DOI https://doi.org/10.30525/978-9934-26-684-3-10

РОЗДІЛ 10
КІБЕРБЕЗПЕКА НАЦІОНАЛЬНОЇ ЕКОНОМІКИ В УМОВАХ ГЛОБАЛЬНИХ ТА ВОЄННИХ ТРАНСФОРМАЦІЙ

Завгородня Є. О., Шестак Я. І.

ВСТУП

У сучасних умовах глобальної цифровізації економічних процесів кібербезпека набуває статусу одного з ключових чинників забезпечення стабільного функціонування національних економік. Розвиток цифрових платформ та електронної комерції, хмарних сервісів, систем електронного урядування тощо формують нову архітектуру суспільних та економічних відносин, у межах якої інформаційні ресурси, ІКТ-інфраструктура та дані перетворюються на стратегічні економічні активи. Водночас всі ці процеси супроводжуються підвищенням вразливостей економічних систем до кіберзагроз, наслідком яких можуть бути фінансові втрати, порушення функціонування критичної інфраструктури та послаблення економічної стабільності держави. Відповідно, згадані кіберризики створюють потребу в посиленні кібербезпеки як на рівні державного управління, так і на рівні суб'єктів господарювання [1].

Особливої актуальності питання кібербезпеки набуває для України, яка перебуває в умовах одночасних глобальних та воєнних трансформацій. З однієї сторони, держава активно інтегрується у світову цифрову економіку (розвиває електронні державні послуги, цифрові платформи, інноваційні технології тощо). З іншої сторони, повномасштабна військова агресія російської федерації супроводжується масштабними кібератаками на об'єкти інфраструктури різного ступеню національної критичності [2]. У цьому контексті кіберпростір стає одним із ключових театрів гібридного протистояння, де економічні, інформаційні

[1] Вдовічен А., Королюк Ю., Вдовічен Д. Цифрові технології та кібербезпека в стратегії відновлення післявоєнної економіки України. *Вісник Чернівецького торговельно-економічного інституту*. 2025. Т. II, № 98. С. 8–29. DOI: https://doi.org/10.34025/2310-8185-2025-2.98.01

[2] Zavhorodnya E., Melnyk T. Ukraine's digital frontier: a deep dive into ICT sector competitiveness. *Traditional and innovative approaches in economics: theory, methodology, practice* : Collective monograph. Riga, Latvia. P. 137–170. 2024. DOI: https://doi.org/10.30525/978-9934-26-407-8-7

та технологічні інструменти використовуються для досягнення стратегічних цілей.

Крім того, сучасні тенденції розвитку світової економіки свідчать про трансформацію кіберпростору на важливу сферу економічної конкуренції між державами. Кібератаки, промислове шпигунство, несанкціонований доступ до інформаційних ресурсів та маніпуляції з даними часто використовуються як інструменти впливу та отримання стратегічних переваг. Таким чином, підтримка належного рівня кібербезпеки є не лише технічною та інформаційною проблемою, а й комплексним завданням економічної політики та національної безпеки.

10.1. Кібербезпека як складова економічної безпеки держави

У науковій літературі питання кібербезпеки розглядається як важлива складова економічної безпеки держави та необхідна умова для розвитку цифрової економіки. Кібератаки здатні спричиняти значні економічні збитки, порушувати роботу стратегічних галузей, ускладнювати функціонування державних інституцій та негативно впливати на інвестиційну привабливість країни [3]. Зазначимо, впродовж останніх років географія наукових публікацій (переважно з США, Китаю та Індії) про питання кібербезпеки в системі економічної безпеки додатково підтверджує глобальний характер проблеми та її стратегічне значення для розвитку національних економік [4].

Загальнотеоретичні підходи до розуміння категорії «економічної безпеки держави» наразі розглядають її як комплексну систему захисту національних економічних інтересів від внутрішніх і зовнішніх загроз для забезпечення стабільного розвитку вітчизняної економіки [5, 6]. До того ж, економічна безпека виступає однією з ключових складових національної

[3] Оксінь В. Ю., Левченко Д. С., Костенко І. В. Кібербезпека держави як інструмент сталого розвитку цифрового середовища. *Аналітично-порівняльне правознавство*. 2025. Т. 2, № 6. С. 411–415. DOI: https://doi.org/10.24144/2788-6018.2025.06.2.67

[4] Койбічук В. В. Роль кібербезпеки в системі економічної безпеки: бібліометричний аналіз. *Інноваційна економіка*. 2024. № 2. С. 150–158. DOI: https://doi.org/10.37332/2309-1533.2024.2.19

[5] Зуб В.В. Сутнісна характеристика економічної безпеки держави. *Аналітично-порівняльне правознавство*. 2024. № 2. С. 457–462. DOI: https://doi.org/10.24144/2788-6018.2024.02.77

[6] Франчук В. І., Корчинський І. О. Економічна безпека держави: історичні аспекти та характеристика сутності. *Ефективна економіка*. 2019. № 8. DOI: https://doi.org/10.32702/2307-2105-2019.8.7

безпеки, формуючи підґрунтя для інших її елементів (військової, енергетичної, продовольчої, екологічної та ін.) [7].

Враховуючи значну залежність сучасних економічних систем від ІКТ-інфраструктур, інформаційних систем (ІС) та мережевих технологій, наголосимо, що кіберзагрози дедалі більше впливають не лише на інформаційну сферу, але й на фінансову стабільність, промислове виробництво, логістику, енергетичні системи тощо. Важливість кібербезпеки зумовлена й тим, що сучасна економіка дедалі більше залежить від ІКТ-інфраструктури та інформаційних ресурсів. Тобто, розвиток цифрової економіки та рівень кіберстійкості держави перебувають у взаємозв'язку: підвищення рівня кібербезпеки сприяє більш активному використанню ІКТ (інформаційно-комунікаційних технологій), прискоренню цифрової трансформації та зростанню загального економічного добробуту [8]. Водночас, недостатній рівень кібербезпеки потенційно стримує цифровий розвиток, знижує довіру до цифрових ресурсів і сервісів, а також створює додаткові економічні ризики. Отже, постає нагальне питання концептуального інтегрування кібербезпеки в структуру економічної безпеки держави. Зокрема, пропонуємо розглядати кібербезпеку в межах трьох підходів:

(1) *Економічний підхід*, тобто кібербезпека спрямована на захист економічних цифрових активів та операцій (є незалежним компонентом економічної безпеки держави) від фінансових кіберзлочинів (фінансового шахрайства, атак на цифрові платіжні системи, крадіжок та маніпуляцій комерційними або фінансовими даними), промислових та корпоративних атак (викрадень комерційної інформації, атак на системи управління виробництвом, порушень в роботі онлайн-платформ), атак на державні економічні системи (реєстри, системи державних закупівель та статистичного обліку) тощо. Тобто, основними об'єктами управління та захисту є:

- ІС державного управління економікою;
- фінансові та банківські ІС;
- цифрові платформи електронної комерції;
- системи управління виробництвом;

[7] Франчук В. І., Корчинський І. О. Економічна безпека держави: історичні аспекти та характеристика сутності. *Ефективна економіка*. 2019. № 8. DOI: https://doi.org/10.32702/2307-2105-2019.8.7

[8] Кіндзерський Ю. В.. Кібербезпека та становлення цифрової економіки: проблеми взаємозв'язку. *Економічний вісник Дніпровської політехніки*. 2020. № 71. С. 18–26. DOI: https://doi.org/10.33271/ebdut/71.018

- ІС державних реєстрів;
- інформаційні ресурси наукових і освітніх установ;
- системи управління інвестиційними та інноваційними проєктами;
- цифрові системи державної статистики;
- ІС підприємств стратегічних галузей економіки.

Зацікавленими сторонами виступають суб'єкти господарювання з різних секторів національної економіки та державні установи, які відповідають за регулювання економічної діяльності, наприклад: фінансові установи (банки, платіжні системи); підприємства промисловості та аграрного сектору; державні органи економічного управління; органи статистики та макроекономічного аналізу; установи соціального забезпечення; наукові та освітні установи; державні та приватні інституції, що реалізують інвестиційно-інноваційні проєкти; підприємства продовольчого сектору; екологічні та природоохоронні організації.

