8.3. Управління економічною безпекою в умовах цифрової економіки

Повод Т.М.,
кандидат економічних наук, доцент,
доцент кафедри підприємництва, обліку та фінансів,
Жосан Г.В.,
кандидат економічних наук, доцент,
завідувач кафедри менеджменту, маркетингу та IT,
Херсонський державний аграрно-економічний університет

Ключові слова: цифрова економіка, фінансова безпека, управління, економічна безпека, цифрові фінанси, поведінкові фінанси, банківська система, технологія Blockchain, цифровий розвиток.

Питання забезпечення економічної безпеки в умовах стрімкого розвитку цифрової економіки набуває особливої актуальності та багатовимірності, оскільки трансформаційні процеси, пов'язані з диджиталізацією, супроводжуються появою якісно нових загроз, ризиків і вразливостей, які виходять далеко за межі традиційних економічних і фінансових загроз. Сучасний етап еволюції економічних систем характеризується посиленням впливу сукупних технологічних, інформаційних, когнітивних та соціальних факторів, що зумовлює необхідність перегляду підходів до управління економічною безпекою та її системного забезпечення.

Технічний, технологічний та цифровий розвиток створює передумови для інтенсифікації економічних процесів, пришвидшення інформаційних потоків, глобалізації фінансових ринків та формування нових бізнес-моделей. Водночас, ці процеси генерують нові загрози: кіберзлочинність, інформаційні маніпуляції, втручання у критичну інфраструктуру, несанкціоноване використання великих даних, руйнування традиційних ланцюгів доданої вартості та появу цифрових монополій. Відтак, забезпечення економічної безпеки вимагає не лише адаптації існуючих моделей ризик-менеджменту та інституційного регулювання, але й вироблення нових концептуальних підходів до оцінки цифрових ризиків та створення гнучких механізмів їх мінімізації.

Розвиток цифрової економіки зумовлює необхідність формування якісно нової парадигми управління економічною безпекою, яка базується на синергетичному поєднанні технологічних, організаційних, правових та когнітивних інструментів. До ключових аспектів забезпечення економічної безпеки у цифровій економіці доцільно віднести:

Цифрову гігієну — комплекс заходів із забезпечення інформаційної безпеки, включаючи захист від кіберзагроз, управління інформаційними

потоками, забезпечення цілісності, конфіденційності та доступності даних, а також формування критичного ставлення до джерел інформації та їхньої достовірності.

Когнітивне цілепокладання — усвідомлення суспільством, бізнесом та державою стратегічних пріоритетів, меж і напрямів цифрової трансформації, зокрема оцінка її потенційного впливу на соціально-економічну стабільність, конкурентоспроможність національної економіки та стійкість інституцій.

Інституційні трансформації — адаптація правових, регуляторних та управлінських механізмів до умов цифрової економіки, включаючи створення цифрових інституцій, модернізацію системи моніторингу економічних загроз у кіберпросторі та підвищення ефективності державної політики у сфері економічної безпеки.

Сучасні технології, зокрема Blockchain, штучний інтелект та великі дані, відіграють подвійне значення у контексті забезпечення економічної безпеки: з одного боку, вони створюють нові інструменти моніторингу, прогнозування та мінімізації загроз, а з іншого — генерують додаткові ризики, пов'язані з кібератаками, маніпуляціями даними, технологічною залежністю та розмиванням національного економічного суверенітету. Відповідно, ефективність управління економічною безпекою в умовах цифрової економіки значною мірою залежатиме від здатності поєднати потенціал новітніх технологій із системною політикою ризик-менеджменту та стратегічного планування у сфері безпеки. Саме інтеграція технологічних можливостей із продуманими регуляторними та управлінськими механізмами стане визначальним фактором стійкості цифрової економіки у довгостроковій перспективі.

Формування дієвої системи управління економічною безпекою потребує чіткого визначення її цілей, завдань, інструментів та ресурсного забезпечення. Водночас, вихідною передумовою побудови такої системи є уточнення понятійно-категоріального апарату, зокрема дефініції «безпека», та виокремлення ключових засадничих основ, які формують її сутність у контексті цифрової економіки.

Згідно з Державним стандартом України ДСТУ 2293-99, безпека визначається як стан захищеності особи та суспільства від ризиків, що можуть завдати шкоди їх життєво важливим інтересам. Конституція України закріплює, що людина, її життя та здоров'я, честь і гідність, недоторканність та безпека визнаються найвищою соціальною цінністю держави (ст. 3) [1,2]. Ці положення створюють загальнонаціональну основу для формування системи безпеки, яка має враховувати як традиційні, так і цифрові загрози, що виникають у сучасних умовах технологічної трансформації.

Окрему увагу слід приділити конституційним засадам економічної безпеки, адже відповідно до статті 17 Конституції України забезпечення економічної та інформаційної безпеки є однією з найважливіших функцій держави поряд із захистом суверенітету та територіальної цілісності. При цьому, стаття 16 підкреслює обов'язок держави забезпечувати екологічну безпеку, що також має враховуватися при розробленні комплексних стратегій управління національною безпекою в умовах цифрової економіки [1,2].

Закон України «Про національну безпеку України» (2018 р.) розкриває поняття «безпека» у контексті захисту ключових національних інтересів у різних сферах, зокрема:

- воєнна безпека — захищеність державного суверенітету, територіальної цілісності та демократичного конституційного ладу від воєнних загроз (ч. 2 ст. 1);
- громадська безпека та порядок — захищеність життєво важливих для суспільства та особи інтересів, прав і свобод людини і громадянина, що забезпечується шляхом узгодженої діяльності державних органів, місцевого самоврядування, сил безпеки та громадськості щодо реалізації та захисту національних інтересів (ч. 3 ст. 1);
- державна безпека — захищеність суверенітету, територіальної цілісності та демократичного конституційного ладу від реальних і потенційних загроз невоєнного характеру (ч. 4 ст. 1);
- національна безпека України — захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших життєво важливих національних інтересів від реальних та потенційних загроз (ч. 9 ст. 1) [2,3].

В умовах цифрової економіки ці підходи потребують суттєвого розширення та доповнення, зокрема включення до системи економічної безпеки таких компонентів, як:

- цифрова безпека — захищеність економічних суб'єктів та національних економічних інтересів від кіберзагроз, цифрового шпигунства, незаконного збору та використання даних;
- технологічна безпека — спроможність національної економіки забезпечувати стійкість критичних цифрових інфраструктур, зберігати технологічний суверенітет та мінімізувати залежність від іноземних технологічних платформ;
- інформаційна безпека — захищеність інформаційних ресурсів, інформаційно-аналітичних систем та інформаційного простору держави від маніпуляцій, деструктивних впливів та інформаційних диверсій.

Згідно із Законом України «Про національну безпеку України», до сил безпеки належать правоохоронні та розвідувальні органи, державні органи спеціального призначення з правоохоронними функціями, сили цивільного захисту, а також інші державні інституції, на які Конституцією та законами України покладено функції із забезпечення національної безпеки України (ч. 17 ст. 1). У контексті цифрової економіки коло суб'єктів забезпечення економічної безпеки суттєво розширюється за рахунок інституцій, відповідальних за захист інформаційного простору, кібербезпеки та критичної цифрової інфраструктури. Це створює передумови для формування багаторівневої системи управління економічною безпекою, де традиційні силові органи мають взаємодіяти з регуляторами цифрових ринків, секторальними аналітичними центрами та приватними операторами цифрових платформ.

