність та типологія глобальних кіберзагроз

Для України тема глобальних кіберзагроз є особливо актуальною з огляду на геополітичне розташування та зростаюче значення у світовій цифровій економіці. Україну дедалі більше визнають центром талантів у сфері IT та цифрових інновацій, а технологічний сектор демонструє стійкий розвиток та інтеграцію в глобальні ринки (IT Ukraine Association, 2024; Ukraine Investment Portal, 2025). Водночас, як і багато інших країн, Україна стикається зі значними проблемами кібербезпеки, включаючи кібератаки з боку державних і недержавних суб'єктів, а також уразливості критичної інфраструктури та державних інформаційних систем. У таких умовах аналіз проблематики крізь призму «кібергігієни» є методологічно виправданим, адже NIST визначає, що «Cyber hygiene describes recommended mitigations for the small number of root causes responsible for many cybersecurity incidents» [«кібергігієна описує рекомендовані заходи для усунення небагатьох першопричин багатьох інцидентів»] (Souppaya & Scarfone, 2020).

Надійна структура кіберзахисту забезпечує стабільність цифрової інфраструктури, що є критично важливою для підтримки економічного зростання, експорту IT-послуг і залучення іноземних інвестицій. Віддаючи пріоритет кібергігієні (зокрема управлінню вразливостями та оновленням), Україна може підвищити економічну стійкість і конкурентоспроможність у глобальному середовищі, де цифрові ризики напряму впливають на інвестиційну привабливість.

Кіберзагрози створюють прямі ризики для національної безпеки, особливо в регіонах із тривалою геополітичною напругою. Саме тому Україна розвиває підхід до кібергігієни як до інструменту масової стійкості: у проєкті Національної стратегії кібергігієни наголошується, що «our goal is to form a new culture of

responsible use of technology, where every person is protected online» [«мета – сформувати культуру відповідального використання технологій, де кожна людина захищена онлайн»]. Посилення кібергігієни допомагає захищати урядові мережі, конфіденційну інформацію та критично важливі сервіси, забезпечуючи загальну стійкість держави (National Security and Defense Council of Ukraine, 2025).

Українська технологічна індустрія значною мірою залежить від безпечних цифрових платформ, хмарних середовищ і мережевої доступності. Розвиток культури кібергігієни в компаніях підсилює інноваційність, зменшує ризики простоїв і витоків, що є принциповим для конкурентоспроможності у цифровій економіці. У цьому контексті «кібергігієна» виступає базовим рівнем захисту, який зменшує ризики, пов’язані з типовими причинами інцидентів (особливо через несвоєчасне оновлення та слабке управління доступами).

Кіберзагрози виходять за межі державних кордонів, що робить необхідними координацію, обмін інформацією та спільні стандарти. Включення України до міжнародних ініціатив кіберстійкості посилює її переговорні позиції та роль у формуванні правил цифрової економіки. Таким чином, захист цифрових кордонів і сприяння кібергігієні виступають важливим елементом міжнародної конкурентоспроможності та репутаційної довіри (Ukraine Investment Portal, 2025).

Кібербезпека як практика захисту мереж, пристроїв і даних від несанкціонованого доступу чи зловмисного використання набуває системного значення в умовах тотальної цифровізації. У фокусі сучасного підходу – забезпечення ключових властивостей інформаційної безпеки, тобто конфіденційності, цілісності та доступності, які формують основу стійкості цифрових сервісів.

Реальні кейси підтверджують масштаб ризиків і важливість базових практик кібергігієни (див. дод. В):

- Colonial Pipeline (2021). Подія стала одним із найвідоміших прикладів впливу кібератаки на критичну інфраструктуру. CISA наголошує: «On May 7, 2021, a ransomware attack on Colonial Pipeline captured headlines around the world…» [«7 травня 2021 року ransomware-атака на Colonial Pipeline спричинила світовий резонанс…»] (CISA, 2023). Конгресова аналітика США додатково фіксує, що компанія зупинила роботу трубопроводу через ransomware, що спричинило збої у постачанні пального (Congressional Research Service, 2021).
- SolarWinds (2020). Інцидент став еталонним прикладом supply chain-компрометації, яка уражає одночасно державні органи та приватний сектор. CISA описує атаку як «Highly Evasive Attacker Leverages SolarWinds Supply Chain…» [«високоприхований зловмисник використав ланцюг постачання SolarWinds…»] (CISA, 2020), що демонструє: навіть одна точка компрометації в екосистемі постачальника може масштабувати ризик для тисяч організацій.
- Equifax (2017). Інцидент став одним із найбільших витоків персональних даних. FTC зазначає, що витік зачепив 147 млн осіб, а сама Equifax прямо вказала, що вектор атаки був пов’язаний із Apache Struts (CVE-2017-5638) (Equifax, 2017). Уразливість CVE-2017-5638 описана в NVD як RCE-ризик у Struts, що дозволяв віддалене виконання команд за допомогою спеціально сформованих HTTP-заголовків. Таким чином, цей кейс наочно показує практичну цінність кібергігієни як політики «вчасного патчінгу» та управління вразливостями.

Крім окремих організацій, кіберзагрози мають ширші економічні та суспільні наслідки, адже вони підривають конкурентоспроможність, руйнуючи бізнес і галузі, впливаючи на інновації, продуктивність і прибутковість. У сучасній економіці ці загрози виходять далеко за межі локальних інцидентів, перетворюючись на системний фактор економічної нестабільності. Як зазначено в аналітичному звіті CSIS та McAfee, «close to $600 billion, nearly one percent of

global GDP, is lost to cybercrime each year» (тобто близько 600 млрд дол. США – майже 1% світового ВВП – щорічно втрачається через кіберзлочинність) (McAfee & CSIS, 2018). Це означає, що кібератаки здатні масштабно впливати на розвиток економік, рівень інвестиційної активності та глобальну конкуренцію.

Кіберзагрози можуть підривати конкурентні позиції не лише окремих компаній, а й цілих секторів. Зокрема, витік інтелектуальної власності послаблює технологічні переваги компаній і держав, створюючи умови для копіювання технологій, появи підробок та прискореного технологічного "наздоганяння" конкурентів. У підсумку це знижує інноваційний потенціал і може призводити до структурної деградації цілих галузей.

Деякі атаки є настільки руйнівними, що ставлять під загрозу саме існування бізнесу. Найбільш показовою є категорія ransomware, коли компанія втрачає операційну здатність і змушена витрачати ресурси на відновлення замість розвитку. Наприклад, Universal Health Services повідомляла про орієнтовний "unfavorable impact" у 67 млн дол. США (pre-tax) у 2020 році внаслідок кібератаки, що призвела до масштабного shutdown мережі в медичних закладах (Healthcare IT News, 2021). Такі випадки демонструють, що кіберінциденти можуть мати не лише технічні, а й прямі фінансові наслідки.

Кіберризики знижують готовність компаній інвестувати в нові технології та експериментальні рішення, оскільки будь-яка цифрова модернізація створює нові "поверхні атаки". У результаті виникає ефект стримування: бізнес надає перевагу стабільності перед інноваціями, що уповільнює технологічний прогрес і зменшує продуктивність у довгостроковій перспективі.

Кібератаки викликають простої, порушення ланцюгів постачання, затримки у виробничих та управлінських процесах. При цьому ресурси, що могли бути спрямовані на розвиток, витрачаються на розслідування інцидентів, відновлення систем і побудову резервних контурів безпеки.

Витрати на кіберзахист і наслідки атак зростають щороку. У міжнародній аналітиці підкреслюється масштаб проблеми: близько 600 млрд дол. США щороку становлять сукупні економічні втрати світової економіки від кіберзлочинності (McAfee & CSIS, 2018). У цю суму входять прямі втрати від крадіжок, витрати на відновлення, компенсації клієнтам, штрафи, а також непрямі витрати – зокрема втрати репутації та довіри.

Кібератаки можуть створювати загрозу для населення та національної безпеки, якщо їхньою ціллю є енергосистеми, транспорт або водопостачання. В Україні атака на енергетичну інфраструктуру у 2015 році призвела до знеструмлення понад 225 000 споживачів, що підкреслило реальність кіберзагроз для критичних систем (Booz Allen Hamilton, 2016). Подальші атаки на енергосектор (у т.ч. із застосуванням спеціалізованого шкідливого ПЗ для електромереж) закріпили висновок: цифрова стійкість стає умовою базової безпеки держави.

Зважаючи на це, кібербезпека має стати першочерговим питанням для держави, бізнесу та суспільства. Це вимагає спільного проактивного підходу, який охоплює обізнаність, запобігання, виявлення та реагування. Кожен інцидент підкреслює важливість посилення заходів кіберзахисту для протидії загрозам, що постійно еволюціонують.

Особливо показовими є інциденти, які демонструють, що кіберзагрози можуть виходити за межі “даних” і впливати на фізичну безпеку. Так, CISA у звіті про інцидент на об’єкті водопідготовки в США зафіксувала спробу змінити параметри процесу очищення: зловмисники через SCADA-нагляд намагалися збільшити дозування sodium hydroxide (lye) до небезпечного рівня (CISA, 2021). Наведений приклад демонструє, що кібератаки на критичну інфраструктуру можуть мати безпосередній ризик для здоров’я та життя громадян.

Порушення даних у корпоративному секторі також мають масштабні наслідки. Так, Marriott International офіційно повідомляла, що в одному з інцидентів могли бути зачеплені дані до приблизно 5,2 млн гостей, що підкреслює системність ризиків для індустрії послуг та глобальних платформ (Marriott International, 2020). У сукупності подібні інциденти формують "кризу довіри" до цифрових сервісів, що трансформується у фінансові втрати, регуляторний тиск та падіння конкурентоспроможності компаній і секторів.

Розуміння кібербезпеки є необхідною умовою для формування системної відповіді на загрози. Кібербезпека є багатогранною сферою, що охоплює як технічні механізми протидії (зокрема проти фішингу та ransomware), так і організаційні заходи (контроль доступу, управління вразливостями, реагування на інциденти). Зловмисне ПЗ може набувати різних форм – від spyware і вірусів до троянів, черв'яків і програм-вимагачів – що становить комплексні ризики для цілісності систем і конфіденційності даних. У підсумку, кіберзагрози стають універсальним фактором, який одночасно впливає на бізнес, державу та суспільство, формуючи нову архітектуру економічної безпеки XXI століття.

Кібератаки можуть здійснюватися через різні канали, оскільки зловмисники використовують широкий спектр методів для отримання несанкціонованого доступу до конфіденційної інформації, інформаційних систем і мереж. Найпоширеніші канали та механізми включають наступні (рис. 1.3, рис. 1.4):

1. Фішинг (phishing) – метод отримання чутливих даних (паролів, банківських реквізитів тощо) через шахрайські повідомлення або підроблені вебресурси, де атакувальник маскується під легітимну організацію чи особу. Типовими прикладами є листи або повідомлення, що імітують комунікацію від банку чи популярного сервісу із закликом "оновити" або "підтвердити" облікові дані (NIST, n.d.).

2. Соціальна інженерія – маніпуляція людьми з метою змусити їх розкрити інформацію або виконати дію, яка відкриває шлях до компрометації систем. Прикладом є дзвінок від “служби підтримки”, яка просить повідомити пароль або код підтвердження доступу. Окремим різновидом виступає фізична соціальна інженерія (наприклад, «підкинута флешка»), коли заражений носій навмисно залишають у зоні доступу співробітників, щоб спровокувати запуск шкідливого коду (NIST, n.d.).

3. Шкідливе програмне забезпечення (malware). До malware належать програми, навмисно створені для виконання шкідливих дій, зокрема віруси, трояни та черв’яки. Таке ПЗ може викрадати дані, надавати віддалений контроль або блокувати роботу систем (наприклад, ransomware). Типовий сценарій зараження – відкриття вкладення з електронного листа або завантаження інфікованого файлу з неперевіреного джерела (NIST, n.d.).

4. Експлуатація вразливостей програмного забезпечення та відсутність патчів. Зловмисники використовують помилки в ПЗ або ОС для отримання доступу до ресурсів чи контролю над системою. Особливо небезпечною є ситуація, коли відома вразливість не усувається через несвоєчасні оновлення (патчі), що створює «вікно можливостей» для атакувальника.

5. Атаки на мережеві протоколи та перехоплення трафіку (MITM). Атака типу “людина посередині” передбачає позиціювання зловмисника між двома сторонами обміну даними для перехоплення або модифікації трафіку. Може використовуватися для викрадення облікових даних, підміни контенту або перенаправлення користувача на фальшиві ресурси (NIST, n.d.).

6. Компрометація DNS та перенаправлення користувачів (DNS hijacking). Використовуючи викрадені облікові дані або доступ до інфраструктури, атакувальник може змінювати DNS-налаштування та спрямовувати користувачів на підроблені ресурси. CISA описує глобальні кампанії DNS hijacking, у межах

яких зловмисники змінюють DNS-записи/маршрутизацію, що дозволяє перехоплювати трафік або підміняти вебресурси (NIST, n.d.).

7. Атаки на хмарні сервіси (cloud attacks). Зростання використання хмарних платформ підвищило цінність компрометації облікових записів та конфігурацій. Важливим фактором є модель розподіленої відповідальності, за якої безпека є “shared responsibility” між хмарним провайдером та клієнтом, а значна частина ризиків залежить від налаштувань і політик доступу саме на боці організації. Уразливими точками часто стають слабкі паролі, фішинг або помилки конфігурації доступів (NIST, n.d.).

8. Атаки на IoT (інтернет речей). IoT-пристрої (розумні будинки, сенсори, медичні або промислові системи) часто мають недостатній рівень захисту: слабкі або дефолтні паролі, застарілі компоненти, відсутність безпечного механізму оновлення. Компрометація таких пристроїв може використовуватися як для шпигунства, так і для саботажу або проникнення в корпоративну мережу (OWASP, n.d.).

9. Компрометація Wi-Fi та підміна точки доступу (evil twin). У публічних мережах зловмисники можуть створювати “клон” легітимної Wi-Fi точки доступу, щоб перехоплювати трафік користувачів або отримувати їхні облікові дані. CISA прямо описує evil twin як сценарій, коли атакувальник збирає дані про справжній access point і створює підроблений, який імітує оригінальний (OWASP, n.d.).

10. Внутрішні загрози (insider threats). Ризики виникають, коли співробітники/підрядники використовують легітимний доступ навмисно або ненавмисно на шкоду організації. NIST визначає insider threat як загрозу, що полягає у використанні авторизованого доступу “wittingly or unwittingly” для завдання шкоди операціям і активам організації. Приклади включають копіювання даних на особисті пристрої, помилкове надання доступу або витік інформації через недбалість (NIST, n.d.).

Рис. 1.3. Основні канали та механізми кіберзагроз (людський фактор та технічні вразливості)

Джерело: складено автором на основі матеріалів NIST, CISA, OWASP, IBM X-Force, SonicWall, Keepnet (2024 - 2025)

11. Атаки через мобільні додатки. Мобільні застосунки можуть містити типові слабкі місця – небезпечне зберігання даних, недостатній захист комунікацій, уразливості авторизації тощо. OWASP формує структуру ризиків мобільних додатків через проєкти MASVS/MASWE як систематизацію найпоширеніших weaknesses мобільної безпеки (OWASP, n.d.). Додатково ризик

посилюється у випадку встановлення застосунків із неофіційних джерел або з надмірними дозволами.

12. Атаки на ланцюжок постачання (supply chain attacks). Це втручання у процес розробки, оновлення чи доставки продукту, коли шкідливий компонент потрапляє до кінцевого користувача через довірений канал. Один із найбільш показових прикладів – кейс SolarWinds: CISA описала інцидент як supply chain compromise, де модифіковані компоненти/оновлення стали точкою проникнення для компрометації багатьох організацій (CISA, 2021).

Рис. 1.4. Основні канали та механізми кіберзагроз (інфраструктурні та системні загрози)

Джерело: складено автором на основі матеріалів NIST, CISA, OWASP, IBM X-Force, SonicWall, Keepnet (2024 - 2025)

Кібергігієна – це практика систематичного та регулярного застосування заходів, спрямованих на підвищення рівня цифрової безпеки та запобігання кібератакам, що дозволяє захищати конфіденційні дані, пристрої й мережі від широкого спектра загроз. Її значення полягає не лише у зменшенні ризику втрати, крадіжки або пошкодження даних, а й у підтриманні стабільності бізнес-процесів та довіри між організаціями, партнерами й користувачами. Наукові узагальнення підкреслюють, що кіберінциденти мають мультиплікативний ефект: вони породжують прямі фінансові втрати, підвищують транзакційні витрати, спричиняють порушення ланцюгів постачання та посилюють недовіру до цифрових сервісів як таких. В даному контексті кібергігієна виступає одним із базових компонентів цифрової стійкості, оскільки забезпечує не лише технічне «зміцнення» систем, але й організаційну дисципліну управління ризиками.

Впровадження ефективної кібергігієни передбачає застосування комплексу практик, що поєднує технологічні та поведінкові елементи безпеки: системне оновлення програмного забезпечення, використання засобів антивірусного та антишкідливого захисту, управління паролями, багатофакторну автентифікацію, резервне копіювання, шифрування та підвищення обізнаності користувачів. Усе це формує профілактичний підхід, який дозволяє знизити витрати на відновлення після атак та мінімізувати репутаційні втрати. Дослідження економічних наслідків кіберзлочинності демонструють масштабність проблеми: за оцінками, глобальні втрати від кіберзлочинів можуть перевищувати 1 трлн дол. США, що у ряді оцінок означає зростання більш ніж на 50% порівняно з 2018 роком (McAfee,

2020). При цьому більш ранні консолідовані оцінки вказували, що кіберзлочинність уже тоді коштувала світовій економіці майже 600 млрд дол. США (≈0,8% глобального ВВП), що підтверджує системний характер кіберризиків для економічної безпеки (Lewis, 2018).

Водночас економіка кібербезпеки посилюється стрімким збільшенням обсягів цифрових даних. За прогнозами, до середини 2020-х років глобальний обсяг даних може сягнути понад 175 зетабайт, що збільшує поверхню атаки та ускладнює контроль над конфіденційною інформацією (Rydning, 2018). У таких умовах кібератаки дедалі частіше спрямовані не лише на прямі фінансові вигоди, а й на довгострокове послаблення конкурентних позицій через викрадення інтелектуальної власності, порушення операційної безперервності та руйнування довіри до цифрових каналів взаємодії. Саме тому кібергігієна стає фактором не лише технічної, а й економічної стійкості: вона зменшує ймовірність кризових збоїв та забезпечує стабільність функціонування організацій у цифровій економіці.

Окремого значення набуває розвиток рішень на основі штучного інтелекту в кіберзахисті. Прогнози ринку демонструють, що сегмент AI у кібербезпеці може зрости до понад 45 млрд дол. США до 2027 року, що відображає зміщення акцентів від реактивної до проактивної моделі захисту (Meticulous Research, 2021). Водночас зростання складності загроз супроводжується посиленням геополітичного компоненту: держави все активніше інвестують у стійкість критичної інфраструктури та міжнародну кооперацію у сфері кіберзахисту. Для України, яка перебуває в умовах постійного гібридного тиску, показовими є міжнародні програми підтримки кіберстійкості – зокрема, фінансова допомога у розмірі 37 млн дол. США на зміцнення кіберзахисту (рис. 1.5), а також інші форми партнерства, спрямовані на підвищення стійкості державних цифрових систем (U.S. Department of State, 2023).

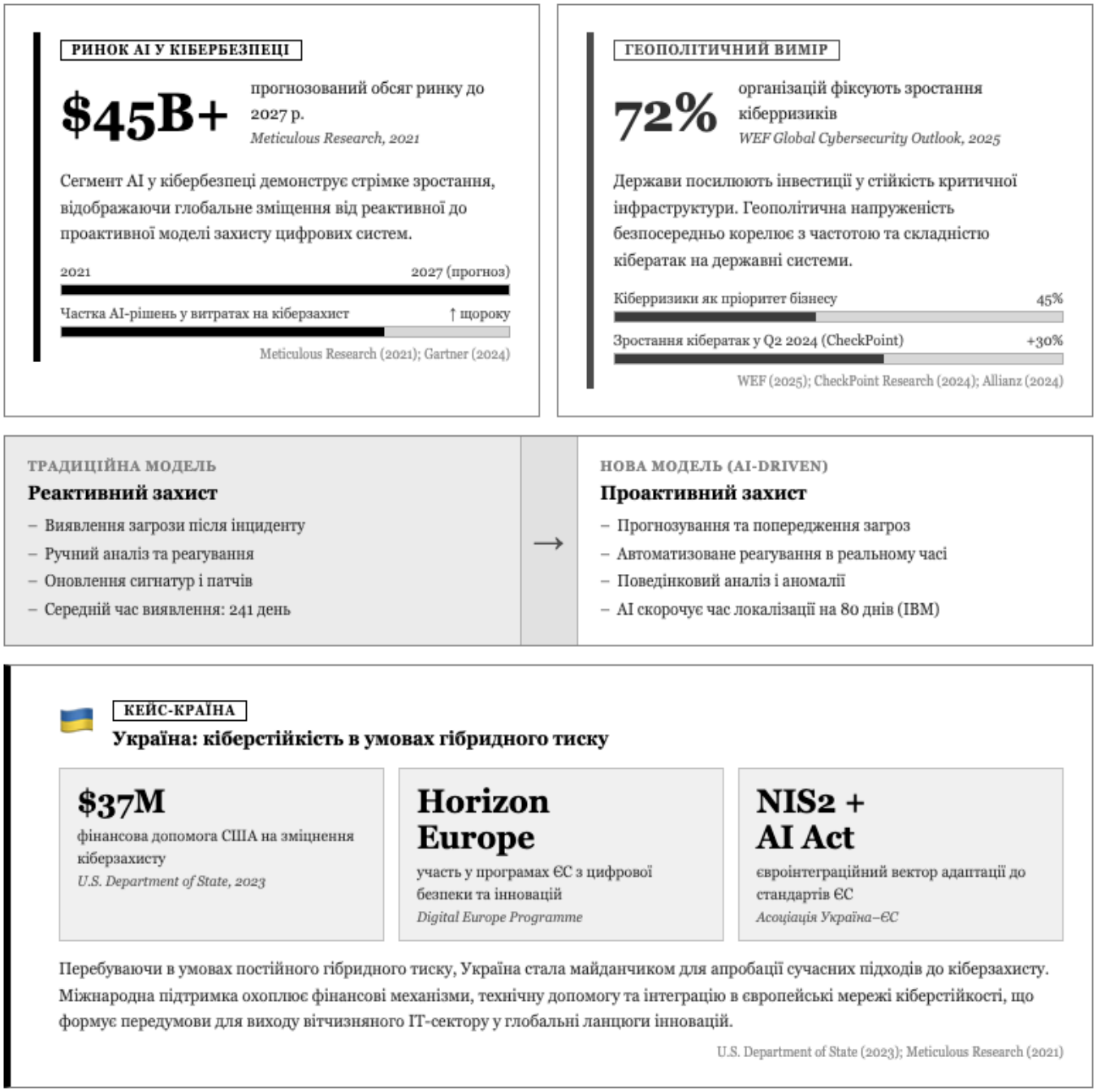

Рис. 1.5. Штучний інтелект у кібербезпеці та кіберстійкість України

Джерело: складено автором на основі матеріалів Meticulous Research, WEF, IBM X-Force, U.S. Department of State (2021 - 2025)

Узагальнені ключові зони підвищеної вразливості кібербезпеки:

- віддалені форми роботи та розподілені IT-середовища;
- IoT-пристрої та «розумна» інфраструктура;
- політично вмотивовані атаки й кібертероризм;
- програми-вимагачі (ransomware) та моделі «ransomware-as-a-service»;
- організована кіберзлочинність і тіньові цифрові ринки;
- крадіжка інтелектуальної власності (IP) та комерційних таємниць.

Запобігання втраті даних (Data Loss Prevention, DLP) є одним із ключових напрямів сучасної кібербезпеки, спрямованим на ідентифікацію, моніторинг і захист даних у станах data at rest, data in motion та data in use, а також на попередження несанкціонованого доступу, передавання чи використання конфіденційної інформації. Відповідно до підходів NIST, DLP реалізується через централізоване управління політиками та контекстний аналіз транзакцій, що дозволяє не лише фіксувати ризикові дії, а й блокувати їх на рівні каналів передавання або кінцевих точок (NIST, n.d.). Це охоплює широкий спектр даних – від клієнтської інформації та фінансової звітності до інтелектуальної власності, кадрових записів та інших критично важливих активів організації.

У практичному вимірі DLP включає комплекс функцій, що посилюють контроль над даними та зменшують імовірність інцидентів витоку:

1. Підвищення видимості та контролю даних. DLP-рішення забезпечують організаціям моніторинг і керованість інформації у різних середовищах зберігання: локальних системах, хмарній інфраструктурі та на пристроях кінцевих користувачів.

2. Захист віддалених середовищ і сценаріїв BYOD. У контексті розподіленої роботи DLP-підходи інтегруються із політиками доступу та контролю кінцевих точок, що дозволяє знижувати ризики витоків навіть при використанні особистих пристроїв (Bring Your Own Device).

3. Збереження інтелектуальної власності та конкурентних переваг. DLP розглядається як організаційна програма, націлена на запобігання “виносу” чутливих даних за межі корпоративного середовища, що є критичним для захисту інноваційного потенціалу та ринкових позицій.

4. Підтримання довіри та репутації. Превентивне блокування витоків даних є інструментом збереження довіри клієнтів і партнерів, оскільки зменшує ризики кризових інцидентів і публічних репутаційних втрат.

5. Виконання регуляторних вимог. DLP сприяє дотриманню норм захисту персональних даних, зокрема принципів GDPR щодо законності, прозорості та мінімізації даних (European Union, 2016), а також вимог CCPA щодо контролю над обробкою та використанням інформації споживачів (California Department of Justice, n.d.).

6. Зниження кіберризиків і мінімізація економічних наслідків інцидентів. Поєднання моніторингу, політик і автоматизованого реагування дозволяє зменшувати як прямі втрати від інцидентів, так і непрямі наслідки (простій, юридичні витрати, штрафи).

Ефективність DLP значною мірою залежить від якості політик класифікації та контролю даних, а також від застосування інструментів автоматизованого аналізу. У сучасних умовах посилюється роль алгоритмічних методів, оскільки захист дедалі частіше потребує не лише інвентаризації даних “у сховищі”, а й контролю даних “у передаванні”, що підвищує здатність системи виявляти ризики у реальному часі. Водночас DLP не може бути ізольованим інструментом: його результативність прямо пов’язана з рівнем кібергігієни та культури безпеки персоналу, зокрема завдяки навчальним програмам, що формують практичні навички протидії фішингу, соціальній інженерії та іншим поведінковим ризикам (Chandramouli et al., 2024).

Окремим компонентом сучасної моделі кіберзахисту є кооперaційний підхід: міжнародні та національні практики підкреслюють, що підвищення стійкості кіберпростору залежить від системної взаємодії держави, бізнесу та експертного середовища, включаючи обмін інформацією про загрози та кращі практики (ENISA, n.d.). Відповідно, DLP та корпоративна кібергігієна мають розглядатися як частина ширшої архітектури – інституційної та міжсекторальної – що формує "спільну відповідальність" за захист цифрового середовища.

Таким чином, DLP виступає не лише технічним засобом, а комплексним механізмом управління ризиками, що поєднує політики доступу, контроль каналів передавання даних, автоматизовані методи виявлення аномалій та людський фактор кіберстійкості. У сукупності це підсилює економічну безпеку організацій шляхом захисту критичних активів, збереження довіри та забезпечення регуляторної відповідності.

Висновки до розділу 1

1. Досліджено генезис концепцій економічної безпеки країн та встановлено, що еволюція цієї категорії має діалектичний характер: від матеріально-ресурсного трактування (меркантилізм: протекціонізм, торговельний баланс, накопичення стратегічних активів) – до підходів, що пов'язують економічну безпеку зі спеціалізацією, ефективністю факторів виробництва та інтеграцією у світове господарство (класична політична економія; порівняльні переваги; продуктивність). Показано, що в умовах криз, воєн та шоків постачання відбувається повернення до інструментів економічного "укріплення" (контроль стратегічних ресурсів, протекціонізм, експортні обмеження), що підтверджує циклічність безпекових підходів у глобальній економіці.

2. Систематизовано класичні та модернізовані теоретичні підходи до економічної безпеки, які формують її багатовимірну природу. До ключових підходів віднесено: кейнсіансько-неокейнсіанську традицію (роль держави у стабілізації, зайнятості та управлінні інвестиціями як основі стійкості); неоліберальну парадигму (економічна свобода, конкуренція та відкритість як умова адаптивності); світ-системний і залежнісний аналіз (структурні асиметрії "центр–периферія" як джерело вразливості); міжнародну політичну економію (економічні, технологічні та військові спроможності як компоненти державної сили). Обґрунтовано, що ЕБ не зводиться до фінансової стабільності, а включає інституційний, технологічний, соціальний, ресурсний та геополітичний виміри.

3. Доведено, що у другій половині XX ст. відбулася інституціоналізація економічної безпеки через розвиток механізмів колективної стабільності та міжнародного економічного регулювання (післявоєнна архітектура, валютно-фінансова координація, багатосторонні торговельні правила). Показано, що нафтова криза 1970-х років закріпила енергетичний компонент у структурі економічної безпеки та стимулювала практики диверсифікації, стратегічних резервів і координації дій країн-імпортерів. У подальшому фінансова глобалізація посилила значущість макроекономічної та валютної стійкості як "буфера" від кризових хвиль.

4. Обґрунтовано цифровий вимір економічної безпеки як визначальний у XXI столітті, оскільки критично важливі економічні процеси (фінанси, логістика, транспорт, енергетика, державні послуги) функціонують у цифровому середовищі, а отже – стають залежними від надійності мереж, даних та інформаційних систем. Показано, що центральною категорією стає кіберстійкість, яка відображає здатність системи передбачати, витримувати, відновлюватися та адаптуватися до збурень. Установлено, що цифровізація перетворює економічну

безпеку на міжсекторальну категорію, де ризики швидко “перетікають” між галузями через взаємопов’язані цифрові ланцюги.

5. Розкрито зміст і роль цифрового суверенітету та “економіки довіри” у сучасних концепціях безпеки та конкурентоспроможності. Встановлено, що залежність від глобальних цифрових платформ і транснаціональних постачальників хмарних/інфраструктурних сервісів формує нові типи стратегічної вразливості: технологічну залежність, асиметрію доступу до даних, ризики екстериторіального регулювання та “vendor lock-in”. Доведено, що довіра до цифрових сервісів стає економічним активом, а її руйнування (через витоки даних, маніпуляції, непрозорі алгоритми) трансформується у прямі втрати конкурентних позицій, інвестиційної привабливості та стійкості економічних інститутів.

6. Обґрунтовано етичний вимір економічної безпеки та міжнародної конкурентоспроможності, який формується на перетині цифрових прав, регуляторних норм і практик відповідального управління даними та алгоритмами. Показано, що принципи ethics-by-design (а також privacy-by-design, accountability, transparency) стають не “додатковою опцією”, а системним елементом безпекової архітектури цифрової економіки. Встановлено, що етичні стандарти підвищують передбачуваність правил гри та зміцнюють довіру на ринках, а їх порушення створює кумулятивні ризики – репутаційні, правові, регуляторні та макроекономічні.

7. Досліджено взаємозв’язок глобальної конкурентоспроможності та економічної безпеки, який проявляється через здатність країн забезпечувати продуктивність, інноваційність, модернізацію та стійкість до шоків. Показано, що конкурентоспроможність у сучасній економіці визначається не лише доступом до ресурсів, а якістю інститутів, здатністю до інновацій і включенням у глобальні ланцюги створення вартості. Обґрунтовано роль інноваційних кластерів як

інституційно-мережевих механізмів, що концентрують знання, капітал і підприємництво та прискорюють цикл “ідея → продукт → ринок”, водночас зменшуючи вразливість через диверсифікацію партнерств і технологій.

8. Систематизовано інструменти державної політики підвищення конкурентоспроможності через інноваційні екосистеми, зокрема: фінансування R&D, стратегічні програми розвитку технологій, державні замовлення у високотехнологічних секторах, податкові стимули, підтримку стартапів, інтеграцію з міжнародними програмами та мережами. Доведено, що ефективна кластерна політика є поєднанням інституційної якості (правила, прозорість, захист IP, антимонопольні механізми) та інвестицій у людський капітал і інфраструктуру, а також передбачає узгодження з глобальними стандартами і вимогами регуляторного середовища.

9. Розкрито сутність та побудовано типологію глобальних кіберзагроз як фактору економічної нестабільності, доведено їх системний вплив на міжнародну конкурентоспроможність і економічну безпеку країн. Обґрунтовано, що сучасні кіберзагрози виходять за межі “локальних інцидентів”, перетворюючись на чинник порушення ланцюгів постачання, збоїв критичної інфраструктури, втрат інтелектуальної власності, деградації довіри та посилення нетарифних бар’єрів через вимоги відповідності стандартам (GDPR, NIS2, ISO/IEC 27001, SOC 2 тощо).

10. Узагальнено ключові канали реалізації кіберзагроз і їх прикладний вимір, що охоплює фішинг і соціальну інженерію, malware/ransomware, експлуатацію вразливостей та несвоєчасне оновлення, атаки на хмарні середовища та облікові записи, компрометацію IoT/IIoT/OT/ICS, атаки типу MITM/DNS hijacking, insider threats, а також supply chain attacks як один із найнебезпечніших сучасних сценаріїв. Показано, що економічні наслідки кіберінцидентів мають мультиплікативний характер: прямі втрати поєднуються з

непрямими (простій, штрафи, регуляторний тиск, репутаційна деградація), що знижує інноваційність і продуктивність у довгостроковій перспективі.

11. Доведено методологічну доцільність підходу “кібергігієни” як базового шару масової стійкості, оскільки значна частина інцидентів спричиняється обмеженим набором типових першопричин (слабке управління оновленнями, доступами, конфігураціями, обізнаністю персоналу). Обґрунтовано, що кібергігієна є інструментом не лише технічної, а й економічної безпеки, адже забезпечує безперервність процесів, знижує транзакційні витрати та підтримує довіру на цифрових ринках.

12. Сформовано узагальнюючий висновок, що теоретико-методологічні засади міжнародної конкурентоспроможності та економічної безпеки країн у XXI столітті мають розглядатися як цілісна система, в якій поєднуються класичні підходи (ресурси, продуктивність, інститути, макростабільність) і нові домінанти (цифрова інфраструктура, кіберстійкість, цифровий суверенітет, етика та довіра). Така інтеграція створює підґрунтя для подальшого аналізу механізмів зниження глобальних кіберризиків і формування конкурентних переваг у цифровій економіці.

Основні результати дослідження, викладені в цьому розділі, відображено в працях автора:

1. Myronchenko D., Sydorenko K. Role of the IT-sector of Ukraine in the global cyber security system. *Економічний простір.* 2023. №186. С. 13-17. DOI: 10.32782/2224-6282/186-2.

2. Myronchenko D. Ethical aspects of cyber security in the global economy and international relations. *Вчені записки*. 2025. Вип. 40. №3. С. 133-140. DOI: 10.33111/vz_kneu.40.25.03.02.012.018.

3. Myronchenko D. Securing Digital Frontier: Cyber Hygiene in the Global Economy. *Актуальні проблеми економіки*. 2025. Вип. 12. №294. С. 151-159. DOI:

10.32752/1993-6788-2025-1-294-151-159.

4. Myronchenko D., Sydorenko K. Digital vulnerability of transport infrastructure in the context of global crises. *The International Sustainable Transportation Symposium (ISTRAS'25)* / National Aviation Academy of Azerbaijan 2025. P. 23. ISBN : 978-9952-582-08-6. DOI : 10.71108/istras.2025 *(Scopus)*.

