МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХЕРСОНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ БІЗНЕСУ І ПРАВА
КАФЕДРА ЕКОНОМІКИ, МЕНЕДЖМЕНТУ ТА АДМІНІСТРУВАННЯ

СТРАТЕГІЧНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ В УМОВАХ ЦИФРОВІЗАЦІЇ

Кваліфікаційна робота (проєкт)
на здобуття ступеня вищої освіти «бакалавр»

Виконав: здобувач 4 курсу 10-471 групи
Спеціальність 051 Економіка
Освітньої програми: Економіка
Осіпов Олександр Русланович

Керівник: докторка економічних наук, професорка Ушкаренко Ю.В.
Рецензент: директор ПП «Інтер Склад», Сопін М.А.

Івано-Франківськ – 2026

ЗМІСТ

ВСТУП

Актуальність дослідження. Інтенсивна цифровізація економічних процесів супроводжується трансформаціями механізмів функціонування держави, фінансової системи та ринкових інститутів, які формують принципово новий контекст забезпечення економічної безпеки. Поширення інформаційних технологій, автоматизація управлінських рішень і залежність ключових секторів від цифрової інфраструктури посилюють вразливість національної економіки перед кіберзагрозами, які здатні порушувати стабільність фінансових потоків, функціонування критичних систем і довіру до державних інституцій. У результаті виникає потреба переосмислення теоретичних засад економічної безпеки з урахуванням нових ризиків, що мають комплексний і динамічний характер.

Особливо проблема посилилась в умовах воєнного протистояння, коли цифровий простір стає одним із ключових полів впливу на економічну стійкість держави. Кібероперації, інформаційні атаки та втручання в роботу фінансових і енергетичних систем здатні спричиняти значні економічні втрати та дестабілізувати внутрішні процеси. За таких обставин традиційні підходи до забезпечення економічної безпеки виявляються недостатньо ефективними, оскільки формувалися без урахування масштабності та складності цифрових загроз, що постійно еволюціонують.

Саме тому наукове обґрунтування оновлених підходів до забезпечення економічної безпеки в умовах цифрових загроз набуває вирішального значення для зміцнення національної безпеки та сталого розвитку.

Стан наукового дослідження. Проблематика формування економічної безпеки держави в умовах цифрової трансформації привертала значну увагу вітчизняних дослідників. Значний внесок у

розвиток відповідних підходів здійснили такі науковці, як Баглай Р., Бієвець А., Виговська О., Вишневський О., Городиський М., Дячек С., Живко З., Живко М., Занора В., Зачосова Н., Карчева Г., Копитко М., Козловський С., Краус Н., Лисяк О., Литвинчук І., Ляшенко В., Полчанов А., Руденко М., Середа В., Соколова Г., Черевко О. та інші, праці яких формують теоретичне підґрунтя для подальших досліджень.

Водночас динамічний розвиток цифрового середовища та загострення безпекових викликів, спричинених воєнними подіями, зумовлюють появу нових ризиків для національної економіки. У зв'язку з постійною трансформацією характеру загроз існуючі наукові підходи потребують подальшого переосмислення та поглиблення. Наявні напрацювання створюють важливу основу, проте сучасні умови вимагають розширення дослідницького поля, уточнення категоріального апарату та розроблення більш адаптованих моделей забезпечення економічної безпеки з урахуванням цифрового фактору.

Метою дослідження є обґрунтування теоретичних підходів та розроблення науково-практичних засад забезпечення економічної безпеки держави в умовах поширення цифрових загроз.

Відповідно до поставленої мети, можна запропонувати наступні **завдання:**

– охарактеризувати поняття, сутність та механізм забезпечення економічної безпеки держави;

– визначити вплив цифровізації на ключові складові економічної безпеки держави;

– здійснити аналіз чинників цифровізації та їх впливу на економічну безпеку України (динаміка показників та сучасні тенденції);

– проаналізувати вплив воєнного стану та кібератак рф на економічну безпеку України;

– запропонувати напрями зміцнення економічної безпеки України в умовах цифрових загроз;

– охарактеризувати формування ефективної державної політики та стратегічні механізми забезпечення економічної безпеки в умовах цифрової трансформації.