У глобальному вимірі забезпечення економічної безпеки тісно пов'язане з міжнародним співробітництвом та імплементацією універсальних стандартів безпеки у цифровій сфері. Відповідно до Статуту ООН, одним із головних завдань міжнародної організації є об'єднання зусиль країн для підтримання миру та безпеки, зокрема шляхом реагування на сучасні транснаціональні загрози, включаючи кіберзлочинність та економічний саботаж у цифровому середовищі. Держави-учасниці ОБСЄ, у межах виконання положень Заключного акта від 01.08.1975 р., взяли на себе зобов'язання утримуватися від дій, які можуть загострювати безпекові ситуації та створювати нові загрози економічній стабільності та розвитку цифрової інфраструктури.

У вітчизняному правовому полі поняття «безпека» охоплює як захист особи та суспільства від небезпек та ризиків, так і забезпечення державного суверенітету та захист національних інтересів від загроз різного характеру, включаючи економічні й цифрові [2]. Це формує методологічну основу для розбудови національної системи економічної безпеки в умовах цифрової трансформації, де ключову роль відіграють ідентифікація, прогнозування та нейтралізація цифрових ризиків.

Аналіз наукових та методичних джерел свідчить про наявність різноманітних підходів до трактування сутності безпеки, серед яких: безпека як стан діяльності, за якого з певною ймовірністю виключається реалізація потенційних загроз; безпека як відсутність неприпустимого рівня ризику, пов'язаного із завданням шкоди критично важливим інтересам держави, суспільства, бізнесу чи окремих осіб; безпека як такий стан складної соціально-економічної системи, за якого дія зовнішніх та внутрішніх факторів не призводить до її деградації, руйнування або втрати здатності до сталого функціонування та розвитку.

В умовах цифрової економіки такі підходи потребують суттєвого доповнення, зокрема врахування технологічних факторів та особливостей функціонування цифрових платформ, кіберфізичних систем і глобальних інформаційних потоків. При цьому, управління економічною безпекою має враховувати не лише обмеження та мінімізацію ризиків, а й створення умов для використання цифрових можливостей, що виникають унаслідок технологічних інновацій. Саме баланс між управлінням ризиками та реалізацією можливостей цифрової економіки є стратегічним орієнтиром сучасної системи економічної безпеки.

Варто наголосити, що в системі ризик-менеджменту абсолютна ліквідація небезпек чи повне усунення ризиків є не лише неможливою, а й небажаною, оскільки це водночас блокує можливості для розвитку, інновацій та отримання конкурентних переваг. Відтак, управління економічною безпекою в умовах цифрової економіки має ґрунтуватися на концепції керованої ризикованості (managed risk), що дозволяє знаходити оптимальний баланс між безпекою та розвитком, створюючи умови для стійкого функціонування національної економіки у глобальному цифровому середовищі.

При формуванні сучасної системи управління економічною безпекою в умовах цифрової економіки виникає необхідність чіткого визначення допустимих рівнів ризику (або небезпеки у вужчому сенсі) — як з точки зору їхньої прогнозованості та керованості, так і з урахуванням потенційних наслідків їх реалізації. Особливу увагу слід приділити ефектам кумуляції та мультиплікації ризиків, коли поєднання окремих загроз у цифровій сфері, економіці та соціальному середовищі створює синергетичний ефект, що посилює загальний рівень небезпеки.

У контексті цифрової економіки доцільно визначити економічну безпеку як такий стан економічної системи (її суб'єктів, процесів та інституцій), за якого з певною ймовірністю виключається ризик неконтрольованих, руйнівних наслідків, здатних порушити стабільність функціонування та розвитку економіки в умовах цифрової трансформації. Це визначення тісно пов'язане з категорією «ризикового апетиту», тобто рівня ризику, який держава, бізнес чи інші суб'єкти економічної діяльності готові прийняти з урахуванням стратегічних цілей, пріоритетів розвитку та оцінки потенційних вигід від використання нових цифрових технологій.

Формування системи управління економічною безпекою передбачає балансування на кривій «ризик – дохідність», що є особливо актуальним для цифрової економіки, де висока технологічна динаміка створює одночасно і значні можливості, і нові загрози. Чим вищий рівень прийнятих ризиків, тим нижчим

може бути рівень ліквідності та стійкості системи в кризових умовах. Таким чином, кожен суб'єкт – від держави до окремого підприємства – визначає прийнятне співвідношення ризиків і можливостей, враховуючи особливості власної економічної політики, стратегічні пріоритети та рівень цифрової зрілості.

З урахуванням зазначеного, економічна безпека в умовах цифрової економіки — це керований ризик, який передбачає не лише встановлення та контроль допустимих рівнів загроз, а й вибір оптимальних інструментів управління ризиками з урахуванням специфіки цифрових активів, процесів та технологічних платформ. При цьому особливої ваги набуває здатність до гнучкого адаптивного управління, побудованого на принципах моніторингу, прогнозування та оперативного реагування на нові загрози, що виникають у цифровому середовищі.

Основні інструменти управління ризиками включають:

- уникнення ризику;
- передачу ризику;
- попередження ризику;
- придушення ризику;
- усунення ризику (збитків);
- фінансування ризику.

Кожен з цих інструментів застосовується у поєднанні з іншими залежно від об'єкта ризику, ступеня його значущості та характеру цифрових загроз.

Таблиця 1

Види безпеки та їхній зв'язок із економічною безпекою в умовах цифрової економіки

Вид безпеки	Зміст та основні загрози	Зв'язок з економічною безпекою в цифровій економіці
Фізична безпека	Захист об'єктів критичної інфраструктури від фізичних атак і диверсій	Порушення фізичного доступу до центрів обробки даних або серверних потужностей
Інформаційна безпека	Захист даних та інформаційних систем від несанкціонованого доступу	Викрадення комерційної та фінансової інформації, порушення конфіденційності бізнес-процесів
Соціальна безпека	Захист соціальних прав та стабільності суспільства	Цифрова нерівність, зростання безробіття внаслідок автоматизації та цифровізації
Екологічна безпека	Мінімізація негативних екологічних наслідків цифрових технологій	Вплив виробництва та утилізації цифрового обладнання на довкілля
Військова безпека	Захист держави від кібервоєн, атак на стратегічні об'єкти	Кібератаки на фінансову систему, енергетичні та промислові об'єкти

Політична безпека	Захист політичної системи від зовнішніх цифрових впливів	Втручання у вибори, інформаційні кампанії з дестабілізації економічної ситуації
Цифрова безпека	Захист цифрових платформ, даних та систем управління	Атаки на платіжні системи, електронні реєстри, торгові платформи
Продовольча безпека	Захист аграрного сектору від цифрових загроз	Порушення ланцюгів постачання продовольства через кібератаки
Когнітивна безпека	Захист суспільної свідомості від маніпулятивного впливу	Дезінформаційні кампанії щодо економічних процесів і державної політики

Економічна безпека в цифровій економіці є інтегральним поняттям, яке включає сукупність заходів із захисту економічних інтересів держави, бізнесу та суспільства в умовах функціонування цифрового середовища. Її забезпечення потребує комплексного підходу, що об'єднує економічні, інформаційні, соціальні та технологічні аспекти та враховує високу динаміку змін у цифровій економіці.

У контексті управління економічною безпекою в умовах цифрової економіки особливої актуальності набуває проблема вибору стратегічних пріоритетів у сфері безпеки, адже цифрова трансформація загострює існуючі суперечності між окремими видами безпеки, зокрема економічною, екологічною, соціальною, інформаційною, когнітивною тощо. Зокрема, прискорена цифровізація економічних процесів може сприяти зростанню економічної ефективності, але водночас породжувати екологічні ризики через інтенсивне використання ресурсів для створення та підтримки цифрової інфраструктури. Аналогічно, впровадження автоматизованих систем управління та цифрових платформ може посилювати соціальну нерівність або створювати передумови для маніпуляцій суспільною свідомістю, підриваючи когнітивну безпеку суспільства.

