http://doi.org/10.26565/1727-6667-2024-2-17
УДК 351.863:338.2:343.326

Папирін Денис Олександрович,
аспірант кафедри економічної політики та менеджменту
Навчально-наукового інституту «Інститут державного управління»
Харківського національного університету імені В. Н. Каразіна,
майдан Свободи, 4, м. Харків, 61022, Україна
ORCID ID: http://orcid.org/0009-0001-2292-6483
e-mail: papyrin.denys@ukr.net

ТРАНСФОРМАЦІЯ МЕХАНІЗМІВ ДЕРЖАВНОГО РЕГУЛЮВАННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ В УМОВАХ СУЧАСНИХ ГІБРИДНИХ ЗАГРОЗ: ЄВРОПЕЙСЬКИЙ ДОСВІД ТА УКРАЇНСЬКІ РЕАЛІЇ

Анотація. У статті досліджено теоретико-методологічні засади та практичні аспекти трансформації механізмів державного регулювання економічної безпеки в умовах сучасних гібридних загроз. На основі системного аналізу виокремлено та критично осмислено чотири ключові методологічні підходи до забезпечення економічної безпеки держави: неокласичний, інституційний, мережевий та проактивний. Розкрито їх особливості, переваги та обмеження в контексті протидії гібридним загрозам. Проаналізовано європейський досвід трансформації механізмів економічної безпеки. Виявлено тенденцію до комплексного поєднання різних методологічних підходів та інструментів: від класичних ринкових та інституційних до інноваційних мережевих та форсайтних. На основі порівняльного аналізу європейського досвіду та українських реалій обґрунтовано концептуальні засади модернізації вітчизняної системи державного регулювання економічної безпеки. Запропоновано матрицю трансформації регуляторних механізмів, яка враховує поточний стан та визначає пріоритетні напрями змін за кожним методологічним підходом. Аргументовано необхідність поетапного впровадження запропонованих механізмів з урахуванням наявних ресурсів та інституційної спроможності держави. Особливу увагу приділено ролі цифрової трансформації та державно-приватного партнерства як ключових драйверів модернізації системи економічної безпеки. Окреслено перспективи подальших досліджень, зокрема щодо розробки методології комплексної оцінки ефективності регуляторних механізмів та адаптації європейських практик до українських реалій післявоєнного відновлення.

Ключові слова*: економічна безпека, механізми державного регулювання, гібридні загрози, цифрова трансформація, державно-приватне партнерство, європейський досвід, стратегічне планування, проактивне управління, післявоєнне відновлення.*

Як цитувати: Папирін Д. О. Трансформація механізмів державного регулювання економічної безпеки в умовах сучасних гібридних загроз: європейський досвід та українські реалії. *Теорія та практика державного управління*. 2024. Вип. 2 (79). С. 342 – 362. http://doi.org/10.26565/1727-6667-2024-2-17

Актуальність дослідження. В умовах безпрецедентних гібридних загроз, з якими зіткнулась Україна та інші країни Європи протягом останніх років, питання трансформації механізмів державного регулювання економічної безпеки набуває критичної важливості. Російська збройна агресія проти України, що розпочалась у 2014 році з анексії Криму та розв'язання конфлікту на Донбасі, а переросла у повномасштабне вторгнення 24 лютого 2022 року, стала найбільшим викликом європейській безпеці з часів Другої світової війни. За оцінками Світового банку, через руйнування інфраструктури, зупинку підприємств, розрив логістичних ланцюгів та міграцію робочої сили економіка України у 2022 році скоротилась на 35%. Загальні економічні втрати від війни оцінюються у $600 млрд.

Одночасно з прямою військовою агресією, Росія веде проти України та її союзників гібридну війну, що включає інформаційні та кібератаки, економічний тиск, енергетичний шантаж. За даними СБУ, лише у 2022 році було нейтралізовано понад 4500 кібератак на критичну інфраструктуру України. Україна та ЄС також стали об'єктами безпрецедентної дезінформаційної кампанії. Маніпулюючи цінами на енергоносії та продовольство, Росія спровокувала зростання інфляції та загрозу рецесії в Європі. Все це вимагає принципово нових підходів до протидії гібридним загрозам на національному та наднаціональному рівнях.

Актуальність дослідження також обумовлена тим, що в процесі євроінтеграції та набуття статусу кандидата на вступ до ЄС у 2022 році, Україна взяла на себе зобов'язання привести свою систему економічної безпеки у відповідність до європейських стандартів і практик. Це відкриває можливості для системної трансформації існуючих механізмів державного регулювання на основі досвіду країн ЄС, які вже тривалий час розвивають комплексні підходи до протидії гібридним загрозам. Наприклад, у 2022 році ЄС ухвалив Стратегічний компас – план дій із посилення безпекової та оборонної політики до 2030 року. Один з його чотирьох напрямів повністю присвячений захисту від гібридних загроз.

Огляд останніх досліджень. Проблематика економічної безпеки в умовах гібридних загроз привертає дедалі більше уваги дослідників, міжнародних організацій та аналітичних центрів. Світовий економічний форум у своєму звіті Global Risks Report 2023 [27] виділив кібератаки, дезінформацію та економічні конфлікти серед топ-10 глобальних ризиків. У доповіді НАТО 2024 року [7] зазначається, що гібридні загрози стануть визначальним фактором безпеки та оборони альянсу в найближчому майбутньому. Організація економічного співробітництва та розвитку (ОЕСР) у звіті 2024 року [20] акцентує увагу на економічному вимірі гібридних загроз та наголошує на необхідності адаптації регуляторних механізмів.

В українській науковій літературі дослідження трансформації механізмів економічної безпеки в умовах гібридних загроз представлені в роботах В. Горбуліна, О. Власюка, Я. Жаліла, А. Сухорукова та ін. Зокрема, в колективній монографії «Світова гібридна війна: український фронт» [4] розроблено концептуальні засади протидії гібридним загрозам. У статті О. Власюка та С. Кононенко [1] проаналізовано вплив гібридної війни на економічну безпеку України.

Серед досліджень у країнах Східної Європи варто відзначити роботи Центру передового досвіду НАТО з питань енергетичної безпеки у Литві, зокрема ана-

літичну записку Hybrid Warfare Against Critical Energy Infrastructure (2022) [18]. Експерти Міжнародного центру оборони та безпеки в Естонії у звіті [15] зосереджують увагу на уроках агресії проти України для країн Балтії та НАТО в цілому. Польський Фонд імені Казиміра Пуласького видав спеціальний звіт 2021 р. [6], в якому узагальнено передові практики протидії гібридним загрозам.

Зв'язок між сучасними гібридними загрозами та економічною безпекою держави, зокрема стратегічних державних підприємств і корпорацій, привертає дедалі більше уваги дослідників. У статті «Hybrid threats and the critical infrastructure protection challenge» в журналі Technology in Society (2021) підкреслюється, що критична інфраструктура, така як енергетика, транспорт і зв'язок, стає пріоритетною ціллю гібридних атак [16]. Дослідження Європейського центру боротьби з гібридними загрозами (2020 р.) акцентує увагу на використанні економічних інструментів у гібридних конфліктах, зокрема через вплив на енергетичну безпеку [14]. У звіті Офісу з фінансових та економічних злочинів Великобританії (OFSI) «National Risk Assessment of Proliferation Financing» [21] наголошується на зростанні ризиків фінансування розповсюдження зброї масового знищення через державні підприємства. Свіжа стаття харків'ян [3; 2] розкриває вразливості українських державних корпорацій (на прикладі Укрзалізниці і АМПУ) в умовах російської агресії. Однак, незважаючи на зростаючу кількість публікацій, бракує комплексних досліджень трансформації механізмів регулювання економічної безпеки, які б поєднували європейський досвід та українські реалії в умовах триваючої агресії.