Об'єктом дослідження виступають суспільні відносини у сфері забезпечення економічної безпеки держави в умовах цифрової трансформації.

Предметом дослідження є теоретичні підходи, механізми та інструменти забезпечення економічної безпеки держави під впливом цифрових загроз.

Методи дослідження. Методологічну основу дослідження становлять загальнонаукові методи, застосування яких забезпечило досягнення поставленої мети та вирішення визначених завдань. Метод аналізу використано для вивчення сутності економічної безпеки держави та впливу цифрових загроз на її стан, що дозволило виокремити ключові проблемні аспекти. Синтез застосовано з метою поєднання отриманих результатів у цілісну систему теоретичних положень і висновків. Узагальнення сприяло формуванню комплексного бачення досліджуваної проблематики на основі опрацьованих наукових підходів. Метод порівняння використано для зіставлення різних теоретичних концепцій і підходів до забезпечення економічної безпеки в умовах цифровізації. Аналогія дала змогу виявити спільні риси між традиційними та сучасними загрозами економічній безпеці. Класифікація застосована для систематизації цифрових загроз та їх впливу на економічні процеси, що забезпечило структурованість дослідження.

Практичне значення одержаних результатів полягає у можливості використання запропонованих положень і рекомендацій органами державної влади при формуванні політики у сфері економічної безпеки, удосконаленні механізмів протидії цифровим загрозам, а також у впровадженні розроблених підходів у діяльність підприємств і установ з метою підвищення рівня їхньої стійкості до сучасних ризиків.

Структура роботи: Робота складається змісту, вступу, основної частини (трьох розділів, поділених на підрозділи), висновків та списку використаних джерел. Загальний обсяг курсової роботи становить 40 сторінок, список використаних джерел складає 25 найменувань.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ В УМОВАХ ЦИФРОВІЗАЦІЇ

1.1. Поняття, сутність та механізм забезпечення економічної безпеки держави

У сучасних умовах сила країни, добробут населення та динаміка її поступу, а відтак і рівень захищеності від загроз, значною мірою залежать від стану та ефективності функціонування економічної сфери.

Під національною безпекою держави розуміють спроможність соціуму завчасно ідентифікувати можливі загрози, здійснювати їх комплексну оцінку та застосовувати відповідні заходи для нейтралізації або мінімізації їх впливу, враховуючи наявний потенціал країни й довгострокові пріоритети розвитку, а також беручи до уваги міжнародну взаємодію у зазначеній сфері. Економічна безпека створює передумови для такого функціонування господарської системи, яке забезпечує належний рівень добробуту населення, сприяє всебічному розвитку особистості, підтримує соціально-економічну та військово-політичну рівновагу, а також протидіє як внутрішнім, так і зовнішнім викликам. Ефективно організований механізм гарантування економічної безпеки виступає ключовою передумовою стабільності соціально-економічного розвитку та збереження державного суверенітету.

На думку З. Живка, категорія національної безпеки втрачає зміст без урахування стійкості економічної системи та її здатності витримувати потенційні загрози внутрішнього й зовнішнього характеру, оскільки економічна складова належить до базових чинників життєдіяльності суспільства, державних інститутів і кожної особи [1, с. 124]. Аналізуючи питання національної безпеки, неможливо ігнорувати економічний вимір. Економічна безпека посідає провідне місце серед напрямів державної

політики у сфері гарантування безпеки, виступає її стратегічним елементом і визначальним компонентом загальної системи, формуючи матеріальне підґрунтя як для безпеки країни загалом, так і для окремих її складових, зокрема продовольчої, енергетичної, науково-технічної, демографічної, екологічної та інших.