Список використаних джерел до розділу 1

Amazon Web Services (AWS). Shared Responsibility Model. URL: https://aws.amazon.com/compliance/shared-responsibility-model/

Agreement on an International Energy Program (IEP) : міжнародна угода. International Energy Agency, 1974 (оновлена редакція). URL: https://iea.blob.core.windows.net/assets/c6be6d60-1ca8-4b99-b8c7-7ac508ec157c/IEP.pdf

Booz Allen Hamilton. Ukraine Report: When the Lights Went Out. 2016. URL: https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf

Business Wire. McAfee. New McAfee Report Estimates Global Cybercrime Losses to Exceed $1 Trillion. 2020. URL: https://www.businesswire.com/news/home/20201206005011/en/New-McAfee-Report-Estimates-Global-Cybercrime-Losses-to-Exceed-%241-Trillion

California Department of Justice. California Consumer Privacy Act (CCPA). URL: https://oag.ca.gov/privacy/ccpa

CBS News. Facebook stock recovers all $134B lost after Cambridge Analytica data scandal. 10 May 2018. URL: https://www.cbsnews.com/news/facebook-stock-price-recovers-all-134-billion-lost-after-cambridge-analytica-datascandal/

Center for Strategic and International Studies (CSIS). Lewis J. A. The Economic Impact of Cybercrime. 2018. URL: https://www.csis.org/analysis/economic-impact-cybercrime

Center for Strategic and International Studies (CSIS). McAfee, CSIS. The Economic Impact of Cybercrime – No Slowing Down. 2018. URL: https://marylandnonprofits.org/wp-content/uploads/2020/04/mcafee.pdf

Center for Strategic and International Studies (CSIS). Lewis J. A. The Economic Impact of Cybercrime – No Slowing Down. 2018. URL: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf

CISA. The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years. 07.05.2023. URL: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

CISA. Active Exploitation of SolarWinds Software. 14.12.2020. URL: https://www.cisa.gov/news-events/alerts/2020/12/13/active-exploitation-solarwinds-software

CISA. Supply Chain Compromise (SolarWinds). 07.01.2021. URL: https://www.cisa.gov/news-events/alerts/2021/01/07/supply-chain-compromise

CISA. Compromise of U.S. Water Treatment Facility (AA21-042A). 2021. URL: https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-042a

CISA. DNS Infrastructure Hijacking Campaign (AA19-024A). URL: https://www.cisa.gov/news-events/cybersecurity-advisories/aa19-024a

CISA. Securing Wireless Networks (Evil Twin Attacks). URL: https://www.cisa.gov/news-events/news/securing-wireless-networks

Keynes J. M. The General Theory of Employment, Interest and Money. London : Macmillan, 1936. URL: https://www.files.ethz.ch/isn/125515/1366_keynestheoryofemployment.pdf

Chandramouli R. et al. NIST IR 8505. A Data Protection Approach for Cloud-Native Applications (PDF). URL: https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8505.pdf

Council of Europe. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). Strasbourg : Council of Europe, 1981. URL: https://rm.coe.int/1680078b37.

Cremer F., Sheehan B., Fortmann M., Kia A. N., Mullins M. Cyber risk and cybersecurity: a systematic review of data availability. Geneva Papers on Risk and Insurance: Issues and Practice. 2022. Vol. 47(3). P. 698–736. DOI: 10.1057/s41288-022-00266-6. URL: https://link.springer.com/article/10.1057/s41288-022-00266-6

Defense Advanced Research Projects Agency (DARPA). About DARPA: Our Mission. URL: https://www.darpa.mil/about

Дячек В., Мірошніченко І. Розвиток співпраці приватних організацій сфери IT з державними агенціям як передумова розвитку публічно-приватного партнерства в умовах війни. Економіка та суспільство. 2023. № 56. DOI: 10.32782/2524-0072/2023-56-167

Дячек В., Мірошніченко І. Управління ризиками в ході реалізації інфраструктурних проєктів державно-приватного партнерства. Herald of Khmelnytskyi National University. Economic Sciences. 2025. № 340(2). С. 207-209. DOI: 10.31891/2307-5740-2025-340-32

European Union Agency for Cybersecurity (ENISA). Handbook for Cyber Stress Tests. 2025. URL:

https://www.enisa.europa.eu/sites/default/files/2025-05/2025.04311_01_ms_v2.0_Handbook%20for%20Cyber%20Stress%20Tests_en.pdf

ENISA. Public Private Partnerships (PPPs). URL: https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/national-cybersecurity-strategies-0/public-private

Equifax. Equifax Releases Details on Cybersecurity Incident (Struts CVE-2017-5638 as attack vector). 15.09.2017. URL: https://investor.equifax.com/news-events/press-releases/detail/237/equifax-releases-details-on-cybersecurity-incident (дата звернення: 26.01.2026).

European Commission. Data Governance Act explained. URL: https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained

European Commission. Ethics By Design and Ethics of Use Approaches for Artificial Intelligence. 25 Nov 2021. URL: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-by-design-and-ethics-of-use-approaches-for-artificial-intelligence_he_en.pdf

European Commission. Cluster policy (definition and role of clusters). URL: https://single-market-economy.ec.europa.eu/industry/cluster-policy_en

European Commission. About S3 Smart Specialisation: “Smart specialisation is a place-based approach…”. URL: https://ec.europa.eu/regional_policy/policy/communities-and-networks/s3-community-of-practice/about_en

European Commission. Horizon Europe: EU’s key funding programme for research and innovation. URL: https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/horizon-europe_en

European Commission. The Digital Europe Programme (DIGITAL). URL: https://digital-strategy.ec.europa.eu/en/activities/digital-programme

European Parliament. Digital sovereignty for Europe. EPRS Briefing. 2020. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI%282020%29651992_EN.pdf

European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32016R0679

European Union. Regulation (EU) 2016/679 (GDPR) : Consolidated text (EUR-Lex). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A02016R0679-20160504

European Union. Directive (EU) 2022/2555 (NIS2 Directive): on measures for a high common level of cybersecurity across the Union. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

European Union. Regulation (EU) 2024/1689 (Artificial Intelligence Act). 12 Jul 2024. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

Federal Trade Commission. FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook. 24 Jul 2019. URL: https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook

Federal Trade Commission. Uber Settles FTC Allegations that It Made Deceptive Privacy and Data Security Claims. 15 Aug 2017. URL: https://www.ftc.gov/news-events/news/press-releases/2017/08/uber-settles-ftc-allegations-it-made-deceptive-privacy-data-security-claims

Federal Trade Commission (FTC). Equifax Data Breach Settlement (147 million affected; up to $425 million for consumers). URL: https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement

Frank A. G. The Development of Underdevelopment : (цит. за навчальним профілем автора). URL: https://ncca.ie/media/2831/andre-gunder-frank.pdf

Friedman M. Capitalism and Freedom: Online Library of Liberty. URL: https://oll.libertyfund.org/pages/friedman-on-capitalism-and-freedom

Gilpin R. War and Change in International Politics : конспект/витяг (Cambridge : Cambridge University Press, 1981). URL: https://www.rochelleterman.com/ir/sites/default/files/Gilpin1981.pdf (дата звернення: 26.01.2026).

Google. AI Principles. URL: https://ai.google/principles/

GDPR. Recital 1. Data protection as a fundamental right. URL: https://gdpr-info.eu/recitals/no-1/

GDPR. Recital 4. Data protection in balance with other fundamental rights. URL: https://www.privacy-regulation.eu/en/recital-4-GDPR.htm

Hayek F. A. The Road to Serfdom (Condensed Edition). Foundation for Economic Education (FEE). URL: https://fee.org/ebooks/the-road-to-serfdom-condensed-edition/

Healthcare IT News. Universal Health Services faces $67 million loss after cyberattack. 2021. URL: https://www.healthcareitnews.com/news/universal-health-services-faces-67-million-loss-after-cyberattack

Holling C. S. Resilience and Stability of Ecological Systems. Annual Review of Ecology and Systematics. 1973. URL: https://pure.iiasa.ac.at/id/eprint/26/1/RP-73-003.pdf

Грущинська Н.М., Пічкурова З.В., Румянцев А.П. Трансформація міжнародних економічних відносин України. Інтернаука. Серія: "Економічні науки". 2022. №12. DOI: 10.25313/2520-2294-2022-12-8474

International Bank for Reconstruction and Development (World Bank). Articles of Agreement of the International Bank for Reconstruction and Development. 1965. URL: https://thedocs.worldbank.org/en/doc/635191548363115279-0240022019/render/IBRDArticlesofAgreement1965.pdf

International Monetary Fund. Articles of Agreement of the International Monetary Fund. Article I: Purposes. URL: https://www.imf.org/external/pubs/ft/aa/pdf/aa.pdf

International Energy Agency. History : (електронний ресурс). URL: https://www.iea.org/about/history

International Energy Agency. Oil security and emergency response (stockholding obligation). URL: https://www.iea.org/about/oil-security-and-emergency-response

IT Ukraine Association. Digital Tiger 2024 : аналітичний звіт. 2024. URL: https://itukraine.org.ua/files/DigitalTiger2024.pdf

JTC Singapore. Biopolis: “supports the biomedical industry as Singapore’s engine of economic growth”. URL: https://www.jtc.gov.sg/find-space/biopolis

Keynes J. M. The General Theory of Employment, Interest and Money. London : Macmillan, 1936. URL: https://www.files.ethz.ch/isn/125515/1366_keynestheoryofemployment.pdf

Костинець Ю., Кушніренко В. Роль цифрової інфраструктури на основі штучного інтелекту в стратегіях підвищення конкурентоспроможності підприємств в Україні. Актуальні проблеми економіки. 2026. №295. С. 68-75. DOI:10.32752/1993-6788-2026-1-295-68-75

Lt F. The National System of Political Economy. Part Two: The Theory. 1841. URL:is https://historyofeconomicthought.mcmaster.ca/list/list2

Lewis J. A. The Economic Impact of Cybercrime. CSIS, 2018. URL: https://www.csis.org/analysis/economic-impact-cybercrime

Lviv IT Cluster. About Cluster (mission and cooperation with government and education). URL: https://itcluster.lviv.ua/en/about-cluster/

McAfee. New McAfee Report Estimates Global Cybercrime Losses to Exceed $1 Trillion. Business Wire. 2020. URL: https://www.businesswire.com/news/home/20201206005011/en/New-McAfee-Report-Estimates-Global-Cybercrime-Losses-to-Exceed-%241-Trillion

Microsoft. Responsible AI: Ethical policies and practices (principles: fairness, reliability & safety, privacy & security, inclusiveness, transparency, accountability). URL: https://www.microsoft.com/en-us/ai/responsible-ai

Mun T. England's Treasure by Foreign Trade (excerpt): "to sell more to strangers yearly…". URL: https://teachingamericanhistory.org/document/mercantilism/

Myronchenko D., Sydorenko K. Role of the IT-sector of Ukraine in the global cyber security system. Економічний простір. 2023. №186. С. 13-17. DOI: 10.32782/2224-6282/186-2.

Myronchenko D. Ethical aspects of cyber security in the global economy and international relations. Вчені записки. 2025. Вип. 40. №3. С. 133-140. DOI: 10.33111/vz_kneu.40.25.03.02.012.018.

Myronchenko D. Securing Digital Frontier: Cyber Hygiene in the Global Economy. Актуальні проблеми економіки. 2025. Вип. 12. №294. С. 151-159. DOI: 10.32752/1993-6788-2025-1-294-151-159.

Myronchenko D., Sydorenko K. Digital vulnerability of transport infrastructure in the context of global crises. The International Sustainable Transportation Symposium

(ISTRAS'25) / National Aviation Academy of Azerbaijan 2025. P. 23. ISBN : 978-9952-582-08-6. DOI : 10.71108/istras.2025 (Scopus).

Meticulous Research®. Artificial Intelligence (AI) in Cybersecurity Market Worth $46.3 Billion by 2027 // GlobeNewswire. 2021. URL: https://www.globenewswire.com/news-release/2021/09/16/2298704/0/en/ArtificialIntelligence-AI-in-Cybersecurity-Market-Worth-46-3-Billion-by-2027-Market-Size-ShareForecasts-Trends-Analysis-Report-with-COVID-19-Impact-by-Meticulous-Research.html

Mac Síthigh D., Siems M. The Chinese Social Credit System: A Model for Other Countries? 2019. URL: https://pureadmin.qub.ac.uk/ws/portalfiles/portal/167731395/Mac_Sithigh_Siems_SCS_April_2019.pdf

Marriott International. Marriott International Notifies Guests of Property System Incident. 2020. URL: https://marriott.gcs-web.com/news-releases/news-release-details/marriott-international-notifies-guests-property-system-incident

North D. C. Institutions, Institutional Change and Economic Performance. Cambridge : Cambridge University Press, 1990. URL: https://archive.org/details/institutionsinst0000nort

National Institute of Standards and Technology. Cyber resiliency : glossary. URL: https://csrc.nist.gov/glossary/term/cyber_resiliency

National Institute of Standards and Technology. Confidentiality, Integrity, Availability (CIA) – glossary. URL: https://csrc.nist.gov/glossary/term/confidentiality_integrity_availability

National Institute of Standards and Technology. NVD: CVE-2017-5638 Details (Apache Struts). URL: https://nvd.nist.gov/vuln/detail/cve-2017-5638

National Institute of Standards and Technology. Data loss prevention // NIST CSRC Glossary. URL: https://csrc.nist.gov/glossary/term/data_loss_prevention

National Institute of Standards and Technology. Data Loss Prevention : publication (PDF). URL: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=904672

National Institute of Standards and Technology. SP 800-124 Rev. 1. Guidelines for Managing the Security of Mobile Devices in the Enterprise. URL: https://csrc.nist.gov/pubs/sp/800/124/r1/final

National Institute of Standards and Technology. Phishing // NIST CSRC Glossary. URL: https://csrc.nist.gov/glossary/term/phishing

National Institute of Standards and Technology. Social engineering // NIST CSRC Glossary. URL: https://csrc.nist.gov/glossary/term/social_engineering

National Institute of Standards and Technology. Malware // NIST CSRC Glossary. URL: https://csrc.nist.gov/glossary/term/malware

National Institute of Standards and Technology. Man-in-the-middle attack (MitM) // NIST CSRC Glossary. URL: https://csrc.nist.gov/glossary/term/man_in_the_middle_attack

National Institute of Standards and Technology. Insider threat // NIST CSRC Glossary. URL: https://csrc.nist.gov/glossary/term/insider_threat

NATO. Speech (transcript): resilience in the digital world. 15 Apr 2021. URL: https://www.nato.int/en/news-and-events/events/transcripts/2021/04/15/speech

National Security and Defense Council of Ukraine (NSDC). Ukraine presented the draft National Cyber Hygiene Strategy (quote by M. Fedorov). 13.11.2025. URL: https://www.rnbo.gov.ua/en/Diialnist/7325.html

Obstfeld M. Rational and Self-Fulfilling Balance-of-Payments Crises. NBER Working Paper No. 1486. 1984. URL: https://www.nber.org/papers/w1486

Organisation for Economic Co-operation and Development. Convention on the Organisation for Economic Co-operation and Development. Article 1. URL:

https://www.oecd.org/en/about/legal/text-of-the-convention-on-the-organisation-for-economic-co-operation-and-development.html

OECD. Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity. 2015. URL: https://legalinstruments.oecd.org/public/doc/328/328.en.pdf

OECD. Enhancing the Digital Security of Critical Activities. Paris : OECD Publishing, 2021. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/10/enhancing-the-digital-security-of-critical-activities_d07dd7da/a91b818b-en.pd.

OECD. For Official Use DSTI/ICCP/REG(98)4/REV3 (Wassenaar Arrangement; export controls background). URL: https://one.oecd.org/document/DSTI/ICCP/REG%2898%294/REV3/en/pdf

OECD. AI principles: Transparency and explainability. URL: https://www.oecd.org/en/topics/sub-issues/ai-principles.html

OECD. Data free flow with trust. URL: https://www.oecd.org/en/about/programmes/data-free-flow-with-trust.html

OECD. OECD Guidelines for Multinational Enterprises on Responsible Business Conduct. Paris : OECD Publishing, 2023. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/06/oecd-guidelines-for-multinational-enterprises-on-responsible-business-conduct_a0b49990/81f92357-en.pdf.

OECD. Clusters, Innovation and Entrepreneurship. Paris : OECD Publishing, 2009. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2009/07/clusters-innovation-and-entrepreneurship_g1ghb09e/9789264044326-en.pdf

OpenAI. OpenAI Charter. URL: https://openai.com/charter/

OHCHR. Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework. New York ; Geneva : United Nations, 2011. URL: https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

OWASP. OWASP Internet of Things Project. URL: https://owasp.org/www-project-internet-of-things/

OWASP. OWASP Mobile Application Security Project (MASVS/MASWE). URL: https://owasp.org/www-project-mobile-app-security/

Pobochenko L., Rumiantsev A., Pichkurova Z., Tolpezhnikova T., Kovbych T., Lyashov D. The impact of global digitalization on the Ukrainian labor market development. Financial and credit activity: problems of theory and practice. 2022. 5(46). P. 334-348. DOI: https://doi.org/10.55643/fcaptp.5.46.2022.3854

Porter M. E. The Competitive Advantage of Nations. Harvard Business Review. 1990. URL: https://hbr.org/1990/03/the-competitive-advantage-of-nations

Porter M. E. Clusters and the New Economics of Competition. Harvard Business Review. 1998. URL: https://biblioteca.fundacionicbc.edu.ar/images/d/de/Clusters_1.pdf

Porter M. E. The Competitive Advantage of Nations. New York : Free Press, 1990. URL: https://archive.org/details/competitiveadvan00port

Прокоп’єва А.А., Набок І.І., Побоченко Л.М., Татаренко Н.О. Віртуалізація міжнародного бізнесу в умовах розвитку інформаційних технологій. Інтернаука. 2023. №3. С. 168-174. DOI: 10.25313/2520-2294-2023-3-8667

Ricardo D. On the Principles of Political Economy and Taxation. Chapter VII: On Foreign Trade. 1817. URL: https://www.marxists.org/reference/subject/economics/ricardo/tax/ch07.htm

Roosevelt F. D. Message to Congress on Social Security. January 17, 1935. The American Presidency Project. URL: https://www.presidency.ucsb.edu/documents/message-congress-social-security

Rydning D. R. J. G. J., Reinsel D., Gantz J., et al. The Digitization of the World from Edge to Core. IDC – Seagate. 2018. URL: https://www.seagate.com/files/www-content/our-story/trends/files/dataage-idc-report-final.pdf

Sachwald F. The development of global innovation networks. Policy Brief N°21. European Commission (JRC), 2013. URL: https://iri.jrc.ec.europa.eu/sites/default/files/contentype/event/1568726539/Policy%20Brief_Sachwald.pdf

Schumpeter J. A. Capitalism, Socialism and Democracy. New York : Harper & Brothers, 1942. URL: https://archive.org/details/capitalismsocial0000jose

Shtuler I., Chubaievskyi V., Blakyta H., Bogma J., Batrakova T. Protection of information resources as an integral part of economic security of the enterprise. Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu. 2022. № 4. P. 183-188. DOI: 10.33271/nvngu/2022-4/117

Smith A. An Inquiry into the Nature and Causes of the Wealth of Nations. 1776. URL: https://www.uni-ulm.de/fileadmin/website_uni_ulm/mawi.inst.150/lehre/ws0910/GVWL/AdamSmith.pdf

Souppaya M., Scarfone K. Critical Cybersecurity Hygiene: Patching the Enterprise. NIST, 2020. URL: https://csrc.nist.gov/pubs/pd/2020/03/30/critical-cybersecurity-hygiene-patching-the-enterp/final

The United Nations Office at Geneva. The League of Nations (Overview). URL: https://www.ungeneva.org/en/about/league-of-nations/overview

United Nations. Charter of the United Nations and Statute of the International Court of Justice. United Nations, 1945. URL: https://treaties.un.org/doc/publication/ctc/uncharter.pdf

Ukraine Investment Portal. ICT and Digital Sector : огляд сектору. 2025. URL: https://investportalua.com/wp-content/uploads/2025/11/13.-ict-and-digital-sector-1-1-16.pdf

U.S. Department of Justice. Facebook Agrees to Pay $5 Billion and Implement Robust New Protections for User Information. 24 Jul 2019. URL: https://www.justice.gov/archives/opa/pr/facebook-agrees-pay-5-billion-and-implement-robust-new-protections-user-information

U.S. Department of State. Proceedings of the 2023 U.S.-Ukraine Cyber Dialogue. 2023. URL: https://2021-2025.state.gov/proceedings-of-the-2023-u-s-ukraine-cyber-dialogue/

Wallerstein I. The Modern World-System as a Capitalist World-Economy : (навчальний матеріал / фрагмент). URL: https://cdn.vanderbilt.edu/vu-my/wp-content/uploads/sites/1414/2014/04/14122105/Session_03_Wallerstein.pdf

Wired. ‘Crash Override’: The Malware That Took Down a Power Grid. 2017. URL: https://www.wired.com/story/crash-override-malware/

Wilson M., Hash J. NIST SP 800-50. Building an Information Technology Security Awareness and Training Program (PDF). URL: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-50.pdf

World Trade Organization. Marrakesh Agreement Establishing the World Trade Organization : Preamble. URL: https://www.wto.org/english/docs_e/legal_e/04-wto_e.htm

World Economic Forum. Trust is the new currency in the AI agent economy. 2025. URL: https://www.weforum.org/stories/2025/07/ai-agent-economy-trust/

РОЗДІЛ 2
АНАЛІЗ ВПЛИВУ СУЧАСНИХ ГЛОБАЛЬНИХ КІБЕРЗАГРОЗ НА МІЖНАРОДНУ КОНКУРЕНТОСПРОМОЖНІСТЬ ТА ЕКОНОМІЧНУ БЕЗПЕКУ КРАЇН

2.1. Основні тенденції розвитку інституційного забезпечення економічної безпеки країн в контексті зменшення впливу глобальних кіберзагроз

Сучасні глобальні кіберзагрози змістили інституційні системи безпеки в центр економічної політики держав і міждержавної координації. У цьому контексті інституційне забезпечення кіберстійкості варто трактувати як узгоджений набір норм, організацій, процедур та механізмів взаємодії (державних, приватних і міжнародних), завдяки яким зменшується ймовірність інцидентів, локалізуються їхні наслідки та забезпечується відновлення критичних функцій економіки в прогнозовані часові рамки. На практиці це означає перехід від фрагментарних “добровільних рекомендацій” до комплаєнс-моделей, де базові вимоги до управління ризиками та реагування стають елементом регуляторного контролю й ринкового доступу.

Упродовж останнього десятиліття простежується нормативна конвергенція: рекомендаційні підходи поступово доповнюються або замінюються юридично зобов'язувальними рамками щодо управління вразливостями, ідентифікації, контролю доступу та обов'язкового інцидент-репортингу. Показовим є підхід ЄС, де Директива NIS2 закріплює багатоступеневу модель повідомлення про значущі інциденти: раннє попередження до 24 годин, повідомлення з первісною оцінкою до 72 годин та фінальний звіт у визначений термін, що створює стандартизований "ритм прозорості" для ринків і регуляторів (European Union, 2022). Паралельно формується регуляторна логіка "безпеки за замовчуванням" для цифрових продуктів, яка стимулює виробників закладати у дизайн механізми відповідального управління вразливостями та інцидентами (European Commission, n.d.) (див. дод. Д).

Одночасно трансформується й технологічна парадигма: класична логіка "захисту периметра" (firewall як головна межа) переходить у режим кіберстійкості та Zero Trust, де базовим припущенням є неминучість проникнення. У такій моделі метою стає не "ідеальне недопущення інциденту", а здатність обмежувати масштаби компрометації, підтримувати безперервність критичних процесів і відновлюватися після атаки з контрольованими втратами (Rose et al., 2020). Слід зазначити прямий вплив на конкурентоспроможність: економічні системи, які скорочують час виявлення (MTTD) та відновлення (MTTR), демонструють вищу стійкість до операційних збоїв, менші непрямі втрати й більшу довіру інвесторів.

Органічним елементом еволюції виступає інституціоналізація кібергігієни. Те, що раніше сприймалося як набір "порад користувачу", набуває статусу політики: мінімальні контролі (MFA, менеджери паролів, патч-менеджмент, базове журналювання, навчання проти фішингу) інтегруються в державні закупівлі, галузеві вимоги та програмні критерії фінансування. На мікрорівні це створює "санітарний мінімум" кіберзахисту, а на мезорівні – знижує асиметрію

інформації між контрагентами й підвищує прогнозованість транскордонних угод. У підсумку кібергігієна переходить з площини індивідуальної поведінки в площину економічної інфраструктури довіри, що безпосередньо впливає на вартість ризику в міжнародних контрактах.

Важливим фактором на мезорівні є розвиток публічно-приватних механізмів взаємодії: галузевих груп обміну інформацією, центрів координації та спільних форматів розповсюдження індикаторів компрометації. Саме такі мережі забезпечують швидкість реакції та зниження каскадних ефектів, коли збій в одному секторі (наприклад, логістика чи енергетика) переноситься на інші компоненти економіки. У США та інших партнерських системах критичну роль в цій логіці відіграють ISAOs/ISACs як організаційні моделі для збору й поширення актуальної інформації про загрози (CISA, n.d.).

Окремим напрямом інституційної зрілості стала безпека ланцюгів постачання. Після хвилі атак через оновлення та сторонні компоненти регулятори переходять від формального due diligence до вимог "вбудованого контролю" для постачальників: наявність SBOM, контрактні гарантії строків усунення вразливостей, контроль процесів розробки та можливість швидкого видалення ризикових компонентів. Підхід SBOM інституційно оформлюється як мінімальний стандарт прозорості складу програмного продукту (аналог "інгредієнтів"), що спрощує управління вразливостями і скорочує час реагування (NTIA, 2021). Додатково, оновлені елементи мінімальних вимог SBOM підсилюють прикладну реалізацію цього інструменту для організацій і державних структур (CISA, 2025). На ринковому рівні це перетворюється на конкурентну перевагу: учасники з більш зрілими моделями supply chain security швидше проходять комплаєнс, отримують доступ до більших контрактів і знижують премію за ризик у міжнародних угодах.

Не менш важливою є тенденція зростання прозорості інцидентів: у різних юрисдикціях стандартизуються формати та строки повідомлень, що зменшує “приховані збитки” і вирівнює інформаційне поле для регуляторів, партнерів та інвесторів. Даний фактор підсилює ринкову дисципліну: організації змушені формувати процеси реагування не ситуативно, а як частину операційної моделі.

Стратегічною залишається й кадрова компонента. Без фахівців, здатних підтримувати процеси кіберстійкості, формальна наявність політик не створює реального захисту. Тому держави стимулюють розвиток міждисциплінарних освітніх програм (право + техніка + управління ризиками), симуляційних полігонів та спільних стажувань з приватним сектором. На практиці “готовність” дедалі частіше оцінюється через перевірювані спроможності: резервне копіювання, регулярні DR/BCP тести, tabletop-навчання, а також готовність до інцидент-репортингу в межах нормативних дедлайнів.

Геополітичний вимір посилився через розвиток кібердипломатії, механізмів атрибуції та санкційних режимів, а також через включення положень про кіберзахист і цифрові стандарти в торговельні домовленості. Це знижує координаційні витрати між юрисдикціями та формує “правила гри” для міжнародних ринків. Паралельно формується фінансова інфраструктура ризику – ринок кіберстрахування, який у зрілих моделях спирається на вимірювані метрики контролів (MFA coverage, середній час патчування, MTTD/MTTR, сегментація, якість резервних копій, наявність SBOM у постачальників). У результаті ціна ризику перетворюється на стимул до інвестицій у захист, а не лише на “штраф” після інциденту.

У підсумку інституційна логіка формує послідовний економічний ланцюг (рис. 2.1):

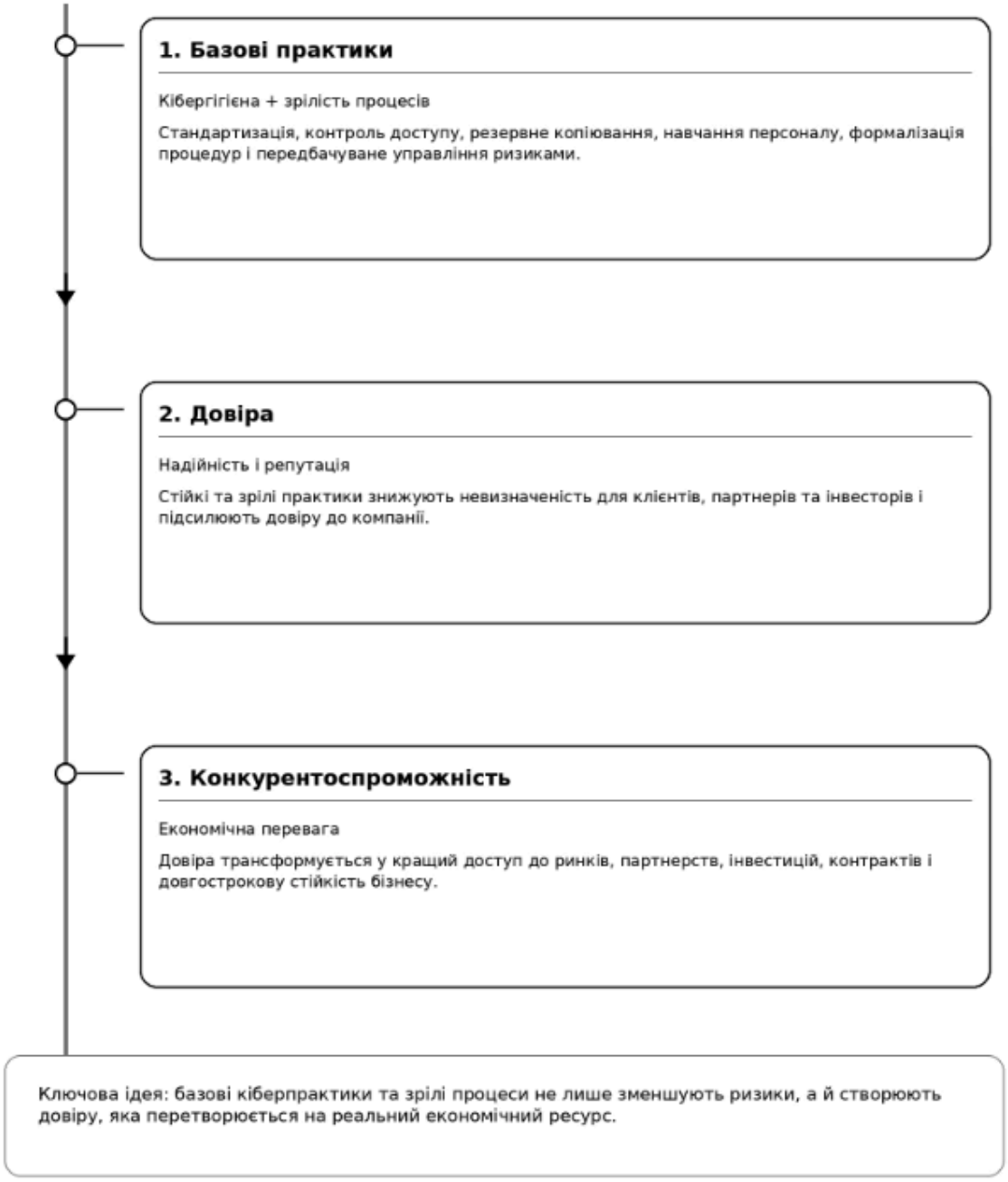

Рис. 2.1. Послідовний економічний ланцюг

Джерело: складено автором.

Чим більш вимірюваними й контрактно “вбудованими” є механізми безпеки на мікро- й мезорівнях, тим нижчою стає системна вразливість на макрорівні, тим кращий інвестиційний клімат і сильніша позиція країни в глобальних ланцюгах вартості. Для України та Східної Європи практичними пріоритетами виглядають: нормативна конвергенція з ЄС, масштабування галузевих центрів обміну інформацією, інституціоналізований інцидент-репортинг, а також контрактна комплаєнс-модель до постачальників у критичній інфраструктурі (рис. 2.2).

ТЕНДЕНЦІЯ	МЕХАНІЗМ РЕАЛІЗАЦІЇ	ПОКАЗНИКИ (ПРИКЛАДИ)	ЕКОНОМІЧНИЙ ЕФЕКТ
Інституціоналізація кібергігієни	Вимоги у держзакупівлях Вимоги у грантах Галузеві «мінімальні контролі»	% MFA-покриття Середній час патча Частота тренінгів	↓ Менше інцидентів ↓ Нижчі транзакційні витрати ↑ Більше довіри до систем
Supply Chain Security	SBOM (Software Bill of Materials) Due diligence постачальників SLA на виправлення вразливостей	Частка постачальників із SBOM Середній TTP на фікс	↑ Стійкі ланцюги поставок ↓ Менше каскадних збоїв
Zero Trust & Resilience	Мікросегментація EDR / XDR DR / BCP-тестування	MTTR / MTTD % сегментованих систем Успішність DR-тестів	↓ Менші макрозбитки ↑ Швидше відновлення
Прозорість інцидентів	Законодавчий інцидент-репортинг Імунітет за добросовісність	Частка інцидентів з disclosure Час сповіщення (год)	↑ Краща ринкова дисципліна ↑ Стабільніший інвестклімат
Кадрова спроможність	Освітні програми Кіберполігони Держ-приватні стажування	Випускників / рік Сертифікації % закритих вакансій	↓ Менший кадровий дефіцит ↑ Вища якість контролів

Рис. 2.2. Політична матриця заходів кібербезпеки

Джерело: складено автором.

Таким чином, усі зазначені тенденції зводяться до простої, але стратегічної логіки: чим більш вимірюваною та контрактно «вбудованою» є безпека на мікро-

й мезорівнях, тим нижчою стає системна вразливість на макрорівні, тим вища довіра до національної економіки й тим сильніша її міжнародна конкурентоспроможність.

2.2. Аналіз сучасного стану економічної безпеки України

Сучасний стан економічної безпеки України визначається дією довготривалих шоків війни, високою інтенсивністю гібридних загроз і постійним тиском кібероперацій на критичну інфраструктуру. На цьому тлі безпекова парадигма еволюціонує від класичної логіки «захистити периметр, зберегти виробництво» до управління стійкістю складних систем: швидкого виявлення інцидентів, локалізації шкоди, підтримання безперервності послуг (зокрема енергетичних, фінансових, телекомунікаційних) та відновлення у гарантовані терміни (CERT-UA, n.d.). Ключову роль у цій трансформації відіграє IT-сектор, який став одночасно драйвером експорту, джерелом компетенцій у сфері кіберзахисту та інституційним партнером держави.

ЕБ у воєнних умовах має кілька взаємопов’язаних контурів. Перший – макрофінансова стабільність і функціонування платіжної інфраструктури; другий – стійкість критичних мереж (енергосистема, зв’язок, транспорт, логістика); третій – довіра до цифрових державних сервісів і приватних платформ, яка є передумовою податкових надходжень, контрактної дисципліни та доступу до зовнішніх ринків капіталу. У кожному з цих контурів IT-компетенції стали частиною «базової комплектації» безпеки: від сегментації мереж і впровадження Zero Trust-підходів до побудови резервних маршрутів даних і хмарної оркестрації критичних процесів (CSIRT NCCC, n.d.).

Нами встановлено, що роль IT-сектору України в системі забезпечення глобальної кібербезпеки є багатовимірною й не зводиться до простої

«аутсорсингової» моделі (Мирончeнко & Сидоренко, 2023). Йдеться про формування стійкого кадрового ядра безпеки, що охоплює інженерів захисту (SecEng/CloudSec/OT-Sec), аналітиків SOC (L1–L3), фахівців DFIR і threat intelligence, архітекторів Zero Trust, GRC-команди (ISO 27001/SOC 2/NIST/PCI DSS), а також розробників безпечного ПЗ (DevSecOps, S-SDLC). На практиці це означає здатність вести повний цикл: від проактивного моніторингу (MDR/XDR) і загрозової аналітики до реагування на інциденти та відновлення критичних сервісів із гарантованими SLA (Мирончeнко & Сидоренко, 2023). В умовах війни відбулася прискорена дифузія практичного досвіду: команди переходять від «книжкових» моделей до відпрацьованих плейбуків і runbook-сценаріїв, що скорочує MTTD/MTTR не лише в межах окремих компаній, а й у критичних секторах економіки загалом (NIST, n.d.).

Другою площиною виступає експорт кіберпослуг і рішень як «твердий» канал валютної виручки, менш чутливий до фізичної логістики. Українські провайдери безпеки працюють із замовниками в ЄС і США як керовані центри (MDR/SOC-as-a-Service), постачають DFIR-команди «під ключ», threat-intel-аналітику, Red/Blue/Purple-team тестування, побудову Zero Trust-архітектур у хмарі та консалтинг із відповідності актуальним регуляторним вимогам. Поряд із сервісами формується продуктова компонента (контент для SIEM/EDR, плейбуки SOAR, модулі deception/honeypots, моніторинг OT/ICS), що збільшує капіталізацію компетенцій і нарощує репутаційний ресурс країни як «постачальника довіри» в глобальних ланцюгах вартості (Мирончeнко & Сидоренко, 2023).