Мета дослідження – на основі аналізу європейського досвіду та українських реалій уточнити концептуальні засади трансформації механізмів державного регулювання економічної безпеки в умовах сучасних гібридних загроз. Поставлена мета вирішується послідовним розв'язанням **трьох задач**:

1) систематизувати теоретико-методологічні підходи до дослідження механізмів регулювання економічної безпеки в умовах гібридних загроз;

2) узагальнити європейський досвід протидії гібридним загрозам економічній безпеці та виокремити кращі практики для імплементації в Україні.

3) критично оцінити ефективність існуючих механізмів державного регулювання економічної безпеки України та обґрунтувати напрями їх трансформації з урахуванням сучасних викликів.

Об'єкт дослідження: механізми державного регулювання економічної безпеки.

Предмет дослідження – процес сучасної повоєнної трансформації механізмів державного регулювання економічної безпеки в умовах сучасних гібридних загроз на основі європейського досвіду та українських реалій.

Використана методологія. Методологічною основою дослідження є діалектичний метод пізнання, системний та інституційний підходи до аналізу механізмів державного регулювання економічної безпеки.

Для розв'язання першого завдання – систематизації теоретико-методологічних підходів – застосовуються методи наукової абстракції, порівняльного аналізу, узагальнення та синтезу. Це дозволяє розкрити еволюцію концепції економічної безпеки, виявити сутність та особливості гібридних загроз, об-

ґрунтувати необхідність трансформації регуляторних механізмів в цифрову епоху. При виконанні другого завдання – узагальнення європейського досвіду – використовуються методи кейс-стаді, аналізу і синтезу й абстрактно-логічний метод. На прикладі у цілому ЄС виокремлюються сучасні механізми забезпечення економічної безпеки, кращі практики протидії гібридним загрозам. Особлива увага приділяється інституційним механізмам координації на рівні ЄС та інноваційним інструментам моніторингу загроз.

Для розв'язання третього завдання – оцінки ефективності існуючих механізмів в Україні – застосовується абстрактно-логічний метод і метод дедукції і метод індукції. На їх основі були визначені прогалини в системі економічної безпеки України, вплив військової агресії на трансформацію безпекових механізмів, проблеми та обмеження в імплементації європейського досвіду. Обґрунтування напрямів вдосконалення механізмів регулювання здійснюється за допомогою методів абстрактно-логічного, дедукції і індукції..

Виклад основного матеріалу. Концепція економічної безпеки держави має давнє коріння в економічній думці, однак в умовах сучасних гібридних загроз вона набуває нового змісту і потребує ґрунтовного переосмислення. Класичні теорії економічної безпеки, розроблені такими вченими-класиками, як Адам Сміт, Давид Рікардо та Фрідріх Ліст, акцентували увагу на захисті національних економічних інтересів в умовах міжнародної конкуренції. Однак в епоху глобалізації та цифрових трансформацій традиційні загрози доповнюються якісно новими, асиметричними викликами, що мають гібридний характер. Гібридні загрози поєднують військові, політичні, економічні, інформаційні та кіберінструменти впливу, розмиваючи межі між війною та миром. Вони націлені на критичні вразливості держави та суспільства, прагнучи підірвати їх стійкість та волю до опору. В економічній сфері гібридні загрози проявляються у формі торговельно-економічних війн, фінансових санкцій, маніпулювання енергетичними ринками, кібератак на критичну інфраструктуру тощо, – і це вимагає розширення традиційних поглядів на економічну безпеку та розробки нових теоретичних підходів.

Сучасні дослідження економічної безпеки спираються на міждисциплінарну методологію, що інтегрує здобутки економічної теорії, політології, теорії міжнародних відносин, безпекових студій. Зокрема, теорія складних адаптивних систем дозволяє розглядати економічну безпеку як емерджентну властивість, що виникає внаслідок нелінійної взаємодії багатьох агентів та інститутів. Мережевий підхід акцентує увагу на ролі взаємозв'язків та взаємозалежностей у забезпеченні стійкості економічної системи перед гібридними загрозами.

Ключовим методологічним зрушенням є відхід від статичного до динамічного трактування економічної безпеки. Якщо раніше вона розглядалась як стан захищеності економічних інтересів від зовнішніх та внутрішніх загроз, то зараз на перший план виходить здатність економічної системи адаптуватись до невизначеності, абсорбувати шоки та відновлюватись після криз [17]. Це передбачає розвиток адаптивних та проактивних механізмів державного регулювання, спрямованих на забезпечення стійкості (резилієнтності) економіки.

Далі зосередимось на порівняльному аналізі цих підходів та їх еволюції в контексті нових викликів.

1. *Неокласичний підхід: від статичної до динамічної рівноваги*. Традиційно економічна безпека розглядалась крізь призму неокласичної парадигми, яка акцентує увагу на досягненні та підтриманні стану рівноваги економічної системи. Згідно з цим підходом, безпека асоціюється з відсутністю значних відхилень ключових макроекономічних показників (ВВП, інфляція, безробіття тощо) від певних цільових орієнтирів [24]. Основним завданням державного регулювання в рамках цієї парадигми є створення умов для ринкового саморегулювання та коригування можливих «провалів ринку». Однак в умовах наростання гібридних загроз та невизначеності неокласична модель виявляє свою обмеженість. По-перше, вона не враховує складні нелінійні взаємодії та кумулятивні ефекти, характерні для гібридних впливів. По-друге, фокус на рівновазі не дає інструментів для адаптації до непередбачуваних шоків та стресів. Тому в сучасних дослідженнях акцент зміщується з статичної до динамічної рівноваги, яка передбачає здатність економічної системи відновлювати баланс після збурень [22]. Відповідно, механізми безпеки мають забезпечувати не лише стійкість параметрів, але й адаптивність структури економіки.

2. *Інституційний підхід: від формальних до неформальних «правил гри»*. Згідно з інституційною теорією, економічна поведінка та результативність значною мірою визначаються якістю інститутів – формальних та неформальних «правил гри», що структурують взаємодії між економічними агентами [19]. Інститути (права власності, контрактне право, антимонопольне регулювання тощо) зменшують невизначеність, координують очікування та стимули, а отже, сприяють стабільності економічної системи. Відповідно, інституційний підхід до безпеки робить наголос на розбудові ефективної регуляторної інфраструктури, що убезпечує економіку від опортуністичної поведінки та «інституційних пасток». Водночас в умовах гібридних загроз самі інститути стають об'єктом атак та деструктивних впливів. Маніпулювання нормативно-правовим полем, експлуатація інституційних прогалин, корупційний тиск підривають ефективність формальних «правил гри». Тому новітні дослідження зміщують фокус на неформальні інститути (цінності, ментальні моделі, соціальний капітал), які визначають стійкість суспільства до гібридних впливів [12]. Зокрема, наголошується на ролі довіри, громадянської активності, критичного мислення у забезпеченні безпеки на мікро- та мезорівні.

3. *Мережевий підхід: від ієрархій до екосистем безпеки*. Класичні теорії безпеки спиралися на ієрархічну модель управління, в якій держава виступає домінантним актором, що забезпечує захист суспільства від зовнішніх та внутрішніх загроз. Однак в епоху глобалізації та дигіталізації така модель втрачає свою релевантність. Гібридні загрози носять мережевий, децентралізований характер, тож протидія їм вимагає горизонтальної координації та колаборації між різними стейкхолдерами [5]. Мережевий підхід акцентує увагу на взаємозалежностях між безпековими акторами (державними органами, бізнесом, експертними спільнотами, громадянським суспільством) та необхідності синергії

їхніх зусиль. В його рамках економічна безпека розглядається не як завдання окремої держави, а як емерджентна властивість складних адаптивних систем – мереж створення цінності, інноваційних екосистем, транскордонних ланцюгів постачання [26]. Відповідно, механізми регулювання мають еволюціонувати від жорстких ієрархічних форматів до гнучких мережевих альянсів, здатних швидко реагувати на турбулентність середовища.