Термін «економічна безпека» вперше почали використовувати у період реалізації антикризових заходів Ф.Д. Рузвельт у межах програм подолання Великої депресії 1933–1937 років. Водночас у той самий історичний відрізок зазначена категорія посідала важливе місце серед напрямів соціально-економічних реформ, що впроваджувалися Демократична партія США [1, с. 125].

На міжнародному рівні офіційне закріплення відповідного терміна відбулося у 1985 році під час 40-ї сесії Генеральної Асамблеї ООН, коли було ухвалено резолюцію щодо міжнародної економічної безпеки. Документ акцентував увагу на необхідності консолідованих зусиль світової спільноти задля забезпечення економічної стабільності, що сприяє розвитку та поступу кожної держави. Подальший розвиток ідей відбувся на 42-й сесії того ж органу, де схвалено концептуальні засади міжнародної економічної безпеки [1, с. 125-126].

На національному рівні в Україні визначення відповідного поняття закріплено у Декларації про державний суверенітет України. У 1990 році сформовано спеціалізований підрозділ, відповідальний за реалізацію політики у зазначеній сфері. Згодом, у 1998 році, було підготовлено Національну програму забезпечення економічної безпеки на період до 2005 року, а вже у 1999 році затверджено першу концепцію, присвячену даній проблематиці [2, с. 41].

На сьогодні законодавче тлумачення економічної безпеки України закріплено у Стратегію економічної безпеки України на період до 2025 року. Згідно з указаним документом, економічна безпека визначається як такий стан національної економіки, за якого забезпечується її стійкість до

внутрішніх і зовнішніх викликів, підтримується належний рівень конкурентоспроможності на міжнародній арені, а також гарантується спроможність до стабільного й збалансованого розвитку [3].

Науковці активно розвивали уявлення про сутність економічної безпеки. Зокрема, О.В. Черевко розглядав її як стан, що забезпечує народу можливість самостійно визначати напрями й моделі економічного розвитку [4, с. 32]. Н.В. Зачосова підкреслювала необхідність дотримання двох ключових умов: збереження економічної незалежності держави з правом ухвалення самостійних рішень, а також підтримання досягнутого рівня добробуту населення з перспективою його підвищення [4, с. 33].

Своєю чергою, О.Є. Денисов трактував національну економічну безпеку як такий стан економічної системи та владних інститутів, який гарантує захист національних інтересів, забезпечує збалансований соціально орієнтований розвиток, а також достатній рівень економічного й оборонного потенціалу навіть за умов несприятливого розвитку внутрішніх і зовнішніх чинників [5, с. 53-54]. В. Гнатенко, у свою чергу, наголошував на багатовимірності даного поняття, пов’язуючи його зі станом захищеності економічних інтересів особи, суспільства та держави, який ґрунтується на самостійності, ефективності й конкурентоспроможності національної економіки [6, с. 68-69].

Провівши узагальнення наукових підходів слід зазначити про відсутність можливості виокремити єдине, найбільш точне й універсальне тлумачення категорії «економічна безпека».

Разом із тим, за умови прийняття припущення щодо існування кількох альтернативних підходів до аналізу економічної безпеки, доцільно відмовитися від прагнення сформулювати одне вичерпне визначення. Натомість варто розглядати категорію «безпека» як змінну за змістом, наповнення якої залежить від конкретних обставин, цілей і завдань, у межах яких формується відповідна аналітична модель. Подібний підхід складно визнати оптимальним із позицій наукової

строгості, однак він найбільш точно відображає сучасну практику, де поняття «безпека» застосовується до надзвичайно широкого кола різнорідних явищ і процесів.

Структура економічної безпеки України охоплює такі ключові елементи: виробничу, демографічну, енергетичну, зовнішньоекономічну, інвестиційно-інноваційну, макроекономічну, продовольчу, соціальну та фінансову складові. Кожен із зазначених компонентів має складну внутрішню будову та може розглядатися як окрема підсистема, а їх взаємозв'язок і взаємодія визначають напрями формування державної економічної політики. Водночас сучасні тенденції свідчать про суттєве посилення значення інформаційної безпеки у функціонуванні національної економіки, що обґрунтовує доцільність її виокремлення як самостійного елементу економічної безпеки.