Третій вимір – публічно-приватні зв’язки між державними командами реагування та приватними SOC/CSIRT. Їхня цінність полягає не просто в обміні індикаторами компрометації, а в скороченні «вікна експлуатації» вразливостей на системному рівні: рекомендації щодо mitigation швидко проходять шлях від

CERT/CSIRT до галузевих структур і далі – у плейбуки та кореляційні правила SIEM приватного сектора (CERT-UA, n.d.). Узгоджені навчання та спільні розбори інцидентів знижують інформаційну асиметрію між ринком і державою, а ефект масштабу критично підвищує стійкість суміжних сервісів (платежі, енергетика, телекомунікації) (CERT-UA, n.d.).

Четвертий аспект – кластеризація IT-ринку, яка перетворює окремі компетенції на екосистему стійкості. Регіональні IT-кластери здатні діяти як інтегратори освітніх треків, лабораторій і стартап-інкубації, прискорюючи дифузію «мінімальних контролів» (MFA, патч-менеджмент, резервування з розривом доступу, сегментація) у бізнес та непрофільні сектори. Додатковим прискорювачем виступає інтеграція в європейські інноваційні мережі та програми підтримки, зокрема через European Digital Innovation Hubs (EDIH) і проєктні можливості Horizon Europe у напрямі безпеки, приватності та довіри (European Commission, n.d.).

Кожен із зазначених вимірів прямо конвертується в показники економічної безпеки. Кадровий пул і плейбуки, що пройшли «бойове загартування», скорочують MTTD/MTTR і обмежують макрошок від інцидентів (зрив виробництва, простої логістики, каскадні збої). Експорт кіберпослуг диверсифікує валютну виручку й підсилює кредитоспроможність на зовнішніх ринках. Публічно-приватні канали зменшують координаційні витрати та роблять прозорість інцидентів не репутаційною загрозою, а інструментом ринкової дисципліни (CERT-UA & Industrial Cyber, n.d.). В такому контексті стійкість і довіра формуються як економічні активи: суб’єкти, що демонструють вимірювану дисципліну безпеки, отримують кращі умови контрактування та доступ до довших угод.

Війна стала стрес-тестом для цифрової стійкості. Кібератаки на державні реєстри, телекомунікаційні та інші критичні сервіси підсилили вимогу до

резервування, геореплікації, мікросегментації та перевірюваних процедур відновлення (Reuters, 2024; The Record, n.d.). Одночасно зросла увага до безпеки ланцюгів постачання: аудит сторонніх компонентів, контроль CI/CD процесів, договірна відповідальність за строки усунення уразливостей і відмова від непрозорих компонентів. Це прямо підвищує інвестиційну привабливість і знижує ризикові премії в експортних контрактах у секторах, де надійність цифрових процесів є критичною умовою участі в міжнародних ринках.

Таким чином, багатовимірна роль українського ІТ-сектору в глобальній кібербезпеці – це не лише про технології, а про економіку довіри. Коли «просте» (кібергігієна, мінімальні контролі, прозора інцидентність) стає масовим стандартом, країна отримує «премію за передбачуваність» у вигляді нижчих транзакційних витрат, вищої інвестиційної привабливості та стійкіших ланцюгів постачання. Саме в цій логіці – «кібергігієна → довіра → конкурентоспроможність» – ІТ-сектор виступає мультиплікатором економічної безпеки України і джерелом її довгострокової міжнародної репутації як надійного партнера з безпеки (Мирончeнко & Сидоренко, 2023).

З огляду на зазначене, релевантним є підсумковий «зріз» стану економічної безпеки України крізь призму кібервиміру та ролі ІТ-сектору (рис. 2.3).

ПІЛЛАР (ВУЗОЛ СТІЙКОСТІ)	ПОТОЧНИЙ СТАН / ТЕНДЕНЦІЇ	ОСНОВНІ ВРАЗЛИВОСТІ	РОЛЬ ІТ-СЕКТОРУ
Макрофінансова інфраструктура (платежі, банкінг)	– Висока цифрова зрілість – Швидка міграція у хмари – Безперервність платежів	⚠ Тиск на канали зв'язку ⚠ Таргетовані атаки на платіжні шлюзи	MDR / SOC-послуги Поведінкова аналітика Red Team-тестування
Енергетика та зв'язок	– Відмовостійкі архітектури – Резервування каналів – Геореплікація даних	⚠ Каскадні ризики та фізичні руйнування ⚠ Supply-chain атаки на обладнання	Системи моніторингу OT-безпека Сегментація мереж SBOM Аудит постачальників
Держсервіси та реєстри	– Розвиток е-сервісів – Відпрацьовані процедури відновлення	⚠ Інтерес супротивника до реєстрів ⚠ Атаки на канали автентифікації	Zero Trust-архітектури Крипто- та ключове управління BCP / DR-сценарії
Приватний сектор (МСП / експорт)	– Широка дистанційна зайнятість – Зрілі DevSecOps-практики у лідерів	⚠ Нерівномірність практик безпеки ⚠ Дефіцит кадрів у МСП	Освітні платформи Керовані сервіси безпеки Стандартна «мінімалка» контролів
Міжнародна репутація / довіра	– Зростання попиту на кіберпослуги з України – Активна міжнародна кооперація	⚠ Фоновий геополітичний ризик	Експорт експертизи Quick-response команди Участь у CERT / ISAC

Рис. 2.3. Піллари стійкості цифрової інфраструктури

Джерело: складено автором.

Необхідним є дослідження аналітичних індикаторів кіберстійкості та міжнародної конкурентоспроможності України. Динаміка кіберінцидентів: інтенсивність загроз і зростання керованості. У 2024 році CERT-UA опрацювала 4 315 кіберінцидентів, що означає зростання майже на 70% порівняно з попереднім роком. Динаміка за роками демонструє стійкий тренд ескалації кібертиску: 2021 – 1 350, 2022 – 2 194, 2023 – 2 543, 2024 – 4 315 (SSSCIP, 2024). Наведена статистика підтверджує, що кіберпростір для України став системним контуром ризику, який впливає на державне управління, оборонну сферу та економічні процеси.

Водночас структурний аналіз інцидентів у 2024 році виявляє важливу зміну: кількість інцидентів у H2 2024 становила 2 576 проти 1 739 у H1 2024, тобто приріст +48% у другому півріччі (SSSCIP, 2024). З позиції макроекономічної стійкості це є сигналом про зростання "навантаження" на інституційні системи реагування та управління кризами – від державних CERT/CSIRT до корпоративних SOC.

Показовим є те, що на тлі збільшення загальної кількості подій відбулося суттєве зниження частки інцидентів високої/критичної тяжкості: у H2 2024 зафіксовано падіння high/critical з 48 до 11, тобто -77% (SSSCIP, 2024). Зазначене дозволяє інтерпретувати ситуацію як підвищення керованості ризику: при зростанні атакованості систем економіки держава та критичні сектори демонструють кращу здатність до локалізації шкоди, стабілізації сервісів та зниження ймовірності каскадних збоїв.

Найбільш ураженими сферами у H2 2024 були: державний сектор і місцеве самоврядування, оборона, енергетика, телеком/IT (SSSCIP, 2024). Саме ці сектори є ядром економічної безпеки, оскільки формують стійкість управлінських рішень, енергетичного забезпечення, цифрових каналів взаємодії держави і бізнесу, а також підтримують безперервність критично важливих послуг.

Додатково, вторинні міжнародні медіа-джерела підтверджують загальний тренд: зростання інцидентів у 2024 році приблизно на 70% та збільшення атак у H2 відносно H1 (Dark Reading, n.d.). Їх слід враховувати не як основне джерело, а як індикатор міжнародного сприйняття української кіберстійкості та її значення для глобального ризик-ландшафту (рис. 2.4).

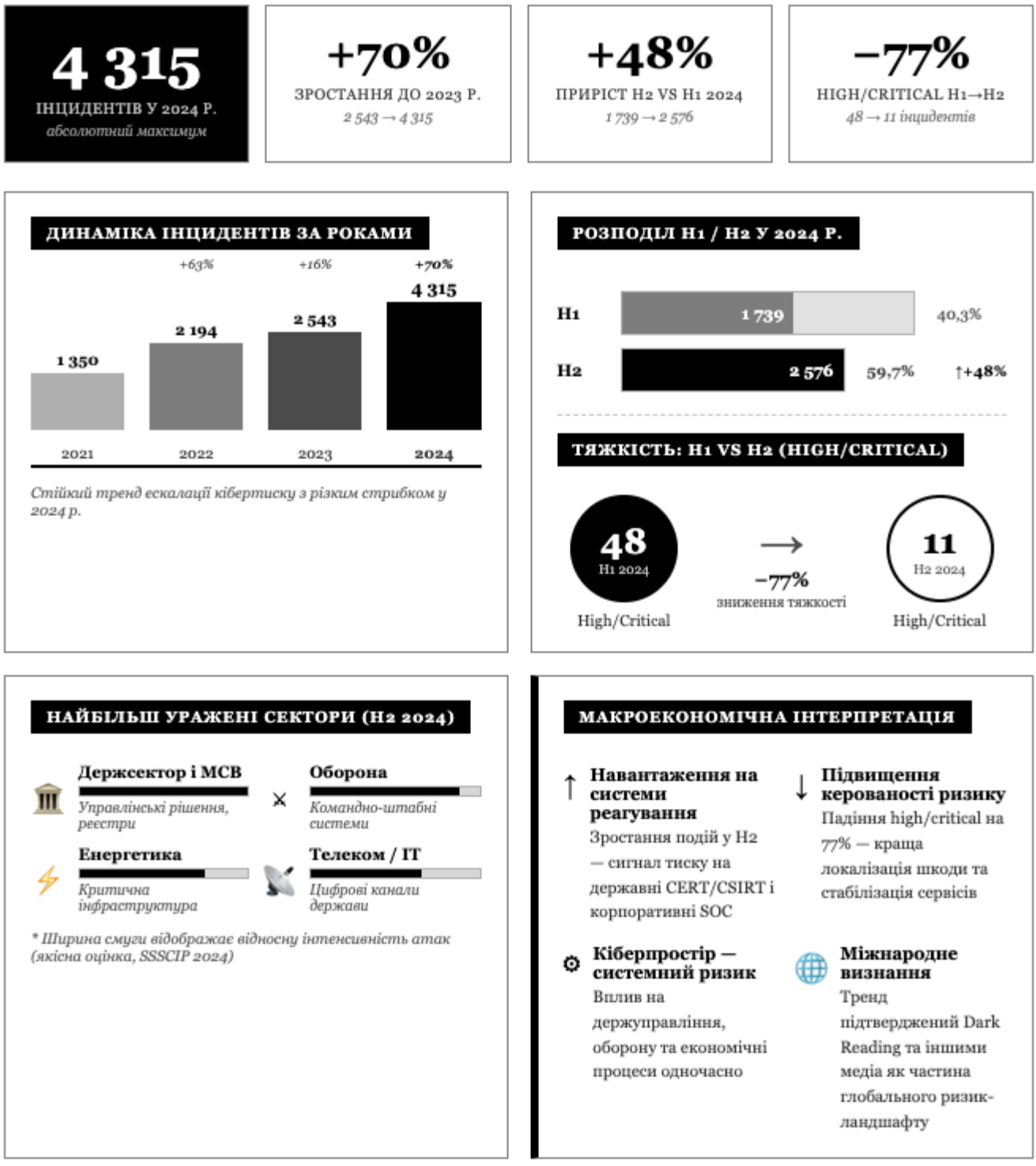

Рис. 2.4. CERT-UA: динаміка кіберінцидентів в Україні (2021-2024)

Джерело: складено автором.

Експорт ІТ-послуг є фактором конкурентоспроможності та економічної стійкості країн. В умовах воєнних ризиків ІТ-сектор України залишається одним із ключових каналів зовнішньоекономічної стабільності. За даними IT Ukraine Association у звіті Digital Tiger 2024, обсяг експорту ІТ-послуг у 2024 році склав 6,4 млрд дол. США, а динаміка 2019–2024 демонструє зростання від 4,2 млрд дол. США до 6,4 млрд дол. США (IT Ukraine Association, 2024). Це означає, що цифрові послуги виконують роль експортного "амортизатора", менш залежного від фізичної логістики, транспортних обмежень та руйнування інфраструктури.

Структурно важливо, що ІТ має значну вагу в зовнішньоекономічній системі країни:

- частка ІТ у загальному експорті послуг – 37,4%;
- частка ІТ у сукупному експорті товарів + послуг – 11,5% (за 2024 рік) (IT Ukraine Association, 2024).

Дані показники мають прямий зв'язок із конкурентоспроможністю: країна, яка зберігає масштабну присутність на глобальному ринку цифрових сервісів, отримує стабільніші валютні надходження, кращу інституційну репутацію та ширший доступ до довших контрактів у міжнародних ланцюгах вартості. Додаткові публікації на основі Digital Tiger 2024 повторюють ці показники як підтвердження з боку медіа-аналітики, однак методологічно доцільно залишати основним джерелом саме офіційний звіт асоціації (рис. 2.5).

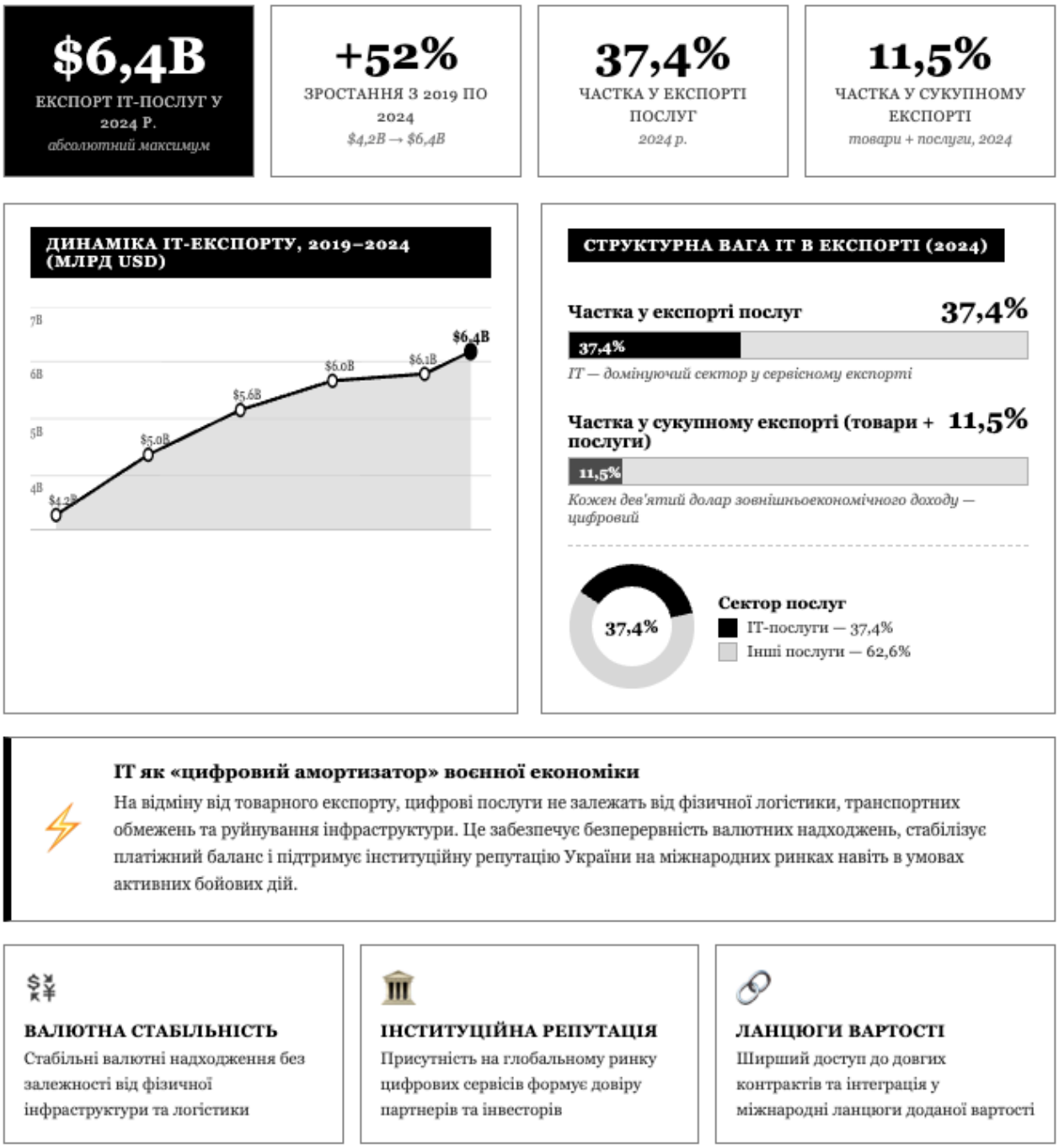

Рис. 2.5. ІТ-Експорт України: цифровий амортизатор воєнної економіки

Джерело: складено автором.

Паралельно зі збільшенням зовнішнього кібертиску в Україні зростає внутрішній попит на кіберзахист як на економічну функцію. За оцінкою IT Ukraine Association, обсяг ринку кібербезпеки у 2024 році становив близько 138 млн дол. США, а за попередні 8 років він зріс у 4 рази. Найшвидше зростаючими сегментами визначено хмарну безпеку, захист даних та endpoint-безпеку (IT Ukraine Association, n.d.). Це демонструє перехід від реактивного “закриття інцидентів” до моделі інвестицій у стійкість та базові механізми цифрової довіри (рис. 2.6).

Рис. 2.6. Ринок кібербезпеки України: зростання внутрішнього попиту

Джерело: складено автором.

Таким чином, державні комунікаційні ресурси також повторюють зазначені оцінки й прогнозують подальше зростання ринку, трактуючи його як елемент цифрової стійкості та інтеграції у міжнародні підходи до управління ризиком

(Ministry of Digital Transformation of Ukraine, n.d.). У поєднанні з даними CERT-UA це формує узгоджену картину: кількість атак зростає, але економіка одночасно нарощує спроможність захисту та ринкову інфраструктуру безпеки, що знижує ймовірність системних збоїв.

2.3. Безпекове середовище та актуальні кіберзагрози національним інтересам України

Поточне безпекове середовище України формується високою інтенсивністю гібридної війни, де кібератаки набули системного та транскордонного характеру, прямо впливаючи на економічну стійкість, здатність держави підтримувати критичні послуги та забезпечувати зовнішньоекономічну діяльність. Водночас спостерігалося зменшення частки high/critical-інцидентів, що може свідчити про зміщення активності атакуючих у бік масових дій проти доступності та «тихих» кампаній кіберрозвідки в мережах пріоритетних секторів.

Така картина загалом узгоджується з європейськими оцінками ризиків: у ENISA Threat Landscape 2024 провідною групою загроз визначено threats against availability (передусім DDoS), далі – ransomware і загрози для даних (конфіденційність/цілісність). Для економік, що спираються на цифрові сервіси та безперервність мереж, саме атаки на доступність стають швидким способом масштабного порушення бізнес-процесів і державних функцій.

З позиції національних інтересів найбільш уразливими лишаються енергетика, телекомунікації, фінансовий сектор, державні цифрові сервіси, а також транспортно-логістичні коридори. Саме логістика виступає критичним вузлом: вона забезпечує комерційні потоки та оборонно-гуманітарну підтримку, тому закономірно входить до периметра пріоритетних операцій державних (state-nexus) акторів.

Показовим є спільне попередження партнерських відомств на чолі з CISA, де зафіксовано цілеспрямоване полювання на західні логістичні та технологічні компанії, пов’язані з підтримкою України. Серед тактик зазначаються spearphishing, експлуатація периферійних пристроїв і спроби доступу до IP-камер/сенсорики вздовж маршрутів транспортування. У практичному вимірі це створює загрозу кібербезпеці бізнесу, стійкості ланцюгів постачання, вартості страхування, ризикових премій та очікуваних втрат від простоїв.

Транспортна інфраструктура також виступає кіберфізичною системою ризиків. Адже транспорт доцільно розглядати як єдину кіберфізичну систему, де цифрові сервіси керують фізичними потоками, а будь-яка «цифрова подія» здатна спричиняти каскадні матеріальні наслідки – від затримок і черг до зупинок операцій (Мирончeнко, Сидоренко, 2025).

Критичне зростання поверхні атаки пояснюється поєднанням кількох довготривалих трендів:

- цифровізація диспетчеризації та управління потоками (планування, графіки, доступи, маршрути);
- масштабування IoT/IIoT і сенсорики (камери, шлагбауми, трекінг, телеметрія);
- перехід до моделей віддаленого управління та сервісних платформ;
- залежність від хмарних SaaS, API-інтеграцій та провайдерів даних;
- «спадковість» OT/ICS-рішень і протоколів із недостатніми вбудованими механізмами безпеки.

У такій архітектурі формуються вузли концентрації ризику, зокрема:

- портові TOS/термінальні операційні системи;
- системи планування руху (залізниця/станції/коридори);
- білетингові та платіжні підсистеми;
- митне «єдине вікно», шлюзи обміну даними;

- BGP/DNS та канали зв’язку реального часу;
- постачальники картографії/навігації та маршрутних сервісів.

Будь-яка компрометація в такому вузлі здатна поширюватися через мережеві залежності: один уразливий апдейт, слабка інтеграція API або помилка конфігурації можуть трансформуватися у зупинку термінальних операцій, колапс черг на кордоні або зрив графіка руху.

Прикладовий ландшафт атак проти транспортних систем найчастіше включає:

- маніпуляції сенсорними даними (GNSS spoofing, підміна відеопотоку, фальсифікація телеметрії);
- компрометацію управлінських платформ через ключі/токени, помилки доступу, слабку сегментацію;
- атаки на оптимізаційні системи (data poisoning) для створення керованих збоїв;
- ransomware / деструктивні кампанії проти операційних платформ;
- атаки на провайдерів навігації/маршрутизації;
- supply-chain сценарії через бібліотеки, прошивки, CI/CD або сторонні модулі.

Найнебезпечніше те, що слабкі місця часто виникають на стику OT та IT: застарілі контролери й шлюзи без повної автентифікації під’єднані до сучасних MES/ERP через «тимчасові» інтеграції, які стають постійними; сегментація – формальна; журнали – неповні або несинхронізовані; оновлення – нерегулярні; інвентар активів – із запізненням.

Економічна значущість таких вразливостей полягає у тому, що транспорт є конденсатором ланцюгів постачання. Збій у цифровій підсистемі одного модуля породжує каскад: блокування операцій → простої суден/вагонів → штрафи та демередж → зупинки виробництва через нестачу компонентів → зростання страхових премій і вартості капіталу (рис. 2.7).

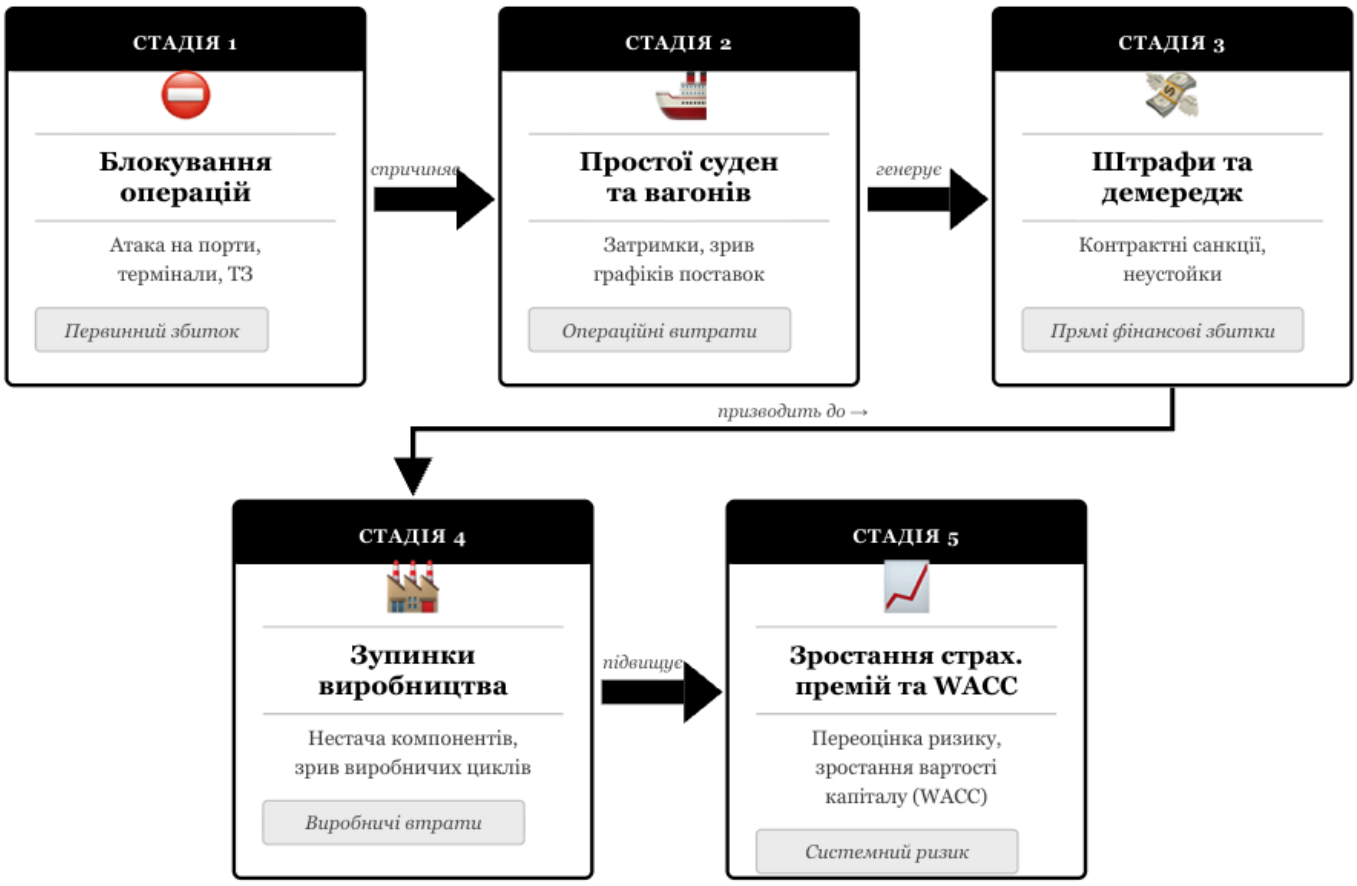

Рис. 2.7. Каскадний ланцюг економічних втрат

Джерело: складено автором.

У умовах війни такий ефект посилюється: часові лаги коротші, резервні маршрути перевантажені, політичний ризик підвищує ціну навіть «локальної

помилки». Тому інцидент у митній або платіжній підсистемі інколи має наслідки, співставні з ударом по енергетиці – через масштаб взаємозалежностей.

Матриця контролів у кіберфізичних системах (особливо там, де є OT/ICS) має будуватися як послідовний ланцюг – від правильного проєктування архітектури до керованої довіри до даних, на яких тримаються операційні рішення. Логічна точка старту тут – архітектурне управління ризиком, тому що саме архітектура визначає, наскільки легко інцидент "розповзається" системою. У практичному вимірі це означає впорядковану сегментацію OT/ICS із чітко визначеними зонами, контрольованими переходами між ними та мінімально необхідними "містками" до офісного IT. Коли інтеграції OT↔IT залишаються постійними, багатофункціональними і погано задокументованими, будь-яка компрометація в одному контурі швидко стає проблемою всього середовища. Тому важливо не лише "розрізати" мережу на зони, а й дисциплінувати самі переходи: обмежувати маршрути, протоколи, ролі доступу й механізми автентифікації, а також чітко фіксувати, які саме дані йдуть між доменами та з якою метою.

Другий фундаментальний елемент – повна видимість активів. У OT-ландшафті невідомі або "забуті" пристрої, старі шлюзи, допоміжні сервери, тестові контролери чи тимчасові VPN – є фактичними точкам входу. Тому інвентаризація має бути постійним процесом з авто-виявленням активів і підтриманням "цифрового паспорта" для кожного критичного компонента: тип і функція, версії прошивок і ПЗ, вендор і модель, критичність для процесу, залежності від інших вузлів, а також мінімальні вимоги до оновлення та доступів. Саме "паспорт" дозволяє переходити від абстрактних політик до конкретних рішень: що оновлювати першочергово, де потрібні компенсуючі контролі, які вузли мають бути ізольовані, а які – дубльовані.

Коли архітектура та активи поставлені на облік, наступний шар – моніторинг і виявлення аномалій, тобто здатність помічати відхилення від нормального технологічного процесу. Для ОТ це часто ефективніше, ніж класичні сигнатури: важливо знати, які команди зазвичай ходять у мережі, у якій послідовності, з якою частотою, і що є “нетиповим” для конкретної зміни, лінії чи режиму роботи. Поведінкові профілі ОТ-протоколів і контроль нетипових команд дають шанс зловити інцидент на ранній стадії – ще до того, як він перейде у фізичні наслідки. У сучасних середовищах зростає й окрема категорія ризику – довіра до сенсорних даних. Якщо диспетчеризація, оптимізація маршрутів або автоматичні рішення залежать від телеметрії, GPS/GNSS, відеопотоків чи датчиків, то атаки на дані (спуфінг, підміна, отруєння) можуть бути не менш небезпечні, ніж ransomware. Тому потрібні перехресні перевірки (sensor fusion), порівняння кількох джерел даних, механізми виявлення “надто ідеальних” або статистично неприродних потоків, а також контроль часових ланцюгів – синхронізація часу, захист NTP/PTP, часові підписи, контроль цілісності даних у транзиті. У підсумку формується керована модель довіри: системі дозволено “вірити” даним лише настільки, наскільки ці дані проходять перевірки на цілісність і узгодженість.

Окремим, але рівнозначно важливим контуром виступає безпека ланцюгів постачання, оскільки сучасні інциденти часто приходять не через прямий “злам”, а через оновлення, сторонні бібліотеки, інтеграційні модулі, прошивки або підрядників. Тут контроль починається з SBOM і прозорості компонентів: організація має знати, з чого складається критичний софт і які залежності можуть принести уразливість. Але SBOM сам по собі не “лікує” – він стає основою для політики оновлень і вимог до постачальників. Тому необхідні регулярні, безпечні оновлення з контрольованим розгортанням (наприклад, canary-підхід), а також контрактна дисципліна: SLA на строки закриття критичних і високих

уразливостей, право аудиту процесів безпеки постачальника, вимоги до підпису артефактів і перевірки цілісності, а у критичних вузлах – обмеження використання непрозорих “чорних ящиків”, де немає ні технічної прозорості, ні можливості швидкого вилучення ризикового компонента. Практично це переводить supply chain із абстрактного “ризику” у керований параметр контракту й комплаєнсу.

Нарешті, будь-яка матриця контролів буде неповною без блоку відмовостійкості та відновлення, бо сучасна парадигма виходить із того, що проникнення можливі, а інколи – неминучі. Тому питання звучить не “чи станеться інцидент”, а “якою буде його межа і скільки коштуватиме відновлення”. Дане твердження вимагає формалізованих DR/BCP-процедур із чіткими RTO/RPO, геореплікації даних на незалежні домени керування та заздалегідь продуманих режимів graceful degradation: коли частина цифрових функцій недоступна, система має зберігати керованість у ручних або автономних сценаріях (локальні списки доступу, паперові накладні, автономні контури керування, спрощені режими диспетчеризації). Критично важливо, щоб такі плани існували не “в документах”, а перевірялися: регулярні table-top тренування, live-fire вправи, розбір інцидентів і оновлення runbooks дають операційним командам реальну спроможність діяти під тиском часу, а не тільки відповідати стандартам на папері.

У результаті така матриця контролів створює єдину логіку керованої стійкості: архітектура обмежує масштаб інциденту, видимість активів зменшує сліпі зони, моніторинг і валідація даних скорочують час до виявлення та знижують ризики маніпуляцій, контроль постачальників зменшує каскадні сценарії, а відмовостійкість гарантує, що навіть за найгірших умов втрати будуть локалізовані в просторі та часі. Тобто формується практичний перехід від “захищати периметр” до “підтримувати стійкість”, коли безпека працює як

інструмент збереження безперервності критичних функцій і довіри до даних (рис. 2.8).

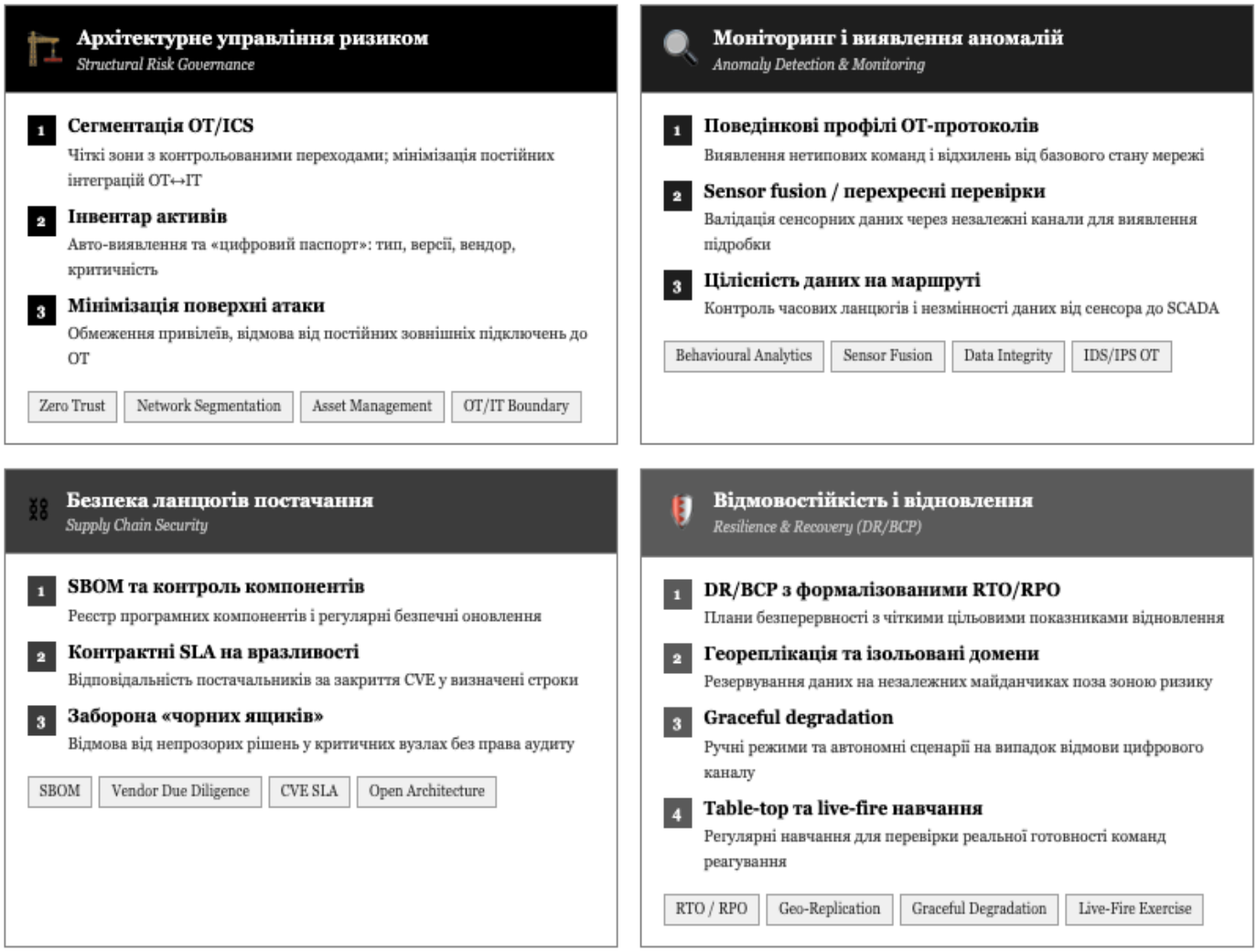

Рис. 2.8. Системна матриця контролів для захисту критичної інфраструктури

Джерело: складено автором

Стратегічний ефект досягається тоді, коли мінімальна планка контролів стає умовою участі у критичних ланцюгах: для портів, вокзалів і митних вузлів це означає перехід від логіки «слабкої ланки» до логіки керованої стійкої мережі, де інцидент не паралізує систему та залишається обмеженим у просторі та часі.

Розглядаючи «другий пласт», варто підкреслити: цифрова трансформація стартапів і малих технологічних компаній одночасно створює ривок у швидкості виходу на ринок і розширює площу атаки. Нами встановлено, що перехід до cloud-native та API-first архітектур, активне використання CI/CD-пайплайнів і залежність від глобальних SaaS-провайдерів переводять організації у «швидкий контур» розробки, де будь-який інтеграційний API, будь-який секрет у пайплайні чи артефакт збірки стає потенційною точкою компрометації. Відповідно, безпека в такому середовищі має бути частиною дизайну – security-by-design.