4. *Проактивний підхід: від реагування до передбачення та формування контексту.* Традиційно безпекова політика мала реактивний характер, тобто була зосереджена на протидії вже наявним або очевидним загрозам. Вона спиралася на лінійні моделі стратегічного планування, які екстраполювали минулі тренди на майбутнє. Однак в умовах експоненційних технологічних зрушень та гібридних впливів, що продукують радикальну невизначеність, такі моделі виявляються неадекватними. Натомість проактивний підхід робить акцент на передбаченні та формуванні контексту – на проактивній ідентифікації потенційних загроз та активному формуванні безпекового середовища [13]. Він спирається на методи форсайту, сценарного планування, стратегічного передбачення, що дозволяють «програвати» можливі варіанти майбутнього та розробляти проактивні стратегії. Ключовим інструментом стає розвиток потенціалу стійкості (резилієнтності) – здатності держави, економіки, суспільства адаптуватись до невизначеності, абсорбувати шоки та продовжувати розвиток [25].

Отже, кожен з розглянутих підходів робить свій внесок у розуміння архітектури безпеки в умовах гібридних загроз. Неокласичний підхід наголошує на важливості динамічної рівноваги, інституційний – на ролі формальних та неформальних «правил гри», мережевий – на потребі горизонтальної координації та співпраці стейкхолдерів, проактивний – вже на передбаченні та формуванні контексту безпеки. Водночас жоден з підходів не є самодостатнім: в практичній площині вони мають розглядатись комплементарно. Синтез розглянутих підходів дозволяє сформувати інтегральне бачення економічної безпеки в епоху гібридних загроз як стану динамічної стійкості, що досягається завдяки проактивним та адаптивним механізмам регулювання, інституціалізованим у формі мережевих екосистем стейкхолдерів. Таке бачення відкриває перспективу для подальшого теоретичного та емпіричного опрацювання проблеми на рівні розробки модельного інструментарію, компаративного аналізу кращих практик, обґрунтування стратегічних напрямів безпекової політики (таблиця 1).

Далі розглянемо, як кожен з чотирьох методологічних підходів може проявлятися в реальних політичних та управлінських ситуаціях, особливо в контексті гібридних загроз. Уявімо, що держава зіткнулася з масштабною кібератакою на критичну інфраструктуру, яка загрожує не лише функціонуванню економіки, але й національній безпеці в цілому.

1) Неокласичний підхід в цій ситуації передбачатиме швидку оцінку економічних збитків від атаки та розробку заходів для відновлення ринкової рівноваги, наприклад, через монетарні чи фіскальні інтервенції, але цей підхід може не повною мірою врахувати довгострокові стратегічні наслідки атаки та необхідність системних змін в архітектурі кіберзахисту.

Таблиця 1

Порівняльний аналіз методологічних підходів до дослідження економічної безпеки в умовах гібридних загроз

Table 1

Comparative Analysis of Methodological Approaches to Studying Economic Security in the Context of Hybrid Threats

Підхід	Неокласичний	Інституційний	Мережевий	Проактивний
Ключові особливості	– фокус на ринковій рівновазі та саморегулюванні – вимірювання безпеки через відхилення макропоказників – держава як коректор «провалів ринку»	– акцент на якості формальних та неформальних інститутів – безпека як результат ефективних «правил гри» – держава як гарант інституційної інфраструк-тури	– увага до взаємозалежностей та колаборації стейкхолдерів – безпека як емерджентна властивість мереж та екосистем – держава як фасилітатор мережевих взаємодій	– орієнтація на передбачення та формування контексту – активна ідентифікація потенційних загроз – розвиток потенціалу стійкості
Недоліки	– не враховує нелінійність та кумулятивні ефекти гібридних загроз – не дає інструментів для адаптації до непередбачуваних шоків	– вразливість інститутів до гібридних впливів – недооцінка ролі неформальних інститутів	– складність координації в умовах турбулентності – ризики розмивання відповідальності та керованості	– потребує значних аналітичних потужностей та компетенцій – часовий лаг між ідентифікацією загроз та вжиттям заходів
Наслідки для публічного управління в епоху «цифри»	– потреба в динамічній оцінці параметрів безпеки на основі великих даних – машинне навчання для прогнозування відхилень та аномалій	– цифровізація регуляторних механізмів та сервісів – блокчейн для підвищення прозорості та довіри	– розвиток цифрових платформ співпраці між стейкхолдерами – зміна управлінської культури в бік горизонтальних взаємодій	– імплемента-ція інструментів цифрового форсайту та моделювання – розбудова потенціалу цифрової резилієнтності

* *Джерело:* розробка автора.

2) Інституційний підхід, натомість, зосередиться на аналізі регуляторних прогалин та інституційних вразливостей, які зробили можливою таку атаку: він може ініціювати перегляд та зміцнення формальних правил та процедур забезпечення кібербезпеки – від законодавства про захист даних до галузевих стандартів безпеки. Але такий підхід ризикує бути надто повільним та забюрократизованим в умовах динамічних гібридних загроз.

3) Мережевий підхід в цьому випадку наголосить на необхідності скоординованої відповіді на атаку з боку всіх зацікавлених сторін – державних органів, приватного бізнесу, експертного співтовариства, громадянського суспільства: він може ініціювати створення ситуативних центрів та платформ обміну інформацією для швидкого реагування на інциденти. Але такий підхід може зіткнутися з проблемами міжвідомчої конкуренції та недовіри між стейкхолдерами.

4) Нарешті, проактивний підхід зосередиться на превентивній ідентифікації та нейтралізації потенційних загроз: він може передбачати регулярне проведення кібернавчань, стрес-тестування систем, розвиток потенціалу стратегічного передбачення кіберзагроз. В довгостроковій перспективі такий підхід спрямований на розбудову цифрової резилієнтності держави, економіки та суспільства до шоків та збурень гібридного характеру.

На практиці найбільш ефективним є комплексне використання всіх чотирьох підходів з урахуванням конкретного контексту та динаміки загроз. Наприклад, на етапі невідкладного реагування на кібератаку критично важливими є інструменти неокласичного (оцінка збитків) та мережевого (координація стейкхолдерів) підходів. У середньостроковій перспективі на перший план виходить інституційний підхід з акцентом на удосконаленні регуляторного середовища, а в довгостроковому горизонті ключову роль відіграє проактивний підхід, спрямований на стратегічну адаптацію до ландшафту майбутніх гібридних загроз. Таким чином, чотири методологічні підходи не є взаємовиключними альтернативами, а скоріше комплементарними перспективами, кожна з яких робить свій внесок у формування цілісної та адаптивної системи економічної безпеки держави. Їх синергетичне поєднання дозволяє сформувати багаторівневу та багатовимірну стратегію протидії гібридним загрозам, яка є одночасно і реактивною (швидко реагує на безпосередні виклики), і проактивною (працює на упередження та формування контексту безпеки). Головним викликом для публічного управління в цьому контексті стає розвиток інституційної спроможності та культури міжвідомчої та міжсекторальної взаємодії, необхідної для ефективної імплементації такої комплексної стратегії.