На основі опрацювання наукових джерел і результатів власного аналізу доцільно визначити основні складові економічної безпеки держави у вигляді рис. 1.1.

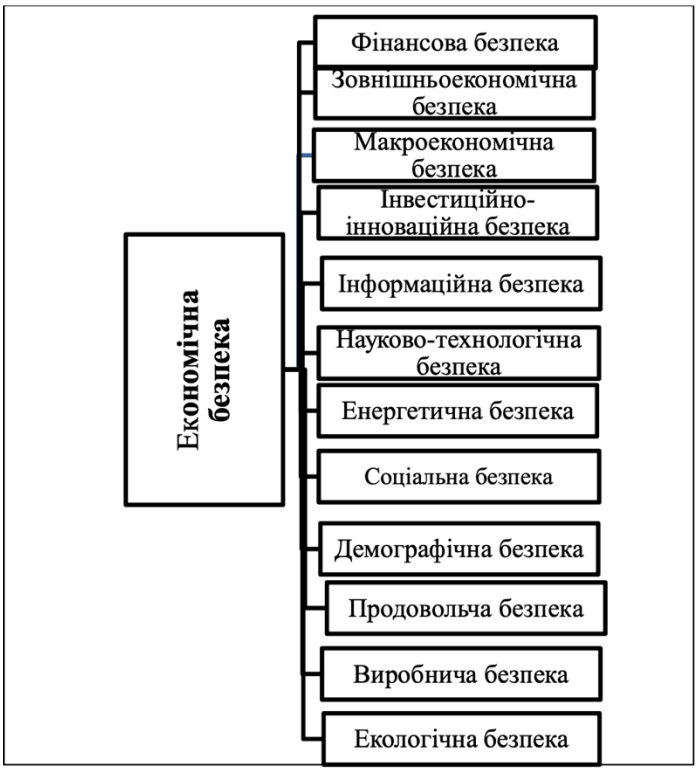

Рис. 1.1. Складові економічної безпеки держави

Джерело: [6, с. 71]

Отже, економічна безпека як наукова категорія посідає ключове місце у системі національної безпеки України та характеризується складною внутрішньою побудовою, про що свідчить різноманітність підходів до її тлумачення.

1.2. Вплив цифровізації на ключові складові економічної безпеки держави

Глобальна цифрова трансформація фундаментально змінює парадигму функціонування національних економік. Стрімке впровадження інноваційних технологій формує новітнє середовище, де традиційні механізми державного управління потребують невідкладної модернізації. У сучасній правовій та економічній науці цифровізацію описують як складний двоєдиний феномен. Зміна технологічного укладу безальтернативно вимагає глибинного переосмислення концепту захищеності національних економічних інтересів [7].

Загалом, цифровізацію доцільно розуміти як всеохоплюючий процес інтеграції сучасних цифрових рішень у різноманітні сфери суспільного життя, від повсякденної комунікації між людьми до функціонування складних виробничих комплексів, а також від звичайних побутових речей до продукції для дітей чи елементів гардероба, який супроводжується трансформацією традиційних біологічних і фізичних систем у нові формати – кіберфізичні та кібербіологічні, що передбачає поєднання матеріальних об’єктів із цифровими та обчислювальними компонентами. Водночас відбувається зміщення значної частини діяльності з матеріального середовища у площину цифрових платформ, онлайн-сервісів і віртуального простору.

Поєднання цих тенденцій формує явище цифрової глобалізації. Поряд із позитивними наслідками, такими як активізація економічного і наукового прогресу, прискорення фінансових процесів та розвиток

людського капіталу, виникають і нові ризики. Серед них поява інструментів для атак на матеріальну й інформаційну інфраструктуру, поширення технологічного шпигунства, втручання у політичні процеси, зокрема вибори, а також масове розповсюдження маніпулятивної інформації та недостовірних повідомлень, що становить серйозну загрозу економічній безпеці держави в умовах цифрового середовища.