Ефективне впровадження та функціонування системи кібербезпеки в межах цього підходу передбачає застосування галузевої моделі управління, у межах якої кібербезпека розглядається як окрема складова економічної політики держави. Основними функціями цієї моделі є прогностична (для аналізу тенденцій кіберзагроз), регуляторна (тобто, формування нормативно-правової бази), контрольна (тобто, аудит та моніторинг стану кіберзахисту), координаційна та оперативна (для реагування на кіберінциденти). Світові практики застосування галузевої моделі передбачають формування спеціалізованої системи органів управління кібербезпекою, до якої входять:

- центральні органи державної влади, що формують політику у сфері кібербезпеки;
- національні центри реагування на кіберінциденти;
- спеціалізовані підрозділи кіберполіції та правоохоронних органів;
- регулятори окремих секторів економіки (фінансового, енергетичного, телекомунікаційного тощо);
- галузеві служби інформаційної та кібербезпеки;
- державні органи спеціального зв'язку, відповідальні за захист критичної інформаційної інфраструктури.

Управління в цій моделі здійснюється через вертикально організовану систему координації, де стратегічні рішення приймаються на державному рівні, а їхня реалізація відбувається через галузеві та інституційні структури. Крім того, у межах цієї моделі застосовується широкий спектр регуляторних, організаційних та технологічних інструментів, а саме:

національні стратегії та доктрини кібербезпеки, законодавство у сфері кіберзахисту, державні стандарти інформаційної та кібербезпеки, системи моніторингу кіберзагроз, механізми обміну інформацією про кіберінциденти, державні програми розвитку кіберстійкості економіки, системи аудиту та сертифікації інформаційних систем, інструменти управління кіберризиками тощо.

(2) *Інформаційний підхід*, тобто кібербезпека спрямована на захист інформаційних ресурсів та інформаційних процесів (є елементом інформаційної безпеки держави, яка вже входить до структури економічної безпеки держави), що забезпечують функціонування національної економіки. Відповідно, кібербезпека опосередковано підтримує компоненти економічної безпеки держави, сприяючи макроекономічній безпеці, науково-технологічній безпеці, безпеці інвестицій та інновацій, а також зовнішньоекономічній безпеці (які залежать від надійних та безперебійних інформаційних потоків та систем даних).

Основними об'єктами захисту є державні ІС управління економікою, державні реєстри, БД органів державної влади, системи електронного урядування, інформаційні ресурси органів статистики, ІС соціального забезпечення, демографічні та міграційні реєстри, системи електронного документообігу, ІС наукових і освітніх установ, інформаційні архіви держави, системи електронної взаємодії органів влади та комунікаційні мережі органів державного управління.

Стейкхолдерами об'єктів захисту виступають державні органи, що працюють з економічною інформацією, органи статистики та аналітики, наукові та освітні установи, підприємства, що використовують інформаційні системи управління, організації соціальної сфери (лікарні, установи соціального захисту), органи, що ведуть демографічні та соціальні реєстри.

В межах цього підходу передбачається використання ієрархічної моделі управління, у якій кібербезпека підпорядкована системі інформаційної безпеки держави. Головними функціями цієї моделі управління кібербезпекою національної економіки є: *нормативно-регуляторна* (у сфері захисту інформації), *організаційна* (для створення інституційної системи інформаційної безпеки), *контрольна, захисна* (для забезпечення конфіденційності, цілісності та доступності інформації і ресурсів), *координаційна* та *аналітична*.

Відповідно, у межах цієї моделі формується система органів, що підпорядкована органам управління інформаційною безпекою, а саме

політико-стратегічного рівня управління (центральні органи державної влади, що формують політику у сфері інформаційної безпеки), *операційно-безпекового рівня* (державні органи, відповідальні за захист інформаційного простору; спеціалізовані підрозділи кіберзахисту в межах органів інформаційної безпеки), *внутрішнього організаційного рівня* (служби захисту інформації в державних установах, підрозділи захисту ІС органів влади, підрозділи інформаційної безпеки державних підприємств), *інфраструктурно-технологічного рівня* (адміністратори державних інформаційних ресурсів, державні ЦОДи), *контрольно-регуляторного рівня* (органи контролю у сфері технічного та криптографічного захисту інформації) та *науково-освітнього рівня* (спеціалізовані науково-дослідні установи з інформаційної безпеки).

Основні інструменти та підходи до підтримування належного рівня кібербезпеки економіки держави налічують державну політику інформаційної безпеки, законодавство про захист інформації, державні стандарти інформаційної безпеки, криптографічний та технічний захист інформації, системи управління доступом до інформаційних ресурсів, системи резервного копіювання та відновлення даних, сертифікацію програмно-технічних засобів захисту інформації, державний аудит ІС, моніторинг інформаційних потоків, системи виявлення кіберінцидентів та системи захисту електронного документообігу.

Варто зазначити, обидва підходи та моделі управління кібербезпекою є характерними для ранніх етапів розвитку політик кібербезпеки, коли основний акцент робиться на захисті інформації, а не на забезпеченні стійкості всієї цифрової економічної інфраструктури. Проте, у сучасних умовах цифровізації економіки та воєнних конфліктів ці підходи й моделі необхідно доповнювати більш інтегрованими підходами, які розглядають кібербезпеку як міжгалузеву основу функціонування різних складових економічної безпеки держави.

(3) *Системний підхід*, тобто кібербезпека спрямована на захист ІКТ-інфраструктури функціонування економіки держави (є міжгалузевим компонентом). За такого підходу кібербезпека безпосередньо підтримує всі основні компоненти економічної безпеки (фінансову безпеку, інвестиційно-інноваційну безпеку, інформаційну безпеку, науково-технологічну безпеку, енергетичну безпеку, соціальну безпеку, демографічну безпеку, продовольчу безпеку тощо), оскільки стабільне функціонування цих секторів дедалі більше залежить від безпечної ІКТ-інфраструктури. Таким чином, до об’єктів захисту належить широкий спектр компонентів цифрової економіки держави: *базова*

ІКТ-інфраструктура (національні телекомунікаційні мережі, ЦОДи, хмарна інфраструктура), *фінансово-економічні цифрові системи* (системи електронних платежів, цифрові платформи електронної комерції), *виробнича та галузева інфраструктура* (промислові системи управління виробництвом, системи управління енергетичною інфраструктурою, транспортні та логістичні інформаційні системи, цифрові системи аграрного виробництва), *інфраструктура управління економічними процесами* (системи управління ланцюгами постачання, системи цифрової взаємодії бізнесу і держави), *державні та соціально значущі ІС* (платформи електронного урядування, інформаційні системи соціального забезпечення), а також науково-аналітична та моніторингова інфраструктура (наприклад, системи екологічного моніторингу та науково-дослідницька ІКТ-інфраструктура).

Основними стейкхолдерами об'єктів захисту є: оператори критичної інфраструктури, підприємства промисловості, енергетичні компанії, аграрні та продовольчі підприємства, установи охорони здоров'я, органи соціального захисту, демографічні та статистичні установи, органи екологічного моніторингу, освітні та наукові організації, транспортні та логістичні компанії тощо.

Системний підхід передбачає застосування мережевої або інтегрованої моделі управління, що передбачає координацію між різними секторами економіки та державними інституціями задля підтримки належного рівня кібербезпеки в різних секторах економіки держави. Модель називається мережевою, оскільки управління здійснюється через взаємодію великої кількості державних, приватних і суспільних інституцій, пов'язаних між собою горизонтальними зв'язками та механізмами координації. Функціональне призначення мережевої моделі передбачає забезпечення захисту ІКТ-інфраструктури цифрової економіки держави, організацію координації між різними секторами економіки, виявлення та запобігання кіберзагрозам, аналіз та реагування на кіберінциденти в галузях економіки, формування загальнонаціональних та галузевих стандартів кібербезпеки, а також адаптацію системи захисту до нових технологічних загроз.

Суб'єкти захисту в системному підході охоплюють центральні органи державної влади, що формують політику кібербезпеки; національні центри кіберзахисту; галузеві регулятори економіки; оператори критичної інфраструктури; телекомунікаційні оператори; постачальники цифрових платформ і хмарних сервісів; фінансові установи; промислові підприємства; енергетичні компанії; транспортні оператори; науково-

дослідні установи; університети; компанії з кібербезпеки; професійні галузеві асоціації; міжнародні організації та партнерські мережі кібербезпеки.