Ефективна протидія гібридним загрозам економічній безпеці держави вимагає комплексного та адаптивного використання методологічних підходів, які було розглянуто вище: неокласичного, інституційного, мережевого та проактивного. Кожен з них робить свій внесок у розуміння природи гібридних викликів та формування релевантних механізмів реагування. На практиці це означає поєднання інструментів швидкого відновлення ринкової рівноваги, зміцнення інституційної інфраструктури безпеки, розбудови колаборативних екосистем стейкхолдерів та стратегічного передбачення ландшафту загроз. Нижче буде

розглянуто, як цей комплексний підхід реалізується в європейському досвіді протидії гібридним загрозам та які уроки з нього може винести Україна.

Варто зазначити, що гібридні загрози для економічної безпеки мають комплексний та багатовимірний характер. Вони можуть включати торговельно-економічні війни, фінансові санкції, маніпулювання енергетичними ринками, кібератаки на критичну інфраструктуру, промислове шпигунство тощо. Ці загрози експлуатують вразливості та взаємозалежності глобалізованої економіки, розмиваючи межі між зовнішніми та внутрішніми викликами. Відповідно, протидія їм вимагає комплексного та адаптивного підходу, що поєднує інструменти різних методологічних парадигм.

З точки зору неокласичного підходу, ключовим завданням є забезпечення стійкості економіки до шоків та збурень, спричинених гібридними атаками. Це передбачає розвиток механізмів ринкової адаптації, таких як диверсифікація торговельних партнерів, розвиток внутрішнього виробництва, формування стратегічних резервів критичної сировини тощо. Наприклад, у відповідь на російські енергетичні маніпуляції та зростання цін на газ, багато країн ЄС (Німеччина, Італія, Франція) активізували політику розвитку відновлюваної енергетики та пошуку альтернативних постачальників [23]. Це дозволило зменшити залежність від російського імпорту та стабілізувати енергетичні ринки.

Водночас, інституційний підхід наголошує на важливості розбудови ефективної регуляторної інфраструктури, здатної протидіяти гібридним загрозам. Це може включати посилення антимонопольного законодавства для запобігання економічній концентрації, вдосконалення системи експортного контролю для протидії передачі чутливих технологій, розвиток механізмів скринінгу іноземних інвестицій в стратегічні сектори тощо. Показовим прикладом є ухвалення в ЄС у 2019 році Регламенту про скринінг прямих іноземних інвестицій [9]. Він створює правову рамку для моніторингу та потенційного блокування інвестицій, що становлять ризик для безпеки та громадського порядку. Багато країн ЄС (Франція, Німеччина, Італія, Польща) вже імплементували цей механізм на національному рівні.

Мережевий підхід, в свою чергу, фокусується на розвитку колаборативних форматів протидії гібридним загрозам, що залучають недержавних стейкхолдерів. Це особливо важливо в контексті захисту критичної економічної інфраструктури, значна частина якої перебуває в приватній власності. Наприклад, після серії кібератак на енергетичні та фінансові компанії ЄС, у 2016 році була створена Мережа організацій з кібербезпеки в енергетиці (ENCS) [10]. Вона об'єднує операторів інфраструктури, регуляторів, експертів та представників індустрії задля обміну інформацією, розробки стандартів безпеки та координації дій з кіберзахисту.

Нарешті, проактивний підхід до економічної безпеки передбачає розвиток спроможностей стратегічного передбачення та превентивної адаптації до гібридних загроз. Тут показовим є досвід Фінляндії, яка однією з перших в ЄС запровадила систему комплексної оцінки безпекових ризиків (Comprehensive Security Assessments) [11]. Ці оцінки проводяться щорічно із залученням ши-

рокого кола державних та недержавних акторів і дозволяють ідентифікувати потенційні гібридні загрози на ранніх стадіях. Їх результати використовуються для коригування стратегічних документів (Стратегія національної безпеки, Стратегія кібербезпеки тощо) та розробки превентивних заходів.

Цікавим також є приклад Естонії, яка після масштабних кібератак з боку Росії у 2007 році перетворилась на європейського лідера з розвитку цифрової економіки та електронного врядування [8]. Естонія інвестувала значні ресурси в захист своєї цифрової інфраструктури, розвиток технологічного сектору та цифрових компетенцій населення. Це дозволило не лише мінімізувати ризики кібератак, але й стимулювати інноваційний розвиток та міжнародну конкурентоспроможність країни.

Аналізуючи представлений досвід використання різних методологічних підходів до протидії гібридним загрозам, для України у перспективі найближчих 2-3 років можна виділити кілька важливих стратегічних напрямків покращення економічної безпеки.

1) По-перше, критично важливим є формування багаторівневої системи реагування на гібридні загрози, яка б поєднувала механізми швидкого відновлення (як у випадку з диверсифікацією енергопостачання в ЄС) з довгостроковими інституційними змінами (як впровадження скринінгу іноземних інвестицій), при цьому особливу увагу слід приділити синхронізації зусиль різних відомств та створенню єдиного координаційного центру за прикладом фінської моделі комплексної оцінки безпекових ризиків.

2) По-друге, враховуючи досвід країн ЄС, Україні необхідно суттєво посилити залучення приватного сектору до системи економічної безпеки через створення галузевих платформ обміну інформацією та спільного реагування на загрози, подібних до європейської Мережі організацій з кібербезпеки в енергетиці (ENCS).

3) По-третє, надзвичайно важливим є розвиток проактивних механізмів виявлення та нейтралізації гібридних загроз, включаючи регулярні стрес-тестування критичної інфраструктури, формування стратегічних резервів та розбудову системи раннього попередження, що дозволить підвищити стійкість економіки до потенційних шоків та криз.

4) По-четверте, в умовах післявоєнної відбудови особливого значення набуває інтеграція механізмів економічної безпеки в загальну архітектуру державного управління через впровадження єдиних стандартів, процедур та протоколів реагування, що має супроводжуватися розвитком відповідних компетенцій у державних службовців та створенням культури міжвідомчої співпраці.

Як де все це відображається станом як є зараз в Україні і на Україну? Для України ці уроки європейського досвіду мають значення з огляду на тривалу гібридну агресію з боку Росії. З одного боку, Україна вже розвиває окремі елементи комплексної системи економічної безпеки. Наприклад, після торговельних обмежень з боку РФ Україна суттєво диверсифікувала структуру експорту, переорієнтувавшись на ринки ЄС та Азії. Розпочато процес інтеграції української енергосистеми з європейською ENTSO-E, що зменшить залежність від росій-

ських енергоресурсів. На законодавчому рівні ухвалені важливі документи, такі як Стратегія національної безпеки, Стратегія кібербезпеки тощо. Водночас, ці кроки поки що не складаються в цілісну проактивну модель економічної безпеки, здатну ефективно протидіяти гібридним загрозам. Ключовими напрямами її розбудови, з урахуванням європейських практик, можуть бути:

1) Розвиток системи багаторівневого стратегічного планування економічної безпеки із залученням державних та недержавних стейкхолдерів. За аналогією з фінським досвідом, доцільно запровадити регулярний процес комплексних оцінок безпекових ризиків, результати яких інтегруватимуться в цикл формування політики.

2) Удосконалення законодавства для протидії економічним інструментам гібридних впливів. Зокрема, це може включати посилення механізмів контролю за іноземними інвестиціями в стратегічні сектори, запровадження санкційної політики проти юридичних та фізичних осіб, причетних до гібридної агресії проти України тощо.

3) Розвиток державно-приватного партнерства у сфері захисту критичної економічної інфраструктури, особливо в енергетиці, транспорті, телекомунікаціях та фінансовому секторі. Це може передбачати створення галузевих центрів обміну інформацією про гібридні загрози, розробку спільних протоколів реагування на інциденти, проведення регулярних навчань із залученням державних та приватних операторів інфраструктури.