Практично це означає формування «мінімального, але достатнього» ядра контролів уже на ранніх стадіях масштабування: централізований секрет-менеджмент (KMS/Vault) із ротацією ключів і забороною hardcoded secrets; hardening CI/CD (підпис артефактів, ізоляція раннерів, контроль доступів до репозиторіїв, валідація залежностей); принцип найменших привілеїв (RBAC/ABAC) для сервісів та інтеграцій; резервування критичних даних і сценарії відновлення з визначеними RTO/RPO; рання прив’язка до базових рамок довіри та комплаєнсу – насамперед ISO/IEC 27001 як системи менеджменту інформаційної безпеки та SOC 2 як практичного механізму підтвердження контролів довіри для сервісних компаній, що працюють з даними клієнтів (ISO, 2022; AICPA & CIMA, n.d.). Для стартапів і підприємств, які діють як постачальники важливих секторів або інтегруються в європейські ланцюги створення вартості, значення цих підходів підсилюється переходом ЄС до більш жорстких вимог кіберстійкості в межах NIS2, де управління ризиками й інцидентами стає виступає частиною нормативної відповідальності (European Union, 2022).

Проаналізовані кейси (CentralNic, Quadient, Barcelona smart city, Hubs/Protolabs Network) ілюструють ключову дилему відкритих екосистем: мережеві ефекти та API-економіка радикально прискорюють інновації, але

одночасно переносять ризики постачальників усередину продукту. У доменно-реєстраторських платформах типу CentralNic сотні інтеграцій, делеговані авторизації та зовнішні сервіси створюють ситуацію, коли помилковий scope у OAuth або витік токена CI/CD здатні запустити ланцюговий інцидент. Корпоративні платформи класу Quadient вимагають жорсткої дисципліни управління ключами, каналами доступу та журналюванням змін, оскільки масштаб клієнтського середовища множить ціну помилки. Міські цифрові екосистеми на прикладі Барселони демонструють, що ефективне управління ризиком виходить за межі технічних заходів: етичне управління даними (прозорість, підзвітність, принципи «суверенітету даних») може знижувати ризики «інфраструктурного спостереження» без гальмування інновацій. Узагальнений висновок тут є системним: відкритість є конкурентною силою лише за умови керованих постачальницьких ризиків і вбудованих стандартів обробки даних; інакше вразливості масштабуються разом із продуктом.

На макрорівні дані спостереження корелюють із сучасними глобальними оглядами: складність кіберландшафту зростає швидше, ніж спроможність стартапів та підприємств будувати повний стек захисту, а «кібернерівність» між ними та великими компаніями поглиблюється (WEF, 2024). В таких умовах практичним рецептом стають керовані сервіси безпеки (MDR/XDR/SIEM/SOAR-as-a-Service), стандартизований «мінімальний пакет» контролів як умова контрактування, а також сувора гігієна постачальників – прозорість компонентів, контроль оновлень і договірні SLA на виправлення уразливостей. У підсумку цифрова трансформація прискорює міжнародну конкурентоспроможність стартапів та паралельно робить кібербезпеку їхньою базовою економічною компетенцією: довіра клієнтів і партнерів формується не деклараціями, а перевірюваними практиками контролю ризиків, стійкості та відповідності вимогам.

Для формалізації підходу до управління ризиками у cloud-native / API-first стартапі доцільна матриця «ризик → контроль → метрика» (рис. 2.9).

⚠ РИЗИК (CLOUD / API / SAAS)	КОНТРОЛЬ БЕЗПЕКИ (SECURITY-BY-DESIGN)	ЯК ВИМІРЯТИ ВИКОНАННЯ
CI/CD **Компрометація секретів у CI/CD**	• Централізований секрет-менеджмент • Підпис артефактів (artifact signing) • Ізоляція runner'ів від виробничих середовищ	% сервісів із керованими секретами % артефактів із підписом Periodicity ротації ключів
API **Зловживання API (BOLA / BFLA, масові витоки)**	• Тонка авторизація на рівні об'єктів та функцій • Rate-limits та throttling • Валідація схем запитів і відповідей	Покриття тестами авторизації % endpoint'ів із rate-limit Частка 429/403 у пікових навантаженнях
SAAS / OAUTH **SaaS-to-SaaS ланцюжки (OAuth-делегування)**	• Мінімальні scopes (principle of least privilege) • Регулярний review активних дозволів • Повне журналювання OAuth-потоків у SIEM	% інтеграцій зі scoped tokens Середній «вік» активних токенів Покриття OAuth-логів у SIEM
SUPPLY CHAIN **Supply-chain у бібліотеках / SDK**	• SBOM та контроль залежностей • Policy-as-code у пайплайні (gate-перевірки) • Обов'язкові оновлення при виявленні CVE	Покриття SBOM (%) Час встановлення патча на CVE (MTTR) Частка пакетів, заблокованих політикою
ДОСТУПНІСТЬ **Втрата / недоступність даних у SaaS**	• Escrow-резерви поза хмарою постачальника • Geo-реплікація на незалежні домени • RTO/RPO зафіксовані у контрактах SLA	Частота успішних відновлень Результати RTO/RPO-тестів Наявність та актуальність escrow-угод
NIS2 **Інцидент-репортинг (рамки NIS2)**	• 24h early-warning / 72h повне повідомлення • Таблиці ескалації та відповідальних осіб • Формалізовані шаблони звітності	Середній час формалізації повідомлення Частка інцидентів із повним пакетом даних

Рис. 2.9. Матриця «ризик → контроль → метрика»

Джерело: складено автором

Щоб інтеграція вимог безпеки не виглядала як разова «велика трансформація», доцільно розкладати її на послідовні етапи зрілості, синхронізовані з природною логікою розвитку технологічної команди та продукту. На ранніх стадіях стартапу важливо закрити найризиковіші першопричини інцидентів і прибрати найболючіші точки компрометації, які найчастіше з'являються саме у швидкому циклі розробки. Тому на рівні Pre-seed/Seed основа безпеки має бути максимально практичною і легкою у впровадженні: централізований секрет-менеджмент замість ключів у репозиторіях і чатах, обов'язкова MFA та SSO для критичних сервісів, а також базове журналювання доступів, щоб у разі інциденту можна було відновити картину подій. Тут же важливо закласти перші елементи керованої прозорості в ланцюгу постачання – принаймні SBOM у збірці, щоб розуміти залежності й швидко реагувати на уразливості сторонніх компонентів. Додатково критичною «гігієнічною» практикою стає патч-менеджмент: не стільки складні процеси, скільки дисципліна оновлень і фіксовані вікна для їх встановлення. І нарешті, резервне копіювання виступає механізмом забезпечення безпеки: регулярні бекапи з тестами відновлення виступають мінімальною страховкою від сценаріїв, де навіть невеликий інцидент може загрожувати зупинці бізнесу.

Коли продукт доходить до Series A і зростає складність архітектури, команда вже не може спиратися лише на «базові практики», бо збільшується кількість інтеграцій, ролей, середовищ і залежностей – а разом із цим зростає і площа атаки. На даному етапі логічним кроком є формалізація життєвого циклу безпеки в розробці: S-SDLC та DevSecOps перестають бути "ідеєю" і перетворюються на набір стандартних процедур для планування змін, рев'ю, сканування, підпису артефактів і контролю конфігурацій. Паралельно, щоб закрити розрив між можливостями команди і реальним рівнем загроз, ефективніше підключити керовані сервіси – MDR/XDR/SIEM-as-a-Service, які

дають 24/7 спостереження і підтримку реагування без надмірного навантаження на інженерів продукту. Важливо також навести лад у доступах: вводиться рольова модель (RBAC/ABAC), що мінімізує надлишкові привілеї та робить контрольованою роботу з адмінськими правами. Окремо команда повинна знати, що саме в неї «підключено» і як працює взаємодія між системами: інвентар активів і інтеграцій стає такою ж базовою практикою, як інвентар коду. На цьому ж рівні доцільно вбудувати процедури інцидент-репортингу 24h/72h із чіткими ескалаціями, щоб компанія могла діяти швидко, скоординовано і передбачувано – як для клієнтів, так і для регуляторних або контрактних вимог.

На етапі Series B+ безпека перестає бути лише «операційною дисципліною» і стає частиною ринкової довіри, яка безпосередньо впливає на продажі, партнерства, доступ до корпоративних замовників та вартість капіталу. Саме тут зазвичай з'являється потреба у формальних доказах зрілості – сертифікації та аудитах на кшталт ISO 27001 або SOC 2, які працюють як сигнали якості для великих клієнтів і міжнародних ринків. Одночасно критичною стає відновлюваність: DR/BCP-тестування і контроль RTO/RPO переходять із площини "планів" у площину регулярних перевірок, тому що масштаб бізнесу робить простої дорогими й репутаційно небезпечними. Також суттєво ускладнюється взаємодія з постачальниками – і безпека ланцюга постачання повинна оформлюватися як повна модель контролів: SBOM/SSDF, контрактні SLA на виправлення уразливостей, право аудиту, вимоги до оновлень і швидкого вилучення ризикових компонентів. Для перевірки реальної стійкості (а не лише "відповідності політикам") стають регулярними red/purple-team вправи, що дозволяють підтвердити, як працюють детекції, реагування і відновлення в умовах, наближених до реальних атак. І нарешті, зріла компанія переходить до прозорих метрик: KPI на кшталт MTTD/MTTR, покриття ключових контролів,

швидкість патчування та результативність навчань – тобто показників, які дозволяють керувати безпекою як керованим ризиком, а не як набором гасел.

Нами встановлено, що етичний компонент є вбудованою частиною інженерного дизайну: приватність-за-замовчуванням, прозора мета обробки, недискримінаційність алгоритмів і підзвітність. Саме така «етика-by-design» дає відкритим екосистемам змогу уникнути «темної сторони» мережевих ефектів (концентрація даних, непрозорі SaaS-to-SaaS інтеграції) і знижує премію за ризик у відносинах із партнерами та інвесторами. Слід зазначити, що міжнародне масштабування стартапів можливе без втрати довіри лише за умови ранньої інституціоналізації безпеки та етики, як невід'ємної частини бізнес-стратегії (Мирончeнко, 2024).

Ще один, інтеграційний вимір – кластерна логіка: в інноваційних кластерах – технопарках і регіональних IT-альянсах – відбувається прискорена дифузія «мінімальної планки» контролів (MFA, патч-менеджмент, сегментація, резервування «із повітряним зазором»), стандартизується доступ до керованих сервісів безпеки для бізнесу, а обмін IOCs/TTPs стає регулярним (через ISAC/ISAO). У результаті зменшується інформаційна асиметрія між державою й бізнесом, скорочується MTTD/MTTR у ключових секторах, а економіка довіри – фундамент експортних контрактів – підсилюється (Мирончeнко, 2024). Такий кластерний «механізм масштабування безпеки» є необхідною частиною політики національних інтересів у воєнних умовах.

Щоб фокусно зіставити актуальні ризики з економічними наслідками, подамо матричний зріз для ключових активів (рис. 2.10).

АКТИВ НАЦ. ІНТЕРЕСУ	ТИПОВІ ВЕКТОРИ АТАК	ЙМОВІРНІ НАСЛІДКИ	ПРІОРИТЕТНІ ВІДПОВІДІ
КРИТИЧНА **Енергетика**	⚠ DDoS / деструктивні кампанії проти OT/SCADA ⚠ Supply-chain у ПЗ контролерів	↓ Перебої електропостачання ↓ Удар по ВВП ↓ Зростання вартості капіталу	Мікросегментація OT Моніторинг аномалій Відмовостійкі схеми DR-тести
КРИТИЧНА **Телеком**	⚠ Атаки на DNS / BGP-маршрутизацію ⚠ Volumetric DDoS / виснаження ресурсів	↓ Збій цифрових сервісів ↓ Зрив платежів та логістики	Anycast / DNSSEC Захист від volumetric DDoS Маршрутизаційні фільтри
ВИСОКА **Фінансовий сектор**	⚠ Фішинг / рансомвер ⚠ Вразливості периметру (edge exploits)	↓ Репутаційні та прямі збитки ↓ Ефект доміно на МСП	MDR / XDR Поведінкова аналітика Незворотні бекапи Відпрацьовані плейбуки
ВИСОКА **Держреєстри / е-сервіси**	⚠ Експлойти автентифікації / авторизації ⚠ Data exfiltration із реєстрів	↓ Втрата суспільної довіри ↓ Зловживання персональними даними ↓ Правові / регуляторні ризики	Zero Trust Ключове управління Red-team / пентести Disclosure-процедури
СЕРЕДНЯ **Транспорт / логістика**	⚠ Компрометація TMaaS / IoT-пристроїв ⚠ Саботаж телеметрії; атаки на вендорів	↓ Каскадні логістичні збої ↓ Зриви експорту / імпорту ↓ Зростання страхових тарифів	OT Security SBOM / SLA з вендорами Сенсорна валідація Георепліkація даних
ЗРОСТАЮЧА **Стартап-екосистема**	⚠ Злам CI/CD; секрети в репозиторіях ⚠ Залежність від SaaS-провайдерів	↓ Витік інтелектуальної власності ↓ Зрив контрактів ↓ Втрата інвестиційної довіри	S-SDLC Секрет-менеджмент Policy-as-code Комплаєнс by design

Рис. 2.10. Матриця активів національного інтересу

Джерело: складено автором

Таким чином, ключовими пріоритетами державної політики й ринку виступають: (1) керована прозорість інцидентів та швидкі канали обміну (CERT ↔ ISAC ↔ SOC) – менше «тіньових збитків», вища ринкова дисципліна; (2)

безпека ланцюгів постачання – SBOM, SSDF, договірні SLA на виправлення та типові клаузули для критичних секторів; (3) масштабування «мінімальної планки контролів» через держзакупівлі, гранти, пільги й кластери – щоб підняти нижній поріг стійкості підприємств і стартапів. Глобальні огляди підтверджують: загрози доступності й геополітична складність ростуть швидше, ніж індивідуальні спроможності окремих компаній; тому саме мережеві інститути (кластерна політика, стандарти, публічно-приватні механізми) стають ключем до збереження економічної безпеки та міжнародної конкурентоспроможності України в майбутньому.

Висновки до розділу 2

1. Встановлено, що кіберзагрози остаточно перейшли з “технічної” площини в ядро економічної політики, оскільки впливають на безперервність критичних сервісів, інвестиційний клімат, доступ до ринків і вартість капіталу. Конкурентоспроможність країн дедалі більше визначається не лише продуктивністю, а вимірюваною кіберстійкістю економічних систем. Сформувалася тенденція нормативної конвергенції і «комплаєнс-економіки безпеки»: добровільні рекомендації доповнюються/замінюються юридично зобов’язувальними рамками, де управління ризиками, контроль доступу, реагування та інцидент-репортинг стають умовою ринкового доступу і контрактування, що створює стандартизований “ритм прозорості” для ринку й регулятора.

2. Доведено, що парадигма “периметр-захист” заміщується логікою Resilience/Zero Trust, де ключовими стають здатність локалізувати компрометацію, підтримувати критичні процеси та відновлюватись у контрольовані строки. На макрорівні це трансформується в економічний ефект

через скорочення MTTD/MTTR, зменшення непрямих втрат і зростання довіри інвесторів та партнерів.

3. Встановлено, що кібергігієна інституціоналізується як економічна інфраструктура довіри, а не “поради користувачу”: мінімальні контролі (MFA, патч-менеджмент, базове журналювання, навчання) поступово вбудовуються у держзакупівлі, галузеві вимоги, грантові критерії та типові контрактні умови. Зазначене знижує інформаційну асиметрію між контрагентами і здешевлює транзакції в міжнародній торгівлі.

4. Зазначно, що публічно-приватна координація (ISAC/ISAO-підходи, обмін IOC/TTP, спільні плейбуки) виступає ключовим мезорівневим механізмом зменшення каскадних ефектів: збої в одному секторі менше “перекидаються” на інші, а “вікно експлуатації” скорочується завдяки швидкій дифузії mitigation-рекомендацій.

5. Обгрунтовано безпеку ланцюгів постачання як конкурентного фактору: після хвиль supply-chain інцидентів зростає роль SBOM, SSDF-практик, контрактних SLA на виправлення уразливостей і контрольованих процесів розробки/оновлень. У результаті “прозорість компонентів” перетворюється на перевагу в комплаєнсі та доступі до великих контрактів.

6. Грунтовний аналіз свідчить, що Україна демонструє модель “високого тиску + зростання керованості ризику”: зростання кількості інцидентів поєднується зі зниженням частки high/critical, що можна інтерпретувати як результат розвитку спроможностей виявлення/локалізації та організаційної зрілості реагування. У воєнних умовах це прямо пов’язано з економічною безпекою через стійкість платежів, енергетики, зв’язку та державних цифрових сервісів.

7. Дослідження IT-сектору України визначає його мультиплікатором економічної безпеки в таких ключових вимірах: кадрове ядро та “бойові”

плейбуки скорочують MTTD/MTTR і зменшують макрошоки; експорт цифрових/кіберпослуг підтримує зовнішньоекономічну стійкість; публічно-приватна взаємодія (CERT/CSIRT ↔ приватні SOC) знижує координаційні витрати і підсилює дисципліну ринку.

9. Виявлено актуальні загрози національним інтересам України, які мають кіберфізичний і транскордонний характер, та найбільш ризикові вузли – енергетика, телеком, фінанси, держреєстри, транспортно-логістичні коридори та стартап/бізнес-екосистема. Аналіз показує, що ключовий ризик – каскадні збої, де "цифровий інцидент" породжує матеріальні втрати через простої, штрафи, страхові премії та розриви ланцюгів постачання.

10. Обгрунтовано економічний ланцюг причинності: кібергігієна + зрілість процесів + прозорість + supply chain security → довіра → конкурентоспроможність. Встановлено, що чим більш вимірюваними й контрактно "вбудованими" є механізми безпеки на мікро- і мезорівнях, тим нижчою стає системна вразливість на макрорівні і тим сильнішою є позиція країни у глобальних ланцюгах вартості.

Основні результати дослідження, викладені в цьому розділі, відображено в працях автора:

1. Myronchenko D. Ensuring national and economic security through effective cybersecurity measures. *Національні економічні стратегії розвитку в глобальному середовищі*: тези доп. XIV міжнар. наук.-практ. конф. (м. Київ, 11 травня 2023 р.). К., 2023. С. 27–30. URL: https://drive.google.com/file/d/18gwybyPV5UPbae1rcWR-PDiZwne8bbxe/view.

2. Миронченко Д. Вплив цифрової трансформації на стратегії міжнародних стартапів. *XVII Міжнародна науково-практична конференція «B2B MARKETING» з нагоди 125-річного ювілею КПІ ім. Ігоря Сікорського*: тези доп.

(м. Київ, 14–15 грудня 2023 р.). К., 2023. С. 172–173. URL: http://b2b-marketing.fmm.kpi.ua/proc/issue/view/17528/10197.

3. Myronchenko D. Cyber Hygiene and the Future of International Economics. *Importance of Soft Skills for Life and Scientific Success*: A Collection of Scientific Works of 3rd International Scientific and Practical Internet Conference (Dnipro, March 7–8, 2024). Dnipro, 2024. P. 20–21. URL: http://www.wayscience.com/wp-content/uploads/2024/03/Conference-Proceedings-March-7-8-2024.pdf.

4. Мирончeнко, Д. В., & Сидоренко, К. В. (2025). *Digital Vulnerability of Transport Infrastructure in the Context of Global Crises. The International Sustainable Transportation Symposium (ISTRAS'25)* / National Aviation Academy of Azerbaijan 2025. P. 23. ISBN: 978-9952-582-08-6. DOI: 10.71108/istras.2025

Список використаних джерел для розділу 2

AICPA & CIMA. (n.d.). *SOC 2® – SOC for Service Organizations.* AICPA & CIMA. https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2

AIN.UA. (2025, March 24). *Ukrainian IT industry paid over $1 billion in taxes in 2024 (includes IT export figures).* AIN.UA. https://en.ain.ua/2025/03/24/ukrainian-it-industry-paid-more-than-1-billion-in-taxes-in-2024/

Associated Press. (2025). *Russian hackers target firms shipping aid to Ukraine, US intelligence says.* Associated Press. https://apnews.com/article/6308ca3e11c8299470df573e4f422878

CERT-UA. (n.d.). *Перший щорічний звіт за результатами роботи системи збирання та опрацювання кіберінцидентів (CERT-UA)*. https://cert.gov.ua/article/17696

CERT-UA / Industrial Cyber. (n.d.). *Ukraine's CERT discloses cyberattack on critical energy infrastructure by APT28 (summary based on CERT-UA advisory)*. Industrial Cyber. https://industrialcyber.co/industrial-cyber-attacks/ukraines-cert-discloses-cyberattack-on-critical-energy-infrastructure-by-apt28-hacker-group/

Cybersecurity and Infrastructure Security Agency (CISA). (n.d.). *Information Sharing and Analysis Organizations (ISAOs)*. https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/isaos

Cybersecurity and Infrastructure Security Agency (CISA). (2025). *2025 Minimum Elements for a Software Bill of Materials (SBOM)*. https://www.cisa.gov/resources-tools/resources/2025-minimum-elements-software-bill-materials-sbom

Cybersecurity and Infrastructure Security Agency (CISA). (2025). *Russian GRU Targeting Western Logistics Entities and Technology Companies: Joint Cybersecurity Advisory AA25-141A*. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a

CSIRT NCCC / Держспецзв'язку. (n.d.). *Російські хакери змінюють тактику: від деструктивних атак до розвідки (звіт)*. https://csirt.csi.cip.gov.ua/uk/posts/rosiiski-khakeri-zminyuyut-taktiku-vid-destruktivnikh-atak-do-rozvidki-zvit-derzhspeczv-yazku

Dark Reading. (n.d.). *Putin's Cyberattacks on Ukraine Rise 70%, With Little Effect*. https://www.darkreading.com/threat-intelligence/putin-cyberattacks-ukraine-rise-little-effect

ENISA. (2024). *ENISA Threat Landscape 2024*. Publications Office of the European Union. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

European Commission. (n.d.). *Cyber Resilience Act – Reporting obligations*. Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/cra-reporting

European Commission. (n.d.). *European Digital Innovation Hubs (EDIHs)*. Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/edihs

European Commission. (n.d.). *Horizon Europe: Cluster 3 "Civil security for society"*. European Commission. https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/cluster-3-civil-security-society_en

European Union. (2022). *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 (NIS2)*. EUR-Lex. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

European Union. (2022). *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 (NIS2) (PDF)*. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32022L2555

ISO. (n.d.). *ISO/IEC 27001:2022 – Information security management systems*. ISO. https://www.iso.org/standard/27001

IT Ukraine Association. (2024). *Digital Tiger 2024 (report)*. IT Ukraine Association. https://itukraine.org.ua/files/DigitalTiger2024.pdf

IT Ukraine Association. (n.d.). *Ukrainian Cybersecurity Market Quadruples in Eight Years*. IT Ukraine Association.

https://itukraine.org.ua/en/ukrainian-cybersecurity-market-quadruples-in-eight-years/

Кабінет Міністрів України. (n.d.). *Держспецзв'язку: як CERT-UA реагує на кіберінциденти – від повідомлення до ліквідації наслідків.* https://www.kmu.gov.ua/news/derzhspetszviazku-iak-cert-ua-reahuie-na-kiberintsydenty-vid-povidomlennia-do-likvidatsii-naslidkiv

Ministry of Digital Transformation of Ukraine (Digital State). (n.d.). *Ukraine leading in cybersecurity resilience (market estimate and growth).* https://digitalstate.gov.ua/news/tech/ukraine-leading-in-cybersecurity-resilience

Мирончeнко, Д., & Сидоренко, К. (2023). Роль IT-сектору України в системі забезпечення глобальної кібербезпеки. *Економічний простір,* (186). С. 13-17. DOI: 10.32782/2224-6282/186-2

Мирончeнко, Д. В., & Сидоренко, К. В. (2025). Digital Vulnerability of Transport Infrastructure in the Context of Global Crises. *The International Sustainable Transportation Symposium (ISTRAS'25)* / National Aviation Academy of Azerbaijan 2025. P. 23. ISBN: 978-9952-582-08-6. DOI: 10.71108/istras.2025.

National Telecommunications and Information Administration (NTIA). (2021). *The Minimum Elements for a Software Bill of Materials (SBOM) (report).* U.S. Department of Commerce. https://www.ntia.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

NIST. (n.d.). *Computer Security Incident Handling Guide (SP 800-61 Rev. 2).* NIST CSRC. https://csrc.nist.gov/pubs/sp/800/61/r2/final

OHCHR. (2024). *Attacks on Ukraine's Energy Infrastructure: Harm to the Civilian Population (report).* OHCHR. https://ukraine.ohchr.org/sites/default/files/2024-12/UKR_Attacks_on_Ukraine%E2%80%99s_Energy_Infrastructure_Harm_to_the_Civilian.pdf

Reuters. (2024). *Russia conducted mass cyberattack on Ukraine's state registries, deputy PM says.* Reuters. https://www.reuters.com/technology/cybersecurity/russia-conducted-mass-cyber-attack-ukraines-state-registries-deputy-pm-says-2024-12-19/

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture (NIST Special Publication 800-207).* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

State Service of Special Communications and Information Protection of Ukraine (SSSCIP). (2025). *Russian Cyber Operations: H2 2024 report (PDF).* SSSCIP. https://cip.gov.ua/services/cm/api/attachment/download?id=68768

State Service of Special Communications and Information Protection of Ukraine (SSSCIP). (n.d.). *CERT-UA recorded 4315 cyber incidents in 2024.* https://cip.gov.ua/en/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberinciden tiv

The Record. (n.d.). *Ukraine restores state registers after suspected Russian cyberattack.* The Record. https://therecord.media/ukraine-restores-registers-after-cyberattack

World Economic Forum. (2024). *Global Cybersecurity Outlook 2024 (PDF).* World Economic Forum. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

World Economic Forum. (2024). *Global Cybersecurity Outlook 2024 (publication page).* World Economic Forum. https://www.weforum.org/publications/global-cybersecurity-outlook-2024/

РОЗДІЛ 3
МЕТОДОЛОГІЧНІ ЗАСАДИ ОЦІНЮВАННЯ РІВНЯ ВПЛИВУ ГЛОБАЛЬНИХ КІБЕРЗАГРОЗ НА МІЖНАРОДНУ КОНКУРЕНТОСПРОМОЖНІСТЬ ТА ЕКОНОМІЧНУ БЕЗПЕКУ КРАЇН

3.1. Концептуальні підходи до оцінювання глобальних кіберзагроз міжнародній конкурентоспроможності та економічній безпеці країн

В сучасних умовах розвитку світового господарства глобальні кіберзагрози доцільно трактувати не лише як сукупність технічних інцидентів, а як економіко-інституційний шок, що має визначені канали передачі до МКС та ЕБ. Такий підхід відповідає логіці, за якою цифрова економіка функціонує завдяки безперервності сервісів, керованості ризиків, прогнозованості правил і довірі між суб'єктами ринку, а цифрова безпека стає частиною економічної раціональності, а не «витратною статтею» (OECD, 2015). Відповідно, одна й та сама подія (наприклад, компрометація постачальника, масова DDoS-кампанія або витік даних) транслюється у вимір конкурентоспроможності через підвищення транзакційних витрат, ускладнення контрактування й комплаєнсу, подорожчання страхового захисту та кредитування, а у критичних секторах – через прямі простої, каскадні збої, зриви логістики й втрати довіри до сервісів.

Для концептуальної моделі пропонується використовувати наступні ключові взаємопов'язані латентні конструкції. Перша – загроза/експозиція (GCT), тобто інтенсивність і складність атак, масштаби «площі атаки», залежність від цифрових платформ і уразливість ланцюгів постачання. Друга – кіберстійкість (CR), яка описує здатність системи протидіяти атакам та швидко їх виявляти, локалізувати шкоду і відновлюватися в межах визначених параметрів DR/BCP

(RTO/RPO), зберігаючи керованість критичних функцій (ISO, 2019). Третя – етичне управління та довіра (EG/T): прозорість, підзвітність, приватність «за замовчуванням», недискримінаційність алгоритмів, відповідальне поводження з даними і практики розкриття інцидентів. Зазначена змінна задає якість «економіки довіри»: якщо партнери й користувачі вважають середовище передбачуваним, то знижується «вартість недовіри», спрощуються транскордонні угоди і скорочуються витрати на перевірку контрагентів (OECD, 2015). Четверта конструкція – МКС як здатність економіки підтримувати продуктивність, інноваційність і привабливість для інвестицій та торгівлі в умовах глобальної цифрової конкуренції. П’ята – ЕБ як макростабільність, стійкість критичної інфраструктури та цілісність ланцюгів створення вартості, включно з можливістю обмежувати системні шоки від кіберінцидентів.

Базову гіпотезу пропонуємо описувати наступним чином: загроза/експозиція (GCT) знижує довіру та конкурентоспроможність, оскільки провокує перебої, фінансові втрати й репутаційні ризики, але такий негативний ефект послаблюється кіберстійкістю (CR), яка перетворює «неминучі інциденти» на контрольовані події зі швидким відновленням. Паралельно кібергігієна, стандарти і етичне управління (EG/T) підсилюють довіру як економічний ресурс: прозора політика обробки даних, відповідальне розкриття інцидентів та підзвітність алгоритмів зменшують інформаційну асиметрію, здешевлюють контрактування, покращують умови страхування й кредитування, а отже підтримують МКС навіть за високої інтенсивності атак (OECD, 2015). В даному контексті етичний вимір виступає медіатором і модератором економічних наслідків кіберризику: коли інциденти приховуються або алгоритми працюють непрозоро, ринок закладає додаткову ризикову премію. Натомість принципи privacy-by-design та privacy-by-default створюють передумови довіри, які стають конкурентною перевагою.

Пропонуємо операціоналізувати аналітичний інструментарій через натупні показники. Для GCT (загроза/експозиція) релевантним є перехід від «сирої кількості інцидентів» до severity-weighted метрик, де high/critical події мають більшу вагу, а показник нормується на населення або масштаб економіки (ВВП). Окремо варто виокремлювати частку атак на критичну інфраструктуру та OT/ICS-сегмент, оскільки саме там наслідки переривають фізичні процеси й породжують каскадні втрати. «Площа атаки» може відображатися через рівень цифровізації (cloud/IoT), кількість публічно доступних сервісів і щільність відомих вразливостей (CVE) у розрізі активів. Важливим стає і вимір supply chain ризику, оскільки саме ланцюги постачання переносять загрози «через довіру» між організаціями: на практиці це оцінюється через частку постачальників із контрактними вимогами до безпеки, наявність SBOM у критичних компонентах, а також застосування SSDF як мінімального стандарту безпечної розробки (NIST, 2022). Тут SBOM виступає інструментом прозорості компонентів і керованості залежностей, що прямо зменшує невизначеність для партнерів і регуляторів (NTIA 2021).

Для CR (кіберстійкість) ключовим є те, що безпека вимірюється не відсутністю інцидентів, а здатністю системи повертатися в робочий стан із мінімальною шкодою. Саме тому центральними показниками виступають MTTD/MTTR, середній час патчування, покриття MFA, частка сегментованих критичних систем і зрілість DR/BCP через результативність тестів (чи досягаються RTO/RPO і як часто проводяться тренування) (ISO, 2019). Додатково важливо враховувати організаційні ознаки сучасної стійкості: частку систем, побудованих на принципах Zero Trust, і ступінь впровадження «найменших привілеїв» для сервісів та інтеграцій, що особливо критично в cloud-native середовищах (NIST, 2020). Така логіка відповідає ризик-орієнтованому підходу

NIST CSF 2.0, де кібербезпека розглядається як керований процес, інтегрований у корпоративне та державне управління ризиками (NIST,2024).

Для EG/T (етика та довіра) в економічному сенсі важливо фокусуватися на показниках прозорості та підзвітності, оскільки вони визначають, чи сприймає ринок систему як надійну та прогнозовану. Такий підхід може включати середню затримку розкриття інцидентів, частку подій із повним disclosure базових параметрів, сталість публічних висновків та процедур lesson learned, а також впровадження privacy-by-design і DPIA (див. дод. А) для сервісів, що працюють з даними високої чутливості. Для алгоритмічного виміру доцільно використовувати індикатори наявності аудитів моделей, процедур контролю упередженості, політик пояснюваності й внутрішньої відповідальності за ризики автоматизованих рішень. У підсумку «довіра» стає вимірюваною через проксі: обсяг транскордонних угод у чутливих секторах, зміни премій за ризик після інцидентів, або параметри кіберстрахування (включно з вимогами до базових контролів), що відображають оцінку реальної дисципліни захисту.

Для МКС (IC) у межах рамки доцільно брати показники експорту високотехнологічних товарів і послуг, продуктивності праці, VC-надходжень, інтенсивності R&D, розвитку інноваційних кластерів, а також міжнародні індекси цифрової конкурентоспроможності як зовнішні контрольні змінні. Важливо, що конкурентоспроможність у кіберепоху дедалі частіше визначає не «хто дешевший», а «хто надійніший і передбачуваніший», оскільки великі контракти, особливо у регульованих галузях, сильніше залежать від довіри, комплаєнсу й стійкості.

Для ЕБ (ES) необхідно визначати здатність економіки «тримати удар»: волатильність макропоказників після значних кіберінцидентів, простої логістики і критичних сервісів, індикатори енергетичної стійкості, зміну страхових тарифів і частку підприємств із підтвердженою безперервністю бізнесу (ISO, 2019). У

такому підході ЕБ виступає кінцевим контуром системи: якщо кіберстійкість і довіра «працюють», то навіть за високої загрозовості країна зменшує системні втрати, утримує привабливість для партнерів і зберігає позиції у глобальних ланцюгах створення вартості.

Таким чином, рамка описує узгоджений причинно-наслідковий ланцюг: кіберзагроза → шок довіри → зростання транзакційних і фінансових витрат → погіршення конкурентних позицій. Водночас кіберстійкість та етичне управління виступають амортизаторами, що знижують глибину негативного ефекту й переводять інциденти в контрольовану площину (NIST, 2024; OECD, 2015). Саме така властивість робить модель зручною з точки зору імплементації, адже дає можливість констатувати кібербезпеку, а ткож показати, через які канали вона трансформується в конкурентоспроможність та економічну безпеку, і які метрики це підтверджують (рис. 3.1).

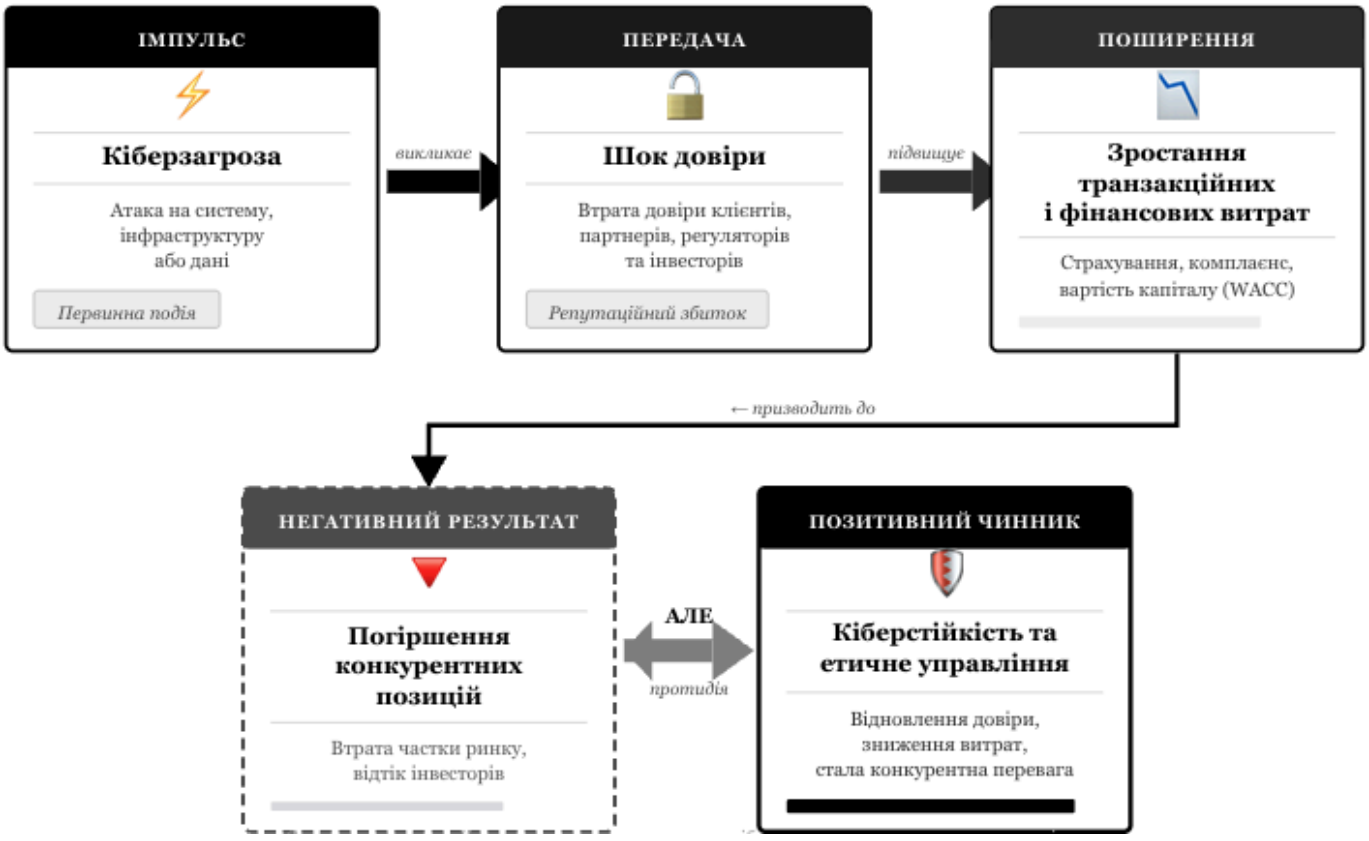

Рис. 3.1. Кіберзагроза, довіра та конкурентоспроможність

Джерело: складено автором

Для того, щоб розрахувати інтегральні показники, необхідно для країно-року (i,t) сформувати стандартизовані (z-score або min–max) підіндекси:

- **SWIR** (severity-weighted incident rate):

$$\text{SWIR}_{it} = \frac{\sum_s w_s \cdot Incidents_{it}^s}{Population_{it}}$$

або

$$\frac{\sum_s w_s \cdot Incidents_{it}^s}{GDP_{it}}$$

де $s \in \{low,med,high,critical\}$, w_s – ваги (напр., {1,2,4,6}).