Мережева модель передбачає використання комплексного набору інституційних, технологічних і організаційних інструментів, а саме: національні стратегії кіберстійкості економіки, системи управління кіберризиками, центри реагування на кіберінциденти, галузеві системи моніторингу кіберзагроз, платформи обміну інформацією про кіберзагрози, системи захисту критичної інфраструктури, стандарти кібербезпеки для економічних секторів, системи аудиту кібербезпеки, технології захисту промислових систем управління, системи захисту цифрових ланцюгів постачання, системи управління цифровою ідентифікацією, інструменти тестування кіберстійкості інфраструктури, кібернавчальні полігони, механізми кіберстрахування, цифрові платформи координації реагування на кіберінциденти.

Крім того, важливим залишаються етичні аспекти підтримки кібербезпеки (зокрема, питання захисту персональних даних, корпоративної відповідальності та формування довіри у міжнародному економічному середовищі) [9]. У цьому контексті, формулювання та застосування принципів кібербезпеки є необхідним для створення узгодженої концептуальної основи захисту цифрових основ національної економіки, оскільки ці принципи визначають ключові підходи до управління кібербезпекою, сприяють координації між державними установами, суб'єктами приватного сектору та іншими зацікавленими сторонами, а також допомагають збалансувати вимоги до безпеки з цілями економічного розвитку.

Стратегічні та управлінські принципи визначають, як організовано управління кібербезпекою на національному рівні, тобто визначають стратегічну візію, інституційну архітектуру, механізми координації та розподіл відповідальності між зацікавленими сторонами, відповідальними за захист національної економіки. До того ж, ці принципи визначають механізми інтеграції кібербезпеки до ширшої системи економічної та національної безпеки держави. Важливим завданням є створення умов для ефективної міжінституційної взаємодії, запобігання дублюванню функцій різних органів та формування прозорої системи управління кібербезпекою. Принципи в цій групі налічують:

[9] Мирончeнко Д. В. Етичні аспекти кібербезпеки у світовій економіці та міжнародних відносинах. *Вчені записки*. 2025. Т. 40(3). С. 133–140. DOI: https://doi.org/10.33111/vz_kneu.40.25.03.12.081.087

– *принцип системного підходу* (тобто кібербезпека розглядається як комплексна система, що охоплює всі взаємопов'язані елементи національної економіки та ІКТ-інфраструктури);

– *принцип спільної відповідальності* (кібербезпека є відповідальністю державних установ, організацій приватного сектору, науково-дослідних установ та суспільства);

– *принцип державно-приватного партнерства* (стійкість кібербезпеки вимагає співпраці між державою та приватними операторами ІКТ-інфраструктури);

– *принцип пропорційного розподілу відповідальності* (відповідальність за кіберзахист повинна відповідати рівню ризику та важливості цифрових активів);

– *принцип підзвітності* (приватні організації та державні інституції, відповідальні за ІКТ-інфраструктуру, повинні нести відповідальність за забезпечення кібербезпеки та управління кіберризиками);

– *принцип міжнародної співпраці* (управління кібербезпекою повинно враховувати співпрацю з іноземними урядами, міжнародними організаціями та світовими мережами кібербезпеки);

– *принцип багаторівневого управління* (управління кібербезпекою діє на національному, галузевому, регіональному та організаційному рівнях для забезпечення ефективного впровадження заходів безпеки);

– *принцип координації з політикою національної безпеки* (політика кібербезпеки повинна бути узгоджена з стратегіями національної та економічної безпеки).

Правові та регуляторні принципи формують нормативно-правову базу системи кібербезпеки, визначаючи правила, стандарти та вимоги, які регулюють діяльність державних органів, підприємств, операторів критичної інфраструктури та інших суб'єктів у сфері захисту ІС та даних (тобто створюють інституційно-правове середовище, яке забезпечує ефективну реалізацію державної політики кібербезпеки). Крім того, ці принципи спрямовані на забезпечення балансу між потребами безпеки та захистом прав і свобод людини, а саме у сфері персональних даних, конфіденційності інформації та свободи економічної діяльності. Також, важливим аспектом є гармонізація національного законодавства з міжнародними стандартами. Отже, основні приклади принципів цієї групи враховують:

– *принцип правової визначеності* (управління кібербезпекою має бути підкріплене чітким та послідовним законодавством, яке визначає

зобов'язання, відповідальність та механізми забезпечення дотримання встановлених норм);

− *принцип прозорості* (політика, правила та процедури кібербезпеки повинні бути прозорими та доступними для відповідальних сторін);

− *принцип захисту цифрових прав* (заходи кібербезпеки повинні враховувати конфіденційність, захист даних та основні свободи людини);

− *принцип пропорційності та адекватності* (заходи безпеки повинні відповідати рівню загрози та не повинні безпідставно обмежувати економічну діяльність чи технологічний розвиток);

− *принцип регуляторної координації* (нормативно-правові акти у сфері кібербезпеки повинні бути гармонізовані з політикою у сфері цифрової економіки, захисту даних та національної безпеки);

− *принцип регуляторної адаптивності* (законодавство про кібербезпеку слід періодично оновлювати з урахуванням технологічних змін та нових кіберзагроз);

− *принцип відповідності та аудиту* (тобто необхідно регулярно оцінювати дотримання правил та стандартів кібербезпеки).

Принципи управління ризиками керують ідентифікацією, оцінкою та управлінням кіберризиками, що впливають на економіку та ІКТ-інфраструктуру держави. Відповідно, принципи цієї групи передбачають використання превентивних і аналітичних механізмів, спрямованих на попередження кіберінцидентів, а також на зменшення можливих економічних втрат у разі їх виникнення. Додатково, ці принципи передбачають створення систем моніторингу загроз, обміну інформацією про кіберінциденти та координації дій між суб'єктами кібербезпеки. До основних прикладів принципів цієї групи можемо віднести:

− *принцип ризик-орієнтованого управління* (політика кібербезпеки повинна ґрунтуватися на систематичній оцінці ризиків та пріоритезації найбільш критичних загроз);

− *принцип проактивного захисту* (превентивні заходи повинні бути пріоритетними для зменшення вразливостей та запобігання кіберінцидентам);

− *принцип безперервного моніторингу* (ІКТ-інфраструктура на всіх рівнях повинна постійно моніторитися для виявлення кіберзагроз та підозрілої діяльності);

− *принцип раннього попередження та розвідки про загрози* (системи кіберзахисту повинні включати механізми виявлення нових кіберзагроз та обміну розвідувальними даними про загрози);

– *принцип готовності до інцидентів* (організації на всіх рівнях повинні підтримувати готовність реагувати на кіберінциденти за допомогою механізмів кризового управління та планів реагування);

– *принцип управління вразливостями* (тобто, слід регулярно проводити оцінку та усунення вразливостей в ІС).

Принципи стійкості та сталого розвитку спрямовані на забезпечення довгострокової стабільності, стійкості та сталого функціонування цифрової економіки держави в умовах кіберзагроз. У сучасних умовах нейтралізувати всі кіберзагрози неможливо, тому в багатьох задачах систем кібербезпеки є формування стійких та адаптивних економічних систем, які можуть функціонувати навіть у разі часткового порушення ІКТ-інфраструктури. Принципи цієї групи передбачають впровадження механізмів резервування критичних систем, диверсифікації технологічних рішень, планування безперервності господарських процесів та швидкого відновлення систем і ресурсів після кіберінцидентів. Як приклад, до цієї групи належать принципи:

– *стійкості та безперервності* (економічні системи повинні бути здатними підтримувати свою діяльність та швидко відновлюватися після кіберінцидентів);

– *принцип адаптивності та постійного вдосконалення* (системи кібербезпеки повинні розвиватися у відповідь на технологічні зміни та нові загрози);

– *принцип сталості* (політика кібербезпеки повинна підтримувати довгостроковий захист ІКТ-інфраструктури, зберігаючи при цьому економічну ефективність);

– *принцип диверсифікації технологічних рішень* (тобто, мінімізація залежності від одного постачальника технологій або систем).