Враховуючи це, ефективне управління економічною безпекою в цифровій економіці потребує вироблення механізмів подолання антагоністичних суперечностей між різними видами безпеки та ухвалення управлінських рішень на основі аналізу альтернативних витрат (opportunity cost), що дозволяє оцінити цінність нереалізованих сценаріїв у процесі забезпечення одного пріоритету за рахунок іншого.

Економічна безпека в умовах цифрової економіки має набувати характеру інтеграційної категорії, що поєднує інтереси всіх суб'єктів та координує баланс між економічними вигодами та безпековими обмеженнями. Водночас, одним із ключових викликів є обмежена раціональність суб'єктів прийняття рішень, особливо в умовах інформаційних асиметрій, низької цифрової грамотності та

високої швидкості технологічних змін. Це створює своєрідну суперечність між індивідуальними та колективними (суспільними) інтересами у сфері безпеки, коли окремі цифрові ініціативи чи бізнес-моделі, вигідні для окремих суб'єктів, можуть підривати довгострокову стійкість національної економіки чи інформаційного простору.

Рівень забезпечення економічної безпеки в цифровій економіці безпосередньо залежить від стану та якості інституційного середовища. Формальні інститути, такі як законодавча база щодо цифрової економіки, інформаційної та кібербезпеки, а також неформальні правила та практики поведінки у цифровому середовищі, визначають ефективність запровадження стратегій економічної безпеки. Зокрема, високий рівень неформальної інклюзивності цифрового середовища, тобто залучення широких верств суспільства до процесів ухвалення рішень щодо цифрових ризиків, створює передумови для підвищення стійкості економічної системи. Натомість екстрактивні інститути, які концентрують контроль над критичними цифровими активами в руках обмеженого кола суб'єктів, підвищують системні ризики та знижують адаптивність до нових цифрових загроз.

Інституційні трансформації можуть як бути наслідком об'єктивних економічних та технологічних змін, так і самі виступати каталізаторами подальших перетворень в економічній системі. Цей взаємозв'язок набуває особливої ваги в умовах цифрової економіки, де інститути не просто фіксують правила гри, а активно впливають на траєкторії цифрової трансформації, визначаючи прозорість цифрових ринків, рівень кіберзахисту, правила збору та обробки даних, а також механізми залучення громадян до контролю за цифровими платформами.

Фундаментальна дискусія щодо первинності економічних або інституційних факторів у забезпеченні економічної безпеки набуває нового звучання у цифрову епоху. Представники політико-економічної школи традиційно наголошують на домінуючій ролі географічних, ресурсних, військово-історичних та інших об'єктивних чинників у формуванні національної системи безпеки, а інститути розглядають як похідні від економічного базису, які закріплюють та легітимізують існуючі економічні відносини у формі правових норм, адміністративних процедур та соціальних практик.

Натомість представники інституціоналізму, зокрема прихильники неоінституціональної теорії, акцентують увагу на самостійному значенні інститутів як ключових чинників, що визначають ефективність використання економічного потенціалу та рівень економічної безпеки в умовах цифрової економіки. Вони звертають увагу на випадки, коли за схожих стартових

економічних передумов саме завдяки різним інституційним практикам формувалися суттєво відмінні моделі економічного розвитку та забезпечення безпеки. Показовими прикладами є Південна та Північна Корея, Західна та Східна Німеччина, різні траєкторії цифрової трансформації в країнах Північної та Південної Америки, що підтверджує критичну роль інституційних конфігурацій у забезпеченні економічної безпеки.

Цифровізація економіки, з одного боку, значно ускладнює економічні відносини, розширює спектр суб'єктів та об'єктів ризику, а з іншого — створює передумови для принципово нових моделей економічної діяльності, заснованих на цифрових платформах, великих даних, блокчейні та штучному інтелекті. Водночас стрімкий розвиток цифрових технологій об'єктивно провокує необхідність масштабних інституційних змін — від оновлення законодавства у сфері цифрової економіки та інформаційної безпеки до створення нових механізмів міжнародного співробітництва у сфері цифрових загроз та забезпечення економічної безпеки у глобальному кіберпросторі.

Управління економічною безпекою в умовах цифрової економіки передбачає не лише адаптацію існуючих інститутів до нових технологічних викликів, але й формування нової інституційної архітектури, яка буде здатна забезпечити баланс між інноваційним розвитком, цифровими правами, інформаційною та економічною безпекою як на національному, так і на міжнародному рівнях.

Аналізуючи процеси цифровізації та формування цифрової економіки, доцільно розглядати питання забезпечення економічної безпеки в двох взаємопов'язаних, але функціонально відмінних площинах:

- Цифровізація класичних економічних процесів та управлінських комунікацій, яка передбачає переважно технологічну модернізацію існуючих бізнес-моделей та управлінських систем за рахунок переходу до цифрових каналів передачі, обробки та зберігання інформації (персональної, виробничої, фінансової тощо). В такій площині цифровізація створює нові ризики інформаційної безпеки, включаючи загрози конфіденційності, цілісності та доступності даних, що вимагає додаткових інструментів забезпечення економічної безпеки.

- Власне цифрова економіка, яка формується як нова модель господарювання, заснована на створенні та обігу цифрових товарів і послуг у межах електронного бізнесу та електронної комерції. Цифрова економіка відрізняється принципово новими джерелами формування доданої вартості, які пов'язані з генерацією та комерціалізацією цифрових економічних благ. Це визначає необхідність розроблення нових концепцій забезпечення економічної

безпеки, адаптованих до специфіки цифрових активів, платформних бізнес-моделей та глобальних інформаційних потоків.

Головною характеристикою цифрової економіки виступає створення доданої вартості через розробку та масштабування цифрових економічних благ, серед яких цифрові продукти, послуги, програмні рішення та цифрові платформи, що інтегрують учасників ринку та формують нові ланцюги створення цінності.

Функціонування цифрової економіки базується на широкому впровадженні електронно-цифрових інновацій, зокрема:

- технологій цифровізації діяльності (автоматизації бізнес-процесів, цифрового документообігу тощо);
- комплексних цифрових технологій (великих даних, хмарних обчислень, штучного інтелекту);
- інформаційно-комунікаційних технологій;
- технологій віртуальної та доповненої реальності;
- P2P-мереж та Blockchain-рішень, що забезпечують прозорість і довіру в децентралізованих системах.

В умовах цифрової трансформації одним із ключових факторів впливу на економічну безпеку стають фінансові технології (FinTech), які забезпечують розвиток нових платіжних систем, інструментів мобільного банкінгу, цифрових валют та інших рішень, що одночасно створюють можливості для зростання фінансової інклюзивності та формують нові вразливості фінансової системи до кібератак, шахрайства та втручання з боку недружніх суб'єктів.

Цифровізація економічних процесів ґрунтується на широкому застосуванні новітніх технологічних рішень, які, у свою чергу, детермінують трансформацію інституційного середовища. Спочатку цифрові інновації модифікують неформальні інститути, зокрема правила ділової етики, принципи конкурентної боротьби, моделі формування ділової репутації в цифровому середовищі. Згодом ці зміни закріплюються на рівні формальних інститутів, включаючи оновлення законодавства, створення спеціальних регуляторних режимів для цифрових компаній, формування національних стратегій цифрової трансформації та забезпечення кібербезпеки.

Характерною ознакою цифрової економіки є поява нових інститутів цифрового ринку, які забезпечують взаємодію між суб'єктами господарювання у нових умовах. Прикладами таких інституційних змін є:

- перехід до цифрових платформ як основи функціонування секторів економіки;
- впровадження ICO та інших механізмів цифрового залучення капіталу;

- створення нових цифрових механізмів регулювання (регуляторні «пісочниці», спеціальні цифрові режими для стартапів).