За таких умов дедалі більшої ваги набувають інформаційні складові економічної безпеки. Їх значення постійно зростає, оскільки посилення ролі інформаційних ресурсів, цифрових технологій та знань у розвитку економічних систем висуває інформаційний вимір на провідні позиції у структурі забезпечення безпеки на рівні держави, суспільства, бізнесу та окремої особи. Розширення інформаційної економіки супроводжується суттєвим загостренням питань, пов’язаних із гарантуванням захищеності економічних процесів в інформаційному середовищі [8].

Пріоритетними завданнями забезпечення економічної безпеки в інформаційній площині виступають охорона економічних інтересів держави, надання органам влади, суб’єктам господарювання та громадянам повної, достовірної й оперативної інформації, а також гарантування можливості вільно отримувати, поширювати й використовувати інформаційні ресурси(рис 1.2) [8].

Для чіткого розуміння масштабу трансформацій доцільно виокремити два найбільш вразливі вектори впливу цифрових технологій на базові підсистеми держави:

– Фінансовий суверенітет: масове поширення віртуальних активів зумовлює нагальну необхідність тотальної адаптації нормативно-правової бази. Неконтрольований обіг криптовалют створює ідеальні передумови для тінізації капіталу.

– Інформаційна стійкість: кібернетичні атаки на державні реєстри здатні паралізувати життєдіяльність регіонів, беззаперечно вимагаючи імплементації жорстких протоколів криптографічного захисту [9, с. 42].

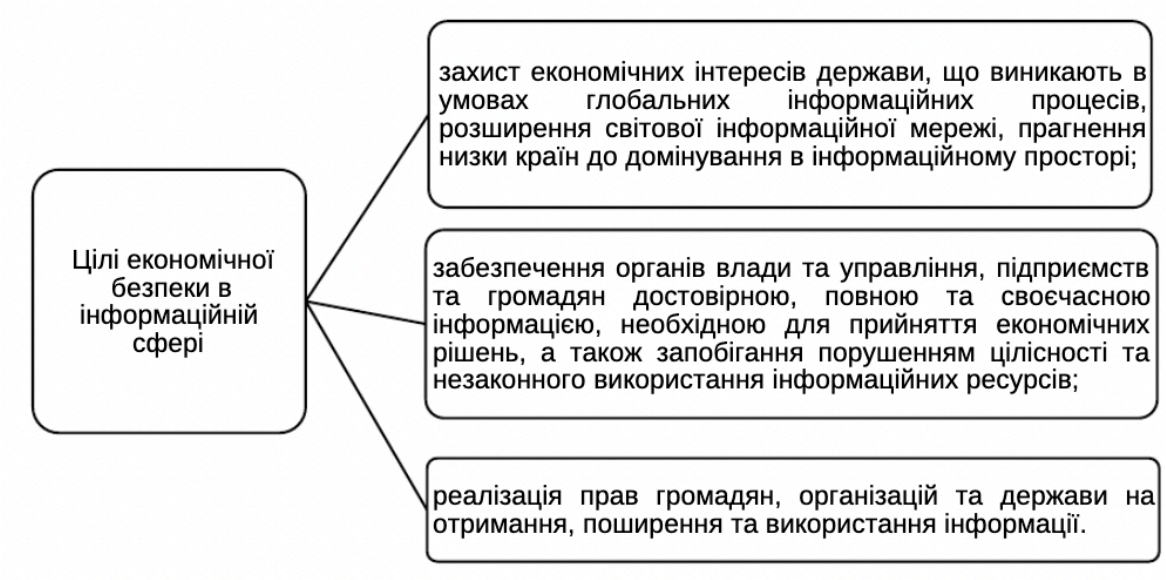

Рис. 1.2. Цілі Економічної безпеки в інформаційній сфері

Джерело: [8]

З метою комплексної систематизації слід розглянути наведене у вигляді таблиці, котра наочно продемонструє дуалістичну природу цифрових перетворень (табл. 1.1).