– У підсумку, застосування цих принципів сприяє надійності та стабільності функціонування економіки держави, зменшує економічні втрати та зміцнює довірю до ІКТ.

Економічні принципи, в свою чергу, пов’язані з формуванням економічних та інституційних передумов для довгострокового розвитку системи кібербезпеки. Забезпечення належного рівня кібербезпеки потребує значних інвестицій у технології, інфраструктуру та розвиток людського капіталу. Відповідно, важливим завданням державної політики є створення умов для розвитку національної екосистеми кібербезпеки, яка складається з наукових установ, освітніх організацій, технологічних компаній та державних структур. Економічні принципи спрямовані на підтримування інновацій у сфері кібербезпеки, розвиток компетентних

фахівців, стимулювання досліджень та створення конкурентоспроможної індустрії кібербезпеки. Завдяки реалізації цих принципів формується стійка та ефективна система кібербезпеки, яка здатна підтримувати розвиток цифрової економіки та забезпечувати захист економічних інтересів держави.

Приклади принципів із цієї групи включають:

− *принцип нарощування потенціалу* (держава повинна підтримувати освіту, професійну підготовку та розвиток навичок з кібербезпеки);

− *принцип підтримки інновацій* (заохочення R&D та інновації в технологіях кібербезпеки);

− *принцип інвестування в інфраструктуру кібербезпеки*;

− *принцип секторальної адаптації* (заходи кібербезпеки повинні враховувати специфічні характеристики та вимоги різних секторів економіки);

− *принцип технологічного суверенітету* (передбачає зменшення залежності від іноземних технологій у критично важливих системах кібербезпеки);

− *принцип захисту стратегічної інтелектуальної власності та економічних даних*;

Підсумовуючи, категорія «кібербезпека» поступово трансформується від проблеми захисту окремих інформаційних систем до складного макроекономічного явища, пов'язаного із забезпеченням стійкості функціонування держави, економіки та суспільства в цифровому середовищі [10, 11].

10.2. Кібербезпека в системі міжнародних економічних відносин

Водночас, кібербезпека дедалі більше виходить за межі національного рівня та стає важливим фактором функціонування світової економіки, оскільки розвиток глобальних цифрових мереж, міжнародної електронної торгівлі та транснаціональних інформаційних потоків зумовлює потребу в формуванні міжнародних механізмів співпраці у сфері кіберзахисту. В цьому контексті кібербезпека розглядається як стратегічний інструмент забезпечення стабільності міжнародних економічних відносин та захисту

[10] Білявська Ю., Шестак Я. Кібербезпека та кібергігієна: нова ера цифрових технологій. *Товарознавство. Технології. Інжиніринг*. 2022. Т. 43, № 3. С. 47–59. DOI: https://doi.org/10.31617/2.2022(43)04

[11] Горбаченко С. Кібербезпека як складова економічної безпеки України. *Галицький економічний вісник*. 2020. Т. 66, № 5. С. 180–186. DOI: https://doi.org/10.33108/galicianvisnyk_tntu2020.05.180

економічних інтересів держав і корпорацій [12]. Варто зазначити, що глобальному інформаційному простору властиві наступні особливості, зокрема:

1) міжнародні економічні відносини дедалі більше залежать від транскордонних потоків даних, отже обмеження, перебої або порушення потоків даних може негативно впливати на економічні та геополітичні процеси;

2) системність ризиків, тобто кіберінцидент в одній країні чи секторі може поширюватися через кордони, одночасно впливаючи на кілька національних економік (оскільки ІКТ-інфраструктури об'єднують фінансові системи, ланцюги вартості, виробничі мережі в різних країнах в єдину глобальну систему);

3) основні компоненти цифрової економіки (хмарні сервіси, ЦОДи, платформи, платіжні системи тощо) працюють глобально, а не національно (відповідно, держави залежать від інфраструктури, яка контролюється іноземними суб'єктами, що створює стратегічні вразливості та обмежує національний контроль над економічними процесами);

4) значна частка глобальної ІКТ-інфраструктури та послуг контролюється невеликою кількістю транснаціональних технологічних корпорацій (що створює поодинокі точкові відмови, системні ризики у разі кібератак, економічну залежність від конкретних постачальників), в той час як відповідальність за безпеку часто є обов'язком держав;

5) країни суттєво відрізняються своїм технологічним розвитком, потенціалом у сфері кібербезпеки та інституційною спроможністю;

6) цифровізація зробила ланцюги поставок дуже взаємопов'язаними та залежними від технологій, відповідно кібератаки на один елемент (наприклад, логістичну платформу, систему постачальників і т.д.) можуть порушувати виробничі процеси та міжнародні торговельні потоки;

7) кібератаки часто здійснюються через кордони різних держав, до того ж зростання попиту на Інтернет речей, хмарні обчислення та цифрові платформи збільшує кількість потенційних точок входу для зловмисників;

8) технологічно розвинені держави можуть використовувати ІКТ-інфраструктуру та кіберінструменти в геополітичній конкуренції для

[12] Заяць Д.Ф., Кицюк І.В. Роль кібербезпеки в міжнародних економічних відносинах. *Науковий вісник Ужгородського національного університету*. 2024. № 53. С. 14–19. DOI: https://doi.org/10.32782/2413-9971/2024-53-2

отримання економічних вигод, обмеження технологій з міркувань безпеки та фрагментування глобального цифрового простору.

Кібербезпека в системі міжнародних економічних відносин є багатогранним явищем, яке охоплює інституційні, технологічні, правові та економічні механізми, що спрямовані на захист глобальної ІКТ-інфраструктури, транскордонних потоків даних та економічної взаємодії держав від потенційних кіберзагроз (табл. 1). Таким чином, кібербезпеці в системі міжнародних економічних відносин (МЕВ) характерна низка специфічних рис, які слідують з транснаціонального, багатостороннього та високо взаємопов'язаного характеру глобальної цифрової економіки, що збільшує як складність управління, так і масштаб потенційних ризиків.

Відповідно, кібербезпека діє в середовищі без кордонів, де кіберзагрози, атаки та вразливості виникають та поширюються одночасно в декількох юрисдикціях. Важливою характеристикою є множинність залучених сторін, що призводить до децентралізованої та багаторівневої моделі управління (оскільки кібербезпека в глобальному економічному середовищі охоплює держави, ТНК, міжнародні організації, глобальні цифрові платформи та транснаціональні мережі кіберзлочинців). Як наслідок, система кібербезпеки діє в рамках фрагментованого регуляторного середовища, тобто системи співіснування різноманітних національних правил, стандартів та політик (що вимагає постійної координації та адаптації в різних правових системах).

Крім того, підтримування кібербезпеки ускладнюється проблемами атрибуції, підзвітності та вирішення міжнародних спорів (через технічну складність кібератак, фрагментацію юрисдикцій та навмисне приховування джерел атак), перешкоджаючи ідентифікації відповідальних сторін. В свою чергу, це пояснює необхідність міжнародних механізмів координації (завдяки міжнародним двостороннім та багатостороннім угодам, спільним системам реагування та механізмам обміну інформацією), оскільки кібербезпека світової економіки залежить від колективних дій, а не виключно від зусиль на національних рівнях.

На рис. 1 відображено частки країн у різних регіонах світу, які беруть участь у двосторонніх або багатосторонніх угодах з кібербезпеки, зокрема з питань обміну інформацією та розвитку потенціалу, демонструючи стабільно високий рівень участі у міжнародній співпраці у сфері кібербезпеки в усіх регіонах світу.