Формування цифрової економіки відбувається в контексті становлення економіки нового технологічного укладу, який, з одного боку, базується на широкому використанні цифрових технологій, а з іншого — формує нову модель соціально-економічних відносин, засновану на двох ключових концептах:

- Економіка талантів, у якій ключовим ресурсом є креативний людський капітал, здатний до генерування інноваційних цифрових рішень та створення високотехнологічних продуктів;
- Регенеративна економіка, яка спрямована на створення самовідтворюваних соціально-економічних систем, що поєднують технологічний прогрес із соціальною справедливістю та екологічною відповідальністю.

Забезпечення економічної безпеки в умовах цифрової економіки тісно пов'язане з формуванням інституційних основ, які забезпечують прозорість цифрових ринків, захист прав власності на цифрові активи, ефективне врегулювання конфліктів між суб'єктами цифрової економіки та попередження цифрових загроз. Від рівня інклюзивності цих інституцій, їхньої гнучкості та здатності адаптуватися до нових технологічних викликів залежить загальний рівень економічної безпеки та конкурентоспроможність національної економіки в глобальному цифровому просторі.

Економічна безпека в умовах цифрової економіки є інтегральною характеристикою, що відображає баланс між ефективністю цифрових перетворень, стійкістю економічної системи до цифрових загроз та здатністю державних та корпоративних інститутів забезпечувати контроль за критичними цифровими активами та захист економічних інтересів у цифровому середовищі.

Розглядаючи інституційні зміни в контексті забезпечення економічної безпеки в умовах цифрової економіки, доцільно наголосити, що будь-які інституційні трансформації — зокрема пов'язані з цифровізацією – обумовлюють перегляд щонайменше трьох ключових параметрів, які визначають функціонування системи економічної безпеки в цілому:

1. Обмеження

Інституційні зміни, що супроводжують цифрову трансформацію економіки, встановлюють нові обмеження для всіх учасників економічних відносин — від розробників цифрових продуктів і платформ до користувачів, регуляторів, платформних посередників, споживачів цифрових послуг та суспільства загалом. Цифрові технології та платформи створюють нові канали взаємодії та обміну даними, які потребують правової регламентації, включно з

регулюванням захисту персональних даних, кібербезпеки, ліцензування цифрових фінансових послуг, протидії монополізації цифрових ринків тощо. Розширення нормативних обмежень у цифровій сфері впливає на структуру економічних відносин, визначає правила гри для учасників цифрової економіки та створює нові точки напруги між державою, бізнесом і суспільством.

2. Пріоритети

Зміна обмежень автоматично трансформує систему пріоритетів ключових суб'єктів цифрової економіки. В умовах ліберального регулювання цифрові платформи та технологічні компанії орієнтуються на максимізацію кількості користувачів, зростання обсягу оброблюваних даних, розширення пропозиції цифрових послуг та проникнення на нові ринки. Водночас посилення регуляторних вимог (наприклад, щодо відповідності стандартам кібербезпеки, захисту прав користувачів або боротьби з цифровим шахрайством) змінює пріоритети: замість масштабування на перший план виходять питання відповідності регуляторним вимогам та мінімізації репутаційних і фінансових ризиків.

Подібні процеси характерні не лише для великих технологічних компаній, а й для цифрових фінансових посередників (FinTech-компаній), маркетплейсів, онлайн-банкінгу та платформ колективного фінансування. Наприклад, посилення вимог до перевірки клієнтів (KYC/AML) змушує фінансових посередників скорочувати обсяги обслуговування ризикових клієнтів, навіть якщо це знижує їхню прибутковість. Зі свого боку, користувачі, стикаючись із надмірними вимогами щодо верифікації, можуть відмовлятися від користування офіційними цифровими послугами на користь тіньових платформ, що спричиняє нові ризики для економічної безпеки.

3. Відносини

Зміна пріоритетів неминуче модифікує характер відносин між усіма учасниками цифрової економіки та інституційного середовища. Це стосується не лише регуляторів і бізнесу, а й відносин між цифровими платформами, споживачами, посередниками, контент-мейкерами, фінансовими установами та навіть державними органами, які здійснюють нагляд за цифровими ринками. Цифрова економіка сприяє формуванню складних багатосторонніх платформних відносин, які поєднують елементи кооперації та конкуренції, посилюючи інформаційну асиметрію між учасниками.

Ці трансформації створюють ґрунт для специфічного явища, яке можна визначити як псевдокооперацію або псевдоінновації. Йдеться про ситуації, коли учасники цифрової економіки створюють видимість інноваційних змін, що насправді не підвищують якість цифрових продуктів чи послуг, а лише слугують

формальним підтвердженням відповідності регуляторним вимогам. Подібна поведінка, яка нерідко є наслідком надмірного регулювання або неузгоджених правил на цифрових ринках, призводить до зростання опортуністичних практик, коли окремі суб'єкти цифрової економіки навмисно використовують регуляторні прогалини або інформаційну асиметрію для отримання короткострокових вигод на шкоду довгостроковій економічній безпеці.

Подібні ефекти можна спостерігати як на традиційних ринках (наприклад, банківському чи страховому), так і в нових секторах цифрової економіки. Зокрема, на ринку цифрових фінансових послуг кожен ключовий суб'єкт (державні регулятори, платіжні системи, цифрові банки, платформи краудфандингу та краудлендингу) одночасно виконує свою функцію у забезпеченні стабільності фінансової системи, але водночас створює нові опортуністичні ефекти. Наприклад, надмірне ускладнення процедур ідентифікації клієнтів може стимулювати розвиток тіньових цифрових платформ або офшорних криптовалютних сервісів, що прямо підриває економічну безпеку.

На небанківському фінансовому ринку, включно із сегментами мікрофінансування, страхування та цифрових кредитних платформ, ці явища проявляються ще локальніше — у взаємодії між страховиками, цифровими брокерами, мікрокредитними організаціями та їхніми клієнтами. Кожен з учасників формує свою стратегію управління ризиками, створюючи нові інформаційні асиметрії, які в умовах цифровізації посилюються за рахунок використання даних із соціальних мереж, онлайн-платформ та інших цифрових слідів. Це формує нові вразливості для економічної безпеки, пов'язані зі зростанням ризиків маніпуляцій даними, шахрайства, витоку інформації та зловживань з боку цифрових платформ.

У цифровій економіці інституційні трансформації не лише змінюють правила функціонування економічних відносин, а й переформатовують баланс інтересів між учасниками ринку, створюючи нові загрози та виклики для економічної безпеки. Управління економічною безпекою в умовах цифрової економіки потребує гнучкої адаптації інституційного середовища до нових викликів, включаючи системний моніторинг цифрових ризиків, адаптивне регулювання та формування культури цифрової відповідальності серед усіх учасників цифрових ринків.

У контексті забезпечення економічної безпеки в умовах цифрової економіки особливої уваги потребує проблема впровадження інституційних (зокрема, регуляторних) змін без належного врахування економічних передумов і технологічної зрілості середовища. Аналіз показує, що такі дисбаланси провокують виникнення двох взаємопов'язаних негативних явищ:

- Зростання транзакційних витрат для всіх груп економічних суб'єктів, які змушені адаптуватися до нових регуляторних вимог, незалежно від їхньої доцільності чи відповідності реальним викликам цифрової економіки.

- Формування регуляторного арбітражу — ситуації, за якої різні сегменти цифрової економіки або окремі категорії суб'єктів господарювання підпадають під нерівномірне регуляторне навантаження. Внаслідок цього бізнес прагне переміщувати свою активність у ті сфери або юрисдикції, де інституційні та регуляторні вимоги є менш жорсткими.

В умовах цифрової економіки регуляторний арбітраж набуває особливої значущості, оскільки цифрові технології дозволяють суб'єктам господарювання оперативно змінювати юрисдикцію реєстрації, місце зберігання даних, структуру власності або навіть бізнес-модель, обходячи надмірне регулювання. Така практика широко поширена у сфері цифрових фінансових послуг, криптовалютних платформ, цифрових маркетплейсів, трансграничної електронної комерції тощо.