4) Інвестиції в розвиток цифрової економіки, кіберзахисту та технологічних інновацій як драйверів довгострокової економічної стійкості. Тут важливо поєднувати економічні стимули для інноваційного бізнесу, розвиток цифрових компетенцій населення та зміцнення інституційної спроможності держави з управління цифровою трансформацією. Естонський досвід електронного врядування та цифрової дипломатії може бути особливо корисним в цьому контексті.

Але тут слід критично визнати: реальне запровадження європейського досвіду протидії гібридним загрозам в українських реаліях 2025 року стикається з серйозними викликами, пов'язаними з тривалою війною та невизначеністю щодо її завершення. Разом з тим, саме зараз критично важливо розпочати стратегічне планування повоєнного відновлення України з урахуванням не лише поточних, але й потенційних загроз.

По-перше, досвід країн Балтії, які також стикаються з ризиком повторної агресії з боку РФ, показує важливість проактивного зміцнення стійкості ключових секторів економіки та суспільства. Тут можуть бути корисними такі інструменти, як регулярні комплексні оцінки ризиків (за аналогією з фінською практикою) та розробка галузевих планів забезпечення безперервності бізнесу (business continuity planning). Наприклад, для критичної інфраструктури (енергетики, транспорту, телекомунікацій) це може передбачати створення резервних потужностей, диверсифікацію постачальників, регулярні тренування з кризового менеджменту тощо. Для фінансового сектору – це розвиток механізмів стрес-тестування та планів відновлення після шоків. А от на загальнодержавному рівні доцільно розробити рамковий документ (на кшталт Стратегії наці-

ональної стійкості), який би задавав цільові орієнтири та координував зусилля різних стейкхолдерів. Методологічно цей процес може спиратись на поєднання неокласичного (оцінка потенційних збитків та необхідних резервів) та інституційного (розвиток регуляторної бази) підходів.

По-друге, в умовах гібридних загроз критично важливою є розбудова ефективної моделі державно-приватного партнерства у сфері безпеки. Бізнес володіє значною частиною інфраструктурних та технологічних активів, а також унікальними компетенціями з управління ризиками. Тому його залучення до процесів стратегічного планування та оперативної координації зусиль з протидії загрозам має бути максимальним. Європейський досвід пропонує різні організаційні формати такого партнерства: від галузевих та кроссекторальних платформ обміну інформацією (Information Sharing and Analysis Centers) до спільних державно-приватних проєктів з розвитку інновацій та цифрової трансформації. Для України актуальним може бути створення національного Центру передового досвіду з протидії гібридним загрозам (за аналогією з європейським Hybrid CoE) як платформи для багатосторонньої взаємодії держави, бізнесу, наукових та експертних кіл. Це відповідає мережевому підходу до економічної безпеки, який наголошує на важливості колаборативних рішень в умовах складних взаємозалежностей.

По-третє, повоєнне відновлення відкриває для України унікальне вікно можливостей для інноваційного стрибка та цифрової трансформації економіки. Інвестиції в розвиток сучасної цифрової інфраструктури (від оптоволоконних мереж до центрів обробки даних) мають стати пріоритетом національних та міжнародних програм реконструкції. Цифровізація не лише підвищить ефективність та прозорість економічних процесів, але й зменшить вразливість до традиційних гібридних впливів. Водночас вона вимагатиме комплексних рішень з кібербезпеки як на рівні технологій, так і регуляторної бази та компетенцій. Тут може бути корисним досвід Естонії та інших цифрових лідерів ЄС зі створення захищених екосистем електронних послуг (на кшталт X-Road) та колаборативних моделей управління кіберризиками (Trust Services). На методологічному рівні цей курс відповідає проактивному підходу до економічної безпеки, який робить ставку на стратегічну адаптацію та формування контексту через інноваційний розвиток.

Безумовно, реалізація окреслених напрямів вимагатиме політичної волі, ресурсів та часу. Але саме зараз Україна має унікальний шанс, спираючись на підтримку міжнародних партнерів, закласти фундамент нової моделі економічної безпеки, більш стійкої до гібридних впливів. І європейський досвід тут може стати цінним джерелом практик та уроків, які потрібно творчо адаптувати до українських реалій.

Далі розглянемо ефективність існуючих механізмів державного регулювання економічної безпеки України крізь призму чотирьох методологічних підходів, які ми обговорили раніше – неокласичного, інституційного, мережевого та проактивного. Це дозволить нам виявити прогалини та обґрунтувати напрями трансформації цих механізмів з урахуванням викликів, які стоять перед Україною в найближчі роки.

Почнемо з неокласичного підходу, який акцентує увагу на забезпеченні макроекономічної стабільності та ринкової рівноваги як фундаменту економічної безпеки. З цієї точки зору, Україна за останні роки досягла певного прогресу. Зокрема, після кризи 2014-2015 років вдалося стабілізувати валютний курс, приборкати інфляцію, перезапустити економічне зростання. Важливу роль тут відіграли реформи в монетарній політиці (перехід до інфляційного таргетування) та фіскальній консолідації (зменшення дефіциту бюджету). Водночас, ці здобутки залишаються крихкими перед обличчям нових шоків, таких як пандемія COVID-19 чи ескалація безпекових ризиків. Тому в наступні роки критично важливо буде забезпечити стійкість макрофінансової стабільності через розбудову фіскальних буферів, зміцнення незалежності центрального банку, розвиток ринків капіталу тощо.

З позиції інституційного підходу, ключовим фактором економічної безпеки є якість формальних та неформальних «правил гри», які структурують економічні взаємодії. Тут Україна стикається з серйозними викликами, пов'язаними з недосконалістю ринкових інститутів, корупцією, недовірою до судової системи, регуляторним тиском на бізнес тощо. Хоча за останнє десятиліття було ухвалено низку важливих законів та запроваджено нові антикорупційні органи (НАБУ, САП, ВАКС), їх вплив на реальні практики поки що обмежений, а інколи – і відверто сумнівний за підсумками 2024 року (враховуючи пряму залежність від окремих органів (напр., НАБУ) від американських урядових грошей і замалу кількість доведених до судового вироку кримінальних справ). Тому наступні роки (напр., 2025-2027 рр) мають стати періодом інтенсивної «інституційної терапії»: дуже глибинних і системних реформ в Україні, спрямованих на зміцнення верховенства права, захист прав власності, забезпечення рівних правил гри для бізнесу, дебюрократизацію економіки. Особливу увагу варто приділити «цифровізації» регуляторного середовища, що дозволить підвищити його прозорість та зменшити корупційні ризики.

Мережевий підхід до економічної безпеки наголошує на важливості взаємодії та координації зусиль різних стейкхолдерів – держави, бізнесу, громадянського суспільства. В Україні поки що переважають ієрархічні та фрагментовані моделі управління, з низьким рівнем довіри між різними групами інтересів. Хоча в останні роки з'явились певні платформи для діалогу (наприклад, Національна рада реформ), їх вплив на процес вироблення політики залишається обмеженим. Тому в найближчій перспективі важливо розбудовувати інклюзивні та колаборативні механізми координації – як на національному рівні (через удосконалення консультативних процедур), так і на рівні окремих секторів та екосистем (через розвиток галузевих асоціацій, кластерів, мереж трансферу технологій тощо). Саме у взаємодії різних акторів народжуються інноваційні рішення, здатні посилити адаптивність та стійкість економіки перед лицем гібридних загроз.