Таблиця 1.1

Вплив цифрових технологій на підсистеми економічної безпеки

Складова безпеки	**Стимулюючий вплив(можливості)**	**Деструктивний вплив(загрози**
Фінансова	Зниження транзакційних витрат, абсолютна прозорість державних видатків завдяки фінтех-рішенням.	Легалізація незаконних доходів через неврегульований обіг віртуальних активів.
Виробнича	Автоматизація ланцюгів (Індустрія 4.0), стрімке підвищення конкурентоспроможності підприємств.	Технологічна залежність від вузького кола транснаціональних IT-корпорацій.
Соціальна	Поява дистанційної зайнятість, надзвичайна гнучкість сучасного ринку праці.	Зростання структурного безробіття, поглиблення глобальної цифрової нерівності.
Інституційна	Мінімізація корупційних ризиків за допомогою інструментів електронного урядування.	Критичні ризики масштабного витоку персональних даних громадян із державних баз.

Джерело: розроблено автором самостійно

Досліджуючи вказану багатогранну проблематику, варто звернутися до концептуальних праць провідних фахівців галузі. О. В. Пустовойт у власному дослідженні аргументовано стверджує, що цифровізація економіки формує безумовний імператив переходу від реактивної до проактивної моделі гарантування національної безпеки, де ключовим ресурсом стає безперебійний потік верифікованих даних, а головною загрозою – критична втрата контролю над національним сегментом кіберпростору [10, с. 9-10]. Відштовхуючись від наведеної вище тези, стає очевидною нагальна потреба негайної розбудови багаторівневої системи нормативно-правового захисту об'єктів критичної інфраструктури.

Нематеріальні активи, унікальні алгоритми та пропрієтарні програмні коди сьогодні генерують левову частку доданої вартості сучасних корпорацій. Легкість несанкціонованого копіювання контенту стрімко знецінює класичні методи патентного захисту. Відповідно, вітчизняна юриспруденція постає перед надскладним викликом розробки новітніх інструментів фіксації авторства. Належне законодавче регулювання застосування технології розподіленого реєстру (блокчейн) здатне надійно убезпечити інвестиції у науково-дослідні розробки.

Щодо соціально-демографічного виміру, О. В. Пустовойт безапеляційно наголошує що стрімкий технологічний прогрес без проведення відповідної випереджальної інституційної адаптації соціально-правових механізмів неодмінно загрожує незворотною маргіналізацією значних верств населення. Уникнення окреслених вкрай негативних сценаріїв вимагає кардинального реформування застарілого трудового законодавства та стабільного фінансового стимулювання державних програм перекваліфікації кадрів [10, с. 11].

Загалом, доцільно констатувати наявність поглибленої амбівалентності впливу процесів діджиталізації на сучасне суспільство.

Стрімкий розвиток інноваційних технологій, зокрема інформаційно-комунікаційних систем, штучного інтелекту та великих даних, виступає потужним каталізатором соціально-економічного прогресу, сприяючи оптимізації управлінських процесів, підвищенню ефективності виробництва та розширенню доступу до інформації. Водночас такі трансформації зумовлюють появу нових форм соціальної взаємодії, які змінюють традиційні уявлення про правовідносини, комунікацію та безпеку в цифровому середовищі.

Паралельно з позитивними ефектами діджиталізація генерує специфічний комплекс новітніх загроз, що мають асиметричний та часто латентний характер, включаючи кіберзлочинність, порушення конфіденційності даних, маніпуляції інформаційними потоками та ризики цифрової нерівності. Ефективна нейтралізація таких системних викликів об’єктивно потребує не лише формального оновлення чинної законодавчої бази, а й глибинної трансформації доктринальних підходів до праворозуміння. Відповідні зміни мають бути спрямовані на адаптацію правових механізмів до динамічних умов віртуального простору, забезпечення балансу між інноваційним розвитком і гарантіями прав людини, а також формування нових принципів регулювання цифрових відносин.