Яскравими прикладами прояву регуляторного арбітражу є розбіжності у правовому статусі та вимогах до різних фінансових посередників у цифровому середовищі. Наприклад, на фінансовому ринку можна спостерігати суттєві відмінності у регулюванні діяльності банківських установ, небанківських кредитних організацій, платіжних платформ та криптовалютних обмінників. У сфері страхування аналогічні диспропорції виникають між страховими агентами та брокерами, що створює можливості для переміщення ризикової діяльності у менш регульовані сегменти.

В умовах інституційної незрілості цифрової економіки поле для регуляторного арбітражу значно розширюється. Це, у свою чергу, звужує простір легального інституціоналізованого ринку, де взаємодія суб'єктів відбувається у прозорих правових рамках. У підсумку, така фрагментація регуляторного поля створює передумови для підвищення системних ризиків та загального зниження рівня економічної безпеки.

Особливу загрозу становить мультиплікація цього ефекту в умовах кризових явищ або періодів економічної турбулентності. За умов скорочення платоспроможного попиту, характерного для кризових періодів, економічні суб'єкти зазнають прямих втрат доходів та прибутків. Це провокує масовий вихід окремих компаній з ринку, що у фінансовому секторі особливо болісно відображається на стабільності системи через можливі дефолти, невиконані зобов'язання перед клієнтами, зростання соціальної напруги та втрату довіри до інституційних механізмів.

У відповідь на ці процеси регулятори зазвичай посилюють наглядові та контрольні функції, що призводить до ще більшого зростання транзакційних і комплаєнс-витрат для учасників цифрової економіки. Особливо це характерно для секторів цифрових фінансових послуг, платіжних систем, ринку цифрових активів та онлайн-страхування. В умовах падіння попиту такі додаткові витрати стають критичним бар'єром для збереження прибутковості, що стимулює пошук обхідних шляхів для мінімізації регуляторного тиску.

Як наслідок, зростає попит на регуляторний арбітраж, коли суб'єкти економіки переміщують свої операції у менш регульовані сегменти (тіньову цифрову економіку, офшорні юрисдикції, децентралізовані платформи), що у підсумку підриває ефективність державного контролю та знижує загальний рівень економічної безпеки.

Окрім безпосередніх економічних наслідків, регуляторний арбітраж у цифровій економіці створює нові виклики для захисту прав споживачів. Переміщення цифрових фінансових та комерційних операцій у нерегульовані зони значно посилює інформаційну асиметрію між споживачами та постачальниками послуг, ускладнює доступ до правового захисту та створює передумови для зростання шахрайства. Усвідомлюючи ці ризики, споживачі починають змінювати свої пріоритети щодо управління власними ризиками, що може включати:

- відмову від користування формально регульованими послугами на користь альтернативних (наприклад, самостійне зберігання криптоактивів замість використання послуг бірж);
- пошук послуг у юрисдикціях із менш жорсткими вимогами;
- зростання попиту на анонімні або частково анонімні фінансові послуги.

Зрештою, такі тенденції провокують звуження формального ринку (наприклад, легального страхування чи цифрового кредитування), поглиблюють тінізацію цифрових секторів економіки та створюють негативний зворотний зв'язок. Надмірне регуляторне втручання в умовах відсутності належних економічних та технологічних передумов лише посилює кризові явища та знижує рівень економічної безпеки у цифровій економіці.

Дослідження системи ризиків цифрової економіки в контексті забезпечення економічної безпеки передбачає виділення чотирьох ключових об'єктів, стабільність і захист яких визначатимуть довгострокову стійкість суспільства та ефективність функціонування цифрової економіки. Цими об'єктами є:

1. Людина

Цифрова економіка докорінно змінює роль людини в економічних процесах, формуючи нові виклики для системи управління економічною безпекою. Серед ключових питань:

- Якою буде роль людини у цифровій економіці — чи залишиться вона лише пасивним споживачем цифрових послуг, вузькоспеціалізованим виконавцем технічних операцій або спостерігачем за автоматизованими процесами?
- Чи зберігатиметься незамінність людини у ключових сегментах створення доданої вартості, чи цифрові технології поступово витіснять людину з усіх етапів створення економічних благ?
- Які функції та компетенції залишаться виключно людськими, якщо штучний інтелект та автоматизовані системи забезпечуватимуть виконання як рутинних, так і висококваліфікованих функцій?

Наукова дискусія вказує на те, що відповіді на ці питання лежать у площині так званих «тонких відмінностей», які принципово не піддаються алгоритмізації та цифровізації. Йдеться про етичні, моральні та естетичні аспекти діяльності, суб'єктивне сприйняття цінностей, індивідуальне трактування понять добра і зла, краси чи справедливості. Формування цифрової ідентичності, баланс між особистим, корпоративним, національним та глобальним рівнями ідентичності також стає новим фактором, що впливає на економічну безпеку в умовах цифрової економіки.

2. Технології

Цифрова економіка безпосередньо залежить від технологічного розвитку, що породжує низку фундаментальних ризиків для економічної безпеки, пов'язаних як із самими технологіями, так і з їхнім інституційним та соціальним контролем. Основні питання:

- Керованість технологіями: наскільки стійким є контроль за розробкою та використанням технологій? Чи можлива ситуація, за якої ключові технології вийдуть з-під контролю суспільства або концентруватимуться в руках вузької групи суб'єктів?
- Кіберзлочинність та кіберконфлікти: як цифрові загрози впливатимуть на функціонування економічних систем, фінансових ринків та критичної інфраструктури?
- Самовідтворення технологій: у який момент ми зіткнемося з феноменом самостійного створення та розвитку технологій без залучення людини — через системи штучного інтелекту, роботизовані платформи та автономні виробничі

системи? Якими будуть наслідки для економічної безпеки у випадку втрати контролю над такими системами?

3. Інформація

Цифрова економіка базується на постійному створенні, обробці та монетизації великих обсягів інформації, що зумовлює появу принципово нових ризиків для економічної безпеки. До основних викликів належать:

- Достовірність інформації: зі зростанням інтенсивності інформаційних потоків підвищується ризик поширення недостовірних або маніпулятивних даних. Це ускладнює процеси прийняття рішень у системах управління як на макро-, так і на мікрорівні.

- Інформаційні фальсифікації: автоматизовані системи, які приймають рішення на основі поверхневого аналізу або неперевірених даних, створюють додаткові загрози для економічної безпеки.

- Розмиття категорії істини: інформаційна надлишковість, плюралізм джерел та відсутність єдиних критеріїв перевірки сприяють формуванню інформаційної невизначеності. Це ускладнює формування узгоджених стратегій забезпечення економічної безпеки, сприяє зростанню когнітивної вразливості суспільства та збільшує кількість точок біфуркації у системах управління.

4. Економіка

Трансформація економічних відносин у цифрову форму створює як нові можливості, так і нові системні загрози для економічної безпеки. Ключові питання:

- Зміна структури витрат: цифровізація змінює співвідношення змінних та постійних витрат, знижує частку витрат на фізичні активи, але водночас підвищує вразливість до кібератак, втрати даних та маніпуляцій цифровими активами.

- Перегляд суспільного договору: автоматизація, цифрові платформи та штучний інтелект витісняють значну частину традиційних професій, змінюючи баланс на ринку праці та створюючи нові виклики для системи оподаткування, соціального захисту та державного регулювання.

- Безумовний базовий дохід: у перспективі розглядається як можливий компенсаторний механізм для суспільства в умовах масштабної автоматизації та витіснення людини з ринку праці. Водночас впровадження таких механізмів потребує перегляду базових принципів економічної політики, системи перерозподілу доходів та формування нових соціальних цінностей.