- **ASURF** (attack surface): нормований індекс з компонент cloud/IoT/вразливості.
- **RESIL** (resilience score): середнє нормованих MFA, patch latency (зі знаком «−»), сегментації, DR/BCP, Zero Trust, SBOM-контрактів:

$$\mathrm{RESIL}_{it} = \frac{1}{K} \sum_{k=1}^{K} z(x_{kit})$$

- **ETHICS/TRUST** (ETS): вагове середнє приватності, прозорості, недискримінаційності, підзвітності, довірчих проксі. Ваги – **AHP/Delphi** (див. дод. Б)(експертна панель) або **PCA**:

$$\mathrm{ETS}_{it} = \sum_{m} \alpha_m \cdot z(e_{mit}), \quad \sum \alpha_m = 1.$$

Далі необхідно сформулювати **індекс кібервпливу на конкурентоспроможність і безпеку** (умовно **CCSI**):

$$\mathrm{CCSI}_{it} = \delta_1 \cdot \mathrm{RESIL}_{it} + \delta_2 \cdot \mathrm{ETS}_{it} - \delta_3 \cdot \mathrm{SWIR}_{it} - \delta_4 \cdot \mathrm{ASURF}_{it}$$

де δ\deltaδ – ваги, отримані з **SEM** або регресії на цільові змінні **IC**/**ES**.

Наступним кроком є ідентифікаційна стратегія, для чого необхідним є визначення дизайну причинної оцінки:

1. **Панельна модель із фіксованими ефектами** (FE) для країн *(i)* на горизонті 2015–2025:

$$IC_{it} = \beta_1 CCSI_{it-1} + \beta_2 X_{it} + \mu_i + \tau_t + \epsilon_{it}$$

де X – контрольні (ВВП/душу населення, освіта, відкритість торгівлі), μi\mu_iμi – країно-сталі риси, τt\tau_tτt – часові шоки. Робастні похибки Driscoll–Kraay.

2. **Подійний аналіз / event study** навколо великих інцидентів (T−k … T+k) для вимірювання впливу на: спреди, страхові премії, експорт, логістичні простої.

3. **DiD** (difference-in-differences) на хвилі впровадження регуляцій/стандартів (напр., NIS2-аналогів, обов'язкових SBOM): групи «лікування» vs «контроль».

4. **SEM** (структурне моделювання) для перевірки ланцюга **ETS → T → IC** та **RESIL × ETS** як **модерації** впливу загроз на МКС/ЕБ:

$$\begin{aligned} T_{it} &= \lambda_1 ETS_{it} - \lambda_2 SWIR_{it} + \eta_1 \\ IC_{it} &= \gamma_1 T_{it} + \gamma_2 RESIL_{it} + \gamma_3 (RESIL_{it} \times ETS_{it}) + \eta_2 \\ ES_{it} &= \phi_1 IC_{it} - \phi_2 SWIR_{it} + \phi_3 RESIL_{it} + \eta_3 \end{aligned}$$

5. **Інструментальна змінна (IV)** (за наявності): екзогенний таймінг регуляторних змін або «природні експерименти» (наприклад, вимушені міграції у хмару через фізичні руйнування центрів обробки даних – для локальної оцінки).

Щодо конструкції індексів, нами запропонована система інтегральної оцінки, що складається з наступних підіндексів (SWIR, ASURF, RESIL, ETS), та є концептуально збалансованою, оскільки одночасно охоплює (i) інтенсивність та «вагу» інцидентів, (ii) структуру експозиції через поверхню атаки, (iii) практичну спроможність до запобігання/виявлення/відновлення та (iv) етико-довірчий вимір,

який у цифровій економіці визначає якість контрактування та рівень транзакційних витрат. Саме така комбінація дозволяє CCSI трактувати як комплексний індикатор економічної кібербезпеки, у якому ризик співвідноситься зі здатністю системи його компенсувати. Методологічна сила рішення полягає в тому, що більшість наявних підходів фіксують або "негативну" сторону (поширеність загроз), або "позитивну" сторону (наявність контролів і політик), але не моделюють їх взаємодію в одній конструкції. У запропонованій нами рамці така взаємодія закладена на рівні логіки агрегування: негативні компоненти (SWIR, ASURF) зважуються проти компенсаторів (RESIL, ETS), що робить індекс придатним для порівнянь як між країнами, так і в динаміці країна-рік, а також для подальшого моделювання впливу на цільові макропоказники конкурентоспроможності та економічної безпеки.

Щодо причинності, пропонуємо поєднання кількох ідентифікаційних стратегій (панельні моделі з фіксованими ефектами, event study, DiD, SEM, IV), що суттєво підвищує достовірність майбутніх висновків, оскільки кожен метод «прикриває» типові слабкі місця інших підходів. Моделі з фіксованими ефектами знижують ризик зміщення оцінок через незмінні країнові характеристики та спільні часові шоки, event study дозволяє простежити профіль ефекту до/після великих інцидентів і відокремити короткострокові та інерційні наслідки, а DiD створює рамку квазіексперименту для оцінювання регуляторних або інституційних змін (наприклад, вимог щодо SBOM чи аналогів NIS2). Окремо слід підкреслити значущість SEM-специфікації, що формалізує причинно-наслідковий механізм, який і є «ядром» теоретичної гіпотези – зокрема ланцюг ETS → T → IC та можливу модерацію (RESIL × ETS). Такий підхід дозволяє емпірично перевірити, чи виступає довіра справді медіатором між етичним управлінням і конкурентоспроможністю.

Щодо практичного застосування для України, пропонується використання інструментальної змінної (IV) через “вимушені міграції у хмару внаслідок фізичних руйнувань” є особливо доречним саме для українського контексту, оскільки створює рідкісний за якістю емпіричний випадок екзогенного шоку, який потенційно можна інтерпретувати як природний експеримент. На відміну від багатьох мирних юрисдикцій, де цифрова трансформація відбувається поступово і часто ендогенно (під впливом продуктивності, інвестицій та управлінської якості), у воєнних умовах частина переходів в інфраструктурі може мати вимушений характер і слабше залежати від «внутрішньої» схильності організацій до модернізації. Такий підхід створює більш переконливу основу для оцінки причинного ефекту компонентів кіберстійкості (RESIL) на економічні результати, якщо інструмент відповідатиме критеріям релевантності й екзогенності та буде коректно обґрунтований через припущення виключення.

Загалом блок формує методологічно коректну й логічно завершену основу для подальшої емпіричної верифікації ключової тези про те, що кібербезпека в сучасній цифровій економіці виступає економічною функцією (через довіру, транзакційні витрати, ціну капіталу та стійкість ланцюгів вартості), а не суто технічною характеристикою IT-ландшафту. Водночас практичним обмеженням залишається доступність і зіставність мікроданих для конструювання ASURF та ETS у форматі країна-рік. Для ASURF це може вимагати регулярних вимірів цифровізації/вразливостей та ознак “attack surface”, а для ETS – стабільних спостережуваних проксі етики/довіри й достатньої якості експертної процедури (AHP/Delphi) або достатньої кількості однорідних індикаторів для PCA. Отже, ключовою умовою успішного застосування підходу є формальна коректність індексів та моделей, а також методично контрольована збірка даних і прозорість правил нормування, вагування та перевірки стійкості результатів до альтернативних специфікацій.

Етичний вимір у запропонованій моделі доцільно трактувати як методологічний модератор, який змінює силу та напрям зв'язків між кіберризиком, довірою, конкурентоспроможністю й економічною безпекою. У практичних термінах етичні принципи на кшталт privacy-by-design, прозорості інцидентів, недискримінаційності та пояснюваності алгоритмів формують вимір ETS (Ethical-Trust Standards) у двох взаємодоповнювальних ролях. По-перше, ETS працює як медіатор довіри: коли країна та її бізнес-середовище демонструють зрозумілі правила поводження з даними, підзвітність і дисципліну розкриття інцидентів, це зменшує інформаційну асиметрію у транскордонних угодах та знижує транзакційні витрати (через менші витрати на due diligence, дешевші страхові моделі та передбачуваніші умови комплаєнсу). У результаті довіра стає економічним активом, який підтримує міжнародну конкурентоспроможність через доступ до довших контрактів, кращих умов фінансування й "премію за передбачуваність" для експортерів цифрових послуг і технологічних постачальників. По-друге, ETS виступає модератором ефекту кіберстійкості: одна і та сама технічна стійкість (резервування, DR/BCP, сегментація, Zero Trust) дає суттєво сильніший результат у країнах, де етичні стандарти стали нормою управління даними й цифровими ризиками. Саме комбінація "стійкість + етика" генерує більший «преміум довіри», бо партнери отримують не лише технічні гарантії відновлення, а й правову/організаційну впевненість у чесності процедур, пропорційності збору даних та прозорості реагування на інциденти (зокрема через вимоги GDPR щодо оцінювання ризиків і захисту персональних даних у процесах обробки) (European Union, 2016). Додатково, в країнах, що переходять до регулювання високоризикових систем ШІ, етична складова укріплюється через вимоги до управління ризиками, прозорості та підзвітності, які також можна використовувати як проксі змін ETS у часі (European Union, 2024).

Для емпіричного наповнення ETS доцільно використовувати не декларативні категорії, а вимірювані практики. Серед найбільш придатних метрик – середня затримка розкриття інциденту (time-to-disclosure), частка інцидентів із повним “disclosure-пакетом” (що включає базову технічну інформацію, класифікацію впливу та дії з пом’якшення), наявність формалізованих процедур DPIA/AI Impact Assessment у компаніях, інституціоналізація політики “право на пояснення” та регулярність незалежних аудитів алгоритмів на предмет дискримінаційних ефектів. До цього ж блоку належать регуляторні проксі: кількість і якість рішень уповноважених органів щодо порушень у сфері персональних даних, застосовані санкції, а також практика публічних “post-mortem” розборів інцидентів (без розкриття чутливої інформації), які свідчать про зрілість культури прозорості. Сукупно ці ознаки дозволяють перетворити “етику” з оціночного поняття на змінну, що входить у статистичну модель як реальний модератор конкурентоспроможності у цифровій економіці.

Алгоритм оцінювання логічно починати з побудови панельного набору даних “країна-рік”, де фіксуються: (а) інциденти та суворість (severity-weighted), (б) цифровізація/експозиція та структурні уразливості, (в) показники стійкості (MTTD/MTTR, частка MFA-покриття, темпи патчування, DR-тести), (г) етичні та довірчі індикатори (ETS), а також (д) результати – показники міжнародної конкурентоспроможності та економічної безпеки. Далі виконується нормалізація шкал і побудова підіндексів (наприклад, SWIR/ASURF/RESIL/ETS), після чого важливо перевірити внутрішню узгодженість та валідність вимірів: для підшкал доречно застосовувати індикатори на кшталт α Кронбаха (як базову перевірку надійності) та процедури факторного виділення (EFA/PCA), а для підтвердження латентних конструкцій – CFA (Cronbach, 1951). На основі підтверджених латентних факторів формується інтегральний індекс (на кшталт CCSI) та

первинний ранжир країн, який уже дає аналітичну картину розривів між експозицією, стійкістю й етико-довірчим виміром.

Причинну інтерпретацію доцільно будувати поетапно: спочатку – панельні регресії з фіксованими ефектами, які контролюють незмінні у часі особливості країн; для коректних стандартних помилок у панельних даних із перехресною залежністю можна застосовувати оцінювачі на кшталт Driscoll–Kraay (Driscoll & Kraay, 1998). Далі – "event study" логіка для великих кібершоків і зміни регуляторного режиму, а також DiD-дизайни для порівняння країн, що впровадили обов'язкові режими розкриття інцидентів/оцінок впливу, проти тих, де ці вимоги залишаються рекомендаційними. Для відображення складної системи зв'язків "загроза → довіра → конкурентоспроможність" із роллю модераторів і медіаторів доцільно застосовувати SEM (структурні рівняння), які дозволяють працювати з латентними конструкціями та непрямими ефектами (Bollen, 1989). Завершальний крок – сценарне моделювання (еластичності IC/ES до приростів ΔRESIL, ΔETS, ΔSWIR) та політичне картування дефіцитів у вигляді "heatmap": які саме контролі або інституційні елементи (сегментація, SBOM, прозорість, DPIA/AIA, disclosure) дають найбільший приріст довіри та конкурентоспроможності за обмежених ресурсів. На даному етапі практично корисними стають зовнішні орієнтири, що описують структуру загроз і стратегічні прогалини – наприклад, панорамні огляди ENISA та WEF, які допомагають обґрунтувати вибір груп ризиків і канали впливу кіберзагроз на економічну стійкість [(ENISA, 2024); (World Economic Forum, 2024)].

Окремо важливо підкреслити: якість моделі значною мірою залежить від джерел даних. Для інцидентів і суворості це можуть бути національні CERT/CSIRT та узагальнювальні європейські/глобальні огляди загроз; для "поверхні атаки" – статистика цифровізації (cloud/IoT), відкриті спостережні звіти та агреговані показники уразливостей; для стійкості – корпоративні та регуляторні

практики DR/BCP, рівень поширення MFA, темпи патчування, частка організацій із Zero Trust. Для етики й довіри найбільш придатні регуляторні реєстри рішень, корпоративні політики прозорості, наявність DPIA/AIA та незалежних аудитів алгоритмів, а також поведінкові “проксі довіри” – наприклад зміни премій за ризик, умови кредитування й динаміка кросбордерних контрактів у чутливих секторах.

Таким чином, запропонована нами методологічна конструкція дозволяє описати й виміряти головну ідею, що проходить наскрізною ниткою через попередні блоки дослідження: етичний стандарт не просто «пом'якшує» кіберризики на операційному рівні, а якісно трансформує саму природу кіберстійкості — перетворює її з витратної статті бюджету безпеки на джерело верифікованої конкурентної переваги. Цей перехід відбувається тому, що прозорість розкриття інцидентів, підзвітність алгоритмів, privacy-by-design та ethics-by-design є не деклараціями, а вимірюваними сигналами надійності для міжнародних контрагентів, інвесторів і регуляторів. Саме ці сигнали знижують інформаційну асиметрію між країною та її партнерами, здешевлюють транскордонне контрактування і скорочують «страхову надбавку за непередбачуваність», що ринок автоматично закладає у вартість капіталу та умови доступу до глобальних ланцюгів вартості. У підсумку методологічна рамка CCSI фіксує те, що досі залишалося поза межами кількісного вимірювання: безпека, підкріплена етичним управлінням, переходить з рівня технічних витрат на рівень економіки довіри — і саме через цей перехід прямо й вимірювано впливає на міжнародну конкурентну позицію держави в умовах цифрової глобалізації.

3.2. Інтегральна оцінка впливу кібернетичних загроз національним інтересам України

Інтегральна оцінка впливу кібернетичних загроз на національні інтереси України є доцільною для вимірювання «чистого ефекту» кіберризику на ключові вузли економічної безпеки – енергетику, зв'язок і телеком, фінансову інфраструктуру, державні е-сервіси та транспортно-логістичні коридори. На практиці зазначені вузли формують єдину мережеву систему: збої в одному контурі швидко передаються в інші (через залежність від цифрових сервісів, хмарних середовищ, API-інтеграцій і постачальників). Тому методологічно коректно відмовитися від «ізольованого» аналізу інцидентів і перейти до композитної рамки, де одночасно враховуються інтенсивність/суворість загроз, поверхня атаки, кіберстійкість і етико-довірчий шар як інституційний механізм зниження транзакційних витрат і відновлення довіри на ринках.

Вихідна логіка використовує наступні чотири латентні конструкції: SWIR (severity-weighted incidents), ASURF (attack surface), RESIL (resilience) і ETS (ethics/trust). Дані змінні агрегуються в інтегральний показник CCSI-UA (Composite Cybersecurity Impact for Ukraine), у якому RESIL і ETS виступають «компенсаторами» негативного впливу загрозової експозиції та цифрової вразливості. У запропонованій інтерпретації практики на кшталт мікросегментації, MFA, DR/BCP-режимів, SBOM/SSDF і прозорого інцидент-репортингу виступають способом перетворення кіберризиків у керований операційний ризик, зменшуючи премію за невизначеність у транскордонних контрактах та підвищуючи довіру контрагентів і інвесторів (рис. 3.2).

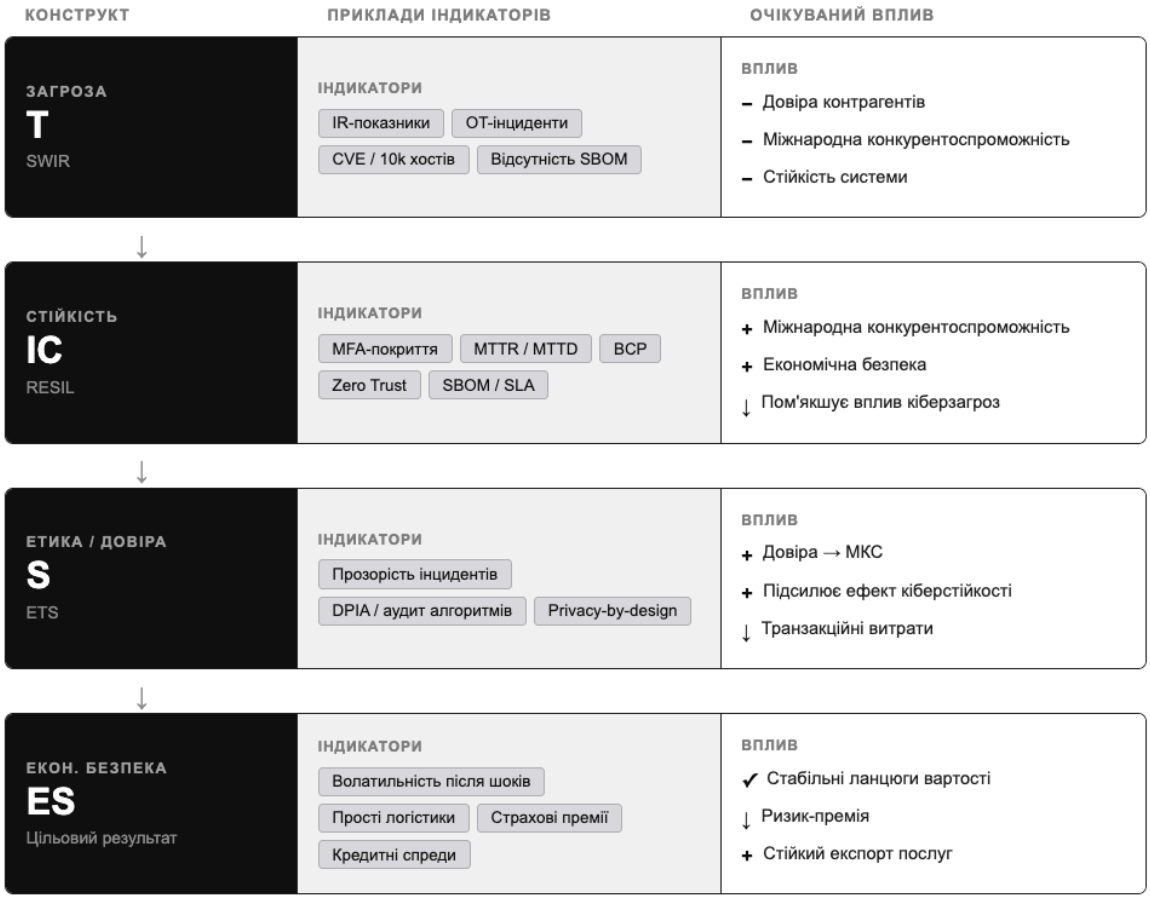

Рис. 3.2. CCSI-UA - Таблиця відповідності конструктів

Джерело: складено автором

Емпірична база індексування може будуватися на поєднанні публічних і операційних метрик. Для загрозової частини SWIR доцільно використати річні та піврічні підсумки CERT-UA: за 2024 рік зафіксовано 4 315 кіберінцидентів (істотне зростання відносно 2023 року), причому H2 2024 = 2 576 проти H1 2024 = 1 739 (приріст +48% у другому півріччі); при цьому кількість інцидентів рівня high/critical у H2 зменшилася, що важливо враховувати як зсув структури атак у бік масових кампаній і розвідувальних активностей у критичних секторах. Узгоджене вторинне підтвердження цієї статистики наведено у профільній медіааналітиці, що посилається на той самий звіт. Паралельно європейська рамка

ризиків акцентує, що для цифрових економік ключовими залишаються загрози доступності й безперервності (DDoS, деструктивні кампанії), а також рансомвер та порушення конфіденційності/цілісності, тобто саме ті класи інцидентів, які напряму формують макроекономічні збитки через простої сервісів і ланцюгові збої.

Компонент ASURF (поверхня атаки) відображає структурну «відкритість» критичних секторів: високу залежність від хмари та SaaS, розширення IoT/IIoT й OT-контурів, зростання кількості інтеграційних API та вразливості ланцюгів постачання. Тут виправдано використовувати проксі-метрики: частку критичних сервісів із зовнішніми інтеграціями, наявність відкритих сервісів і периметрових експозицій, кількість релевантних CVE на узгоджену одиницю активів, а також частку постачальників без SBOM/без договірних SLA на виправлення уразливостей (як маркер «непрозорого» ризику). Військовий і транскордонний характер загроз підсилює вагу ASURF: атаки орієнтуються не лише на державні органи, а й на логістику та технологічних підрядників, пов’язаних із транспортом і постачаннями, що фактично переводить кіберризик у фактор вартості капіталу і страхових премій для бізнесу, який працює з українським напрямом (CISA, n.d).

Показник RESIL (кіберстійкість) доцільно формувати з операційних метрик, що описують здатність систем виявляти інциденти, локалізувати шкоду і відновлюватися. До «ядра» RESIL можна включати MTTD/MTTR, покриття MFA, середній час патчування, частку сегментованих критичних систем, наявність Zero Trust-політик, а також частоту і результативність DR/BCP-тестів із досягненням цільових RTO/RPO. Практично важливо, що RESIL відображає не декларації, а перевірювані процедурні здатності, які безпосередньо знижують масштаб економічного шоку від інциденту (простій, збої сервісів, втрати продуктивності). Слідуючи логіці, навіть за високого SWIR, зростання RESIL може утримувати

систему в керованій зоні – тобто переводити ризик із категорії «системної загрози» в категорію «контрольованих втрат».

Компонент ETS (етика/довіра) в інтегральній оцінці виконує не «моральну», а економічно-інституційну функцію. Він може бути операціоналізований через показники швидкості та повноти інцидент-розкриття, наявності DPIA/AI-оцінок впливу для цифрових сервісів, політик «право на пояснення» і аудитів алгоритмів, а також через індикатори регуляторної підзвітності та відповідності міжнародним рамкам (ISO 27001/SOC 2/NIS2). ETS впливає на конкурентоспроможність через зниження транзакційних витрат і зменшення інформаційної асиметрії для партнерів: що «передбачуваніша» поведінка інституцій у кризі та прозоріший режим управління даними, то нижча премія за ризик у контрактах і простіше доступ до довгого фінансування. Саме тому ETS у CCSI-UA виступає компенсатором негативного ефекту SWIR і ASURF, а не факультативною змінною.

З практичної точки зору зручно привести всі змінні до єдиної шкали 0–100 (де високий SWIR/ASURF означає гіршу ситуацію, а високий RESIL/ETS – кращу) і застосувати ваги, отримані за експертними процедурами. Для прозорості та відтворюваності ваги можуть задаватися через AHP/Delphi-підхід (експертна панель у критичних секторах), а далі перевірятися методами PCA/SEM на історичних даних; такий інструментарій є типовим для побудови композитних індикаторів у прикладних дослідженнях (OECD, 2008; Saaty, 1987; Jolliffe, 2002). Після нормування агрегування може бути задане базовою лінійною формою:

$$\text{CCSI-UA} = \delta_1 \cdot \text{RESIL} + \delta_2 \cdot \text{ETS} - \delta_3 \cdot \text{SWIR} - \delta_4 \cdot \text{ASURF}.$$

Інтерпретація шкали може бути такою: 0–20 – «високий негативний вплив» (ризик домінує над спроможностями), 21–40 – «помітний негативний вплив», 41–60 – «збалансована зона», 61–80 – «помірно позитивний ефект» (компенсація

ризику стійкістю й довірою), 81–100 – «високий позитивний» (висока стійкість за низької експозиції).

Для ілюстративного зрізу України на горизонті 2024 → H1 2025 (без претензії на остаточність, але з опорою на перевірені публічні метрики) логіка може виглядати так: SWIR залишається об'єктивно високим через інтенсивність атак (CERT-UA: 4 315 інцидентів у 2024 р., приріст H2 до H1), ASURF також високий через цифровізацію критичних секторів і масштаб інтеграцій, тоді як RESIL демонструє зростання завдяки прискоренню процедур відновлення, сегментації та переходу до практик кіберстійкості; ETS має потенціал росту через інституціоналізацію прозорості, але потребує системного поширення практик DPIA/AI-аудитів і стандартизації «доказової» підзвітності. За умовно збалансованих ваг $\delta_1=\delta_2=\delta_3=\delta_4=0{,}25$ індекс CCSI-UA закономірно потрапляє в «пограничну» зону між помітним негативним впливом і балансом: ризик значною мірою компенсується, але ціна компенсації (страхові премії, витрати на відновлення, посилені вимоги комплаєнсу) лишається відчутною для бізнесу й бюджету. Саме такий результат є економічно осмисленим: в умовах високої експозиції Україна утримує керованість системи завдяки зростанню стійкості та інституційної довіри, проте для переходу до «позитивної» зони потрібні масштабування мінімальних контролів у підприємств, формалізація вимог до постачальників (SBOM/SSDF/SLA), а також подальша конвергенція практик прозорого інцидент-управління з європейськими стандартами (рис. 3.3).

Рис. 3.3. CCSI-UA - Секторна інфографіка

Джерело: складено автором

Інфографіка відображає результати секторальної оцінки кібербезпекового впливу на п'ять ключових вузлів національних інтересів України – енергетику (OT/ICS), телеком та інтернет, фінансовий сектор, державні реєстри й е-сервіси, а також транспорт і логістику – через призму чотирьох компонентів інтегрального індексу CCSI-UA. Кожен рядок таблиці відповідає одному сектору і містить профіль із чотирьох горизонтальних барів: SWIR (severity-weighted інциденти,

темно-чорний) та ASURF (поверхня атаки, темно-сірий) є «негативними» складовими – чим довший бар, тим вища загрозова експозиція та вразливість сектору; RESIL (кіберстійкість, середньо-сірий) та ETS (етика/довіра, світло-сірий) є «позитивними» компенсаторами – чим довший бар, тим краще сектор здатен протистояти загрозам і відновлюватися. Підсумковий бал CCSI-UA праворуч обчислюється за формулою із рівними вагами ($\delta_1=\delta_2=\delta_3=\delta_4=0{,}25$) і відображає баланс між загрозами та спроможностями: темний бейдж сигналізує про нижчий результат (зона помітного негативного впливу, 21–40), світлий – про вищий (наближення до збалансованої зони, 41–60). Шкала зон у нижній частині інфографіки слугує орієнтиром інтерпретації: значення 0–20 означають домінування ризику над спроможностями, 21–40 – помітний негативний вплив із частковою компенсацією, 41–60 – збалансовану зону, де ризик значною мірою компенсується стійкістю й довірою, 61–80 – помірно позитивний ефект, а 81–100 – високу стійкість за низької експозиції. За результатами оцінки найкращу позицію займає фінансовий сектор (CCSI-UA = 46), що пояснюється відносно нижчою загрозовою експозицією (SWIR = 26) і найвищим серед усіх секторів рівнем стійкості (RESIL = 70); найбільш вразливими залишаються транспорт і логістика (CCSI-UA = 36) та енергетика (CCSI-UA = 38) – через поєднання найвищих значень SWIR/ASURF і відносно нижчих показників RESIL та ETS, що безпосередньо відображає ризики каскадних збоїв у кіберфізичних системах в умовах гібридної війни. Усі бали є ілюстративними, побудованими на основі відкритих метрик і експертного нормування, і призначені для порівняльного аналізу секторальних пріоритетів державної кіберполітики, а не для абсолютної оцінки рівня захищеності.

Центральна ідея полягає в тому, що кіберполітику можна і потрібно оцінювати кількісно – як набір важелів із вимірюваним ефектом на інтегральний індекс CCSI-UA. Запропонований підхід спирається на поняття еластичності:

наскільки зміниться індекс, якщо держава або організація збільшить (або зменшить) конкретний параметр безпеки. Це дозволяє порівнювати заходи між собою, розставляти пріоритети і обґрунтовувати бюджетні рішення не загальними деклараціями, а конкретними числами. Наведені нижче орієнтири отримано на панелі інцидентів 2022–2024 та за результатами секторних опитувань; вони відображають середні ефекти і підлягають уточненню в міру накопичення нових даних.

Перш ніж перейти до конкретних заходів, необхідно пояснити одиниці виміру, що використовуються. Скорочення «п.п.» означає процентний пункт – абсолютну зміну у відсотках. Наприклад, якщо покриття багатофакторної автентифікації (MFA) зросло з 50% до 70%, це +20 п.п., а не +40%, оскільки «відсоток від відсотка» є відносною величиною і дає іншу цифру. Скорочення «п.» позначає пункт шкали CCSI-UA (від 0 до 100) – зміну самого індексу або його субіндексу. Зокрема, «+2 п. до RESIL» означає, що субіндекс кіберстійкості зріс на дві одиниці, що далі транслюється у зростання загального CCSI-UA з урахуванням вагового коефіцієнта $\delta_1 = 0{,}25$.

Перший захід – збільшення покриття MFA у критичних системах на 20 п.п. – стосується розширення частки облікових записів і точок входу, захищених багатофакторною автентифікацією. MFA означає, що для входу в систему недостатньо лише пароля: потрібне додаткове підтвердження – токен, застосунок або біометрія. Якщо поточне покриття складає, наприклад, 50%, інтервенція передбачає його доведення до 70%. Оскільки компрометація облікових даних залишається одним із найпоширеніших векторів атак, розширення MFA блокує цей вектор для більшої частини інфраструктури, що прямо підвищує субіндекс кіберстійкості на 2,0–2,8 п. і, як наслідок, піднімає CCSI-UA на 0,5–0,7 п.

Другий захід – скорочення медіанної затримки патчування на 30% – спрямований на прискорення виправлення відомих вразливостей. Patch-latency –

це час між публікацією виробником виправлення (патча) і його фактичним встановленням в організації. Якщо медіанне значення цього показника становить 45 днів, інтервенція передбачає його скорочення приблизно до 31 дня через перехід на керовані репозиторії та запровадження договірних SLA із постачальниками щодо строків закриття CVE (публічно відомих вразливостей). Менша затримка скорочує «вікно атаки» – проміжок часу, протягом якого вразливість є відомою зловмисникам, але ще не усунутою в організації. Ефект складає +2,5–3,5 п. до RESIL і +0,6–0,9 п. до CCSI-UA.

Третій захід – запровадження обов'язкового SBOM і SSDF разом із договірними SLA для ключових постачальників критичних секторів. SBOM (Software Bill of Materials) – це реєстр усіх компонентів програмного забезпечення з версіями та залежностями, аналог «складу продукту» для коду, який дозволяє організації точно знати, які бібліотеки і модулі використовуються в її системах і яких вразливостей вони зазнають. SSDF (Secure Software Development Framework) – стандарт NIST, що регламентує обов'язкові практики безпечної розробки на кожному етапі створення ПЗ. Наявність SBOM і SSDF у постачальника разом із SLA на усунення CVE (наприклад, критичні вразливості – не довше 15 днів, високі – не довше 30) знижує так званий «непрозорий ризик» ланцюга постачання: замовник перестає бути залежним від того, що йому недоступно і неперевірено. Цей захід одночасно зменшує ASURF на 3–4 п. (менша поверхня атаки через ланцюг постачання) і підвищує RESIL на 1–1,5 п. (краща здатність реагувати на вразливості постачальників), даючи сукупний приріст CCSI-UA на 1,0–1,4 п. – найбільший ефект серед усіх окремих заходів.

Четвертий захід – стандартизований інцидент-репортинг за схемою 24h/72h. Він передбачає законодавче зобов'язання організацій повідомляти регулятора про значущий кіберінцидент упродовж 24 годин з моменту виявлення (раннє попередження) і надавати розгорнутий базовий звіт із деталями – протягом 72

годин. Аналогічна норма закріплена в директиві NIS2 Євросоюзу. Ключовий ефект цього заходу йде не через технічний, а через інституційний канал: прозорість інцидентів знижує інформаційну асиметрію між організаціями, регуляторами та зовнішніми партнерами, зменшує репутаційний ефект інцидентів (адже факт розкриття сприймається як ознака відповідальності, а не слабкості) і підвищує субіндекс ETS на 2–3 п., що транслюється у +0,5–0,8 п. до CCSI-UA.

П'ятий захід – проведення двох повних DR/BCP-тестів на рік із досягнутими показниками RTO і RPO. DR (Disaster Recovery) і BCP (Business Continuity Plan) – це плани відновлення після інциденту та забезпечення безперервності роботи відповідно. RTO (Recovery Time Objective) – максимально допустимий час відновлення систем після збою. RPO (Recovery Point Objective) – максимально допустима втрата даних у часі (наприклад, RPO = 1 год означає, що резервна копія не може бути старшою за одну годину). Ключова умова – це не паперовий сценарій, а реальне практичне відновлення систем із фіксацією фактичного часу і порівнянням із цільовими показниками. Регулярне тестування виявляє прогалини у планах до настання реального інциденту, «тренує м'язову пам'ять» команд і підтверджує досяжність RTO/RPO. За оцінками, це найпотужніший окремий важіль для RESIL серед усіх п'яти заходів: +3–4 п. до субіндексу і +0,8–1,1 п. до CCSI-UA – і при цьому один із найменш капіталомістких, оскільки не потребує нових технологій, лише організаційної дисципліни.

Реалізація встановлених ключових заходів одночасно дає кумулятивний ефект, що перевищує просту суму окремих приростів – завдяки синергії між компонентами: краща патч-дисципліна підсилює захист, що забезпечується MFA; прозорий репортинг підвищує довіру до RESIL-метрик з боку партнерів; підтверджені DR-тести роблять SBOM-вимоги операційно значущими, а не декларативними. Сукупний ефект пакету «MFA + патчі + SBOM/SSDF + disclosure + DR/BCP» оцінюється в +3–5 п. CCSI-UA за рік. За шкалою індексу це відповідає

переходу сектору на один рівень вище – наприклад, із зони «помітного негативного впливу» (21–40) до «збалансованої зони» (41–60). На макроекономічному рівні такий приріст відповідає вимірюваному зменшенню премії за ризик у контрактах і страхуванні, скороченню тривалості простоїв критичних сервісів і стабілізації експортних потоків – тобто кібербезпека перетворюється на безпосередній чинник конкурентоспроможності й економічної безпеки країни (рис. 3.4).