Нарешті, проактивний підхід до економічної безпеки акцентує увагу на стратегічному передбаченні та формуванні майбутнього контексту. На жаль, система державного стратегічного планування в Україні залишається фрагментованою та реактивною, орієнтованою на короткостроковий горизонт. Хоча розробляються численні стратегії та програми, їх виконання страждає від недофінансування, нескоординованості та політичної волатильності. Тому в наступні роки критично

важливо запровадити цілісну систему стратегічного управління, яка б базувалась на ґрунтовному форсайті безпекових, технологічних, соціальних трендів та поєднувала б планування з механізмами імплементації. Одним з ключових елементів цієї системи має стати розвиток інститутів та інструментів для роботи з майбутнім – від мережі форсайт-центрів до регулярних сценарних вправ за участю широкого кола стейкхолдерів. Це дозволить сформувати спільне бачення викликів та можливостей, напрацювати варіанти політики, підвищити готовність суспільства до змін. Безумовно, окреслені напрями трансформації механізмів регулювання економічної безпеки не вичерпують усього комплексу необхідних змін. Серед інших важливих аспектів варто згадати реформу сектору безпеки та оборони, диверсифікацію енергетичних ринків, розвиток критичної інфраструктури, зміцнення соціальної згуртованості тощо. Але саме поєднання зусиль з макроекономічної стабілізації, інституційної розбудови, мережевої співпраці та адаптації здатне закласти міцний фундамент для довгострокової стійкості та успішності української економіки.

Для узагальнення викладеного аналізу пропонуємо звести ключові висновки в матрицю (таблиця 2).

Таблиця 2

Оновлення концептуальних основ модернізації системи державного регулювання економічної безпеки сучасної України на основі 4-х головних існуючих методологічних підходів до економічної безпеки

Table 2

Updating the Conceptual Foundations for Modernizing the State Regulation System of Economic Security in Contemporary Ukraine Based on Four Main Existing Methodological Approaches to Economic Security

Методологічний підхід	Фокус аналізу	Стан в Україні	Напрями трансформації
Неокласичний	Макроекономічна стабільність	Відносна стабілізація, але вразливість до шоків	Розбудова фіскальних буферів, реформа фінансових ринків
Інституційний	Якість «правил гри»	Інституційні пастки, недовіра до регуляторів	Зміцнення верховенства права, дерегуляція, «цифровізація» середовища
Мережевий	Взаємодія стейкхолдерів	Фрагментація, брак координації	Розвиток інклюзивних платформ діалогу, колаборативних екосистем
Проактивний	Стратегічне передбачення	Короткостроковість, реактивність планування	Розбудова потенціалу та інструментів роботи з майбутнім

* *Джерело:* розробка автора.

Ця матриця (таблиця 2) не лише систематизує результати аналізу, але й задає орієнтири для подальших досліджень та практичних кроків з розвитку системи економічної безпеки України. В прикладній площині вона може бути використана для деталізації пріоритетів та завдань в рамках стратегічних доку-

ментів національного рівня, таких як Стратегія економічної безпеки чи Стратегія розвитку фінансового сектору. Водночас вона окреслює потребу в подальшому теоретичному та методологічному опрацюванні проблематики – зокрема, в напрямку розробки комплексних показників оцінки економічної безпеки, вдосконалення інструментів моделювання та стрес-тестування, обґрунтування оптимальних регуляторних механізмів в умовах гібридних загроз тощо.

Як науковець, критично сприймаючи ці пропозиції щодо трансформації механізмів державного регулювання економічної безпеки України, варто зазначити, що їх успішна реалізація потребує дійсно комплексного і складного підходу та врахування реальних умов 2025 року в умовах великої невизначеності для країни і світу. Розглянемо знизу догори запропоновані напрями та умови їх втілення.

На мою думку, найбільш реалістичним видається впровадження проактивного підходу через розбудову системи стратегічного передбачення, і це потребує найменше ресурсів і може бути реалізовано навіть в умовах обмеженого бюджету через створення мережі аналітичних центрів та експертних платформ. Ключовою умовою успіху тут є політична воля керівництва держави та готовність враховувати експертні рекомендації при прийнятті рішень. Тут важливим фактором підтримки може стати міжнародна технічна допомога та залучення провідних світових аналітичних центрів (think tanks) до розбудови української системи форсайту.

Складнішим є впровадження мережевого та інституційного підходів, оскільки вони вимагають глибинних змін у культурі взаємодії між державою, бізнесом та громадянським суспільством. Реалізація цих напрямів можлива лише за умови успішного просування судової реформи, подолання корупції та розвитку цифрової інфраструктури: у такому разі критично важливою є підтримка міжнародних партнерів (особливо ЄС) у впровадженні кращих практик регулювання та створенні ефективних майданчиків для діалогу. Додатковим стимулом може стати прогрес України у процесі євроінтеграції, який вимагатиме адаптації регуляторних механізмів до європейських стандартів.

Найбільш амбітним є неокласичний напрям, спрямований на забезпечення макроекономічної стабільності. Його реалізація в умовах 2025 року залежатиме від успішності післявоєнної відбудови, доступу до міжнародного фінансування та здатності утримати макрофінансову стабільність. Ключовими факторами підтримки тут мають стати програми МВФ та інших міжнародних фінансових інституцій, а також координація монетарної та фіскальної політики. Важливою передумовою є також збереження незалежності НБУ та продовження реформ фінансового сектору.

Висновки і перспективи подальших досліджень. На основі проведених вище у статті досліджень можна зробити такі декілька висновків.

1) Кожен з 4-х розглянутих методологічних підходів має свої особливості, переваги та обмеження, які визначають його релевантність в умовах гібридних загроз та цифрових трансформацій. Неокласичний підхід, фокусуючись на ринковій рівновазі, не повною мірою враховує нелінійність та непередбачуваність гібридних впливів, але водночас він відкриває можливості для динамічного моніторингу параметрів безпеки на основі технологій Big Data та машинного

навчання. Інституційний підхід акцентує увагу на якості регуляторного середовища, але може недооцінювати роль неформальних інститутів, а в епоху «цифри» він передбачає активну цифровізацію регуляторних механізмів та використання технологій довіри, таких як блокчейн. Мережевий підхід враховує складні взаємозалежності між безпековими акторами, але може генерувати ризики розмивання відповідальності, і його імплементація в публічному управлінні вимагає розвитку цифрових платформ співпраці стейкхолдерів та зміни управлінської культури в бік горизонтальних взаємодій. Нарешті, проактивний підхід орієнтує на передбачення та формування безпекового контексту, але потребує розвинених аналітичних компетенцій, але в умовах цифровізації він передбачає використання інструментів цифрового форсайту, моделювання загроз, а також розбудову потенціалу цифрової резилієнтності держави та суспільства.

2) Європейський досвід протидії гібридним загрозам демонструє важливість комплексного поєднання різних методологічних підходів інструментів: від класичних ринкових та інституційних до інноваційних мережевих та форсайтних. В українському контексті це означає необхідність цілісного осмислення архітектури економічної безпеки з урахуванням національної специфіки та євроінтеграційного вектору розвитку. Ключовим викликом на цьому шляху є розбудова спроможності державних інституцій формувати проактивну та адаптивну політику на основі багаторівневої співпраці зі стейкхолдерами.

3) Аналіз європейського досвіду протидії гібридним загрозам економічній безпеці та його проєкція на українські реалії дозволяє зробити кілька важливих висновків. По-перше, ефективна модель національної економічної стійкості в умовах гібридних впливів має спиратись на проактивний, багаторівневий та адаптивний підхід. Це передбачає розвиток інструментів стратегічного передбачення та планування з урахуванням повного спектру ризиків, інституціалізацію механізмів міжвідомчої та міжсекторальної координації, а також інвестиції в потенціал довгострокової адаптивності через інноваційний розвиток. По-друге, ключовим драйвером безпекових трансформацій має стати розбудова моделі державно-приватного партнерства, яка дозволить мобілізувати ресурси, компетенції та мережі бізнесу і громадянського суспільства для спільного творення стійкості. Нарешті, цифрова трансформація та технологічні інновації мають розглядатись не лише як інструменти підвищення ефективності, але і як стратегічні засоби зміцнення економічного суверенітету та здатності протистояти гібридним впливам. В сукупності, ці висновки окреслюють контури цілісної філософії економічної безпеки, яка може стати орієнтиром для України на шляху повоєнного відновлення та посткризової трансформації.