Таким чином, управління економічною безпекою в умовах цифрової економіки потребує комплексного підходу, який поєднує:

- Оцінку впливу цифрових технологій на економічні, інформаційні та соціальні процеси;
- Створення системи моніторингу цифрових ризиків із фокусом на технологічні, інформаційні та когнітивні загрози;
- Формування адаптивної моделі економічної політики, що враховує нові інституційні, технологічні та соціальні реалії цифрової епохи;
- Забезпечення балансу між економічною ефективністю, соціальною стійкістю та інституційною адаптивністю як основи для довгострокового збереження економічної безпеки у цифровому світі.

В умовах обмеженості ресурсів, спричиненої дефіцитом капіталу, кризовими явищами, високими альтернативними витратами та загальною невизначеністю розвитку глобальної економіки, перед суб'єктами господарювання постає стратегічне завдання варіативного сценарного вибору у сфері забезпечення економічної безпеки. В умовах цифрової економіки цей вибір зводиться до двох базових підходів:

1. Сценарне заміщення – адаптація бізнес-моделей, управлінських рішень та інституційних практик до нових умов функціонування цифрових ринків. Проте цей підхід супроводжується зростанням непередбачених ризиків, зокрема технологічних, інформаційних та регуляторних, робота з якими вимагає не лише додаткових фінансових витрат, а й формування нових компетентностей у сфері цифрової безпеки та цифрового ризик-менеджменту. У багатьох випадках такі компетенції відсутні або перебувають на недостатньому рівні, що підвищує загрози для економічної безпеки суб'єктів.

2. Ресурсне заміщення – залучення додаткових ресурсів (капіталу, технологій, людського капіталу) для забезпечення адаптації до викликів цифрової економіки. Однак у цьому випадку зростають альтернативні витрати, адже ресурсна база формується в умовах загальної економічної нестабільності, а конкуренція за обмежені ресурси загострюється. Це посилює ризики для економічної безпеки, особливо для малих та середніх підприємств, які стикаються зі зростанням вартості фінансування та обмеженим доступом до сучасних технологій.

У цифровій економіці дедалі частіше спостерігається дисбаланс між інституційними новаціями та станом економічного базису, який, відповідно до класичних положень інституціональної теорії, має або випереджати інституційні зміни, або хоча б формуватися під їхнім впливом. У ситуації, коли економічний базис (технологічна інфраструктура, рівень цифрової грамотності, фінансова стійкість) не встигає за стрімкими інституційними нововведеннями, зростають ризики інституційної пастки. Це особливо актуально для цифрових ринків, де

регуляторні зміни часто запроваджуються без урахування технологічної та економічної готовності суб'єктів до їхнього виконання.

У таких умовах набуває поширення домінування екстрактивних інститутів, орієнтованих не на створення нової цінності, а на перерозподіл існуючих ресурсів через регуляторний арбітраж, що є однією з ключових загроз економічній безпеці в умовах цифрової економіки. Регуляторний арбітраж проявляється через створення нерівних умов доступу до цифрових ринків для різних груп суб'єктів, зокрема через лобіювання окремими цифровими платформами вигідних для них регуляторних норм. Це підриває рівні правила гри, створює дисбаланс між великими платформами та малими інноваційними компаніями, гальмує конкуренцію та поглиблює нерівномірність розвитку цифрових секторів.

Паралельно в умовах цифрової економіки спостерігається тенденція до локальної роботи з ризиками на рівні окремих суб'єктів, зокрема середнього бізнесу, який, з одного боку, стикається з обмеженою маржинальністю, а з іншого – накопичує проблеми рентабельності та недооцінки специфічних цифрових ризиків (наприклад, кіберзагроз чи репутаційних атак у цифровому середовищі). Це висуває підвищені вимоги до фінансових ринків, які повинні забезпечувати доступ до фінансування, адаптованого до специфіки цифрової економіки, та до створення інструментів страхування цифрових ризиків. Однак не всі суб'єкти готові до таких змін через обмежену цифрову компетентність, низьку технологічну готовність та недостатню довіру до нових фінансових інструментів.

В умовах таких викликів технологія Blockchain постає як революційний інструмент, здатний трансформувати фінансовий сектор і стати одним із ключових елементів системи економічної безпеки в умовах цифрової економіки. На відміну від тверджень окремих ентузіастів про можливе зникнення фінансового ринку під впливом повсюдного поширення Blockchain, доцільно розглядати цю технологію як каталізатор глибинних змін, які вже назріли у фінансовій системі та в інституційній архітектурі цифрової економіки загалом.

Унікальність технології Blockchain у контексті економічної безпеки визначається поєднанням трьох фундаментальних характеристик:

1. Незмінність минулих записів. Ця характеристика забезпечує неможливість фальсифікації або заднім числом коригування вже здійснених транзакцій. Така властивість створює основу для довіри до цифрових фінансових операцій, підвищує прозорість економічних відносин та знижує ризики маніпуляцій.

2. Децентралізованість. Blockchain не передбачає централізованої точки контролю, що робить систему стійкою до зовнішніх втручань та гарантує надійне

зберігання великих масивів даних, включно з критично важливою інформацією про економічні трансакції, цифрові контракти та ланцюги постачання.

3. Криптографічний захист. Високий рівень криптографічного захисту забезпечує захищеність даних від несанкціонованого доступу, підробки та втручання, що є ключовим елементом економічної безпеки в умовах цифровізації фінансових ринків.

Ключова цінність Blockchain для економічної безпеки. Технологія Blockchain формує новий рівень довіри між учасниками цифрової економіки, забезпечуючи прозорість і достовірність даних, які є основою цифрових економічних відносин. Її використання дозволяє знизити інформаційну асиметрію, мінімізувати ризики опортуністичної поведінки, створити надійні механізми відстеження транзакцій та автоматизованого виконання контрактів (через смарт-контракти). Це перетворює Blockchain на важливий інфраструктурний компонент системи економічної безпеки, здатний підвищити стійкість цифрової економіки до зовнішніх і внутрішніх загроз.

Однією з ключових характеристик Blockchain як технологічного інструменту забезпечення економічної безпеки в умовах цифрової економіки є можливість простежування достовірності походження та руху активів або зобов'язань на всіх етапах їхнього життєвого циклу.

Незалежно від природи об'єкта (чи йдеться про актив у вигляді цифрового або фізичного ресурсу, чи про зобов'язання у фінансовій чи юридичній площині), Blockchain формує альтернативну реальність обліку, де кожна транзакція фіксується незмінно, без можливості ретроспективного коригування. Саме це забезпечує унікальну якість — вбудовану довіру до даних, яка не залежить від централізованих інститутів чи посередників.

Технологія Blockchain забезпечує:

- Фіксацію місцезнаходження активу або зобов'язання (його походження, історію та поточний стан).
- Формування чіткого права власності (належність активу чи зобов'язання конкретному суб'єкту в певний момент часу).
- Реєстрацію змін у праві власності чи характеристиках активу/зобов'язання, фіксуючи кожен перехід або трансформацію.

Завдяки цим властивостям, Blockchain може виконувати функції:

- Зменшення невизначеності шляхом надання повної та достовірної інформації про актив або угоду.
- Захисту від втрати даних через розподілене зберігання та незмінність записів.

- Скорочення трансакційних витрат за рахунок усунення посередників та спрощення перевірки даних.

Особливо важливим аспектом у контексті економічної безпеки є синхронний рух фізичного об'єкта (активу) у реальному середовищі та його цифрового відображення (токена) в системі Blockchain. Відстеження цього процесу стає доступним для всіх зацікавлених сторін, а сама інформація про транзакції є незмінною, що унеможливлює фальсифікацію. Це формує нову парадигму управління економічною безпекою, засновану на технологічно гарантованій довірі до цифрових процесів.