РОЗДІЛ 2
АНАЛІЗ ВПЛИВУ ЦИФРОВІЗАЦІЇ ТА ВОЄННИХ ЧИННИКІВ НА ЕКОНОМІЧНУ БЕЗПЕКУ УКРАЇНИ

2.1. Аналіз чинників цифровізації та їх впливу на економічну безпеку України (динаміка показників та сучасні тенденції)

Як вже було відзначено, економічна безпека держави виступає неподільним сегментом складної системи національної безпеки, визначаючи спроможність суб'єктів владних повноважень гарантувати стійкість фінансових інституцій перед обличчям глобальних трансформацій. У добу тотальної інформатизації суспільних відносин рівень захищеності національних інтересів детермінується спроможністю правоохоронної та фінансової систем нівелювати вплив деструктивних чинників віртуального простору. Вони мають транскордонний характер, що значно ускладнює процес ідентифікації правопорушників та притягнення винних осіб до юридичної відповідальності. Відповідно, слід охарактеризувати природу цифрових загроз для економічної безпеки України.

Згідно з аналітичними даними Департаменту кіберполіції Національної поліції України, протягом останнього триріччя спостерігається експоненціальне зростання кількості зареєстрованих кримінальних правопорушень, вчинених із використанням високих технологій. Якщо у 2021 році правоохоронними органами було опрацьовано близько 38 тисяч звернень громадян, то за підсумками 2023 року вказаний показник перевищив позначку у 50 тисяч офіційних скарг. Найбільш розповсюдженим видом деліктів залишається шахрайство, на яке припадає понад 80% від загального масиву виявлених інцидентів. З наведеного можна побачити вразливість приватного сектору економіки, де фінансові втрати окремих домогосподарств у сукупності завдають

суттєвої шкоди загальному інвестиційному клімату країни [11, с. 1078].

На сьогодні розвиток фінтех-інструментів, за всієї позитивної спрямованості, відкрив простір для застосування методів соціальної інженерії та фішингу. Статистичні звіти провідних банківських установ України(ПриватБанк, Монобанк, ОЩАД) фіксують зростання кількості фішингових ресурсів, мета яких полягає у викраденні персональних даних клієнтів для подальшого несанкціонованого доступу до рахунків. Протягом 2022-2023 років кількість виявлених підроблених вебсайтів, котрі імітували офіційні платіжні сервіси, зросла на 45%. Масштаби фінансових збитків від подібних операцій обчислюються сотнями мільйонів гривень щомісяця, що підриває довіру населення до цифрової валютної системи та стимулює повернення до готівкових розрахунків, посилюючи ризики тінізації господарських процесів [11, с. 1078-1079].

Досліджуючи правову природу інформаційних ризиків, О.В. Калініченко слушно зауважує, що інформаційна складова економічної безпеки сьогодні є домінантною, оскільки будь-яке несанкціоноване втручання в алгоритми роботи державних реєстрів чи автоматизованих систем управління фінансами здатне паралізувати юридично значущі процеси швидше за будь-які економічні санкції [12, с. 28-29].

Слід погодитися з думкою науковця, адже він підкреслює необхідність розгляду технологічних недоліків інфраструктури як прямої загрози державному суверенітету в економічній площині. Наявність застарілих протоколів шифрування у деяких відомчих базах даних створює передумови для рейдерських захоплень активів шляхом несанкціонованого внесення змін до реєстрів речових прав.

Важливим аналітичним індикатором виступає рівень захищеності об'єктів критичної інформаційної інфраструктури. Моніторинг технічних аспектів функціонування енергетичних та транспортних мереж вказує на постійні спроби сканування портів та пошуку «дірок» у програмному забезпеченні. За даними моніторингових центрів, щоденно фіксується від

500 до 1500 спроб неавторизованого проникнення до внутрішніх мереж підприємств, що мають стратегічне значення для життєдіяльності соціуму. Успішна реалізація бодай одного подібного сценарію може призвести до техногенних катастроф із колосальними фінансовими витратами на ліквідацію наслідків, що автоматично лягає тягарем на державний бюджет [13, с. 51-52].