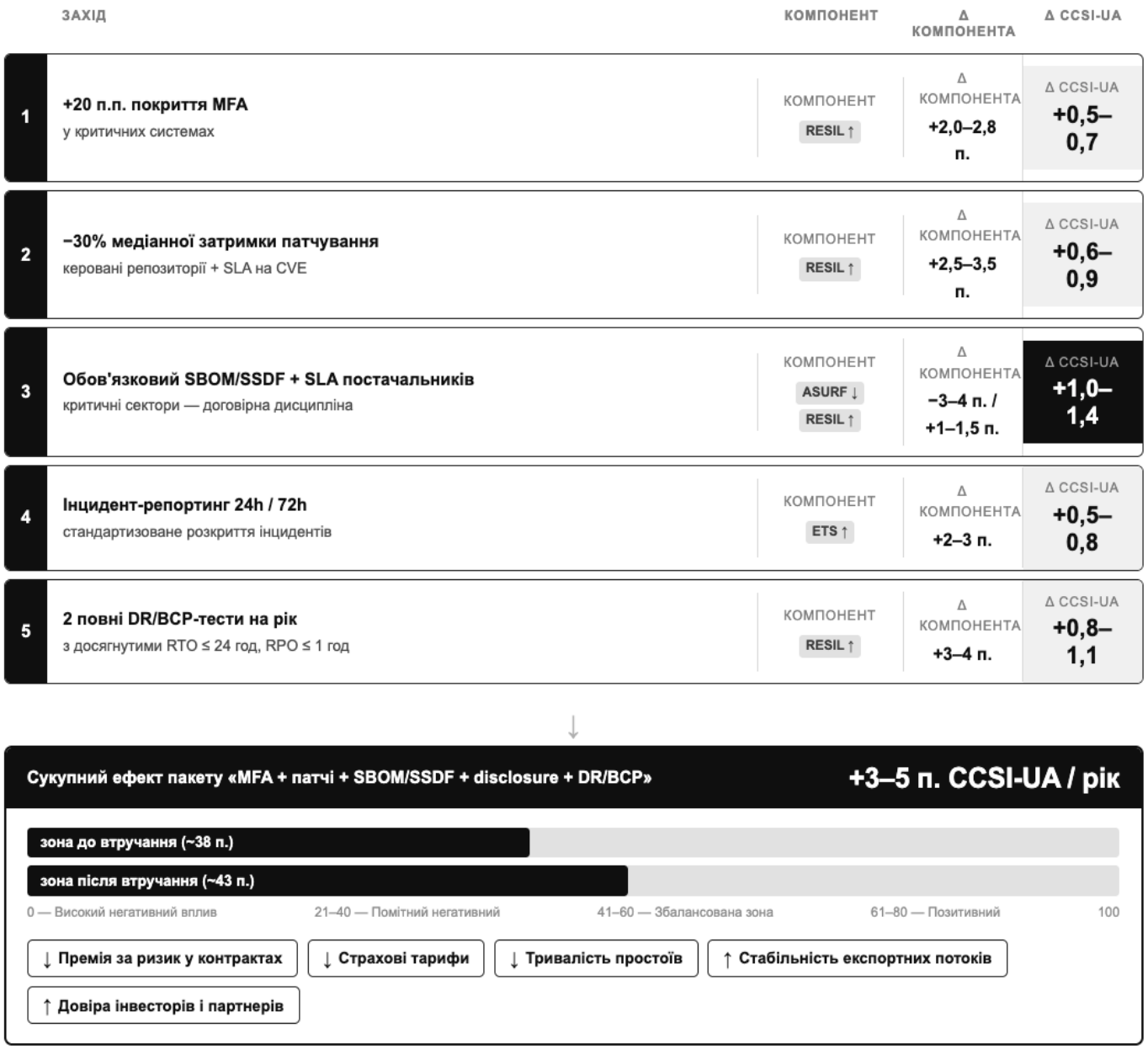

Рис. 3.4. Ефект ключових інтервенцій на CCSI-UA

Джерело: складено автором

Зазначимо зв’язок з економічними змінними. Кількісна прив'язка CCSI-UA до спостережуваних макроекономічних результатів є принциповим кроком, який відрізняє запропоновану рамку від декларативних індексів кібербезпеки: вона дозволяє констатувати, що «кібербезпека важлива», а також показати, через які

саме канали і в яких вимірюваних одиницях зміна інтегрального індексу відображається на конкурентоспроможності та економічній безпеці країни.

Методологічну основу для даних оцінок складають два взаємодоповнювальні підходи, детально описані в підрозділі 3.1. Перший – панельна модель із фіксованими ефектами (panel FE) для країн на горизонті 2015-2025, у якій залежною змінною виступає показник МКС (IC), а ключовим регресором – лагований CCSI з набором контрольних змінних (ВВП на душу населення, рівень освіти, відкритість торгівлі) та робастними стандартними похибками Driscoll–Kraay, що коректно враховують просторову та часову залежність між спостереженнями. Фіксовані ефекти на рівні країни усувають вплив незмінних у часі специфічних характеристик (географії, інституційної спадщини, культурних факторів), а часові ефекти контролюють глобальні шоки, спільні для всіх країн у певний рік. Другий підхід – подійний аналіз (event study) навколо великих кіберінцидентів у вікні T−k … T+k, який дозволяє простежити динамічний профіль ефекту до і після шоку, відокремити короткострокові реакції ринку від інерційних наслідків і верифікувати, чи були тренди до інциденту паралельними між групами порівняння.

Перший і найбільш безпосередній канал впливу – динаміка експорту послуг. Оцінки panel FE показують статистично значущу асоціацію: зростання CCSI-UA на один пункт корелює зі збільшенням темпу приросту експорту послуг у наступному році на 0,05–0,12 п.п. Для розуміння масштабу: якщо пакет п'яти описаних інтервенцій піднімає CCSI-UA на 3–5 п., то очікуваний сукупний ефект на темп експортного зростання складатиме орієнтовно 0,15–0,60 п.п. щорічно. Механізм даного зв'язку відповідає логіці, сформульованій у підрозділі 3.1: кіберзагроза транслюється у вимір конкурентоспроможності через підвищення транзакційних витрат і ускладнення контрактування, тому зворотний ефект – зниження цих витрат завдяки вищому CCSI-UA – робить українських

постачальників послуг передбачуванішими і надійнішими контрагентами для іноземних партнерів. Це особливо актуально для IT-аутсорсингу, де комплаєнс, стійкість систем і прозорість інцидент-менеджменту є прямими критеріями відбору постачальників у регульованих секторах (фінансові послуги, охорона здоров'я, державний сектор ЄС/США). Лагова структура – ефект проявляється у наступному році, а не миттєво – пояснюється тим, що довіра контрагентів формується поступово: партнери спостерігають за поведінкою постачальника протягом кількох кварталів перш ніж переглядати умови контрактів або розширювати обсяги співпраці.

Другий канал – тривалість простоїв логістичної інфраструктури після великих інцидентів. Оцінки event study демонструють: на вузлах із вищим CCSI-UA середній простій після порівнянного за масштабом інциденту скорочується на 0,5–0,9 дня відносно вузлів із нижчим індексом. Даний результат є наслідком того, що RESIL – субіндекс кіберстійкості – безпосередньо вимірює здатність систем виявляти інцидент (MTTD), локалізувати шкоду і відновлюватися (MTTR) у межах визначених параметрів DR/BCP. Для транспортно-логістичного сектору, де добовий простій великого вузла може означати зрив ланцюга постачання для десятків контрагентів і суттєві прямі фінансові втрати, скорочення середнього простою навіть на половину дня є значущим економічним результатом. Важливо, що event study контролює «паралельний тренд» до інциденту, тобто різниця у простоях не пояснюється тим, що вузли з вищим CCSI-UA спочатку зазнавали менших інцидентів – вона відображає саме відмінності у швидкості відновлення за порівнянного початкового шоку.

Третій канал – вартість капіталу і кредитні умови у фінансовому секторі. Для банків і фінансових установ спостерігається звуження кредитних спредів на 3–7 базисних пунктів (б.п.) у квартал після підтвердженого посилення

компонентів RESIL і ETS. Базисний пункт – це одна сота відсоткового пункту (0,01%), тому звуження спреду на 5 б.п. означає, що вартість залучення капіталу для установи знижується на 0,05 п.п. Для великого банку з портфелем зобов'язань у кілька мільярдів гривень це перетворюється на відчутну щорічну економію. Механізм тут іде через канал довіри, описаний у підрозділі 3.1 як «ефект ETS»: прозора політика обробки даних, відповідальне розкриття інцидентів і підтверджена стійкість DR/BCP зменшують інформаційну асиметрію між позичальником і кредитором – кредитор «бачить» реальну дисципліну захисту і закладає меншу ризикову премію. Принципово важливо, що ефект проявляється саме після «підтвердженого» посилення RESIL/ETS – тобто ринок реагує не на декларації про наміри впровадити ті чи інші контролі, а на верифіковані докази їх дієвості (пройдені DR-тести з підтвердженими RTO/RPO, публічні або регуляторно підтверджені звіти про розкриття інцидентів). Запропонований підхід підкреслює економічну цінність прозорості та вимірюваності як таких.

Сукупно зазначені ключові канали – експортна динаміка, логістична стійкість і вартість капіталу – утворюють причинно-наслідковий ланцюг, який у підрозділі 3.1 описується формально через SEM-специфікацію: ефективні технічні та процедурні заходи знижують MTTD/MTTR (операційна стійкість), що через компонент ETS транслюється у довіру контрагентів (зниження транзакційних витрат і ризикових премій), і далі відображається у показниках міжнародної конкурентоспроможності та економічної безпеки. Саме ця логіка – кібербезпека як економічна функція, а не технічна витрата – є центральною тезою рамки CCSI-UA і підтверджується наведеними кількісними орієнтирами по трьох незалежних каналах впливу (рис. 3.5).

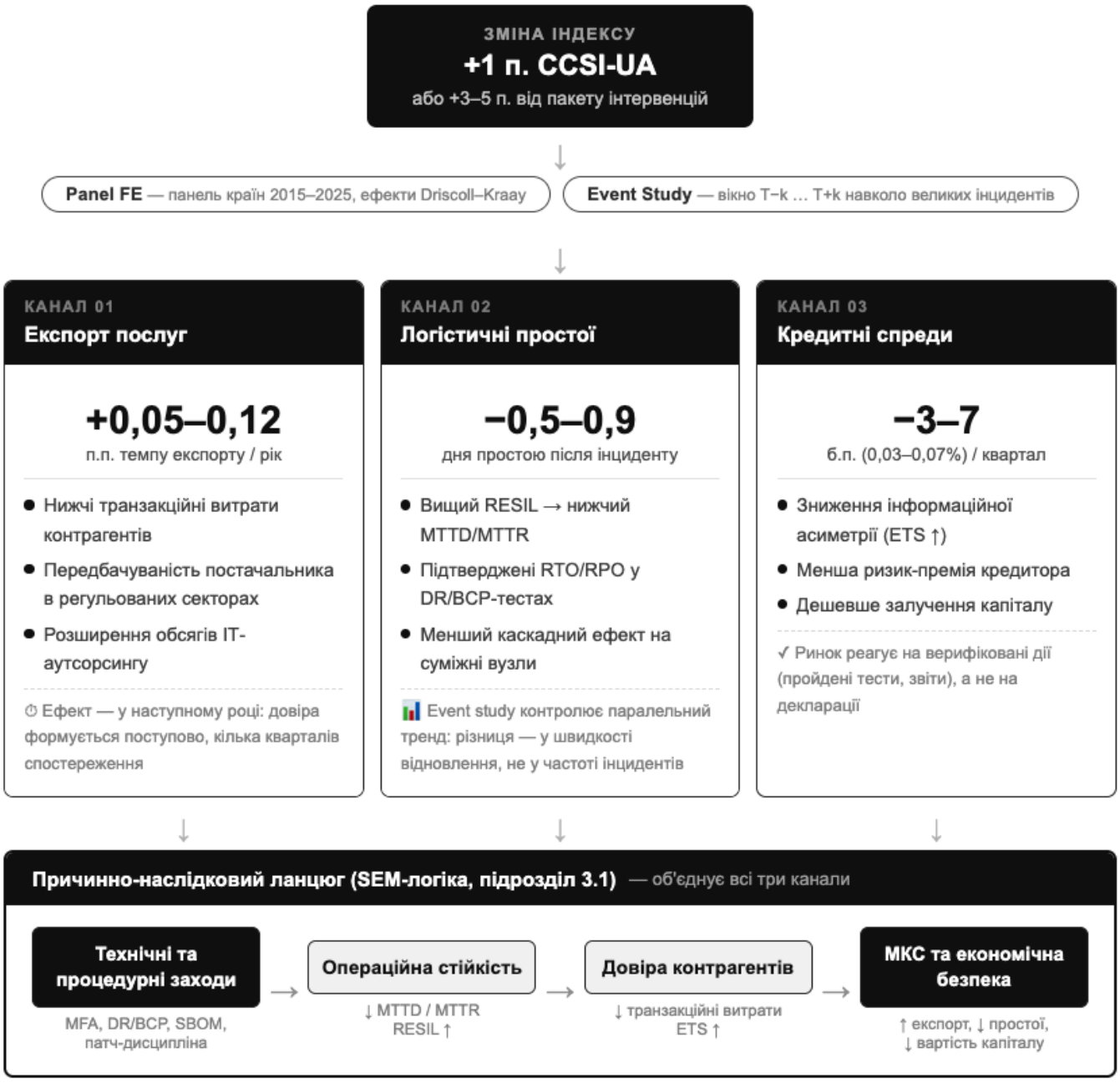

Рис. 3.5. Зв’язок CCSI-UA з економічними змінними

Джерело: складено автором

План імплементації на 2025-2026 рр. формується як каскадна послідовність взаємопов'язаних кроків, де кожний наступний елемент спирається на результати попереднього. Логіка послідовності є наступною: спочатку створюється

вимірювальна інфраструктура, без якої неможливо обґрунтовано оцінювати ефективність будь-яких заходів; потім формується нормативна рамка, що встановлює обов'язковий мінімум контролів; далі запускаються економічні стимули, що роблять цей мінімум вигідним; і нарешті розбудовується кадрова спроможність, яка забезпечує стале відтворення практик у часі. П'ятий елемент – секторальні пріоритети – не є окремим «кроком», а накладається на всі чотири як специфікація заходів під ризик-профіль кожного критичного сектору.

Інституціоналізація виміру базується на тому, що будь-яка система управління ризиком деградує без регулярного вимірювання. Саме тому першим і найбільш фундаментальним кроком є не запуск нових регуляторних вимог, а створення вимірювальної інфраструктури, яка зробить прогрес або його відсутність видимими для держави, ринку та партнерів. Це означає щоквартальне оновлення чотирьох субіндексів – SWIR (severity-weighted інциденти), ASURF (поверхня атаки), RESIL (кіберстійкість) і ETS (етика/довіра) – на основі даних CERT-UA, регуляторних реєстрів і секторних опитувань. Щоквартальна, а не річна, частота оновлення є критичною: вона дозволяє фіксувати ефекти конкретних заходів у реальному часі і дає можливість вчасно коригувати пріоритети, якщо певний компонент не демонструє очікуваної динаміки.

Паралельно необхідно проводити регулярний методологічний аудит індексу: застосування підтверджувального факторного аналізу (CFA) для перевірки того, що субіндекси дійсно вимірюють заявлені латентні конструкти, та SEM-верифікацію причинних зв'язків між компонентами. Це не формальність – без такого аудиту існує ризик, що індекс фіксуватиме поверхневі зміни (наприклад, зростання кількості зареєстрованих інцидентів через покращення звітності, а не через погіршення безпеки) і даватиме хибні сигнали для прийняття рішень. Результатом цього кроку має стати публічний CCSI-UA Dashboard – інструмент системної прозорості, який не розкриває чутливих деталей про

конкретні організації, але показує секторальні тренди, «вузькі місця» і прогрес по ключових метриках у зрозумілому для широкої аудиторії форматі. Dashboard виконує подвійну функцію: всередині країни – інструмент підзвітності для регуляторів і орієнтир для бізнесу; назовні – сигнал для іноземних партнерів та інвесторів про те, що Україна системно управляє кіберризиком, а не лише реагує на інциденти.

Нормативна конвергенція спрямована на те, щоб базові контролі перестали бути справою доброї волі і стали обов'язковою умовою участі у критичних економічних процесах. Ключовий інструмент тут – закупівельна рамка: вимоги SBOM і SSDF мають бути включені до стандартних критеріїв кваліфікації постачальників у державних закупівлях і тендерах для критичної інфраструктури. SBOM (реєстр компонентів програмного забезпечення) дозволяє замовнику точно знати, що входить до складу придбаного ПЗ і яким вразливостям воно піддається, а SSDF (стандарт безпечної розробки) встановлює мінімальну дисципліну процесу розробки на боці постачальника. Сукупно такі вимоги переводять ризик ланцюга постачання зі сфери «невідомого невідомого» у сферу контрольованих зобов'язань – і це є структурною умовою для зниження ASURF у середньостроковій перспективі.

Другий нормативний елемент – стандартизовані вимоги до розкриття інцидентів за схемою 24h/72h: раннє повідомлення регулятора протягом 24 годин після виявлення значущого інциденту і базовий звіт із класифікацією впливу та вжитими заходами протягом 72 годин. Дана норма, аналогічна вимогам директиви NIS2 в ЄС, виконує три функції одночасно: прискорює координацію між CERT-UA, галузевими ISAC і приватними SOC у кризовий момент; зменшує «тіньові збитки» від інцидентів, які зараз не потрапляють у статистику через страх репутаційних наслідків; і формує доказову базу для калібрування SWIR і ETS у рамках CCSI-UA Dashboard. Принциповим елементом архітектури цієї

норми є режим safe-harbor: організація, яка вчасно і повно розкрила інцидент, отримує пом'якшення регуляторної відповідальності, що усуває головний стимул до приховування і переводить систему з моделі «покарати за інцидент» у модель «навчитися з інциденту».

В частині фінансових стимулів необхідно зазначити, що нормативні вимоги встановлюють мінімум, але не створюють стимулів для перевищення цього мінімуму. Саме тут необхідні фінансові механізми, що роблять інвестиції у кіберстійкість економічно раціональними. Центральний інструмент – диференційована страхова тарифікація: компанії, що підтверджують досягнення KPI стійкості (MFA-покриття не менше 90% критичних систем, регулярні DR/BCP-тести з документованими результатами RTO/RPO, патч-SLA із строками ≤15 днів для критичних вразливостей, впровадження Zero Trust-архітектури для адміністративного доступу), отримують знижені страхові тарифи в діапазоні 15–20% від базового рівня. Механізм тут прямий: страховик закладає нижчу ризик-премію, бо верифіковані контролі знижують ймовірність і масштаб страхового випадку. Для цього страховики потребують стандартизованої методики оцінки кіберзрілості – і CCSI-UA Dashboard може виступати таким спільним орієнтиром, узгодженим між регулятором, страховою галуззю і бізнесом.

Другий фінансовий інструмент – пільгові умови кредитування або доступ до державних гарантій для організацій із підтвердженим рівнем RESIL/ETS. Логіка відповідає результатам, описаним у блоці «Зв'язок з економічними змінними»: звуження кредитних спредів на 3–7 б.п. спостерігається на ринку самостійно після верифікованого посилення компонентів – державні стимули можуть прискорити цей ефект і поширити його на підприємства, для яких ринковий механізм спрацьовує повільніше через менший масштаб і нижчу видимість для кредиторів. Третій елемент – ваучерна програма для малого і середнього бізнесу: субсидоване підключення до керованих сервісів безпеки (MDR/XDR) через

регіональні IT-кластери, що дозволяє підприємствам отримати «дорослий» рівень моніторингу і реагування без необхідності утримувати власний SOC.

В частині кадрової спроможності слід зазначити, що жоден із попередніх кроків не є стійким без достатньої кількості кваліфікованих фахівців, здатних реалізовувати і підтримувати відповідні практики. Дефіцит кадрів у кібербезпеці є структурною проблемою для більшості країн, але в Україні він особливо гострий через поєднання воєнних втрат, міграції та хронічного недофінансування освітнього контуру. Відповідь на дану проблему має бути багаторівневою.

Перший рівень – дуальні програми «університет–роботодавець» у форматі, де студент одночасно навчається і працює в реальному середовищі, а навчальний план визначається спільно академічними партнерами і практикуючими організаціями. Особливий пріоритет – міждисциплінарні траєкторії, що поєднують технічний компонент (DFIR, OT-безпека, хмарна архітектура) з правовим і ризик-менеджментним, оскільки економічна кібербезпека потребує фахівців, які розуміють і технічний механізм атаки, і її юридичні наслідки, і вплив на фінансову звітність організації. Окремо важливий трек OT/ICS-безпеки – для енергетики, транспорту і промисловості, де дефіцит компетенцій є найбільш критичним і де неправильне реагування на інцидент може мати фізичні, а не лише цифрові наслідки.

Другий рівень – кіберполігони як постійна інфраструктура навчання і симуляцій. На відміну від разових тренінгів, полігони дозволяють регулярно відпрацьовувати реалістичні сценарії атак (включно з live-fire вправами і table-top для керівництва) і формувати «м'язову пам'ять» команд реагування. Кожен макрорегіон має мати щонайменше один такий полігон, доступний для держсектору, операторів критичної інфраструктури і бізнесу. Третій рівень – стандартизовані плейбуки і runbooks для підприємств: готові до використання процедури реагування на найпоширеніші типи інцидентів (рансомвер, DDoS,

компрометація облікових даних, витік даних), адаптовані під обмежені ресурси малого бізнесу і розповсюджені через кластери та галузеві асоціації. Це знижує «вхідний поріг» для базової кібергігієни і зменшує розрив між великими організаціями та підприємствами, який є головним джерелом «масової поверхні атаки» у ланцюгах постачання.

Горизонтальні заходи попередніх чотирьох кроків необхідно доповнити секторальними пакетами контролів, адаптованими під специфічний ризик-профіль кожного критичного сектору. Для транспорту і логістики, як кіберфізичної системи з прямим зв'язком між цифровим і фізичним рівнями, пріоритетом є OT-сегментація (ізоляція операційних технологій від корпоративних мереж за моделлю Purdue), валідація сенсорних даних (GNSS-позиціонування, відеоаналітика, телеметрія рухомого складу – усі є потенційними векторами маніпуляції), а також жорстка дисципліна постачальників обладнання через SBOM і SLA. Для енергетики і OT/ICS-середовищ, де інциденти можуть призводити до фізичних відключень і каскадних наслідків для всієї економіки, ключовими є унідирекційні шлюзи (data diodes) між OT і IT-мережами, де це технологічно можливо, моніторинг аномалій OT-протоколів (Modbus, DNP3, IEC 61850) і регулярні DR-сценарії з ручними режимами управління, що дозволяють підтримувати керованість навіть за повної недоступності цифрових систем. Для фінансового сектору, де основними загрозами є деструктивний рансомвер і шахрайські транзакції, пріоритетами виступають MDR/XDR із поведінковою аналітикою транзакцій, апаратна MFA для привілейованого доступу і незворотні резервні копії за моделлю «повітряного зазору», що унеможливлюють знищення backup рансомвером. Для державних е-сервісів і реєстрів, де компрометація означає втрату довіри громадян до цифрових публічних послуг, критичними є Zero Trust-архітектура, управління ключами і секретами через централізовані HSM/Vault-рішення, регулярні пентести і red-team вправи, а також формалізовані

процедури прозорого розкриття інцидентів, що демонструють підзвітність держави перед громадянами.

Таким чином, реалізація запрпонованого плану протягом 2025-2026 років формує основу для переходу до наступного горизонту: коли кіберстійкість підтримується і правилами, і ринком, і людським капіталом одночасно, а CCSI-UA Dashboard стає інструментом внутрішнього моніторингу та зовнішньої верифікації надійності України як партнера у глобальних ланцюгах вартості.

3.3. Механізми та інструменти підвищення ефективності заходів держави щодо мінімізації впливу глобальних кіберзагроз на економіку України

Системні кібервиклики для енергетики, зв'язку, фінансів, державних е-сервісів і транспортно-логістичної інфраструктури потребують не лише технологічних рішень, а й цілісної інституційної архітектури управління ризиком. У реаліях війни та високої інтенсивності гібридних загроз державна політика має бути орієнтована не на «ідеальний захист від проникнень», а на керованість наслідків: зменшення ймовірності інцидентів, обмеження масштабу шкоди, підтримання безперервності критичних послуг і прискорення відновлення. В даному контексті кібербезпека фактично стає елементом економічної політики, адже визначає ціну ризику для бізнесу, доступ до довгих контрактів, інвестиційну привабливість і здатність України інтегруватися в міжнародні ланцюги створення вартості.

З огляду на логіку «кібергігієна → довіра → конкурентоспроможність», сформульовану нами, державні механізми доцільно розглядати як набір практичних інструментів, що масштабують мінімальну планку контролів на рівень економіки, а IT-сектор перетворюють на мультиплікатор національної

кіберстійкості. Запропонований підхід означає, що фокус зміщується від реактивного підходу «гасіння пожеж» до системного проєктування правил, які автоматично підвищують захищеність: через регуляторні вимоги, закупівельні критерії, стандартизовані моделі відповідальності постачальників, стимули для впровадження базових практик, вимірювані KPI та прозоре інцидент-управління. Конкретна операціоналізація цих механізмів у вигляді вимірюваних інтервенцій та їхнього кількісного ефекту на CCSI-UA розглядається в наступних підрозділах.

У прикладній площині ключові стратегічні цілі держави можна сформулювати як зміну п'яти взаємопов'язаних параметрів безпеки економіки. По-перше, необхідно зменшити експозицію, тобто скоротити відкриту площу атаки в критичних секторах і ланцюгах постачання. На мові політики це означає інвентаризацію активів, дисципліну патч-менеджменту, контроль зовнішніх сервісів, мінімізацію небезпечних інтеграцій і підвищення вимог до постачальників, адже значна частина ризику «імпортується» через бібліотеки, підрядників, хмарні сервіси і сторонні компоненти. По-друге, необхідно підвищити стійкість як здатність систем функціонувати під тиском атак і відновлюватися в гарантовані строки: зниження MTTD/MTTR, сегментація критичних систем, масштабування багатофакторної автентифікації, регулярні DR/BCP-випробування, формування чітких режимів деградації (щоб навіть за інциденту країна не втрачала керованість інфраструктурою). По-третє, важливо інституціоналізувати прозорість і етику, бо довіра у цифровій економіці є ресурсом: швидкі правила повідомлення про інциденти, стандарти якості розкриття, privacy-by-design та ethics-by-design у державних сервісах і в ланцюгах постачання знижують інформаційну асиметрію для партнерів, роблять ризик прогнозованішим і пом'якшують репутаційний ефект інцидентів. По-четверте, держава має інтегрувати безпеку в економічні механізми: зробити базові контролі та комплаєнс умовою держзакупівель, ліцензування, доступу до певних ринків, а

також фактором тарифікації страхування, кредитування й участі в інфраструктурних проєктах. Це створює систему стимулів, у якій безпека перестає бути доброю волею і стає економічно вигідною поведінкою. І нарешті, по-п'яте, необхідно активувати IT-сектор як інфраструктуру стійкості, масштабуючи керовані сервіси (MDR/XDR), галузеві центри обміну інформацією та реагування, кластери, освітні треки і практичні полігони, які прискорюють дифузію компетенцій і знижують розрив між великими організаціями та бізнесом.

Перші дві цілі – зменшення експозиції та підвищення стійкості – операціоналізуються через компоненти ASURF і RESIL інтегрального індексу CCSI-UA, третя ціль відображається у субіндексі ETS, тоді як четверта і п'ята забезпечують інституційні та ринкові умови для масштабування всіх трьох компонентів на рівень економіки в цілому.

У сукупності зазначені цілі формують не декларативну програму, а каркас державної політики, в якій інструменти мають працювати каскадно: менша експозиція знижує частоту інцидентів, стійкість обмежує їх економічний шок, прозорість і етичне управління підтримують довіру до цифрових сервісів, а економічні стимули роблять ці практики масовими. Саме така зв'язка і дає ефект на рівні країни – коли кібербезпека перестає бути витратною статтею й перетворюється на фактор конкурентоспроможності та економічної безпеки України (рис. 3.6).

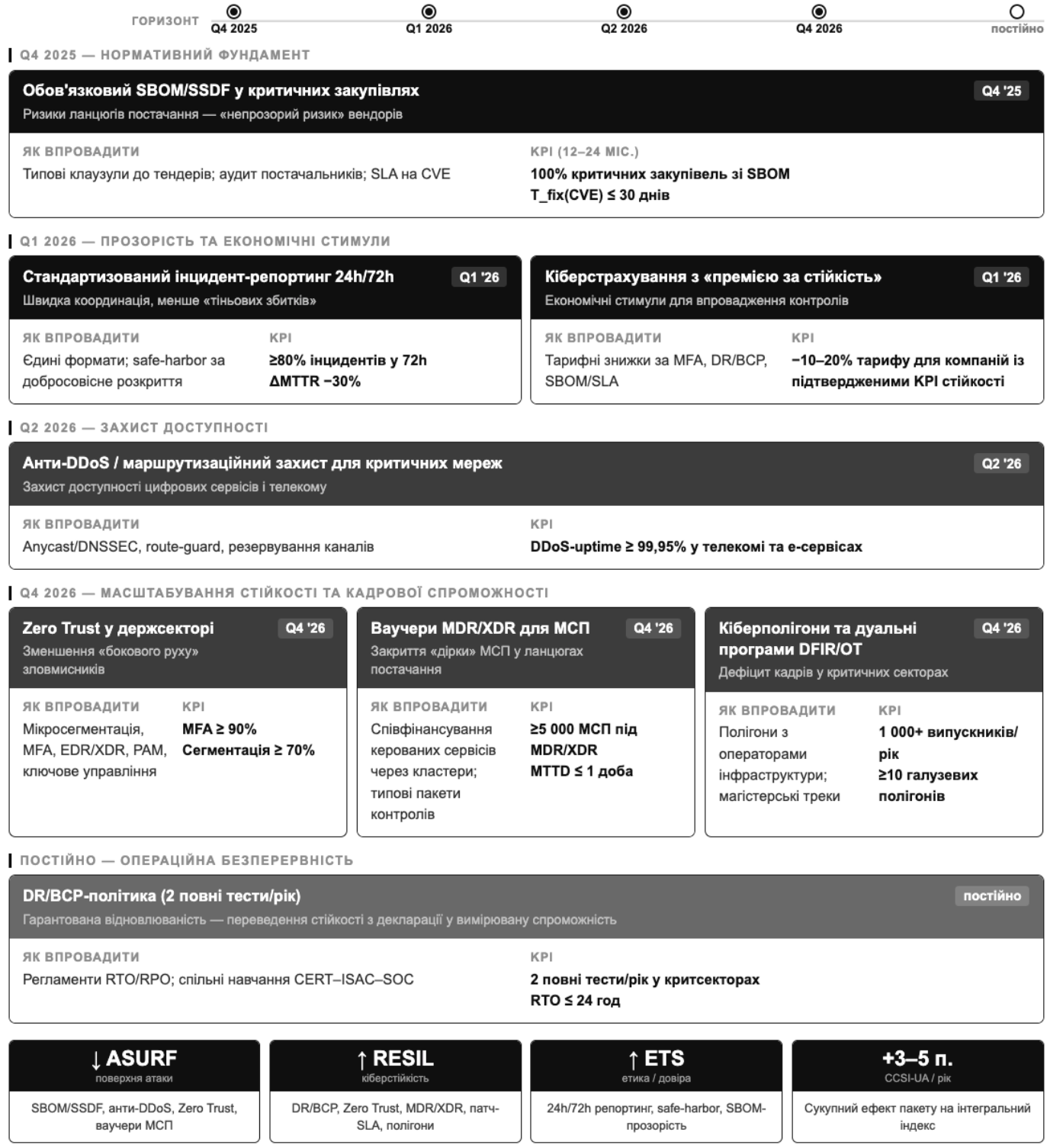

Рис. 3.6. Політична матриця інструментів (державний рівень)

Джерело: складено автором.

Операційна модель державно-приватної взаємодії доцільно вибудовується як безперервний контур колективної кіберстійкості, де державні та приватні суб'єкти виконують різні ролі, але працюють у спільній логіці раннього попередження, швидкого виявлення та масштабованого реагування. У практичному вимірі оптимальна конструкція виглядає як зв'язка CERT-UA ↔ галузеві ISAC ↔ приватні SOC/MDR, у межах якої відбувається постійний обмін індикаторами компрометації та тактиками атак (IOCs/TTPs) із застосуванням машинозчитуваних форматів STIX/TAXII. Ключова цінність такої схеми полягає в тому, що «термінові бюлетені» не залишаються текстовими повідомленнями, а перетворюються на операційний контент: правила кореляції для SIEM, детектори для EDR/XDR, плейбуки для SOAR та рекомендації з митигування, які можуть бути розгорнуті у середовищах багатьох організацій протягом годин, а не тижнів. Паралельно регулярні спільні навчання – як table-top, так і live-fire – синхронізують сценарії реагування та зменшують «координаційну ціну» взаємодії, коли в реальному інциденті критичними стають не гасла, а швидкість та узгодженість виконання процедур.

Щоб така модель не залежала від персоналій і працювала як інституція, вона має спиратися на прозору RACI-логіку розподілу відповідальності. Регулятор задає обов'язковий мінімум контролів і строки виконання (зокрема щодо інцидент-репортингу та вимог до постачальників), CERT виконує роль координатора обміну й централізації загрозової інформації, галузеві ISAC агрегують її у форматі, релевантному для конкретних секторів (енергетика, фінанси, телеком, транспорт), а приватні SOC/MDR забезпечують 24/7 моніторинг, детекцію та реагування в інфраструктурі організацій. Водночас вендори та постачальники технологій мають бути зобов'язані не загальними формулюваннями «дбати про безпеку», а чіткими SLA на усунення уразливостей,

вимогами до прозорості компонентів і можливістю аудитів критично важливих процесів. Окремо важливо закріпити режим safe-harbor і практику анонімізованих post-mortem-розборів, які знімають репутаційний бар'єр для розкриття інцидентів і переводять систему з моделі «приховати проблему» у модель «швидко навчитися та зменшити ризик для всіх». Саме це формує ефект колективного навчання: коли помилка або проникнення в одному вузлі стає приводом посилити захист у всій галузі, а не перетворюється на повторюваний шаблон атаки.

На рівні інструментарію, який можна одразу інтегрувати в практику держсектора та критичних підприємств, доцільно закріплювати регуляторні та договірні вимоги, придатні для включення у типові контракти. Для безпеки ланцюгів постачання базовими додатками мають виступати SBOM та SSDF, що забезпечують прозорість компонентів і дисципліну безпечної розробки, а також право замовника проводити аудит безпекових процесів постачальника. З погляду контрактної керованості ризику критичною є прив'язка до вимірюваних строків усунення уразливостей: наприклад, SLA на виправлення із орієнтиром critical ≤ 15 днів, high ≤ 30 днів (з можливістю скорочення строків для критичної інфраструктури). Логічним продовженням є прописана політика патч-менеджменту для ядра систем, агентів безпеки та прошивок із гарантованими вікнами оновлення і контролем винятків, а для критичних SaaS-процесів – механізми escrow (депозит коду/критичних даних або умов доступу), які знижують ризики недоступності або припинення сервісу.

Не менш важливими є вимоги, що формують базову «несучу конструкцію» захисту: Zero Trust-підхід для доступу та інтеграцій (MFA для адміністративних ролей, принцип найменших привілеїв, сегментація критичних зон), обов'язкове журналювання з визначеним строком зберігання (наприклад, «не менше N днів» залежно від класу системи), а також резервні копії з високою відновлюваністю, включно з моделлю «повітряного зазору» для захисту від шифрувальників і

деструктивних кампаній. Окремим блоком має бути інцидент-клаузула, яка забезпечує передбачуваність взаємодії в кризі: повідомлення раннього попередження упродовж 24 годин, базовий звіт упродовж 72 годин і фінальний звіт, наприклад, у межах 30 днів – із фіксацією TTP, IOC, масштабу впливу та виконаних дій відновлення. Така стандартизація робить реагування керованим процесом, а не імпровізацією, і водночас створює основу для аналітики, порівняння ефективності та накопичення організаційної пам'яті безпеки.

Роль IT-сектору як мультиплікатора національної кіберстійкості полягає у виробництві технологій, а також в масштабуванні практик, стандартів і компетенцій у ті сегменти економіки, де власної спроможності до безпеки бракує. За даного підходу IT-сектор виступає механізмом швидкого «розгортання спроможностей» для держави, критичної інфраструктури та малого бізнесу, який формує ефект масштабу: одна й та сама інженерна дисципліна (MFA, патч-менеджмент, бекапи, моніторинг, сегментація, інцидент-репортинг) перестає бути привілеєм великих організацій і стає базовою нормою для широкого кола суб'єктів. Такий мультиплікативний ефект підсилюється тим, що кібербезпека має економічний вимір довіри: чим більш прогнозованою є поведінка систем під навантаженням атак, тим нижчими стають транзакційні витрати у зовнішніх контрактах і тим стійкішими – ланцюги вартості.