Blockchain як інституційний інструмент економічної безпеки У сучасних умовах технологія Blockchain набуває стратегічного значення для забезпечення економічної безпеки не лише окремих суб'єктів господарювання, а й економічних систем загалом. Її потенціал полягає у створенні принципово нових інституційних форм, здатних замінити або трансформувати традиційні механізми регулювання та контролю.

Зокрема, Blockchain виконує такі функції:

- Руйнування та заміщення традиційних формальних інститутів. Йдеться про заміну класичних регуляторних механізмів (ліцензування, нагляд, адміністрування) технологічними алгоритмами, які забезпечують автоматичну перевірку та верифікацію операцій на рівні смартконтрактів та розподілених реєстрів. Це особливо актуально для цифрових платформ, фінансових ринків та міжнародних торговельних ланцюгів постачання.

- Інститут верифікації активів та зобов'язань. Blockchain дозволяє відмовитися від багаторівневих систем підтвердження прав власності, походження активів чи обґрунтованості зобов'язань, оскільки кожен цифровий об'єкт у Blockchain вже має вбудовану історію, яка не потребує додаткової перевірки на етапі укладання угоди чи передання прав. Це знижує інформаційні бар'єри та мінімізує ризики контрагентів.

- Технологічний інститут як альтернатива класичним юридичним механізмам. Традиційні контракти поступово доповнюються або замінюються смартконтрактами, які автоматично виконуються при виконанні визначених умов. Резервування коштів чи активів може здійснюватися не через банківські депозити або застави, а через випуск і зберігання токенів, які підтверджують фінансові зобов'язання. Це формує нові механізми довіри та економічної безпеки в цифрових транзакціях.

Blockchain та відродження механізмів взаємного фінансування. Особливого значення Blockchain набуває у сегменті цифрових фінансових послуг. Зокрема, в умовах цифрової економіки відбувається відродження інтересу до моделей взаємного фінансування, які свого часу відігравали значну роль у банківських системах ряду країн (Німеччина, Японія). Blockchain дозволяє відновити та модернізувати ці моделі, створивши технологічну платформу для функціонування:

- Товариств взаємного страхування, які можуть працювати на основі смартконтрактів із прозорими умовами внесків, виплат та управління фондами.
- Банків взаємного кредитування, де учасники одночасно виступають і кредиторами, і позичальниками, а всі операції фіксуються у розподіленому реєстрі.

Ці форми цифрових фінансових інститутів, засновані на Blockchain, здатні забезпечити підвищену стійкість до кризових явищ, прозорість та автоматизацію процесів, мінімізуючи ризики зловживань і підвищуючи рівень довіри між учасниками.

Blockchain і соціальна спрямованість. Водночас, варто підкреслити, що Blockchain — це лише технологія, яка сама по собі не є ні гарантом соціальної справедливості, ні чинником автоматичного зростання економічної безпеки. Її реальний вплив залежить від того:

- У яких сферах вона застосовується (фінанси, управління державними реєстрами, ланцюги постачання тощо).
- Хто контролює доступ до технології та управління мережами.
- Які соціальні та економічні інтереси закладаються в алгоритми функціонування смартконтрактів та розподілених реєстрів.

Без належного інституційного супроводу впровадження Blockchain може стати інструментом не посилення економічної безпеки, а, навпаки, формування нових форм цифрової нерівності, коли доступ до переваг технології концентрується у вузького кола суб'єктів, здатних контролювати ключові ланцюги даних та фінансових потоків. Таким чином, ефективне застосування Blockchain у контексті управління економічною безпекою в умовах цифрової економіки потребує синхронізації технологічних можливостей із інституційними гарантіями рівного доступу, прозорості та врахування суспільних інтересів.

На сучасному етапі розвитку цифрової економіки технологія Blockchain демонструє значний потенціал для забезпечення економічної безпеки, проте її практичне застосування далеко не завжди відповідає інтересам суспільства та держави. Навпаки, у низці випадків вона стає інструментом формування нових

загроз та ризиків, що підривають економічну безпеку як окремих суб'єктів, так і економічної системи загалом.

До основних деструктивних напрямів використання Blockchain можна віднести:

- Приховування особистості та анонімізація фінансових потоків, що набуло особливої гостроти у сфері криптовалютних транзакцій, ускладнюючи ідентифікацію кінцевих бенефіціарів та створюючи додаткові виклики для фінансового моніторингу.
- Отримання надприбутків через регуляторний арбітраж – найяскравіше це проявилося у сегменті первинних пропозицій токенів (ICO), які за рівнем регуляторних вимог суттєво поступаються традиційним публічним розміщенням акцій (IPO).
- Формування спекулятивних ринків, де вартість активів визначається не фундаментальними характеристиками, а виключно спекулятивним попитом. Показовим прикладом є феномен Blockchain-гри CryptoKitties, яка створила спекулятивний бум без жодної реальної економічної основи.

Окрім цих ризиків, технологія Blockchain наразі залишається технологічно недосконалою, що створює додаткові бар'єри для її широкого застосування в системах економічної безпеки. Серед основних обмежень:

- Тривалий час підтвердження транзакцій, що робить Blockchain малопридатним для низки операцій у режимі реального часу.
- Високе енергоспоживання, особливо в мережах, які працюють за алгоритмом Proof-of-Work.

Попри ці обмеження, у середньостроковій перспективі Blockchain матиме значний вплив на трансформацію систем управління та контролю у таких секторах, як:

- медицина (ведення електронних медичних записів із захищеним доступом);
- будівництво (цифрові реєстри об'єктів та прав власності);
- освіта (верифікація дипломів та сертифікатів);
- фармацевтика (контроль ланцюгів постачання та походження препаратів);
- облік інтелектуальної власності (реєстрація прав у цифровому середовищі);
- державне управління (впровадження цифрових реєстрів та смартконтрактів у публічному адмініструванні);
- облік нерухомості та податкових зобов'язань (цифровізація державних кадастрів та систем оподаткування).

Враховуючи ці тенденції, питання економічної безпеки в умовах цифровізації та становлення цифрової економіки набуває особливої актуальності. Цифрова економіка формує принципово нові механізми створення вартості, перерозподілу ресурсів та організації виробничих і фінансових процесів, що потребує перегляду інструментів забезпечення економічної безпеки.

Основні інструменти економічної безпеки в умовах цифрової економіки.

1. Цифрова гігієна. Цей інструмент поступово перетворюється на обов'язковий компонент систем управління економічною безпекою як на рівні окремих підприємств, так і в масштабах національних економік. Особливо високі стандарти цифрової гігієни впроваджено у банківському та фінансовому секторах, у сфері електронної комерції та великих торговельних мережах.

Цифрова гігієна включає:

- впровадження систем багаторівневого захисту від зовнішніх загроз (антивірусні програми, системи виявлення вторгнень, резервування даних);
- контрольоване управління доступом до інформаційних систем та баз даних;
- обмеження доступу до небажаних або ризикових ресурсів із робочих пристроїв (зокрема, до соціальних мереж або розважальних платформ під час виконання критично важливих завдань).

Повноцінне функціонування цифрової гігієни можливе лише за умови, що кожен суб'єкт економічної діяльності (організація, підприємство чи окрема особа) матиме сформовану культуру роботи з інформацією та чітко усвідомлюватиме:

- свої інформаційні цілі;
- канали комунікації;
- методи фільтрації та перевірки інформації;
- джерела інформаційних ризиків.

2. Когнітивне цілепокладання

Цей інструмент безпеки передбачає усвідомлене формування цілей цифровізації на рівні як окремих суб'єктів, так і суспільства в цілому. Йдеться про критичне переосмислення:

- впливу цифрових технологій на систему соціально-економічних цінностей;
- ризиків втрати контрольованості над ключовими інституційними процесами у результаті технологічних перетворень;
- межі допустимого втручання технологій у життя людини та суспільства.