Таблиця 1

Сутність кібербезпеки в міжнародних економічних відносинах

Підхід до трактування	Сутнісне вираження кібербезпеки
Функціональний (економічний)	сукупність організаційних, правових та технологічних заходів, спрямованих на захист міжнародної торгівлі, фінансових операцій, інвестиційних потоків та глобальних ланцюгів вартості від кіберзагроз, які можуть порушити економічні процеси або спричинити фінансові втрати
Ризик-орієнтований	система механізмів управління ризиками, що спрямована на виявлення, оцінювання та пом'якшення негативного впливу кіберризиків транскордонної економічної взаємодії, цифрових ринків та глобальних ланцюгів вартості
Інституційний	багаторівнева система управління та координації між державами, міжнародними організаціями та приватними суб'єктами, що спрямована на підтримку безпечного функціонування світової цифрової економіки та регулювання кіберризиків у транснаціональній економічній діяльності
Інфраструктурний	захист глобальної ІКТ-інфраструктури, враховуючи телекомунікаційні мережі, хмарні платформи, фінансові системи та цифрові послуги, які забезпечують міжнародне економічне співробітництво та інтеграцію
Безпековий	складова економічної безпеки, що захищає економічні інтереси, цифрові активи та стратегічні ресурси в глобальному цифровому середовищі, а також мінімізує негативний вплив кіберризиків на економічний розвиток
Управлінський	сфера глобального управління, яка враховує розробку міжнародних норм, стандартів та механізмів співпраці із захисту економічної системи від кіберризиків та підтримки безпечної цифрової взаємозалежності
Технологічний	захист ІКТ та цифрових платформ, які лежать в основі міжнародних торговельних, фінансових та виробничих систем, забезпечення їхньої стійкості, цілісності та безпечного функціонування в глобальній економіці

Джерело: складено авторами

З аналітичної точки зору, ці дані підтверджують, що кібербезпека в МЕВ за своєю суттю є кооперативною та взаємозалежною. Зокрема, обмін інформацією відіграє вирішальну роль у забезпеченні своєчасного реагування на кіберінциденти, тоді як угоди про розвиток потенціалу підтримують зміцнення інституційного, технологічного та людського потенціалу.

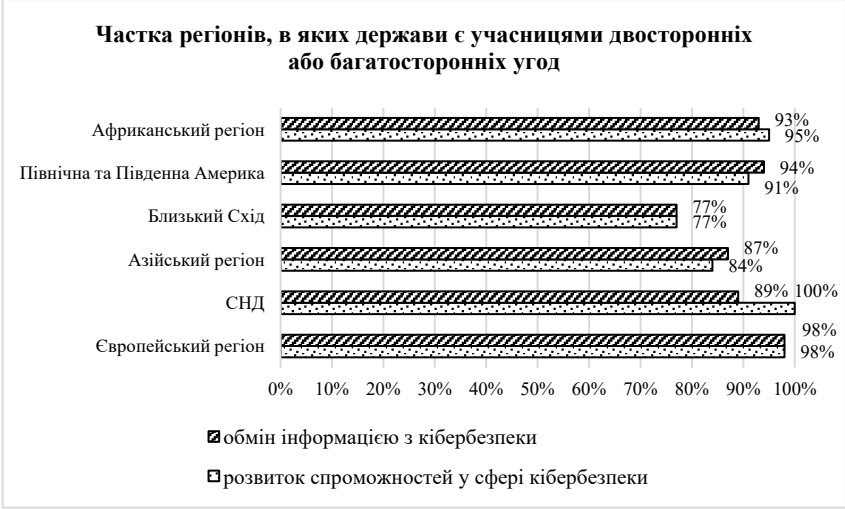

Рис. 1. Участь держав у міжнародних угодах з кібербезпеки

Джерело: перекладено за [13]

Важливо, що фактичний рівень участі держав може бути недооцінений через обмежену обізнаність національних координаторів щодо чинних угод [14]. Це свідчить про те, що глобальний ландшафт управління кібербезпекою є складнішим та комплекснішим, ніж офіційно задокументовано. Крім того, різноманітність угод (від загальних рамкових до дуже специфічних домовленостей) вказує, що держави застосовують неоднорідні підходи до міжнародної співпраці з кібербезпеки. Примітною особливістю також є роль правоохоронних органів та міжнародної поліцейської співпраці (наприклад, Інтерполу та регіональних органів), що відображає важливість боротьби з кіберзлочинністю як транснаціональною економічною загрозою.

Модель Міжнародної спілки електрозв'язку (МСЕ, ITU) [15] щодо міжнародної багатосторонньої співпраці у сфері кібербезпеки спрямована

[13] Заяць Д. Ф., Кицюк І. В. Роль кібербезпеки в міжнародних економічних відносинах. *Науковий вісник Ужгородського національного університету*. 2024. № 53. С. 14–19. DOI: https://doi.org/10.32782/2413-9971/2024-53-2

[14] Global Cybersecurity Index 2024. URL: https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf

[15] Global Cybersecurity Index 2024. URL: https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf

на створення синергії між поточними та майбутніми ініціативами, зосереджуючись на п'яти основних складових, які формують базові елементи національної культури кібербезпеки: правові заходи, технічні заходи, організаційні заходи, заходи з розвитку спроможностей та заходи співробітництва (рис. 2).

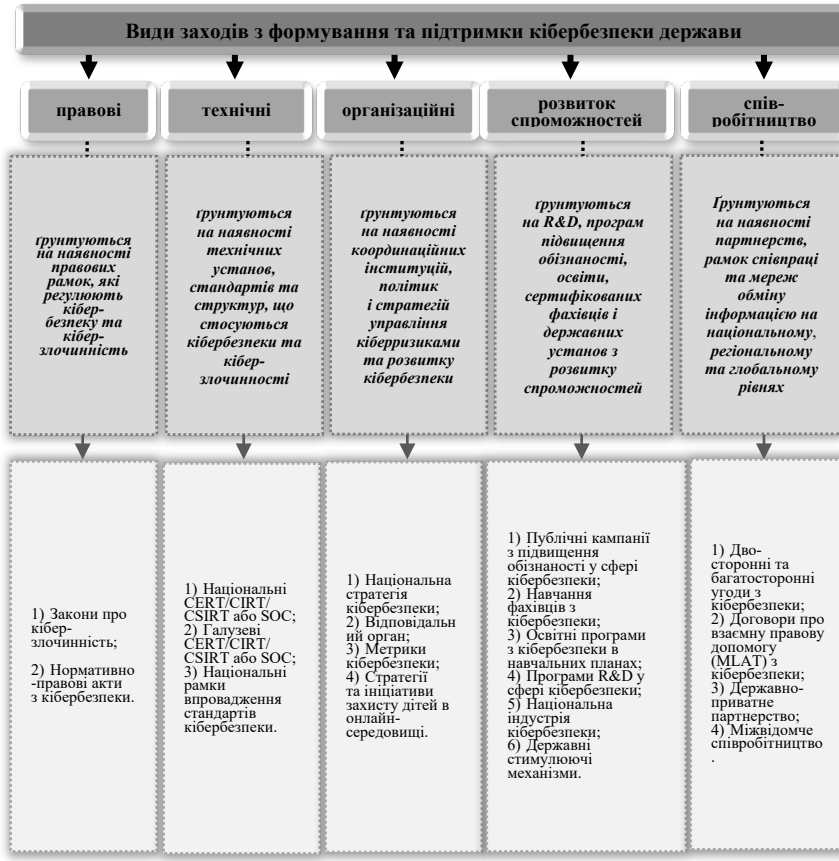

Рис. 2. Система заходів з управління кібербезпекою держави

Джерело: перекладено та доповнено за [16]

[16] Global Cybersecurity Index 2024. URL: https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf

Ще однією особливістю є вплив на динаміку світових ринків, оскільки кібербезпека впливає на міжнародну конкурентоспроможність, інвестиційну привабливість та здатність держави брати участь в глобальних ланцюгах вартості. Додатковим викликом залишається питання балансу між суверенітетом даних та глобалізацією потоків даних (попри те, що світова економіка залежить від вільної передачі даних через кордони, держави прагнуть зберігати контроль над даними з безпекових та стратегічних міркувань). Зрештою, кібербезпека в міжнародних економічних відносинах характеризується високим рівнем невизначеності та складності, оскільки прийняття стратегічних рішень ґрунтується на неповній інформації та вимагає постійної адаптації до технологічних змін, нових кіберзагроз та геополітичної нестабільності.