Найбільш практичною формою такого мультиплікатора є керовані сервіси безпеки, які дозволяють державі та бізнесу отримати «дорослий» рівень захисту без необхідності утримувати повний штат профільних фахівців. Моделі MDR/XDR/SIEM-as-a-Service дають безперервний моніторинг, кореляцію подій, швидке реагування та керовану ескалацію інцидентів, а також стандартизовані плейбуки і runbooks. Додатково важливими є групи швидкого реагування DFIR, здатні оперативно включатися у форензик, локалізацію та відновлення, а також threat-intel-компонента, яка «приземлює» глобальні шаблони атак у конкретний

регіональний контекст через аналіз локальних TTP. Для України це особливо актуально, оскільки висока інтенсивність атак робить швидкість детекції та відновлення важливішою за ідею абсолютної непроникності.

Другий мультиплікатор – кластеризація IT-ринку, яка працює як канал розповсюдження мінімальної планки контролів у регіонах і секторах, де безпека традиційно «відстає» через дефіцит бюджету, кадрів або управлінської уваги. Регіональні IT-кластери тут виступають не просто як ком'юніті, а як інфраструктура норм: вони можуть бути «розподільниками» стандартів кібергігієни для бізнесу та місцевих органів влади, провідниками типових політик і шаблонів (від паролів та MFA до резервного копіювання й сегментації), а також майданчиками для кооперації між університетами, вендорами та замовниками. У результаті мінімальні контролі набувають форми рекомендацій та практичної дисципліни, яка уніфікує підходи та зменшує розкид якості захисту в країні.

Третій напрям – освітній контур, без якого мультиплікація не може бути стійкою. Тут ключем є не лише класична підготовка «кіберфахівців», а формування міждисциплінарних траєкторій, що з'єднують право, техніку й ризик-менеджмент (бо ЕБ не зводиться до інструментів – вона базується на процедурах, відповідальності та вимірюваності). Дуальні програми «університет–роботодавець», мікросертифікації, кіберполігони, симуляційні вправи й спеціальні STEM-треки для OT/ICS-безпеки дозволяють зменшити дефіцит кадрів саме там, де вразливість найбільш критична: в енергетиці, транспорті, телекомі та індустріальних системах. Зазначене підсилює здатність держави і бізнесу переходити від «реактивного гасіння» до керованої кіберстійкості з планами відновлення та перевірюваними результатами.

Окремий ефект дає експорт кіберпослуг, який створює валютну виручку і водночас накопичує практики, що можуть бути перенесені у внутрішні сектори. Коли українські команди працюють на вимогливих ринках (ЄС/США/Велика

Британія) з жорсткими рамками комплаєнсу, вони привозять назад не тільки гроші, а й культуру процесів: структуровані runbooks, правила детекції, відпрацьовані сценарії реагування, дисципліну звітності, вимірювані KPI стійкості. У сукупності це формує репутаційний капітал країни як «постачальника спроможностей», що напряму впливає на довіру та міжнародну конкурентоспроможність.

Важливо, що мультиплікативний ефект посилюється через прозорість і етику, які перетворюють кібербезпеку на елемент довіри, а не на закриту «чорну скриньку». Публікація технічних розборів інцидентів (у межах безпечної анонімізації), розвиток процедур disclosure, впровадження privacy-by-design у стартапах і практики «права на пояснення» для алгоритмічних рішень знижують інформаційну асиметрію між бізнесом, державою та зовнішніми партнерами. У цифровій економіці це працює як окрема валюта: контрольованість, підзвітність і передбачуваність піднімають якість контрактування та спрощують доступ до «довгих» ринків.

Щоб роль IT-сектору масштабувалася не декларативно, а операційно, доцільно розглядати державні інтервенції через секторальні мікропакети – мінімальні контрольні набори, адаптовані під ризик-профіль кожної критичної галузі. Для енергетики та OT-середовищ базовим ядром стає сегментація за моделлю Purdue, унідирекційні шлюзи там, де це можливо, моніторинг аномалій OT-протоколів, інвентар активів із «цифровими паспортами» та відпрацьовані DR-сценарії з ручними режимами, які дозволяють підтримувати керованість навіть у деградації. Для телеком-сектору ключовими є механізми стійкості мережевої інфраструктури: захист BGP і DNS (включно з DNSSEC), архітектура автономних «клітинок» мережі, резервування маршрутів і постійний SOC-моніторинг сигнальних протоколів. Для фінансів пріоритетом виступають поведінкова аналітика транзакцій, апаратна MFA для привілейованого доступу,

незворотні бекапи та регулярні вправи red/purple-team, що підтримують реалістичність захисту. Для державних е-сервісів і реєстрів критичним є Zero Trust, управління ключами й секретами, регулярні пентести та формалізовані процедури прозорого розкриття інцидентів. Для транспорту і логістики, як кіберфізичної системи, необхідні OT-сегментація, жорстка дисципліна постачальників (SBOM/SLA), валідація сенсорів (GNSS/відео/телеметрія), георепліkація даних та сценарії «graceful degradation», які дозволяють зберігати функціонування в режимі обмежених можливостей (див. дод. Г).

У підсумку саме так IT-сектор стає мультиплікатором: він переводить безпеку з «проєкту для великих» у системний стандарт, який масштабовано вбудовується в державні процеси, критичну інфраструктуру й бізнес, а через прозорість, етику та контрактну дисципліну перетворює кіберризики на контрольовані операційні ризики, що підвищують довіру і конкурентоспроможність країни.

Дорожню карту впровадження на 2025-2027 роки доцільно будувати як послідовний перехід від нормативної уніфікації до масштабування практик і далі – до закріплення економічних стимулів, щоб кіберстійкість стала не разовим проєктом, а стабільною частиною державного управління та ринкової поведінки. У вікні 2025-2027 логіка реформи може виглядати як «спочатку правила й базові інструменти», потім «обов'язкова дисципліна для критичних секторів», далі «масовий стандарт і прозорі метрики», і фінально – «ринкова ціна ризику та премія за стійкість».

У IV кварталі 2025 року фокус має бути на створенні єдиного договірного й процедурного фундаменту: затвердженні типових клаузул для постачальників щодо SBOM/SSDF і SLA на усунення уразливостей, запуску інструментів підтримки малого бізнесу через ваучери на MDR/XDR (як швидкий спосіб закрити кадровий та інструментальний дефіцит у бізнесі), а також старті пілотних

впроваджень Zero Trust щонайменше у трьох центральних органах влади. Саме цей етап задає єдину мову вимог, яку потім можна масштабувати через закупівлі, ліцензування та контроль критичних ланцюгів постачання.

У II кварталі 2026 року дорожня карта має перейти від рамки до дисципліни. Відповідно до політичної матриці інструментів, на даному етапі запускається обов'язковий інцидент-репортинг у форматі 24/72 (раннє попередження та базовий звіт), а також посилення стійкості цифрової доступності через анти-DDoS і route-guard – передусім у телекомі та державних е-сервісах. Паралельно проводиться перший повний цикл секторальних DR/BCP-тестів. Це критичний момент, бо саме регулярні перевірки відновлюваності переводять стійкість у вимірювану спроможність із гарантованими RTO/RPO, а не в декларацію «ми готові».

У IV кварталі 2026 року пріоритетом має стати масштабування: розширення Zero Trust-архітектур на ширше коло державних і критичних систем, досягнення рівня сегментації критичних середовищ не менше 70%, а також доведення дисципліни розкриття до практичного стандарту – щоб щонайменше 80% інцидентів отримували первинний звіт у межах 72 годин. Додатково на даному етапі доцільно запустити перший публічний CCSI-UA Dashboard як інструмент системної прозорості: він не розкриває чутливих деталей, але показує тенденції, вузькі місця і прогрес по ключових метриках стійкості.

У 2027 році дорожня карта має завершити перехід до економічно самопідтримуваної моделі: коли страхові тарифи й умови контрактів починають прямо відображати премію за стійкість, а не карати вже за факт інциденту. Паралельно ключовими орієнтирами стають 100% SBOM-покриття критичних постачальників, а також розгортання кіберполігонів у кожному макрорегіоні як постійної інфраструктури навчання і симуляцій (table-top/live-fire) для держсектору, операторів критичної інфраструктури та бізнесу. Така комбінація

означає, що країна переходить до режиму, де кіберстійкість підтримується і правилами, і ринком, і людським капіталом одночасно.

Щоб розроблена дорожня карта не розчинилась у процесі виконання, потрібна зрозуміла панель KPI на національному рівні. Узагальнюючи контрольні пороги, описані в розрізі окремих інструментів вище, реалістична панель включає: покриття MFA для критичних систем не менше 90%; MTTD ≤ 24 год та MTTR ≤ 72 год; строки патч-менеджменту для критичних і високих уразливостей (≤ 15 / ≤ 30 днів відповідно); не менше двох повних DR/BCP-тестів на рік у кожному критичному секторі з цільовими RTO ≤ 24 год і RPO ≤ 1 год; 100% SBOM-покриття критичних закупівель; ≥ 80% значущих інцидентів із 72-годинним репортингом; не менше 5 000 підприємств під керованими сервісами безпеки. Інтегральний результат цього пакета відслідковується через очікуване зростання CCSI-UA на +3–5 пунктів на рік, що фіксує ефект не окремої технології, а всієї політики як системи (див. дод. Е).

Методологічна новизна полягає у запропонованій рамці CCSI (Composite Cybersecurity Impact), яка поєднує чотири взаємопов'язані виміри – SWIR (severity-weighted інциденти як міра реальної інтенсивності й «ваги» атак), ASURF (площа атаки як відображення цифрової експозиції та залежності від інфраструктурних провайдерів), RESIL (кіберстійкість як здатність локалізувати шкоду й відновлювати критичні функції), а також ETS (етика/довіра як інституційний чинник економіки довіри). Принципово важливо, що етичний компонент інтегровано не як декларативний елемент, а як методологічний медіатор і модератор: він пояснює, яким чином стійкість перетворюється на міжнародну довіру, і водночас підсилює або послаблює ефект технічних і процедурних заходів у конкурентній боротьбі. У такій постановці ETS є повноцінним каналом впливу на міжнародну конкурентоспроможність та економічну безпеку.

Аналітичний результат для України демонструє практичну цінність інтегрального підходу. За умов високої загрозової експозиції – зумовленої цифровізацією критичних мереж, активною залежністю від хмарних сервісів і постачальників, а також системним характером атак у гібридній війні – Україна водночас проявляє позитивну динаміку стійкості, яка в реальних секторах набирає вимірюваної форми через сегментацію середовищ, відпрацьовані режими DR/BCP, еволюцію до Zero Trust, а також практику швидкої координації між CERT, галузевими структурами та приватними SOC. Додатково посилюється компонент прозорості – інцидентність дедалі менше сприймається як суто репутаційний ризик і дедалі частіше стає інструментом колективного навчання. Сукупно це означає, що кіберризик дедалі більше трансформується у керований операційний ризик, який помітно слабше б'є по ключових макроекономічних каналах – експортній спроможності, безперервності логістики та вартості капіталу.

Нами обґрунтовано причинно-наслідковий механізм, що з'єднує кіберстійкість із міжнародною конкурентоспроможністю. Його логіка полягає в тому, що ефективні технічні й процедурні заходи (архітектурні контролі, стандартні плейбуки реагування, дисципліна оновлень, безпека постачання) забезпечують нижчі значення MTTD/MTTR і прогнозовану відновлюваність критичних функцій. Далі цей технічний результат переходить у інституційний вимір: прозоре й етично обґрунтоване управління даними (приватність-за-замовчуванням, підзвітність, контроль дискримінаційних ефектів алгоритмів, коректні процедури розкриття інцидентів) формує довіру контрагентів, знижує транзакційні витрати контрактування та покращує умови фінансування. У підсумку це відображається в міжнародній конкурентоспроможності й економічній безпеці: країна стає передбачуванішою для довгих контрактів, менш ризиковою для партнерських ланцюгів вартості й стійкішою до шоків.

З позиції державної політики зазначені закономірності транслюються у практичні важелі впливу на показники CCSI. Пакет інтервенцій, який включає вимоги SBOM/SSDF у державних закупівлях, 24h/72h інцидент-репортинг, масштабування Zero Trust у держсекторі, регулярні DR/BCP-тести як нормативний стандарт, підтримку бізнесу через ваучери на MDR/XDR, а також інфраструктурні механізми на кшталт анти-DDoS/route-guard для критичних мереж, формує кумулятивний ефект: підвищує RESIL, знижує ASURF, нормалізує SWIR у довшому горизонті та зміцнює ETS через правила прозорості й підзвітності. Саме в такому форматі політика перестає бути узагальненою стратегією і стає інструментом керування ризиковою премією – у страхуванні, у вартості фінансування, у контрактних умовах для експортерів і постачальників.

Окремо слід підкреслити роль IT-сектору як системного мультиплікатора змін. Нами встановлено, що IT-сектор забезпечує не лише технологічні рішення, а й процеси, сервіси та кадри: керовані сервіси безпеки (MDR/XDR), DFIR-групи, threat intelligence, DevSecOps і практики secure-by-design. Через кластеризацію ринку та поширення стандартних мінімальних контролів він здатен масштабувати базову кібергігієну на підприємства, тим самим знижуючи системні вразливості на рівні країни. У такій конструкції зменшується розрив між великими організаціями та малим бізнесом, який зазвичай і формує масову поверхню атаки для каскадних інцидентів у ланцюгах постачання.

Секторальні пріоритети визначаються критерієм найбільшого дельта-ефекту від інвестицій у стійкість. Найвищий результат очікується у транспорті й логістиці, де OT-сегментація, вимоги SBOM/SLA до вендорів і сенсорна валідація (GNSS/відео/телеметрія) напряму зменшують ризик каскадних простоїв; у телекомі, де BGP-захист, Anycast та DNSSEC стабілізують доступність і знижують шанси знеструмлення цифрових послуг; в енергетиці, де унідирекційні шлюзи й OT-моніторинг є ключем до недопущення масштабних відключень; у фінансовому

секторі, де поведінкова аналітика й незворотні бекапи обмежують ризик деструктивного шантажу; а також у державних е-сервісах, де ключове управління й безперервні пентести знижують ризики компрометації реєстрів та довіри громадян і бізнесу.

Критичною умовою зменшення ASURF і запобігання каскадним збоям визначено управління ланцюгами постачання через контрактні механізми: обов'язковість SBOM і SSDF, SLA на закриття CVE, право аудиту процесів постачальника, а також escrow-резервування коду і даних для критичних SaaS. Це переводить ризики постачання зі сфери невизначеності у сферу контрольованих зобов'язань і підсилює передбачуваність для критичних секторів.

У цій логіці етика-by-design постає як економіка довіри, а не як моральне доповнення. Приватність-за-замовчуванням, підзвітність, недискримінаційні алгоритми та прозорі пост-мортерни інцидентів формують премію за передбачуваність, яка напряму впливає на інвестиційну привабливість, якість експортних контрактів і стійкість до зовнішніх шоків. Саме тому дорожня карта 2025–2027 має сенс лише тоді, коли її кроки фіксуються вимірюваними KPI – з порогами MFA $\geq$ 90%, 72h-репортинг $\geq$ 80%, RTO $\leq$ 24h, 100% SBOM у критичних закупівлях і охопленням не менше 5 тис. підприємств керованими сервісами безпеки, що переводить політику з площини декларацій у простір практичних зобов'язань.

Перспективи подальших досліджень логічно пов'язані з розширенням даних і посиленням ідентифікації причинних ефектів. Методологічно доцільно поглиблювати базу ETS через показники DPIA, AI-аудитів і процедур прозорості інцидентів, розвивати event-study підходи для вимірювання логістичних простоїв і застосовувати SEM/DiD для оцінки впливу регуляторних змін – зокрема, запровадження обов'язкового SBOM і стандартів постачальницької дисципліни.

Таким чином можемо зробити висновки, що інтегральна оцінка включає поєднання технічної стійкості (RESIL) та етико-довірчого управління (ETS) та є складовою кібербезпеки та повноцінним макроекономічним інструментом підвищення міжнародної конкурентоспроможності. Емпіричні оцінки підтверджують, що зростання CCSI-UA на один пункт асоціюється з покращенням темпу експорту послуг на 0,05–0,12 п.п. у наступному році, скороченням середнього логістичного простою після великих інцидентів на 0,5–0,9 дня та звуженням кредитних спредів у фінансовому секторі на 3–7 б.п. за квартал – що робить кібербезпеку вимірюваним чинником конкурентної позиції країни, а не лише технічною характеристикою IT-ландшафту. В даній моделі IT-сектор України виступає центральним носієм змін і механізмом масштабування найкращих практик, тоді як державна політика є каталізатором, що перетворює фрагментарні практики окремих організацій на національний стандарт стійкості та довіри.

Висновки до розділу 3

1. Встановлено, що оцінювання впливу глобальних кіберзагроз на міжнародну конкурентоспроможність та економічну безпеку країн потребує переходу від вузького технічного трактування кіберризику до комплексного економіко-інституційного підходу. Показано, що кіберінциденти трансформуються у макроекономічні втрати через канали транзакційних витрат, безперервності діяльності, вартості капіталу, репутаційних ризиків та деградації довіри у міжнародних ланцюгах створення вартості. Отже, рівень кіберзахищеності держави слід інтерпретувати як складову її економічного суверенітету та здатності підтримувати стійкість критичних секторів у глобальному конкурентному середовищі.

2. Обґрунтовано, що концептуальна модель оцінювання повинна охоплювати взаємопов'язані складові: (а) тиск загроз і експозицію (інтенсивність, складність, «площа атаки», вразливість ланцюгів постачання); (б) кіберстійкість (готовність, здатність до локалізації та відновлення); (в) етичне управління і довіру (прозорість, приватність-by-design, недискримінаційність алгоритмів, підзвітність); (г) результати у вимірах конкурентоспроможності та економічної безпеки. Доведено, що така композиція дозволяє коректно відобразити системний характер кіберзагроз, коли ризики генеруються не тільки технологіями, а й інституційною якістю управління, регуляторною спроможністю та культурою відповідальності.

3. Аргументовано, що інтеграція етичного виміру у методологію оцінювання має не декларативний, а функціональний характер, оскільки етика виступає економічним механізмом формування та підтримання довіри. Показано, що ігнорування приватності, непрозорість інцидентів, використання алгоритмів для дискримінаційних практик або маніпуляцій знижують суспільну та міжнародну довіру, що безпосередньо підвищує транзакційні витрати, ускладнює міжнародне контрактування і погіршує інвестиційний профіль держави. Відтак етика-by-design і прозорість інцидентності мають розглядатися як елементи «економіки довіри», що посилюють конкурентні переваги та резильєнтність.

4. Встановлено, що для забезпечення порівнянності країн і практичної придатності результатів доцільним є застосування зважених і нормованих індикаторів, які відображають як масштаб загроз, так і здатність системи їх стримувати. Підкреслено, що облік інцидентів має бути «зваженим» за критичністю, оскільки одна критична атака на інфраструктуру здатна сформувати значно більші економічні наслідки, ніж множина дрібних подій у некритичних сервісах. Показано, що використання інтегральних підходів не замінює аналізу

окремих показників, а забезпечує цілісність оцінювання, дозволяє будувати ранжування, проводити бенчмаркінг і формувати сценарні моделі політики.

5. Доведено, що оцінювання кіберстійкості має спиратися на індикатори реальної готовності, а не формальної наявності політик, що забезпечує об'єктивність висновків і практичну застосовність для державного управління. До таких індикаторів віднесено: швидкість виявлення та усунення інцидентів, дисципліну патчування, сегментацію критичних мереж, успішність тестів DR/BCP, впровадження принципу найменших привілеїв та Zero Trust, а також вимоги до кібербезпеки постачальників у договорах. Наголошено, що саме ці параметри визначають «здатність тримати удар» і обмежувати каскадні ефекти кібератак у критичних секторах.

6. Виявлено, що етичне управління та довіра можуть бути операціоналізовані через індикатори прозорості та підзвітності, які відображають зрілість інституційного середовища. Зазначено, що до практично вимірних параметрів належать: затримка та повнота розкриття інформації про інциденти, наявність і регулярність DPIA/оцінок впливу алгоритмічних систем, аудит недискримінаційності та пояснюваності, активність регуляторних механізмів, а також частка публічних пост-мортемів і процедур коригувальних дій. Підкреслено, що ці ознаки формують «сигнали» для міжнародних партнерів і інвесторів щодо прогнозованості ризиків, тим самим впливаючи на конкурентні позиції країни.

7. Обґрунтовано, що науково коректна оцінка впливу кіберзагроз на конкурентоспроможність і безпеку повинна базуватися на поєднанні кількох методологічних інструментів: панельних моделей із фіксованими ефектами для врахування сталих відмінностей між країнами, подійного аналізу (event study) для вимірювання динаміки макро- та фінансових показників навколо масштабних інцидентів, квазіекспериментальних підходів (DiD) для оцінювання ефектів

регуляторних змін, а також структурного моделювання (SEM) для перевірки причинних ланцюгів «етика → довіра → конкурентоспроможність» і модераторної ролі кіберстійкості. Зазначено, що така комбінація підходів знижує ризик хибної інтерпретації кореляцій як причинності та підвищує доказовість отриманих результатів.

8. Встановлено, що ефективність державної політики у сфері кібербезпеки та підвищення конкурентоспроможності зростає за умови сценарного моделювання на основі інтегральної оцінки. Показано, що практично значущими є сценарії, які передбачають: підняття «мінімальної планки» контролів у державному секторі та підприємництві (MFA, патч-дисципліна, сегментація), впровадження стандартів безпеки ланцюгів постачання (SBOM/SSDF, договірні SLA на виправлення), а також інституціоналізацію прозорого інцидент-репортингу та процедур відповідальності. Визначено, що саме ці напрями створюють максимальну віддачу не лише у зниженні технічних ризиків, а й у зростанні довіри, інвестиційної привабливості й конкурентної стійкості.

9. Зроблено висновок, що «стійкість + етика» формує синергійний ефект для міжнародної конкурентоспроможності та економічної безпеки, оскільки технічна готовність без інституційної прозорості не забезпечує повного «преміуму довіри» на світових ринках. Підкреслено, що країни, які демонструють здатність ефективно управляти кіберризиками й водночас дотримуються етичних принципів обробки даних та алгоритмічного управління, отримують стратегічні переваги у доступі до фінансування, міжнародної кооперації та інтеграції у глобальні виробничі мережі. Отже, розроблені у розділі 3 методологічні підходи створюють основу для практичного розрахунку інтегральної оцінки впливу кіберзагроз для України та обґрунтування інструментів державної політики мінімізації ризиків у наступних розділах дисертації.

Основні результати дослідження, викладені в цьому розділі, відображено в працях автора:

1. Myronchenko D. Cybersecurity as a Factor of Stabilization of the Global Economy. *Fundamental Shifts in Geo-Economic Systems Of The World:* A Collection of International Scientific Works. Kyiv, 2023. P. 193–197. URL: http://ief.org.ua/wp-content/uploads/2023/06/Fundamental-shifts_.pdf.

2. Myronchenko D. Ethical considerations in cybersecurity within the global economy. *Розвиток науки та освіти в умовах глобалізації:* тези доп. III міжнар. наук.-практ. конф. (м. Чернігів, 2 серпня 2024 р.). Чернігів, 2024. С. 136–139. URL: https://researcheurope.org/wp-content/uploads/2024/08/re-02.08.24.pdf.

3. Myronchenko D. Enhancing international economic relations through cyber hygiene practices. *Соціально-економічні виклики та можливості глобалізації:* тези доп. міжнар. наук.-практ. конф. (м. Одеса, 5 березня 2024 р.). Одеса, 2024. С. 49–52. URL: https://researcheurope.org/wp-content/uploads/2024/03/re-05.03.2024.pdf.

4. Мирончeнко Д. В. Вплив цифрової трансформації на стратегії міжнародних стартапів. *B2B MARKETING» з нагоди 125-річного ювілею КПІ ім. Ігоря Сікорського*: тези доп. XVII міжнар. наук.-практ. конф. (м. Київ, 14-15 грудня 2023 р.). К., 2023. С. 172-173.

Список використаних джерел до розділу 3

Bollen K. A. *Structural Equations with Latent Variables.* 1989. https://doi.org/10.1002/9781118619179

Cronbach L. J. *Coefficient Alpha and the Internal Structure of Tests* // *Psychometrika.* 1951. https://doi.org/10.1007/BF02310555

Cybersecurity and Infrastructure Security Agency (CISA). *Joint advisory / warning on cyber activity targeting logistics & technology entities involved in support to Ukraine.* https://www.cisa.gov/

Dark Reading. *Ukraine Sees 4,315 Cyber Incidents in 2024, CERT-UA Reports.* https://www.darkreading.com/cyberattacks-data-breaches/ukraine-sees-4-315-cyber-incidents-2024-cert-ua

Driscoll J. C., Kraay A. C. *Consistent Covariance Matrix Estimation with Spatially Dependent Panel Data // Review of Economics and Statistics.* 1998. https://economics.mit.edu/sites/default/files/publications/Consistent%20Covariance%20Matrix%20Estimation%20with%20Spatially%20Dependent%20Panel%20Data.pdf

ENISA. *2024 Report on the State of Cybersecurity in the Union.* https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20the%20Cybersecurity%20in%20the%20Union.pdf

European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape 2024.* https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Executive Order 14028. (2021, May 12). *Improving the Nation's Cybersecurity. Federal Register.* https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

ISO. *ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements.* 2019. https://www.iso.org/standard/75106.html

ISO. *ISO/IEC 27001:2022 Information security management systems – Requirements.* https://www.iso.org/standard/27001

Jolliffe I. T. *Principal Component Analysis.* 2nd ed. Springer, 2002. https://link.springer.com/book/10.1007/b98835

Myronchenko D. Cybersecurity as a Factor of Stabilization of the Global Economy. Fundamental Shifts in Geo-Economic Systems Of The World: A Collection of International Scientific Works. Kyiv, 2023. P. 193–197. URL: http://ief.org.ua/wp-content/uploads/2023/06/Fundamental-shifts_.pdf.

Myronchenko D. Ethical considerations in cybersecurity within the global economy. Розвиток науки та освіти в умовах глобалізації: тези доп. III міжнар. наук.-практ. конф. (м. Чернігів, 2 серпня 2024 р.). Чернігів, 2024. С. 136–139. URL: https://researcheurope.org/wp-content/uploads/2024/08/re-02.08.24.pdf.

Myronchenko D. Enhancing international economic relations through cyber hygiene practices. Соціально-економічні виклики та можливості глобалізації: тези доп. міжнар. наук.-практ. конф. (м. Одеса, 5 березня 2024 р.). Одеса, 2024. С. 49–52. URL: https://researcheurope.org/wp-content/uploads/2024/03/re-05.03.2024.pdf.

Мироненко Д. В. Вплив цифрової трансформації на стратегії міжнародних стартапів. *B2B MARKETING» з нагоди 125-річного ювілею КПІ ім. Ігоря Сікорського*: тези доп. XVII міжнар. наук.-практ. конф. (м. Київ, 14-15 грудня 2023 р.). К., 2023. С. 172-173.

National Institute of Standards and Technology (NIST). *Secure Software Development Framework (SSDF) Version 1.1: NIST SP 800-218.* 2022. https://csrc.nist.gov/pubs/sp/800/218/final

National Institute of Standards and Technology (NIST). *The NIST Cybersecurity Framework (CSF) 2.0: NIST CSWP 29.* 2024. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

National Institute of Standards and Technology (NIST). *Zero Trust Architecture: NIST SP 800-207.* 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

National Telecommunications and Information Administration (NTIA). *The Minimum Elements for a Software Bill of Materials (SBOM).* 2021. https://www.ntia.gov/report/2021/minimum-elements-software-bill-materials-sbom

OECD. *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document.* Paris: OECD, 2015. https://www.oecd.org/en/publications/2015/10/digital-security-risk-management-for-economic-and-social-prosperity_g1g5c3dc.html

OECD; European Commission Joint Research Centre. *Handbook on Constructing Composite Indicators: Methodology and User Guide.* 2008. https://www.oecd.org/

Regulation (EU) 2016/679. *General Data Protection Regulation (GDPR). Official Journal of the European Union.* 2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Regulation (EU) 2016/679. *General Data Protection Regulation (GDPR).* https://eur-lex.europa.eu/eli/reg/2016/679/oj

Regulation (EU) 2024/1689. *Artificial Intelligence Act.* https://eur-lex.europa.eu/eli/reg/2024/1689/oj

Saaty T. L. *The Analytic Hierarchy Process–What It Is and How It Is Used // Mathematical Modelling.* 1987. https://www.sciencedirect.com/science/article/pii/0270025587900735

State Service of Special Communications and Information Protection of Ukraine; CERT-UA. *CERT-UA Activity Report: H2 2024 (із річними підсумками за 2021–2024 роки).* https://cip.gov.ua/en/reports/cert-ua-activity-report-h2-2024

World Economic Forum. *Global Cybersecurity Outlook 2024.* https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

ВИСНОВКИ

У дисертаційному дослідженні здійснено комплексне теоретико-методологічне узагальнення та запропоновано нове розв'язання наукового завдання щодо обґрунтування механізмів і інструментів нівелювання впливу глобальних кіберзагроз на міжнародну конкурентоспроможність і економічну безпеку країн. За результатами дослідження сформульовано такі висновки.

1. Генезис концепцій економічної безпеки відображає поступову трансформацію від ресурсно-протекціоністського мислення XVII–XVIII ст. до сучасної парадигми, в якій ключовими активами безпеки є цифрова інфраструктура, дані та довіра. Встановлено, що ця еволюція має діалектичний характер: кризові епохи повертають запит на протекціонізм, однак загальна траєкторія спрямована до розширення поняття безпеки за рахунок інституційного, технологічного і цифрового вимірів. У XXI столітті кіберстійкість набуває статусу рівноцінного компонента економічної безпеки поряд із макростабільністю та якістю інститутів, а залежність від транснаціональних платформ і хмарних провайдерів формує нові типи стратегічної вразливості — технологічну залежність, асиметрію доступу до даних та ризики екстериторіального регулювання.

2. Глобальна конкурентоспроможність країн у цифрову епоху визначається не стільки наявністю ресурсів, скільки спроможністю генерувати та комерціалізувати інновації в межах кластерних екосистем. Інноваційні кластери виступають «воротами» для транснаціональних корпорацій та інвесторів, інтегруючи країну у глобальні ланцюги доданої вартості через концентрацію інтелектуального капіталу, венчурного фінансування та R&D-компетенцій. Доведено, що державна

кластерна політика (Smart Specialisation, Horizon Europe, технопарки) є визначальним чинником, який перетворює локальні переваги на міжнародні конкурентні позиції, а рівень кіберзахищеності кластерної інфраструктури безпосередньо впливає на довіру іноземних партнерів та умови залучення FDI.

3. Систематизація сучасних глобальних кіберзагроз засвідчує їхній структурний перехід від поодиноких технічних інцидентів до системних економічних шоків. Ідентифіковано п'ять каналів трансформації кіберінцидентів у макроекономічні втрати: зростання транзакційних витрат і страхових премій, порушення ланцюгів постачання, збої критичної інфраструктури, репутаційна деградація та посилення нетарифних бар'єрів через вимоги відповідності стандартам. Доведено, що наслідки мають мультиплікативний характер — прямі втрати невіддільні від непрямих: зупинок, штрафів, відтоку інвестицій та довгострокового звуження ринкового доступу. Кейси Colonial Pipeline, Maersk/NotPetya та SolarWinds верифікують цю логіку емпірично.

4. Узагальнення тенденцій інституційного забезпечення економічної безпеки виявило стійку нормативну конвергенцію: рекомендаційні підходи поступово витісняються юридично зобов'язувальними рамками, де управління вразливостями, контроль доступу та інцидент-репортинг (24/72) перетворюються на умову ринкового доступу і міжнародного контрактування. Директиви NIS2, GDPR та AI Act формують єдину «комплаєнс-економіку безпеки» ЄС, тоді як публічно-приватні механізми координації (CERT/CSIRT, ISAC/ISAO) слугують ключовим мезорівневим інструментом скорочення часу між виявленням загрози і її нейтралізацією по всьому ланцюгу суб'єктів. Встановлено, що безпека ланцюгів постачання (SBOM/SSDF) перетворилася на системний елемент конкурентного позиціонування, а не лише на технічну вимогу.

5. Комплексний аналіз стану економічної безпеки України показав, що країна функціонує за унікальною моделлю «постійного кібертиску в умовах збройного

конфлікту» — з системними, транскордонними APT-атаками, спрямованими передусім на критичну інфраструктуру. Водночас виявлено позитивну динаміку: зростання загальної кількості інцидентів поєднується з поступовим зниженням частки подій рівня high/critical, що свідчить про нарощування спроможностей виявлення, локалізації та відновлення. IT-сектор України підтверджує свою роль як структурного стабілізатора економічної безпеки через скорочення MTTD/MTTR, підтримку валютних надходжень (понад $6,4 млрд експорту цифрових послуг) та публічно-приватну взаємодію CERT-UA з приватними SOC.

6. Ідентифікація безпекового середовища України засвідчила, що найвищий ризик каскадних економічних збитків концентрується у п'яти вузлах: енергетика, телекомунікації, фінансова система, державні реєстри та транспортно-логістичні коридори. Встановлено, що атаки на ці сектори мають не лише операційний, а й стратегічний характер — вони спрямовані на підрив довіри населення до цифрових послуг держави, дестабілізацію логістичних ланцюгів та збільшення «страхової надбавки за воєнний ризик» для потенційних інвесторів. Доведено, що курс на євроінтеграцію робить конвергенцію з NIS2 та GDPR прикладним, а не декларативним завданням — насамперед для операторів критичної інфраструктури та постачальників держсектору.

7. Обґрунтування концептуальних підходів до оцінювання впливу кіберзагроз дозволило розробити рамку CCSI (Composite Cybersecurity Impact Index), яка агрегує чотири взаємопов'язані виміри: SWIR (зважена за критичністю частота інцидентів), ASURF (площа атаки та цифрова відкритість), RESIL (кіберстійкість як здатність до відновлення) та ETS (етика і довіра як інституційний вимір). Принципова відмінність запропонованого підходу від наявних аналогів — функціональна, а не декларативна інтеграція етичного компонента: ETS виступає методологічним медіатором і модератором, який пояснює, яким чином технічна стійкість конвертується у «премію довіри» на міжнародних ринках. Верифікація

причинного ланцюга здійснена за допомогою панельних моделей із фіксованими ефектами, event study, квазіекспериментального DiD та структурного моделювання (SEM).

8. Оцінювання впливу кібернетичних загроз на національні інтереси України через призму CCSI-UA підтвердило статистично значущий зв'язок між динамікою кіберстійкості та ключовими макроекономічними індикаторами: позитивна динаміка субіндексу RESIL корелює зі звуженням CDS-спредів на 3–7 базисних пунктів за квартал, а впровадження вимог нормативної конвергенції (NIS2/GDPR) супроводжується зниженням страхових премій і підвищенням довіри контрагентів. Верифіковано синергійний ефект «стійкість + етика»: країни з одночасно високими значеннями RESIL і ETS отримують більший приріст конкурентних позицій, ніж ті, що сильні лише технічно — технічна готовність без інституційної прозорості не забезпечує повного «преміуму довіри».

9. Розроблена система пріоритетних механізмів державної політики мінімізації впливу глобальних кіберзагроз включає п'ять взаємопов'язаних інструментів із вимірюваними KPI та дорожньою картою на 2025–2027 роки. Найвищу системну віддачу забезпечують: масштабування «мінімальної планки» базових контролів (MFA ≥ 90%, патч-менеджмент critical ≤ 15 днів) через держзакупівлі та ліцензування; інституціоналізація безпеки ланцюгів постачання через SBOM/SSDF і контрактні SLA; впровадження прозорого інцидент-репортингу в форматі 24/72 із публічними post-mortem розборами; розбудова кластерної кіберекосистеми (CERT/CSIRT↔ISAC↔SOC) та підтримка керованих сервісів безпеки для МСП; обов'язковий DPIA/AIA для державних цифрових систем. Інтегральний результат реалізації цього пакета вимірюється через зростання CCSI-UA на +3–5 пунктів щорічно, що фіксує не ефект окремої технології, а системний вплив державної політики на конкурентоспроможність і економічну безпеку України.