Відсутність когнітивного цілепокладання створює загрозу формування технологічної пастки, коли цифрові інновації підміняють собою ціннісні

орієнтири, а суспільство втрачає здатність критично оцінювати наслідки цифрових трансформацій.

3. Інституційні трансформації. Технологічна революція, включно з розвитком цифрової економіки, неминуче спричиняє глибинні інституційні зміни. Це створює низку питань:

- чи здатні формальні інститути своєчасно адаптуватися до змін, спричинених цифровізацією?

- чи можлива гармонізація формальних і неформальних інститутів, що виникають у цифровому середовищі, без порушення основ економічної безпеки?

Ефективність цих інституційних змін значною мірою визначатиме спроможність суспільства забезпечити контроль над цифровими ринками та зберегти баланс між інноваціями та безпекою.

Економічна безпека у цифровій економіці: нові виклики.

Цифрова економіка формує новий економічний простір, у якому рух матеріальних активів супроводжується рухом цифрових даних, а ключові економічні відносини дедалі частіше реалізуються у віртуальній площині. Ця трансформація змінює традиційні уявлення про ризики, розмиває межі між економічними, інформаційними та когнітивними загрозами, формує нові канали реалізації загроз економічній безпеці.

За таких умов виникає об'єктивна потреба у формуванні нового покоління фахівців з економічної безпеки, здатних працювати у цифровому середовищі, аналізувати комплексні цифрові ризики та створювати ефективні системи їхньої мінімізації. Попит на таких фахівців, з огляду на стрімку цифровізацію всіх сфер економіки, буде постійно зростати.

Список використаних джерел:

1. Конституція України. Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

2. Правове регулювання національної безпеки : навч. посіб. / О. Г. Боднарчук, О. І. Боднарчук, М. В. Глух, А. В. Гарбінська-Руденко ; Державний податковий університет. Ірпінь, 2024. 202 с. URL:https://surl.li/wohfsl

3. Закон України «Про національну безпеку України». Відомості Верховної Ради України. 2018. № 31. Ст.241. Із змінами, внесеними згідно із законами України № 522-IX від 04.03.2020, ВВР, 2020. № 34. Ст.241 — № 1702-IX від 16.07.2021 (вводиться в дію з 01.01.2022). URL: https://zakon.rada.gov.ua/laws/show/2469-19#n355 .

4. Стрельбицька Т.А. Опортунізм як загроза економічній безпеці підприємств України. АГРОСВІТ. 2024. № 11. С. 175-180.

5. Савицька Н. Л., Гебер Н. А. Вплив опортуністичної поведінки на кадровий потенціал підприємств мережного ритейлу. Проблеми економіки. 2015. № 4. С. 228-233. URL: https://surl.li/odmmrb

6. Загурський О.М Інституціоналізація корпоративних процесів в аграрній сфері. Економіка АПК. 2014. №1. С. 79-84. https://eapk.com.ua/web/uploads/pdf/Vol.%2021,%20No.%201,%202014_apk-79-84.pdf

7. Елла Лібанова, Сергій Романюк. Концептуалізація полісуб'єктного управління в соціальних відносинах. Демографія та соціальна економіка. 2023, № 3 (53). С. 33-53. URL: https://surli.cc/obdnxf

8. Резнікова, Н., Іващенко, О., & Дворник, І. (2022). Регуляторний арбітраж як інструмент тінізації глобальної економіки: у пошуках балансу між юрисдикційною конвергенцією та конкуренцією на міжнародних ринках. Modeling the development of the economic systems, (4), 179–186. https://doi.org/10.31891/mdes/2022-6-24

9. Дубінка, М. М. (2022). Дослідження питання професійної ідентичності як детермінанти процесу професійного самовизначення у працях зарубіжних учених. Наукові записки. Серія: Педагогічні науки, (206), 113-121. https://doi.org/10.36550/2415-7988-2022-1-206-113-121

10. Краєва О. А. Основні теоретичні підходи вівчення ідентичністьяк міждисциплінарної проблеми сучасної науки. Раціогуманістичні студії збірник наукових статей за матеріалами круглого столу 30 травня 2019 року / за ред. В.Л. Зливков, О.В. Завгородня, Лукомська С.О., Котух О.В. / за гол.ред. Зливкава В.Л., Київ, 2019. 285 с. С. 149-163. URL: https://surl.li/svhuud

11. Мутерко Г. М., Кучерівська С. С., Яцко М. В., Малець В. В. Впровадження блокчейн-технологій в економіці України: переваги та виклики. АКАДЕМІЧНІ ВІЗІЇ. 2023. Вип. 26. С. 1-13. DOI: http://dx.doi.org/10.5281/zenodo.10389773

12. Стащук О. В., Теслюк С. А., Кузьмич І. В. Перспективи використання технології блокчейн у фінансовому секторі. Економіка та суспільство. 2022. Вип. 40. DOI: https://doi.org/10.32782/2524-0072/2022-40-81

13. Givi Bedianashvili, Hanna Zhosan, Sergiy Lavrenko Modern digitalization trends of Georgia and Ukraine. Published in Scientific Papers. Series «Management, Economic Engineering in Agriculture and rural development», Vol. 22 ISSUE 3, 2022 URL: https://surl.li/afuixw

14. Karnaushenko A., Tanklevska N., Povod T., Kononenko L., Savchenko V Implementation of blockchain technology in agriculture: fashionable trends or requirements of the modern economy. Agricultural and Resource Economics: International Scientific E-Journal (Q3), 2023. 9(3), pp. 124-149. https://doi.org/10.51599/are.2023.09.03.06
https://dspace.ksaeu.kherson.ua/handle/123456789/8421 (Scopus)

15. Voloshchuk V., Voloshchuk Y., Varchenko O., Karnaushenko A., Khakhula B. Investment determinant of the sustainability of innovative technologies of energy supply in the agro-food system of Ukraine. Rivista di Studi sulla Sostenibilita, 2023, 2, pp. 373–395. https://doi.org/10.3280/RISS2022-002021 . (Scopus)
https://dspace.ksaeu.kherson.ua/handle/123456789/8419

16. Карнаушенко А., Пантелеймоненко А. Електронна торгівля та її значення в розвитку глобальної економіки. Таврійський науковий вісник. Серія: Економіка, 2023 (16), С. 281-292 https://doi.org/10.32782/2708-0366/2023.16.37
https://dspace.ksaeu.kherson.ua/handle/123456789/8425

17. Карнаушенко А.С. Ефективність впровадження технології блокчейн в страхування. Ефективна економіка. 2022. №11. https://www.nayka.com.ua/index.php/ee/article/view/739

18. Tetiana Povod. Behavioral finance: essence and approaches to definition. Таврійський науковий вісник. Серія Економіка. 2022. №14. С. 102-109. DOI: https://doi.org/10.32851/2708-0366/2022.14.13

19. Tetiana Povod. Peculiarities of the formation of the resource base of banks: essence and significance. Таврійський науковий вісник. Серія Економіка. 2023. №16. С. 236-243. https://doi.org/10.32782/2708-0366/2023.16.31

20. Савченко В., Кононенко Л., Повод Т. напрями удосконалення підготовки фахівців у контексті необхідності забезпечення запитів розвитку фінансового сектору та викликів формування «INDUSTRY 5.0». Таврійський науковий вісник. Серія: Економіка, 2024. (19), 195-201. https://doi.org/10.32782/2708-0366/2024.19.23

21. Повод Т., Адвокатова Н. Фінансовий інжиніринг: світові тенденції та вітчизняні реалії. Таврійський науковий вісник. Серія: Економіка, 2020. (1), С. 214-220. https://surl.li/rfeafq