Крім того, у звіті МСЕ рекомендовано до розгляду наступні зусилля щодо посилення кібербезпеки [17]:

- впроваджувати правові заходи, які можна чітко та справедливо застосовувати в усіх секторах економіки;
- сприяти міжфункціональним ініціативам, що охоплюють не лише інформаційні технології;
- підтримувати добре навчені та оперативно реагуючі національні установи, включаючи групи реагування на комп'ютерні інциденти;
- залучати широке коло зацікавлених сторін до всіх ініціатив у сфері кібербезпеки;
- розробити та регулярно оновлювати національну стратегію кібербезпеки з планом дій, який можна реалізувати;
- впроваджувати ефективні заходи захисту дітей в Інтернеті;
- вирішувати проблеми кібербезпеки, з якими стикається критична інфраструктура;
- проводити кампанії з підвищення обізнаності про кібербезпеку, що спрямовані на вирішення відповідних питань;
- надавати можливості для навчання фахівців з кібербезпеки, операторів критичної інфраструктури та молоді з метою розвитку та вдосконалення навичок кібербезпеки;
- створити механізми стимулювання для заохочення розвитку потенціалу в галузі кібербезпеки, а також досліджень і розробок;
- сприяти внутрішньому та міжнародному співробітництву, а також взаємодії в обміні інформацією та розвитку потенціалу.

[17] Global Cybersecurity Index 2024. URL: https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf

У 2025 р. секторальний розподіл кіберзагроз продемонстрував виражену концентрацію на галузях, що характеризуються високою операційною критичністю, чутливістю даних та системними взаємозв'язками [18].

Промисловість залишається основною мішенню кібератак, значною мірою через її залежність від операційних технологій (ОТ) та систем промислового управління (СПУ), а також складність глобальних ланцюгів поставок (що робить підприємства цього сектору цілями як для атак, спрямованих на порушення роботи, так і для атак, мотивованих фінансовою складовою). Низька толерантність цього сектору економіки до простоїв значно посилює вплив кіберінцидентів: навіть короткочасні перебої можуть зупинити виробничі процеси, що призводить до значних фінансових втрат та потенційних санкцій за договорами.

Привабливість *будівельного сектору* для зловмисників зумовлена терміновим характером проєктів та фрагментованою екосистемою підрядників, субпідрядників та постачальників. Таким чином, ця структурна складність створює численні точки доступу для кібервторгнень, тоді як визначеність термінів виконання проєктів підвищує вразливість до тактик вимагання, спрямованих на максимізацію операційного тиску.

Сектор професійних послуг (а саме юридичних, консалтингових та бухгалтерських) є ще однією критичною цільовою групою суб'єктів господарювання через їхній доступ до великих обсягів конфіденційних даних клієнтів. Кіберінциденти в цьому секторі створюють значні ризики: окрім прямої фінансової та репутаційної шкоди постраждалій організації, скомпрометовані дані можуть слугувати вектором для ширших кібератак на клієнтів та партнерів.

Сектор охорони здоров'я продовжує зазнавати постійного тиску з боку кіберзлочинців. Його вразливість зумовлена, головним чином, необхідністю постійного доступу до даних для догляду за пацієнтами та високою ринковою вартістю конфіденційної медичної інформації, тим самим роблячи заклади охорони здоров'я особливо вразливими до атак програм-вимагачів та витоків даних.

Зрештою, *ІТ-сектор та сектор послуг, що підтримуються ІТ* (з англ. «information technology enabled services»), є стратегічно важливою ціллю кіберзлочинців через свою подвійну роль як сховища інтелектуальної

[18] Global Cybersecurity Report 2025. URL: https://cyble.com/wp-content/uploads/2025/12/Global-Cybersecurity-Report-2025.pdf

власності, так і постачальника ІКТ-послуг для багатьох секторів національної економіки. Кібератаки на ІКТ-компанії, зокрема на постачальників керованих послуг (MSP), мають каскадні ефекти, що дозволяють зловмисникам скомпрометувати численні організації через вектори ланцюгів вартості, посилюючи системний вплив порушень та підкреслюючи критичну важливість захисту екосистем цифрових послуг.

Відповідно до статистики, 94% респондентів опитування Всесвітнього економічного форуму (WEF) вважають штучний інтелект (ШІ) найважливішим фактором змін у кібербезпеці у 2026 р., а 87% позначили *вразливості, пов'язані зі ШІ* (витоки даних; розвиток можливостей для кібератак (фішинг, розробка шкідливого ПЗ та дипфейки); технічна безпека самих систем ШІ; складність управління безпекою; потенційні бекдори; правові питання інтелектуальної власності), як найшвидше зростаючий кіберризик у 2025 р. [19]. Проте приблизно третина організацій досі не мають процесу оцінки безпеки інструментів ШІ перед їхнім розгортанням. Розрив між швидкістю впровадження ШІ та зрілістю управління ШІ продовжує збільшуватися.

Геополітична динаміка стала вирішальним фактором у формуванні сучасних стратегій кібербезпеки. Станом на 2026 р. вона є основним фактором, що впливає на підходи до зменшення ймовірності та негативного впливу кіберризиків. Емпіричні дані свідчать, що приблизно 64% організацій чітко включають загрозу геополітично мотивованих кібератак (особливо на критичну інфраструктуру) або кібершпигунства у свої системи кібербезпеки [20]. Більше того, геополітична нестабільність спонукала до стратегічного перекалібрування (тобто до перегляду своїх стратегій кібербезпеки) 91% великих компаній у відповідь на дедалі більш нестабільне міжнародне середовище.

Водночас, геополітична напруженість сприяє поступовому зменшенню довіри щодо належного рівня відповідності механізмів кіберзахисту на національному рівні (рис. 3). Частка респондентів, які висловили низьку впевненість у здатності своєї держави ефективно реагувати на масштабні кіберінциденти, зросла до 31% порівняно з 26% у 2024 р. [21]

[19] Global Cybersecurity Outlook 2026. URL: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf

[20] Global Cybersecurity Outlook 2026. URL: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf

[21] Global Cybersecurity Outlook 2026. URL: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf

Рис. 3. Ступінь довіри до національних заходів реагування на кібератаки на об'єкти критичної інфраструктури

Джерело: перекладено за [22]

Звіт WEF також демонструє поступовий прогрес у сфері організаційної стійкості: 19% організацій стверджують, що їхня кіберстійкість перевищує вимоги, що більш ніж удвічі порівняно з 9%, які стверджували про це у 2025 р. [23] Проте, 17% все ще повідомляють про недостатній рівень стійкості, і розрив між добре забезпеченими та недостатньо забезпеченими ресурсами організаціями залишається разючим. Крім того, визначальними рисами організацій з високим рівнем стійкості до кіберзагроз є те, що [24]:

– організації з високим рівнем кіберстійкості більш ніж утричі частіше періодично перевіряють безпеку інструментів ШІ (71% проти 20%);

[22] Global Cybersecurity Outlook 2026. URL: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf

[23] Global Cybersecurity Outlook 2026. URL: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf

[24] Global Cybersecurity Outlook 2026. URL: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf

− кіберстійкі організації набагато частіше враховують безпеку в рішеннях щодо закупівель (76% проти 53%);

− кіберстійкі організації оцінюють рівень зрілості безпеки постачальника набагато частіше (74% проти 48%);

− кіберстійкі організації частіше моделюють кіберінциденти з партнерами екосистеми (44% проти 16%);

− 99% кіберстійких організацій повідомляють про залучення ради директорів до питань кібербезпеки, порівняно з лише 87% недостатньо кіберстійких організацій.

Крім того, доведено, що інвестування у системи захисту даних, криптографічні рішення та інструменти кіберзахисту знижує рівень фінансових ризиків суб'єктів господарювання [25]. Відповідно, використання сучасних цифрових інструментів кібербезпеки дозволяє підвищити стійкість комерційних та некомерційних організацій до кіберзагроз, забезпечити захист інформаційних ресурсів і запобігати потенційним атакам [26].

З огляду на вище наведене, аналіз моделей управління кібербезпекою є концептуальною основою для розуміння того, як різні суб'єкти структурують та впроваджують політику кібербезпеки в системі міжнародних економічних відносин (табл. 2).