4) Аналіз запропонованих напрямів трансформації механізмів державного регулювання економічної безпеки України демонструє необхідність їх поетапного впровадження з урахуванням наявних ресурсів та інституційної спроможності держави. Найбільш перспективним видається початок з розбудови системи стратегічного передбачення та проактивного планування, що створить фундамент для подальших змін. Це дозволить сформувати чітке бачення викликів та можливостей, необхідне для впровадження більш ресурсомістких реформ

у сфері інституційної розбудови та макроекономічної стабілізації. Критично важливим елементом успіху є синхронізація внутрішніх зусиль з підтримкою міжнародних партнерів, особливо в контексті євроінтеграційних процесів. При цьому особливу увагу слід приділити розвитку цифрових інструментів та платформ взаємодії, які можуть стати каталізатором позитивних змін навіть в умовах обмежених ресурсів. Такий покроковий підхід, що поєднує стратегічне бачення з прагматичною оцінкою можливостей, здатен забезпечити поступовий, але стійкий прогрес у зміцненні системи економічної безпеки України.

*Перспективи подальших досліджень д*ля сучасної України мають зосередитися на розробці методології комплексної оцінки ефективності механізмів державного регулювання економічної безпеки в умовах гібридних загроз, включаючи створення системи динамічних індикаторів та предиктивних моделей на основі технологій штучного інтелекту. Особливої уваги потребує дослідження синергетичного ефекту від поєднання різних методологічних підходів у практиці державного управління, зокрема через призму цифрової трансформації регуляторних механізмів та розвитку інструментів державно-приватного партнерства у сфері економічної безпеки. Актуальним напрямом наукових розвідок також має стати вивчення можливостей адаптації успішних європейських практик протидії гібридним загрозам до українських реалій післявоєнного відновлення, з особливим фокусом на розбудову інституційної спроможності та цифрової резилієнтності держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Власюк О. С., Кононенко С. В. Кремлівська агресія проти України: роздуми в контексті війни. *Економіка України*. 2017, № 9, с. 3-18. DOI: https://doi.org/10.15407/economyukr.2017.09.003

2. Громов, С. О. Сучасна сутність і склад механізму публічного регулювання корпоратизації великих державних підприємств у сфері транспортної інфраструктури. *Теорія та практика державного управління*, 2204, № 1(78), с. 136-154. DOI: https://doi.org/10.26565/1727-6667-2024-1-08

3. Дунаєв, І., Громов, С. Досягнення і проблеми використання ринкових підходів в сучасному публічному врядуванні для реформування українських державних корпорацій. *Актуальні проблеми державного управління*, 2024, № 1(64), с. 6-25. DOI: https://doi.org/10.26565/1684-8489-2024-1-01. DOI https://periodicals.karazin.ua/apdu/article/view/24058

4. Світова гібридна війна: український фронт / За заг. ред. В. П. Горбуліна. Національний інститут стратегічних досліджень. Київ: НІСД, 2017.

5. Bazilian M., Goldthau A., Westphal K. Model or Ally? How Europe Can Lead on Energy and Climate. 2019. URL: https://surl.li/gktfvv

6. Casimir Pulaski Foundation. How to Defend Against Hybrid Threats. 2021. URL: https://pulaski.pl/wp-content/uploads/2021/11/FOB16_EN.pdf

7. DefencesCoop. NATO seeks to confront the growing 'pressure of hybrid war'. 2024. URL: URL: https://defensescoop.com/2024/07/16/nato-confront-growing-pressure-hybrid-war-russia-china/

8. e-Estonia. (n.d.). We have built a digital society and so can you. URL: https://e-estonia.com/

9. European Commission. EU foreign investment screening regulation enters into force. 2019. URL: https://policy.trade.ec.europa.eu/news/eu-foreign-investment-screening-regulation-enters-force-2020-10-11_en

10. European Network for Cyber Security. (n.d.). European Network for Cyber Security (ENCS). URL: https://encs.eu/

11. Finnish Government. Finland's Cyber security Strategy. 2019. URL: https://turvallisuuskomitea.fi/en/finlands-cyber-security-strategy/

12. Fjäder C. The nation-state, national security and resilience in the age of globalisation. Resilience, 2014, № 2(2), с. 114–129. URL: https://www.tandfonline.com/doi/full/10.1080/21693293.2014.914771

13. Fuerth L. S. (2009). Foresight and anticipatory governance. *Foresight*, 2009, № 11(4), с. 14–32. DOI: https://doi.org/10.1108/14636680910982412

14. Hybrid CoE. Hybrid CoE Paper 12: Deterring hybrid threats: Towards a fifth wave of deterrence theory and practice. 2020. URL: https://www.hybridcoe.fi/wp-content/uploads/2022/03/20220331-Hybrid-CoE-Paper-12-Fifth-wave-of-deterrence-WEB.pdf

15. International Centre for Defence and Security. Russia's Hybrid War in Ukraine. 2022. URL: https://icds.ee/en/russias-hybrid-war-in-ukraine-lessons-for-baltic-security-and-nato/

16. Komljenovic D., & Andersson J. Hybrid threats and the critical infrastructure protection challenge. Technology in Society, 2021, № 66, 101674. DOI: https://doi.org/10.1016/j.techsoc.2021.101674

17. Linkov I., Trump B. Resilience and hybrid threats: Security and integrity for the digital world. *IOS Press*. 2019. DOI: https://doi.org/10.3233/978-1-61499-918-8. ISBN 1643680226. URL: https://surl.li/ecydsq

18. NATO ENSEC COE. Hybrid Warfare Against Critical Energy Infrastructure. 2022. URL: https://www.enseccoe.org/wp-content/uploads/2024/01/2021-03-2.pdf

19. North D. C. Institutions. Journal of Economic Perspectives, 1991, № 5(1), с. 97–112. DOI: https://doi.org/10.1257/jep.5.1.97

20. OECD. Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity, OECD Publishing, Paris, 2024. DOI: https://doi.org/10.1787/d909ff7a-en. URL: https://surl.li/mgutzb

21. OFSI. National Risk Assessment of Proliferation Financing. 2021. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1020695/National_risk_assessment_of_proliferation_financing.pdf

22. Sperling J. The Politics of Resilience and Transatlantic Order: Enduring Crisis? Routledge. 2022. URL: https://www.taylorfrancis.com/books/oa-edit/10.4324/9781003007739/politics-resilience-transatlantic-order-james-sperling

23. Tagliapietra S. REPowerEU: Will EU countries really make it work? Bruegel, 2022. URL: https://www.bruegel.org/blog-post/repowereu-will-eu-countries-really-make-it-work

24. Tamošiūnienė R., Munteanu C. Current research approaches to economic security. Paper presented at the 1st International Conference on Business Management, Valencia, Spain, 2015. DOI: https://doi.org/10.4995/ICBM.2015.1537. URL: https://surl.li/igthtm

25. Trump B. The Science and Practice of Resilience. 2019. DOI: 10.1007/978-3-030-04565-4.

26. Wood D. M., Wright D. Before and After Snowden. *Surveillance & Society*. 2015, № 13(2), с. 132–138. DOI: https://doi.org/10.24908/ss.v13i2.5710