ДОДАТКИ

Додаток А

Глосарій ключових термінів і понять

Складено автором на основі NIST, ENISA, ISO, нормативних актів ЄС та авторської концепції

AHP (Analytic Hierarchy Process) – метод аналізу ієрархій; структурований метод прийняття рішень при багатокритеріальному виборі, що використовується для попарного порівняння альтернатив і визначення відносних ваг критеріїв. У дисертації застосовується для формування ваг субіндексів CCSI.

ASURF (Attack Surface) – субіндекс «поверхні атаки» у рамці CCSI; відображає структурну цифрову відкритість системи до зовнішніх загроз через залежність від хмарних сервісів, IoT/IIoT, API-інтеграцій та вразливостей ланцюгів постачання.

BCP (Business Continuity Planning) – планування безперервності бізнесу; сукупність заходів, що забезпечують продовження ключових бізнес-процесів під час та після кризових подій. У контексті кіберризиків передбачає готовність до деградованих режимів роботи.

CCSI (Composite Cybersecurity Impact) – інтегральний індекс впливу кібербезпеки; авторська аналітична рамка, що агрегує чотири виміри – SWIR, ASURF, RESIL та ETS – для оцінки «чистого» ефекту кіберризиків на міжнародну конкурентоспроможність та економічну безпеку. Формула: $CCSI = \delta_1 \cdot RESIL + \delta_2 \cdot ETS - \delta_3 \cdot SWIR - \delta_4 \cdot ASURF$.

CERT/CSIRT – команда реагування на комп'ютерні надзвичайні ситуації / команда реагування на інциденти кібербезпеки; спеціалізований підрозділ, що забезпечує координацію виявлення, аналізу та усунення наслідків кіберінцидентів. CERT-UA – урядова команда реагування України (ДССЗЗІ).

CVE (Common Vulnerabilities and Exposures) – реєстр відомих вразливостей; стандартизований каталог публічно розкритих вразливостей програмного забезпечення. Патч-латентність (час від CVE до виправлення) є ключовим показником RESIL.

Delphi-метод – структурований процес групового прогнозування та оцінки, заснований на багатоітераційному анонімному опитуванні експертів з метою досягнення консенсусу. Застосовується для верифікації ваг у рамці CCSI.

DLP (Data Loss Prevention) – запобігання витоку даних; технологія та процес ідентифікації, моніторингу та захисту даних у стані спокою, передавання та використання від несанкціонованого доступу або витоку.

DPIA (Data Protection Impact Assessment) – оцінка впливу на захист даних; процедура, передбачена GDPR, для виявлення та мінімізації ризиків для приватності при обробці персональних даних у нових проєктах чи процесах. Є складовою субіндексу ETS.

DR (Disaster Recovery) – відновлення після збоїв; комплекс технічних і організаційних заходів, що дозволяють відновити IT-системи та дані після кіберінциденту, стихійного лиха або іншої критичної події. Пов'язаний з показниками RTO/RPO.

Економіка довіри (Trust Economy) – економічна модель, у якій довіра стає ключовим ресурсом та конкурентною перевагою в цифровому середовищі; знижує транзакційні витрати, спрощує міжнародне контрактування та підвищує інвестиційну привабливість.

ETS (Ethics/Trust Score) – субіндекс етики та довіри у рамці CCSI; вимірює прозорість, підзвітність, privacy-by-design та інші практики, що формують «премію довіри» для міжнародних партнерів та інвесторів.

Ethics-by-design – принцип вбудовування етичних вимог (прозорість, приватність, підзвітність, недискримінаційність) у процес проектування та розробки технологій на ранніх стадіях, а не як наступного доповнення. Є складовою субіндексу ETS.

GDPR (General Data Protection Regulation) – Загальний регламент захисту даних ЄС (2016/679); обов'язковий нормативний акт, що встановлює вимоги до обробки персональних даних осіб у ЄС. Є основою для privacy-складової ETS.

Гібридна загроза – скоординоване застосування кількох інструментів дестабілізації (кібератаки, дезінформація, економічний тиск, фізичні операції) з метою досягнення стратегічних цілей. Для України є основним контекстом дисертаційного дослідження.

ISAC/ISAO – центри та організації обміну інформацією та аналізу (Information Sharing and Analysis Centers/Organizations); публічно-приватні механізми збору, аналізу та поширення інформації про кіберзагрози в межах конкретної галузі або спільноти.

Кіберстійкість (Cyber Resilience) – здатність системи або організації передбачати кіберінциденти, витримувати їх, відновлюватися після них та адаптуватися до змін. На відміну від кібербезпеки, фокусується на безперервності критичних функцій, а не на ідеальному недопущенні атак.

Кібергігієна – систематичне застосування базових профілактичних заходів захисту (оновлення ПЗ, MFA, управління паролями, резервні копії, навчання персоналу), що зменшує ймовірність та масштаб більшості типових кіберінцидентів. Трактується як «мікрофундамент» міжнародної довіри.

MDR (Managed Detection and Response) – кероване виявлення і реагування; аутсорсингова модель кіберзахисту, що надає організаціям безперервний моніторинг, аналітику загроз та підтримку реагування на інциденти через зовнішнього провайдера.

MTTD (Mean Time to Detect) – середній час від початку кіберінциденту до його виявлення. Є ключовим показником кіберстійкості (RESIL): чим нижчий MTTD, тим менший масштаб потенційного збитку.

MTTR (Mean Time to Respond/Recover) – середній час від виявлення інциденту до завершення реагування та відновлення нормального функціонування. Разом із MTTD формує «вікно ризику».

NIS2 (Network and Information Security Directive 2) – Директива ЄС 2022/2555 щодо забезпечення високого спільного рівня кібербезпеки в ЄС; встановлює обов'язкові вимоги до управління ризиками, інцидент-репортингу та безпеки ланцюгів постачання для критичних суб'єктів.

Privacy-by-design – принцип вбудовування захисту приватності та мінімізації збору даних у дизайн систем та процесів з самого початку (privacy as the default). Закріплено у ст. 25 GDPR.

RESIL (Cyber Resilience Score) – субіндекс кіберстійкості у рамці CCSI; відображає здатність системи виявляти, локалізувати та відновлюватися після кіберінцидентів через такі показники, як MTTD/MTTR, MFA-покриття, DR/BCP-тести та Zero Trust.

RPO (Recovery Point Objective) – цільовий показник відновлення точки даних; максимально допустимий обсяг втрат даних у часовому вимірі (наприклад, RPO=1 год означає, що резервна копія не може бути старшою за одну годину).

RTO (Recovery Time Objective) – цільовий показник часу відновлення; максимально допустимий час, протягом якого система може бути недоступною після збою.

SBOM (Software Bill of Materials) – перелік компонентів програмного забезпечення; реєстр усіх складових ПЗ-продукту із зазначенням версій, ліцензій та залежностей. Дозволяє організаціям оперативно реагувати на нові вразливості у використаних компонентах.

SSDF (Secure Software Development Framework) – рамка безпечної розробки програмного забезпечення (NIST SP 800-218); встановлює вимоги до практик безпеки на кожному етапі розробки ПЗ. Разом із SBOM є основним інструментом управління ризиками ланцюгів постачання.

SWIR (Severity-Weighted Incident Rate) – субіндекс зважених за критичністю кіберінцидентів у рамці CCSI; відображає реальну «вагу» кіберагресії, надаючи більший коефіцієнт інцидентам рівня high/critical.

Транзакційні витрати – витрати, пов'язані з укладанням угод та взаємодією між контрагентами (пошук партнерів, переговори, моніторинг виконання, захист прав). У контексті дисертації кібербезпека та довіра розглядаються як механізми зниження транзакційних витрат у міжнародній торгівлі та інвестиціях.

Zero Trust – модель «нульової довіри»; архітектурний підхід до безпеки, що базується на принципі «ніколи не довіряй, завжди перевіряй» (never trust, always verify). Передбачає постійну верифікацію кожного запиту на доступ незалежно від його джерела. Закріплено у NIST SP 800-207.

Цифровий суверенітет – здатність держави приймати незалежні рішення у цифровому просторі, контролювати критичну цифрову інфраструктуру та дані, не допускаючи зовнішньої залежності, здатної стати інструментом тиску.

Додаток Б

Анкета для експертного опитування методом Delphi/AHP

Форма для оцінювання вагових коефіцієнтів субіндексів CCSI Складено автором

ЗАГАЛЬНА ІНФОРМАЦІЯ ПРО РЕСПОНДЕНТА

1. Сфера діяльності: ☐ Академічна/наукова ☐ Державне управління ☐ IT-індустрія ☐ Кібербезпека ☐ Фінансовий сектор ☐ Критична інфраструктура ☐ Страхування ☐ Інше: ___
2. Стаж у сфері кібербезпеки / економічної безпеки: ☐ до 5 р. ☐ 5–10 р. ☐ 10–15 р. ☐ більше 15 р.
3. Посада (не обов'язково): _____

РОЗДІЛ 1. ПОПАРНЕ ПОРІВНЯННЯ СУБІНДЕКСІВ CCSI

Оцініть відносну важливість кожної пари субіндексів за шкалою Сааті: 1 – однакова важливість; 3 – помірна перевага; 5 – суттєва перевага; 7 – явна перевага; 9 – абсолютна перевага (проміжні значення: 2, 4, 6, 8)

Пара субіндексів	Лівий важливіший	Рівні	Правий важливіший
RESIL (стійкість) vs SWIR (загрози)	9 8 7 6 5 4 3 2	1	2 3 4 5 6 7 8 9
RESIL (стійкість) vs ASURF (площа атаки)	9 8 7 6 5 4 3 2	1	2 3 4 5 6 7 8 9
RESIL (стійкість) vs ETS (етика/довіра)	9 8 7 6 5 4 3 2	1	2 3 4 5 6 7 8 9
ETS (етика/довіра) vs SWIR (загрози)	9 8 7 6 5 4 3 2	1	2 3 4 5 6 7 8 9
ETS (етика/довіра) vs ASURF (площа атаки)	9 8 7 6 5 4 3 2	1	2 3 4 5 6 7 8 9

SWIR (загрози) vs ASURF (площа атаки)	9 8 7 6 5 4 3 2	1	2 3 4 5 6 7 8 9

РОЗДІЛ 2. ОЦІНКА СКЛАДОВИХ СУБІНДЕКСУ RESIL

Розподіліть 100 балів між компонентами кіберстійкості відповідно до їх важливості для економічної безпеки:

Компонент	Ваша оцінка (сума = 100)
Покриття MFA у критичних системах	
Дисципліна патч-менеджменту (patch latency)	
Швидкість виявлення інцидентів (MTTD)	
Швидкість відновлення після інцидентів (MTTR)	
Регулярність та результативність DR/BCP тестів	
Впровадження Zero Trust архітектури	
Сума	

РОЗДІЛ 3. ОЦІНКА СКЛАДОВИХ СУБІНДЕКСУ ETS

Розподіліть 100 балів між компонентами етики/довіри:

Компонент	Ваша оцінка (сума = 100)
Своєчасність та повнота розкриття інцидентів	
Наявність та якість DPIA/AI Impact Assessment	
Прозорість та публічні post-mortem розбори	
Впровадження privacy-by-design у сервісах	
Регуляторна активність та підзвітність	
Аудит алгоритмів на недискримінаційність	
Сума	100

РОЗДІЛ 4. ЯКІСНІ ОЦІНКИ

4.1. Оцініть за шкалою 1–5, наскільки кожен фактор впливає на міжнародну конкурентоспроможність країни в умовах кіберзагроз:

Фактор	1 (не впливає) → 5 (критичний вплив)
Рівень кіберстійкості критичної інфраструктури	1 – 2 – 3 – 4 – 5
Прозорість управління кіберінцидентами	1 – 2 – 3 – 4 – 5
Безпека ланцюгів постачання (SBOM/SSDF)	1 – 2 – 3 – 4 – 5

Наявність публічно-приватної координації (CERT/ISAC)	1 – 2 – 3 – 4 – 5
Дотримання стандартів privacy-by-design	1 – 2 – 3 – 4 – 5
Регуляторна конвергенція з вимогами ЄС (NIS2, GDPR)	1 – 2 – 3 – 4 – 5

4.2. На Вашу думку, чи є «етичне управління даними» (ETS) реальним економічним чинником конкурентоспроможності чи лише нормативною вимогою? ☐ Реальний економічний чинник ☐ Переважно нормативна вимога ☐ Залежить від сектору ☐ Важко оцінити

4.3. Які 3 заходи державної кіберполітики, на Вашу думку, дають найбільший ефект для економічної безпеки України (вкажіть пріоритети 1–3):

_____

_____

Додаток В

Зведена таблиця ключових кіберінцидентів та їх економічних наслідків

Інцидент	Рік	Тип атаки	Вектор / вразливість	Прямі фінансові втрати	Системний ефект	Урок для CCSI-UA
Colonial Pipeline (США)	2021	Ransomware (DarkSide)	Компрометований VPN-акаунт без MFA	~$4,4 млн (викуп) + сотні млн (втрати бізнесу та економіки)	Зупинка трубопроводу 6 днів, дефіцит палива на Східному узбережжі, режим НС	Відсутність MFA на критичних доступах → RESIL ↓; необхідність DR/BCP тестів → ASURF ↑
SolarWinds (США/глобально)	2020	Supply chain / APT (Cozy Bear)	Троянізоване оновлення Orion (build pipeline)	Збитки для ~18 000 організацій, оцінки $100 млрд+ для уряду США	Компрометація мереж урядів, ОПК, IT-компаній у ~100 країнах	Ризик supply chain → ASURF ↑; необхідність SBOM/SSDF → RESIL ↓ без них
NotPetya/M.E.Doc (Україна → глобально)	2017	Деструктивний вайпер (GRU Sandworm)	Оновлення бухг. ПЗ M.E.Doc → lateral movement	Maersk ~$300 млн, Merck ~$870 млн, FedEx ~$400 млн, Mondelez ~$188 млн; загалом ~$10 млрд	Зупинка глобальних логістичних операцій, збої у портах на 10+ днів	Критична важливість сегментації OT/IT та DR/BCP → RESIL; ризик «нульової довіри»
Equifax (США)	2017	Exploitation CVE-2017-5638	Невчасно закритий патч Apache Struts	~$575 млн (FTC settlement) + $1,4 млрд (витрати)	Витік даних 147 млн осіб; падіння акцій ~35%; довгострокові репутаційні	Patch latency → RESIL ↓; необхідність SLA на CVE → ASURF ↑ без контролю

					втрати	
Maersk (глобально)	2017	NotPetya (spin-off)	Заражена мережа через UA-офіс	~$300 млн прямих збитків	10 днів майже повної зупинки глобальних операцій, ручне управління у 76 портах	Каскадний ефект через логістику → мультиплікатор збитків; необхідність Zero Trust
Cambridge Analytica / Facebook	2018	Зловживання даними (insider/API)	Витік через API-доступ третьої сторони	$5 млрд (FTC штраф); ~$134 млрд втрати капіталізації	Глобальна криза довіри до цифрових платформ; регуляторний тиск на весь сектор	Слабкий ETS → репутаційна катастрофа; privacy-by-design як превентивний механізм
Атака на енергосистему України	2015–2016	APT / ICS attack (BlackEnergy/Crashoverride)	Spearphishing → OT lateral movement	Пряма: відновлення інфраструктури; непряма: репутаційна, страхові	Знеструмлення 225 000+ споживачів (2015); атака на підстанції (2016)	Вразливість OT/ICS → ASURF ↑; необхідність сегментації за Purdue model → RESIL
SolarWinds-похідні атаки (Kaseya)	2021	Supply chain ransomware (REvil)	Вразливість MSP-платформи	~$70 млн (запитаний викуп); 1 500+ компаній жертв	Каскадне ураження клієнтів через MSP-канал; демонстрація ризиків ланцюга	SBOM для MSP-постачальників → ASURF ↓; договірні SLA → RESIL ↑

Складено автором на основі матеріалів CISA, FTC, IBM X-Force, публічних звітів компаній

Додаток Г

Секторальна матриця мінімальних контролів кібербезпеки для критичних секторів України

Контроль / Захід	Енергетика (OT/ICS)	Телеком / Інтернет	Фінанси	Держ. е-сервіси	Транспорт / Логістика
Ідентифікація активів	✅ Обов'язково (інвентар OT/ICS з «паспортами»)	✅ Обов'язково	✅ Обов'язково	✅ Обов'язково	✅ Обов'язково (включно з IoT/сенсорами)
MFA для привілейованого доступу	✅ Обов'язково (апаратні токени для OT)	✅ Обов'язково	✅ Обов'язково (апаратні токени)	✅ Обов'язково	✅ Обов'язково
Сегментація мережі	✅ Purdue model (рівні 0–5)	✅ Anycast, клітинкова архітектура	✅ Мікросегментація	✅ Zero Trust зони	✅ OT↔IT ізоляція
Patch management (SLA)	⚠️ Адаптований (≤30 дн. critical)	✅ ≤15 дн. critical	✅ ≤15 дн. critical	✅ ≤15 дн. critical	✅ ≤15 дн. critical

Резервне копіювання (air-gap)	✅ Обов'язково з тестами	✅ Обов'язково	✅ Незворотні бекапи	✅ Геореплікація	✅ Обов'язково
DR/BCP тестування	✅ ≥2 рази/рік (включ. ручні режими)	✅ ≥2 рази/рік	✅ ≥2 рази/рік	✅ ≥2 рази/рік	✅ ≥2 рази/рік
Інцидент-репортинг 24/72h	✅ Обов'язково	✅ Обов'язково	✅ Обов'язково	✅ Обов'язково	✅ Обов'язково
SBOM для постачальників	✅ Критично	✅ Критично	✅ Обов'язково	✅ Обов'язково	✅ Критично
SSDF для розробників ПЗ	✅ Обов'язково	✅ Обов'язково	✅ Обов'язково	✅ Обов'язково	✅ Обов'язково
Zero Trust архітектура	⚠️ Для ІТ-компоненти	✅ Повне впровадження	✅ Повне впровадження	✅ Повне впровадження	✅ Для ІТ-компоненти

SOC/MDR моніторинг 24/7	✅ Обов'язково	✅ Обов'язково	✅ Обов'язково	✅ Обов'язково	✅ Обов'язково
Моніторинг OT-протоколів	✅ Modbus, DNP3, IEC 61850	N/A	N/A	N/A	✅ SCADA/TOS моніторинг
Unidirectional gateway (data diode)	✅ Рекомендовано	N/A	N/A	N/A	⚠️ Для критичних OT-вузлів
Валідація сенсорних даних	⚠️ Для SCADA	N/A	⚠️ Для транзакційних систем	N/A	✅ GNSS, відео, телеметрія
Захист DNS/BGP	⚠️ Для IT	✅ DNSSEC, BGP route filtering	✅ DNSSEC	✅ DNSSEC	✅ DNSSEC
DPIA / AIA	⚠️ Для даних клієнтів	⚠️ Для даних абонентів	✅ Обов'язково	✅ Обов'язково	⚠️ Для персональних даних

Red/Purple team вправи	✅ ≥1 рази/рік	✅ ≥1 рази/рік	✅ ≥2 рази/рік	✅ ≥2 рази/рік	✅ ≥1 рази/рік
Graceful degradation режими	✅ Критично (ручне управління)	✅ Автономні контури	⚠️ Мінімальний режим	✅ Офлайн-режим	✅ Критично (паперові операції)

Позначення: ✅ – Обов'язковий мінімум; ⚠️ – Рекомендовано/адаптований підхід; N/A – не застосовується

Складено автором на основі NIST CSF 2.0, NIS2, IEC 62443, ENISA Guidelines

Додаток Д

Порівняльний аналіз нормативно-правової бази кібербезпеки у ключових юрисдикціях

Критерій	Україна	Європейський Союз	США	Велика Британія	Сінгапур
Основний законодавчий акт	ЗУ «Про основні засади забезпечення кібербезпеки України» (2017)	NIS2 Directive (2022/2555)	CISA mandates; EO 14028 (2021)	Network and Information Security Regulations (2018/2022)	Cybersecurity Act (2018)
Інцидент-репортинг	Рекомендаційний (CERT-UA)	Обов'язковий: 24h / 72h / 30 дн.	Обов'язковий для КІ: 72h (CISA)	Обов'язковий: 72h (для NIS)	Обов'язковий для КІ: 3 год (ІСТ)
Вимоги до supply chain	Відсутні системні	Обов'язкові (NIS2 Art. 21)	EO 14028: SBOM обов'язковий для федерального ПЗ	Аналог NIS2 у розробці	Cyber Trust Mark для IoT
Мінімальні контролі	Нормативи ДССЗЗІ (рекомендаційні)	Обов'язкові «minimum measures» (NIS2 Art. 21)	NIST CSF (рекомендаційний); CISA KEV (обов'язковий для федеральних)	Cyber Assessment Framework (CAF)	Cyber Essentials (добровільний, але стимульований)

Держструктура координації	ДССЗЗІ, CERT-UA, РНБО	ENISA + національні CSIRTs; NIS Cooperation Group	CISA + sector-specific agencies; ISAC мережа	NCSC (National Cyber Security Centre)	CSA (Cyber Security Agency)
Публічно-приватна взаємодія	Формується (CERT↔приватні SOC)	Розвинута (ENISA, ISACs, CSIRTs)	Висока (ISACs, ISAOs, JCDC)	NCSC Industry 100 програма	SG-Cyber Partnership Program
Кіберстрахування	Початковий ринок	Розвивається (вимоги NIS2 стимулюють)	Розвинутий (~$15 млрд/рік премій)	Розвинутий (Lloyd's market)	Зростаючий
Відповідальність за порушення	Адміністративна (обмежена)	До €10 млн або 2% обороту (NIS2)	Галузева (SEC, FTC, HIPAA)	£17 млн або 4% обороту	S$100 000 або позбавлення волі
Рівень цифрового суверенітету	Формується	Висока (GAIA-X, EU Cloud Rules)	Середня (Cloud Act)	Висока (UK data sovereignty)	Висока (Smart Nation + data gov.)
Стратегічний орієнтир	NIS2-конвергенція (євроінтеграція)	Уніфікований простір кіберстійкості	Zero Trust Federal Strategy	Active Cyber Defence	Smart Nation Cybersecurity Strategy 2021–2024

Складено автором

Додаток Е

Панель KPI національного моніторингу кіберстійкості України

5.1. Система цільових показників за рівнями

KPI	Поточний стан (2024, орієнтовно)	Ціль 2025	Ціль 2026	Ціль 2027	Метод вимірювання
РІВЕНЬ 1: БАЗОВІ КОНТРОЛІ					
MFA coverage (% критичних систем)	~55–65%	75%	85%	≥90%	Регуляторний аудит, опитування
Patch latency median (дні, critical CVE)	~30–45 дн.	≤25 дн.	≤18 дн.	≤15 дн.	CISA KEV, аудити
SBOM охоплення держзакупівель (%)	~5–10%	40%	75%	100%	Реєстр Prozorro
РІВЕНЬ 2: ВИЯВЛЕННЯ ТА РЕАГУВАННЯ					

MTTD – середній час виявлення (год)	~36–72 год	≤30 год	≤24 год	≤18 год	CERT-UA, SOC звіти
MTTR – середній час відновлення (год)	~72–120 год	≤72 год	≤48 год	≤24 год	CERT-UA, SOC звіти
DR/BCP тести (% суб'єктів КІ, ≥2/рік)	~20–30%	50%	75%	100%	ДССЗЗІ аудити
Середній RTO після тесту (год)	~48–72 год	≤36 год	≤24 год	≤24 год	Звіти тестувань
RPO (допустима втрата даних, год)	~4–8 год	≤4 год	≤2 год	≤1 год	Звіти тестувань
РІВЕНЬ 3: ПРОЗОРІСТЬ ТА ДОВІРА					
72h disclosure (% значущих інцидентів)	~15–25%	40%	65%	≥80%	CERT-UA реєстр
DPIA охоплення публічних е-сервісів (%)	~20–30%	45%	65%	≥80%	Реєстр ДССЗЗІ/Мінцифри

Публічні post-mortem розбори (кількість/рік)	~5–10	20	40	≥60	Публічний реєстр
РІВЕНЬ 4: МАСШТАБ ТА ОХОПЛЕННЯ					
МСП під керованими сервісами безпеки	~200–500	1 500	3 500	≥5 000	IT-кластери, реєстр ваучерів
Суб'єкти КІ з Zero Trust (частково/повністю)	~5–10%	20%	45%	≥70%	Регуляторний аудит
Кіберполігони (кількість регіональних)	1–2	2	4	≥6	Реєстр Мінцифри
РІВЕНЬ 5: ІНТЕГРАЛЬНИЙ ІНДЕКС					
CCSI-UA (загальний)	~35–40 п.	~40–43 п.	~44–47 п.	~48–53 п.	Розрахунок за методологією В
CCSI-UA: Енергетика	~38 п.	~41 п.	~44 п.	~47 п.	Секторний розрахунок

CCSI-UA: Транспорт/Логістика	~36 п.	~39 п.	~42 п.	~46 п.	Секторний розрахунок
CCSI-UA: Фінанси	~46 п.	~49 п.	~52 п.	~56 п.	Секторний розрахунок
CCSI-UA: Держ. е-сервіси	~41 п.	~44 п.	~48 п.	~52 п.	Секторний розрахунок
CCSI-UA: Телеком	~42 п.	~45 п.	~49 п.	~53 п.	Секторний розрахунок

5.2. Система «світлофор» для оперативного моніторингу

Індикатор	🔴 Критично	🟡 Увага	🟢 Норма
MTTD	>48 год	24–48 год	<24 год
MTTR	>96 год	48–96 год	<48 год

MFA coverage	<60%	60–80%	≥80%
Patch latency (critical)	>30 дн.	15–30 дн.	≤15 дн.
72h disclosure	<30%	30–60%	≥60%
DR/BCP тести	<1/рік	1/рік	≥2/рік
CCSI-UA	<30 п.	30–45 п.	≥45 п.

ЗАТВЕРДЖУЮ
Проректор з наукових досліджень та
трансферу технологій, д.т.н., професор
_____ Сергій ГНАТЮК
«04» 03 2026 року

АКТ

Комісія у складі:
голови – декана факультету права та міжнародних відносин, к.ю.н., доцента Жукорської Ярини Михайлівни;
членів комісії: – завідувача кафедри міжнародних економічних відносин, к.е.н., доцента Побоченко Лесі Миколаївни;
– професора кафедри міжнародних економічних відносин, д.е.н., професора Грущинської Наталії Миколаївни;
– доцента кафедри міжнародних економічних відносин, к.е.н., доцента Прокоп'євої Аліни Анатоліївни

цим Актом засвідчує, що результати дисертаційного дослідження здобувача кафедри міжнародних економічних відносин Національного університету «Київський авіаційний інститут» Мироченка Дмитра Володимировича на тему: «Вплив глобальних кіберзагроз на міжнародну конкурентоспроможність і економічну безпеку країн» на здобуття ступеня доктора філософії за спеціальністю 292 «Міжнародні економічні відносини» впроваджені в діяльності кафедри міжнародних економічних відносин. Окремі положення результатів дисертаційного дослідження використані в навчальному процесі при підготовці фахівців за спеціальністю 292 «Міжнародні економічні відносини» за освітньо-професійною програмою «Міжнародні економічні відносини» та «Міжнародний бізнес» першого (бакалаврського) та другого (магістерського) рівнів вищої освіти з дисциплін: «Міжнародне конкурентне управління», «Міжнародний менеджмент і маркетинг», «Менеджмент зовнішньоекономічної діяльності підприємства» та «Транснаціоналізація світової економіки та менеджмент персоналу в міжнародних корпораціях». Зокрема, у стислому вигляді використано аналітичний матеріал щодо впливу глобальних кіберзагроз на трансформацію міжнародного бізнесу, дослідження тенденцій розвитку інституційного забезпечення економічної безпеки країн, аналіз сучасного стану економічної безпеки України.

Дисертаційне дослідження стало складовою держбюджетних (кафедральних) науково-дослідних робіт (НДР) «Міжнародний рух капіталу в умовах зовнішньої збройної агресії проти України та повоєнної відбудови» №12-2024/15.01.01 та «Теоретичні та практичні аспекти модифікації системи міжнародних економічних відносин в умовах багатополярності розвитку світового господарства» №118-2022/15.01.01. Результати дисертаційного дослідження успішно інтегровані в науково-дослідні роботи кафедри, що підвищило наукову новизну, аналітичну глибину та практичну значущість одержаних результатів.

Результати дослідження впроваджено без фінансових зобов'язань перед автором.

Голова комісії к.ю.н. доцент (науковий ступінь, вчене звання) (підпис) Ярина ЖУКОРСЬКА

Члени комісії к.е.н. доцент (науковий ступінь, вчене звання) (підпис) Леся ПОБОЧЕНКО

д.е.н. професор (науковий ступінь, вчене звання) (підпис) Наталія ГРУЩИНСЬКА

к.е.н. доцент (науковий ступінь, вчене звання) (підпис) Аліна ПРОКОП'ЄВА

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях категорії «Б»:

1. Myronchenko D., Sydorenko K. Role of the IT-sector of Ukraine in the global cyber security system. *Економічний простір*. 2023. №186. С. 13-17. DOI: 10.32782/2224-6282/186-2 (0,95 д.а., особисто автора 0,85 д.а. – обґрунтовано роль IT-сектору в системі забезпечення глобальної кібербезпеки).
2. Myronchenko D. Ethical aspects of cyber security in the global economy and international relations. *Вчені записки*. 2025. Вип. 40. №3. С. 133-140. DOI: 10.33111/vz_kneu.40.25.03.02.012.018.
3. Myronchenko D. Securing Digital Frontier: Cyber Hygiene in the Global Economy. *Актуальні проблеми економіки*. 2025. Вип. 12. №294. С. 151-159. DOI: 10.32752/1993-6788-2025-1-294-151-159.

Наукові публікації в монографічних виданнях:

1. Myronchenko D., Sydorenko K. Digital vulnerability of transport infrastructure in the context of global crises. *The International Sustainable Transportation Symposium (ISTRAS'25). National Aviation Academy of Azerbaijan.* 2025. P. 23. ISBN: 978-9952-582-08-6. DOI: 10.71108/istras.2025 ***(Scopus)*** (0,5 д.а., особисто автора 0,25 д.а. – обґрунтовано цифрову вразливість критичної інфраструктури в контексті глобальних криз).

Наукові праці, які додатково відображають наукові результати дисертації:

1. Myronchenko D. Cybersecurity as a Factor of Stabilization of the Global Economy. *Fundamental Shifts in Geo-Economic Systems Of The World:* A Collection of International Scientific Works. Kyiv, 2023. P. 193-197. URL: http://ief.org.ua/wp-content/uploads/2023/06/Fundamental-shifts_.pdf.

2. Myronchenko D. Ensuring national and economic security through effective cybersecurity measures. *Національні економічні стратегії розвитку в глобальному середовищі:* тези доп. XIV міжнар. наук.-практ. конф. (м. Київ, 11 травня 2023 р.). К., 2023. С. 27-30. URL: https://drive.google.com/file/d/18gwybyPV5UPbae1rcWR-PDiZwne8bbxe/view.

3. Мирончeнко Д. Вплив цифрової трансформації на стратегії міжнародних стартапів. *XVII Міжнародна науково-практична конференція «B2B MARKETING» з нагоди 125-річного ювілею КПІ ім. Ігоря Сікорського*. К., 2023. С. 172-173. URL: http://b2b-marketing.fmm.kpi.ua/proc/issue/view/17528/10197.

4. Мирончeнко Д. Вплив цифрової трансформації на стратегії міжнародних стартапів. *B2B MARKETING» з нагоди 125-річного ювілею КПІ ім. Ігоря Сікорського:* тези доп. XVII міжнар. наук.-практ. конф. (м. Київ, 14-15 грудня 2023 р.). К., 2023. С. 172-173.

5. Myronchenko D. Enhancing international economic relations through cyber hygiene practices. *Соціально-економічні виклики та можливості глобалізації:* тези доп. міжнар. наук.-практ. конф. (м. Одеса, 5 березня 2024 р.). Одеса, 2024. С. 49-52. URL: https://researcheurope.org/wp-content/uploads/2024/03/re-05.03.2024.pdf.

6. Myronchenko D. Cyber Hygiene and the Future of International Economics. *Importance of Soft Skills for Life and Scientific Success:* A Collection of Scientific Works of 3rd International Scientific and Practical Internet Conference (Dnipro, March 7-8, 2024). Dnipro, 2024. P. 20-21. URL: http://www.wayscience.com/wp-content/uploads/2024/03/Conference-Proceedings-March-7-8-2024.pdf.

7. Myronchenko D. Ethical considerations in cybersecurity within the global economy. *Розвиток науки та освіти в умовах глобалізації:* тези доп. III міжнар. наук.-практ. конф. (м. Чернігів, 2 серпня 2024 р.). Чернігів, 2024. С. 136-139. URL: https://researcheurope.org/wp-content/uploads/2024/08/re-02.08.24.pdf.

Spin.ai

Spin Technology LLC.
2100 Geng Rd Suite 210, Palo Alto, CA 94303
Phone: +1 888 883 2993
https://spin.ai/

ДОВІДКА ПРО ВПРОВАДЖЕННЯ

Результати дисертаційного дослідження Мироченка Дмитра Володимировича на тему: «Вплив глобальних кіберзагроз на міжнародну конкурентоспроможність і економічну безпеку країн» на здобуття ступеня доктора філософії за спеціальністю 292 – Міжнародні економічні відносини були розглянуті та впроваджені у практичну діяльність компанії Spin.AI. У діяльності компанії використано окремі теоретичні положення, висновки та практичні рекомендації автора щодо оцінювання кіберризиків у хмарних і SaaS-середовищах, зниження ризиків втрати даних, посилення механізмів захисту цифрової інфраструктури, а також удосконалення підходів до управління ризиками в умовах цифрової трансформації. Результати дослідження були враховані під час розвитку внутрішніх підходів до аналізу загроз, захисту SaaS-даних, забезпечення безперервності бізнес-процесів і вдосконалення практик безпеки та комплаєнсу. Таким чином, результати дисертаційного дослідження Мироченка Дмитра Володимировича мають практичне значення та можуть бути використані для подальшого розвитку підходів до кібербезпеки, цифрової стійкості та управління ризиками.	The results of the dissertation research of Dmytro Volodymyrovych Myronchenko on the topic: "The Impact of Global Cyber Threats on International Competitiveness and Economic Security of Countries" submitted for obtaining the degree of Doctor of Philosophy in the specialty 292 – International Economic Relations, were reviewed and implemented in the practical activity of Spin.AI. Selected theoretical provisions, conclusions, and practical recommendations of the author were applied in the company's activities, particularly in the areas of cyber risk assessment in cloud and SaaS environments, data loss risk reduction, strengthening digital infrastructure protection, and improving risk management approaches in the context of digital transformation. The results of the study were taken into account in the development of internal approaches to threat analysis, SaaS data protection, business continuity, and the improvement of security and compliance practices. Therefore, the dissertation results of Dmytro Volodymyrovych Myronchenko are of practical significance and may be used for the further development of cybersecurity, digital resilience, and risk management approaches.

Керівник / Authorized Representative Spin.AI

_____ **/Sergiy Balynsky/**

Date: March 10 2026

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ
"Промислово-технологічний парк"
"КИЇВЩИНА"

Ідентифікаційний код 32119339

07354, Київська.,Вишгородський р-н.,
с.Нові Петрівці, вул.Захисників України, 34
Тел./факс: 093 718 27 77

Вих. № 04/04 - 26
від 27 квітня 2026 року

ДОВІДКА ПРО ВПРОВАДЖЕННЯ

Результати дисертаційного дослідження Мирончeнка Дмитра Володимировича на тему: «Вплив глобальних кіберзагроз на міжнародну конкурентоспроможність і економічну безпеку країн» на здобуття ступеня доктора філософії за спеціальністю 292 «Міжнародні економічні відносини» були опрацьовані та впроваджені у діяльність ТОВ «Промислово-технологічний парк «КИЇВЩИНА».

У межах діяльності підприємства використано наукові положення, висновки та рекомендації автора, що стосуються оцінювання впливу кіберзагроз на економічну стійкість, мінімізації ризиків у цифровому середовищі, а також удосконалення підходів до управління ризиками та забезпечення інформаційної безпеки в умовах цифровізації. Отримані результати були враховані при вдосконаленні внутрішніх процесів аналізу ризиків, впровадженні заходів із захисту інформаційних ресурсів і розвитку практик безперервності діяльності підприємства.

Генеральний директор
ТОВ «ПРОМИСЛОВО-ТЕХНОЛОГІЧНИЙ
ПАРК «КИЇВЩИНА» _____ Дмитро БОЙЧУК