На організаційному рівні управління кібербезпекою концептуалізують як структуру, що забезпечує узгодженість цілей безпеки з ширшими стратегічними та оперативними цілями. Така модель визначає 5 основних компонентів ефективного національного управління: стратегію кібербезпеки, стандартизовані процеси, дотримання нормативних вимог, нагляд з боку вищого керівництва та розподіл ресурсів [27]. У контексті міжнародних економічних відносин такі організаційні можливості є критично важливими, оскільки ТНК та глобальні ланцюги вартості все більше залежать від гармонізованих практик кібербезпеки для підтримування стійкості та довіри в транскордонних операціях.

---

[25] Михальченко Г. Г., Снітко Ю. М., Іваненко В. О. Кібербезпека в економіці: захист від кіберзагроз у диджиталізованому світі. *Наукові записки Львівського університету бізнесу та права*. 2023. № 38. С. 377–384. DOI: https://doi.org/10.5281/zenodo.10012434

[26] Правдивець О. М. Сучасні цифрові інструменти кібербезпеки в системі економічної безпеки підприємств України. *Регіональна економіка*. 2025. № 1(115). С. 109–118. DOI: https://doi.org/10.36818/1562-0905-2025-1-10

[27] Yusif S., Hafeez-Baig A. A Conceptual Model for Cybersecurity Governance. *Journal of Applied Security Research*. 2021. Vol. 16, no. 4. P. 490–513. DOI: https://doi.org/10.1080/19361610.2021.1918995

Таблиця 2

Моделі управління кібербезпекою в міжнародних економічних відносинах

Модель	Сутність	Приклади
Державно-центрична (суверенна)	управління кібербезпекою здійснюється переважно урядом, з сильним акцентом на суверенітеті, контролі над ІКТ-інфраструктурою та захисті національних економічних інтересів	КНР, рф, Іран, КНДР, Туреччина та ін.
За участю багатьох зацікавлених сторін	децентралізоване управління кібербезпекою здійснюється спільно між урядами, суб'єктами приватного сектору, громадським суспільством та міжнародними організаціями	Інтернет-корпорація з присвоєння імен та номерів (ICANN), Форум з управління Інтернетом (IGF), Консорціум Всесвітньої павутини (W3C), Глобальний форум з кіберекспертизи (GFCE) і т.д.
Державно-приватного партнерства	управління кібербезпекою, за якого уряди та суб'єкти приватного сектору спільно розробляють та впроваджують політику та практики кібербезпеки	ініціативи Агентства ЄС з кібербезпеки (ENISA), Альянс кіберзагроз (CTA), Центр обміну та аналізу інформації про фінансові послуги (FS-ISAC) і т.д.
Міжнародна інституційна	ґрунтується на формальній співпраці між державами через міжнародні організації, угоди та нормативно-правової бази	обговорення кібернорм ООН (OEWG), директиви ЄС, співпраця в кібербезпеці НАТО, ОЕСР, МСЕ тощо
Глобальна конституційна (нормативна)	управління кібербезпекою є частиною глобального правового інституційного порядку, що формується на спільних принципах і правилах	норми ООН щодо відповідальної поведінки держав у кіберпросторі, Будапештська конвенція Ради Європи про кіберзлочинність, декларації щодо кібербезпеки G7 тощо

Джерело: складено авторами

Потреба в більш адаптивних моделях управління додатково підкреслюється в наукових дослідженнях. Прикладом є динамічна та адаптивна структура управління кібербезпекою, яка поєднує такі елементи, як державно-приватні партнерства, механізми міжнародної співпраці, R&D, а також підходи до управління на основі ризиків [28]. Важливо, що запропонована модель виходить за межі організацій і чітко враховує регіональні та глобальні виміри управління кібербезпекою.

З точки зору глобального управління, кібербезпеку інтерпретують крізь призму конституціоналізму та колективного нормотворення, тобто вона є динамічною системою та заснована на спільній відповідальності, стійкості та механізмах участі [29]. Такий підхід спирається на принципи управління Інтернетом та пропонує гібридну модель, що поєднує залучення багатьох зацікавлених сторін, встановлення стандартів та правове регулювання.

Ключовим інструментом управління кібербезпекою на національному та міжнародному рівнях є розробка національних стратегій кібербезпеки, які ґрунтуються на чітко визначених пріоритетах, механізмах залучення зацікавлених сторін та узгодженні з міжнародними рамками співпраці [30]. Зазначимо, ці стратегії слугують не лише інструментами внутрішньої політики, але й інструментами міжнародного позиціонування, дозволяючи державам брати участь в альянсах, встановлювати стандарти та впливати на глобальні програми кібербезпеки.

Дослідження також показують як спільні цілі, так і приховані тематичні розбіжності в стратегіях країн G20, розкриваючи складність узгодження національних пріоритетів у глобальних масштабах [31]. Зокрема, найбільш широко визнані цілі (прийняті на рівні 10-17 країн G20) враховують захист критично важливих інфраструктур, мереж та даних; встановлення національної координації та екосистем; участь у

[28] Melaku H. M. A Dynamic and Adaptive Cybersecurity Governance Framework. *Journal of Cybersecurity and Privacy*. 2023. Vol. 3, no. 3. P. 327–350. DOI: https://doi.org/10.3390/jcp3030017

[29] PernicE I. Global cybersecurity governance: A constitutionalist analysis. *Global Constitutionalism*. 2018. Vol. 7, no. 1. P. 112–141. DOI: https://doi.org/10.1017/s2045381718000023

[30] Sabillon R., Cavaller V., Cano J. National Cyber Security Strategies: Global Trends in Cyberspace. International *Journal of Computer Science and Software Engineering*. 2016. Vol. 5, no. 5. P. 67–81. URL: https://www.proquest.com/openview/d678b09e570d574b39f77cf26bb2e9d4/1?pq-origsite=gscholar&cbl=2044552

[31] Çifci H., Ergüner E. Analysis of National Cybersecurity Strategies of G20: objectives, latent themes, latest trends and comparisons. *Data & Policy*. 2025. Vol. 7. DOI: https://doi.org/10.1017/dap.2024.99

міжнародному співробітництві; підтримку індустрії кібербезпеки, R&D та інновацій; а також покращення можливостей кібербезпеки [32]. До помірно та вибірково прийнятих цілей (на рівні 3-8 країн G20) належать: підвищення обізнаності та сприяння культурі кібербезпеки; створення можливостей реагування на інциденти; боротьба з кіберзлочинністю; створення законодавчої та регуляторної бази; надання безпечних продуктів і послуг; повага до прав особистості та фундаментальних цінностей; безпека технологій нового покоління та заохочення використання міжнародних стандартів [33].

Підсумовуючи, управління кібербезпекою перетворилося на критично важливий компонент міжнародних економічних відносин, оскільки діє на кількох рівнях – організаційному, національному та глобальному – і залучає різноманітних учасників та механізми.

ВИСНОВКИ

Наголосимо, в умовах міжнародної економічної інтеграції кібербезпека набуває транснаціонального та системного характеру, оскільки кіберзагрози поширюються за межі національних кордонів, впливають на глобальні ланцюги вартості, фінансові системи та цифрові платформи, а також створюють каскадні економічні ефекти. Кіберзагрози дедалі більше формуються під впливом геополітичних та військових факторів. Кібероперації, що спонсоруються державами, кібершпигунство та атаки на критичну інфраструктуру стали невід'ємними елементами гібридної війни, безпосередньо впливаючи на економічні системи та світові ринки. Як наслідок, кібербезпеку слід розглядати не лише як технічну чи організаційну функцію, а й як стратегічний інструмент економічної безпеки та міжнародної конкурентоспроможності.

Ефективність функціонування кібербезпеки на національному рівні передбачає впровадження комплексної системи принципів, які забезпечують узгодженість між зацікавленими сторонами, адаптивність до нових загроз та баланс між вимогами безпеки та цілями економічного розвитку. Крім того, критично важливими є механізм міжнародної співпраці (а саме угод про обмін інформацією та розвиток потенціалу),

[32] Çifci H., Ergüner E. Analysis of National Cybersecurity Strategies of G20: objectives, latent themes, latest trends and comparisons. *Data & Policy*. 2025. Vol. 7. DOI: https://doi.org/10.1017/dap.2024.99

[33] Çifci H., Ergüner E. Analysis of National Cybersecurity Strategies of G20: objectives, latent themes, latest trends and comparisons. *Data & Policy*. 2025. Vol. 7. DOI: https://doi.org/10.1017/dap.2024.99

яка відіграє вагому роль у боротьбі з транснаціональними кіберзагрозами. Водночас, фрагментація глобального регуляторного середовища та асиметрія можливостей в реалізації заходів кібербезпеки між країнами залишають значними проблемами.