27. World Economic Forum. Global Risks Report 2023. URL: https://www.weforum.org/reports/global-risks-report-2023

Стаття надійшла до редакції 18.11.2024
Стаття рекомендована до друку 17.12.2024

Denys Papyrin, PhD-student at the Department of economic policy and management
Educational and Scientific Institute «Institute of Public Administration»
Educational and Scientific Institute «Institute of Public Administration»,
V. N. Karazin Kharkiv National University, 4 Svobody Sq., Kharkiv, 61022, Ukraine
ORCID ID: http://orcid.org/ 0009-0001-2292-6483 e-mail: papyrin.denys@ukr.net

TRANSFORMATION OF STATE REGULATION MECHANISMS FOR ECONOMIC SECURITY AMID MODERN HYBRID THREATS: EUROPEAN EXPERIENCE AND UKRAINIAN REALITIES

Abstract. This article examines the theoretical-methodological foundations and practical aspects of transforming state economic security regulation mechanisms in the context of modern hybrid threats. Through systematic analysis, four key methodological approaches to ensuring state economic security are identified and critically analyzed: neoclassical, institutional, network-based, and proactive. The study reveals their distinct characteristics, advantages, and limitations in countering hybrid threats. The research analyzes European experience in transforming economic security mechanisms, particularly examining practices from leading EU countries in developing resilient security frameworks and innovative response mechanisms to hybrid challenges. The findings indicate a trend toward comprehensively integrating various methodological approaches and tools, ranging from classical market and institutional mechanisms to innovative network-based and foresight instruments. Based on comparative analysis of European experience and Ukrainian realities, the paper establishes conceptual foundations for modernizing Ukraine's state economic security regulatory system. The study proposes a regulatory mechanism transformation matrix that accounts for current conditions and defines priority directions for change within each methodological approach. The research argues for phased implementation of proposed mechanisms, considering available resources and state institutional capacity. Special attention is given to digital transformation and public-private partnerships as key drivers for modernizing the economic security system, with particular focus on developing resilient institutional frameworks and adaptive response capabilities. The article outlines prospects for further research, particularly regarding development of comprehensive methodology for evaluating regulatory mechanism effectiveness and adapting European practices to Ukrainian post-war recovery realities, emphasizing the importance of building sustainable and resilient security architectures in the face of evolving hybrid threats.

Keywords: *economic security, state regulation mechanisms, hybrid threats, digital transformation, public-private partnership, European experience, strategic planning, proactive management, post-war recovery.*

In cites: Papyrin, D. O. (2024). Transformation of state regulation mechanisms for economic security amid modern hybrid threats: European experience and Ukrainian realities. *Theory and Practice of Public Administration*, 2 (79), 342–362. http://doi.org/10.26565/1727-6667-2024-2-17 [in Ukrainian].

REFERENCES:

1. Vlasiuk, O. S., & Kononenko, S. V. (2017). Kremlin aggression against Ukraine: Reflections in the context of war. Economy of Ukraine, (9), 3-18. https://doi.org/10.15407/economyukr.2017.09.003 [in Ukrainian].

2. Hromov, S. O. (2024). Modern essence and composition of the public regulation mechanism for corporatization of large state enterprises in transport infrastructure. *Theory and Practice of Public Administration*, 1(78), 136-154. DOI: https://doi.org/10.26565/1727-6667-2024-1-08 [in Ukrainian].

3. Dunaiev, I., & Hromov, S. (2024). Achievements and problems of using market approaches in modern public governance for reforming Ukrainian state corporations. *Actual Problems of Public Administration*, 1(64), 6-25. DOI: https://doi.org/10.26565/1684-8489-2024-1-01 [in Ukrainian].

4. Horbulin, V. P. (Ed.). (2017). World hybrid war: Ukrainian front. National Institute for Strategic Studies [in Ukrainian].

5. Bazilian, M., Goldthau, A., & Westphal, K. (2019). Model or ally? How Europe can lead on energy and climate. https://surl.li/gktfvv

6. Casimir Pulaski Foundation. (2021). How to defend against hybrid threats. URL: https://pulaski.pl/wp-content/uploads/2021/11/FOB16_EN.pdf

7. DefencesCoop. (2024). NATO seeks to confront the growing 'pressure of hybrid war'. URL: https://defensescoop.com/2024/07/16/nato-confront-growing-pressure-hybrid-war-russia-china/

8. e-Estonia. (n.d.). We have built a digital society and so can you. URL: https://e-estonia.com/

9. European Commission. (2019). EU foreign investment screening regulation enters into force. URL: https://policy.trade.ec.europa.eu/news/eu-foreign-investment-screening-regulation-enters-force-2020-10-11_en

10. European Network for Cyber Security. (n.d.). European Network for Cyber Security (ENCS). URL: https://encs.eu/

11. Finnish Government. (2019). Finland's cyber security strategy. URL: https://turvallisuuskomitea.fi/en/finlands-cyber-security-strategy/

12. Fjäder, C. (2014). The nation-state, national security and resilience in the age of globalisation. *Resilience*, 2(2), 114-129. URL: https://www.tandfonline.com/doi/full/10.1080/21693293.2014.914771

13. Fuerth, L. S. (2009). Foresight and anticipatory governance. *Foresight*, 11(4), 14-32. DOI: https://doi.org/10.1108/14636680910982412

14. Hybrid CoE. (2020). Hybrid warfare against critical energy infrastructure. URL: https://www.hybridcoe.fi/wp-content/uploads/2022/03/20220331-Hybrid-CoE-Paper-12-Fifth-wave-of-deterrence-WEB.pdf

15. International Centre for Defence and Security. (2022). Russia's hybrid war in Ukraine. URL: https://icds.ee/en/russias-hybrid-war-in-ukraine-lessons-for-baltic-security-and-nato/

16. Komljenovic, D., & Andersson, J. (2021). Hybrid threats and the critical infrastructure protection challenge. *Technology in Society*, 66, 101674. DOI: https://doi.org/10.1016/j.techsoc.2021.101674

17. Linkov, I., & Trump, B. (2019). Resilience and hybrid threats: Security and integrity for the digital world. *IOS Press*. DOI: https://doi.org/10.3233/978-1-61499-918-8

18. NATO ENSEC COE. (2022). Hybrid warfare against critical energy infrastructure. URL: https://www.enseccoe.org/wp-content/uploads/2024/01/2021-03-2.pdf

19. North, D. C. (1991). Institutions. *Journal of Economic Perspectives*, 5(1), 97-112. DOI: https://doi.org/10.1257/jep.5.1.97

20. OECD. (2024). Facts not fakes: Tackling disinformation, strengthening information integrity. *OECD Publishing*. DOI: https://doi.org/10.1787/d909ff7a-en

21. OFSI. (2021). National risk assessment of proliferation financing. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1020695/National_risk_assessment_of_proliferation_financing.pdf

22. Sperling, J. (2022). The politics of resilience and transatlantic order: Enduring crisis? *Routledge*. DOI: https://doi.org/10.4324/9781003007739

23. Tagliapietra, S. (2022). REPowerEU: Will EU countries really make it work? Bruegel. URL: https://www.bruegel.org/blog-post/repowereu-will-eu-countries-really-make-it-work

24. Tamošiūnienė, R., & Munteanu, C. (2015). Current research approaches to economic security. Paper presented at the 1st International Conference on Business Management, Valencia, Spain. DOI: https://doi.org/10.4995/ICBM.2015.1537

25. Trump, B. (2019). The science and practice of resilience. DOI: https://doi.org/10.1007/978-3-030-04565-4

26. Wood, D. M., & Wright, D. (2015). Before and after Snowden. *Surveillance & Society*, 13(2), 132-138. DOI: https://doi.org/10.24908/ss.v13i2.5710

27. World Economic Forum. (2023). Global risks report 2023. URL: https://www.weforum.org/reports/global-risks-report-2023

The article was received by the editors 18.11.2024
The article is recommended for printing 17.12.2024