Незважаючи на проведене дослідження та всебічну наукову та професійну літературу з цієї теми, низка важливих питань потребуватиме подальшої наукової дискусії, а саме: удосконалення міжнародних механізмів управління кібербезпекою (включаючи вивчення перспектив гармонізації правових баз та зміцнення ролі міжнародних угод), цифровий суверенітет та технологічна залежність держав, а також зменшення асиметрії в можливостях кібербезпеки між державами.

АНОТАЦІЯ

Проведене дослідження розглядає роль кібербезпеки у підтримуванні стійкості та сталого розвитку національної економіки в умовах глобальної цифровізації та постійних військових трансформацій. Обґрунтовано, що кібербезпека трансформувалася з технічної функції на стратегічний компонент економічної безпеки держави, безпосередньо впливаючи на стабільність критичної інфраструктури, функціонування ключових секторів та конкурентоспроможність національних економік у глобальному цифровому середовищі.

У дослідженні кібербезпеку концептуалізовано в системі економічної безпеки держави через три основні підходи: як самостійний компонент, як структурний компонент інформаційної безпеки та як міжгалузевий компонент, що забезпечує функціонування всіх складових національної економіки. На основі цих підходів визначено відповідні моделі управління (галузеву, ієрархічну та мережеву). Систематизовано ключові принципи кібербезпеки національної економіки (згруповані в категорії стратегічних, правових, управління ризиками, стійкості та розвитку потенціалу, економічних), які разом утворюють комплексну основу для управління кібербезпекою.

Окрему увагу було приділено секторальному розподілу кіберризиків, зосереджуючись на галузях, які є найбільш вразливими через їхню операційну критичність та інтеграцію в глобальні ланцюги вартості. Додатково, узагальнено та систематизовано моделі управління кібербезпекою в міжнародних економічних відносинах, що допомогло продемонструвати гібридизацію та багаторівневу координацію управління кібербезпекою за участю держав, суб’єктів приватного сектору та міжнародних інституцій. Водночас, наголошено, що

відсутність єдиної системи глобального управління та фрагментація національних стратегій створюють значні ризики для ефективної міжнародної співпраці в сфері кібербезпеки.

Література

1. Вдовічен А., Королюк Ю., Вдовічен Д. Цифрові технології та кібербезпека в стратегії відновлення післявоєнної економіки України. *Вісник Чернівецького торговельно-економічного інституту*. 2025. Т. II, № 98. С. 8–29. DOI: https://doi.org/10.34025/2310-8185-2025-2.98.01
2. Zavhorodnya E., Melnyk T. Ukraine's digital frontier: a deep dive into ICT sector competitiveness. *Traditional and innovative approaches in economics: theory, methodology, practice : Collective monograph*. Riga, Latvia. P. 137–170. 2024. DOI: https://doi.org/10.30525/978-9934-26-407-8-7
3. Оксінь В. Ю., Левченко Д. С., Костенко І. В. Кібербезпека держави як інструмент сталого розвитку цифрового середовища. *Аналітично-порівняльне правознавство*. 2025. Т. 2, № 6. С. 411–415. DOI: https://doi.org/10.24144/2788-6018.2025.06.2.67
4. Койбічук В. В. Роль кібербезпеки в системі економічної безпеки: бібліометричний аналіз. *Інноваційна економіка*. 2024. № 2. С. 150–158. DOI: https://doi.org/10.37332/2309-1533.2024.2.19
5. Зуб В. В. Сутнісна характеристика економічної безпеки держави. *Аналітично-порівняльне правознавство*. 2024. № 2. С. 457–462. DOI: https://doi.org/10.24144/2788-6018.2024.02.77
6. Франчук В. І., Корчинський І. О. Економічна безпека держави: історичні аспекти та характеристика сутності. *Ефективна економіка*. 2019. № 8. DOI: https://doi.org/10.32702/2307-2105-2019.8.7
7. Кіндзерський Ю. В. Кібербезпека та становлення цифрової економіки: проблеми взаємозв'язку. *Економічний вісник Дніпровської політехніки*. 2020. № 71. С. 18–26. DOI: https://doi.org/10.33271/ebdut/71.018
8. Мирончeнко Д. В. Етичні аспекти кібербезпеки у світовій економіці та міжнародних відносинах. *Вчені записки*. 2025. Т. 40(3). С. 133–140. DOI: https://doi.org/10.33111/vz_kneu.40.25.03.12.081.087
9. Білявська Ю., Шестак Я. Кібербезпека та кібергігієна: нова ера цифрових технологій. *Товарознавство. Технології. Інжиніринг*. 2022. Т. 43, № 3. С. 47–59. DOI: https://doi.org/10.31617/2.2022(43)04
10. Горбаченко С. Кібербезпека як складова економічної безпеки України. *Галицький економічний вісник*. 2020. Т. 66, № 5. С. 180–186. DOI: https://doi.org/10.33108/galicianvisnyk_tntu2020.05.180

11. Заяць Д. Ф., Кицюк І. В. Роль кібербезпеки в міжнародних економічних відносинах. *Науковий вісник Ужгородського національного університету*. 2024. № 53. С. 14–19. DOI: https://doi.org/10.32782/2413-9971/2024-53-2

12. Global Cybersecurity Index 2024. URL: https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf

13. Global Cybersecurity Report 2025. URL: https://cyble.com/wp-content/uploads/2025/12/Global-Cybersecurity-Report-2025.pdf

14. Global Cybersecurity Outlook 2026. URL: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf

15. Михальченко Г. Г., Снітко Ю. М., Іваненко В. О. Кібербезпека в економіці: захист від кіберзагроз у диджиталізованому світі. *Наукові записки Львівського університету бізнесу та права*. 2023. № 38. С. 377–384. DOI: https://doi.org/10.5281/zenodo.10012434

16. Правдивець О. М. Сучасні цифрові інструменти кібербезпеки в системі економічної безпеки підприємств України. *Регіональна економіка*. 2025. № 1(115). С. 109–118. DOI: https://doi.org/10.36818/1562-0905-2025-1-10

17. Yusif S., Hafeez-Baig A. A Conceptual Model for Cybersecurity Governance. *Journal of Applied Security Research*. 2021. Vol. 16, no. 4. P. 490–513. DOI: https://doi.org/10.1080/19361610.2021.1918995

18. Savaş S., Karataş S. Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *International Cybersecurity Law Review*. 2022. DOI: https://doi.org/10.1365/s43439-021-00045-4

19. Melaku H. M. A Dynamic and Adaptive Cybersecurity Governance Framework. *Journal of Cybersecurity and Privacy*. 2023. Vol. 3, no. 3. P. 327–350. DOI: https://doi.org/10.3390/jcp3030017

20. PernicE I. Global cybersecurity governance: A constitutionalist analysis. *Global Constitutionalism*. 2018. Vol. 7, no. 1. P. 112–141. DOI: https://doi.org/10.1017/s2045381718000023

21. Sabillon R., Cavaller V., Cano J. National Cyber Security Strategies: Global Trends in Cyberspace. *International Journal of Computer Science and Software Engineering*. 2016. Vol. 5, no. 5. P. 67–81. URL: https://www.proquest.com/openview/d678b09e570d574b39f77cf26bb2e9d4/1?pq-origsite=gscholar&cbl=2044552

22. Çifci H., Ergüner E. Analysis of National Cybersecurity Strategies of G20: objectives, latent themes, latest trends and comparisons. *Data & Policy*. 2025. Vol. 7. DOI: https://doi.org/10.1017/dap.2024.99

Information about the authors:
Elizaveta Zavhorodnya
PhD in International Economic Relations,
Head of the Library Department,
State University of Trade and Economics
19 Kyoto Str., Kyiv, 02156, Ukraine
Yaroslav Shestak
PhD in Computer Sciences, Senior Lecturer,
Department of Software Engineering and Cybersecurity,
State University of Trade and Economics
19 Kyoto Str., Kyiv, 02156, Ukraine