Варто детально зупинитися на чинниках, що обумовлюють стрімкий розвиток тіньового сегменту цифрової економіки. Першим слід відзначити анонімність транзакцій із використанням нерегульованих віртуальних активів, тобто відсутність чіткого законодавчого механізму верифікації походження коштів у криптосфері дозволяє виводити значні капітали за межі національної юрисдикції без сплати податкових зобов'язань. Далі слід виділити використання даркнет-майданчиків для торгівлі викраденими даними, ринок пропрієтарної інформації та баз даних юридичних осіб стає джерелом прибутку для транснаціональних угруповань. Недостатній рівень цифрової грамотності суб'єктів господарювання є критичним, помилки персоналу залишаються «вхідними воротами» для програм-вимагачів (ransomware), котрі блокують роботу великих підприємств, вимагаючи викуп.

Протягом 2023 року зафіксовано зростання використання вірусів-шифрувальників проти українських логістичних компаній. Середній розмір запитуваного викупу за відновлення доступу до даних становить від 10 до 50 тисяч доларів США в еквіваленті криптовалют. Прямі збитки від простою потужностей та втрати клієнтської бази у вказаних випадках перевищують суму викупу в десятки разів. Відповідно, програмний код шкідливого характеру перетворюється на інструмент недобросовісної конкурентної боротьби та дестабілізації галузевих ринків [14, с. 57].

Щодо інституційної стійкості, Ю. Деркаченко наголошує на пріоритетності подальшого нормативного регулювання інформаційної безпеки, він пише, що правове забезпечення економічної безпеки у

цифрову епоху має випереджати технологічні ризики, створюючи систему жорстких санкцій за порушення цілісності державних інформаційних ресурсів [14, с. 57-58].

Отже, слід констатувати, що цифрові загрози перетворилися на постійно діючий чинник дестабілізації національної економіки. Динаміка зростання кількості кіберінцидентів на тлі розширення спектра методів їх вчинення вимагає від держави не лише технічного переоснащення, а й формування гнучкої правової бази. Економічна безпека за даних обставин можлива лише за умови створення ефективної вертикалі взаємодії між державним сектором та приватними ІТ-компаніями. Тільки консолідація зусиль у напрямі розробки власних криптографічних стандартів та регулярного аудиту безпеки інформаційних систем дозволить зберегти стійкість господарського комплексу перед обличчям новітніх викликів віртуальної реальності.

2.2. Вплив воєнного стану та кібератак рф на економічну безпеку України

Збройна агресія Російської Федерації проти України становить серйозне випробування для всієї системи міжнародної безпеки. Наприклад у дослідженні Economist Intelligence Unit (EIU) підтверджено, що наслідки цієї війни виходять далеко за межі регіону та здатні порушити стабільність як світової економіки, так і суспільно-політичних процесів. У сучасних умовах першочергового значення набуває завчасне та активне зміцнення економічної безпеки України, що має забезпечити стійкість національної економіки до комплексу внутрішніх і зовнішніх загроз, з урахуванням процесів цифрової трансформації та пов’язаних із ними ризиків [15, с. 181].

Поширення цифрових технологій фактично змінило характер воєн і конфліктів, перенісши їх частково у віртуальний простір та створивши

нові механізми впливу на економічну і політичну сферу. Інформаційні загрози сьогодні здатні істотно послаблювати обороноздатність держав. Особливо небезпечним явищем виступає кібертероризм, включаючи міждержавні його прояви, який перетворився на ефективний інструмент ведення сучасних війн і реалізації геополітичних інтересів.

Показовим прикладом використання кіберзасобів у військових цілях є російсько-грузинський конфлікт 2008 року, під час якого паралельно з бойовими діями здійснювалися масштабні атаки на інформаційні ресурси: медіа, офіційні вебсайти органів влади, зокрема Національного банку Грузії. Метою таких дій було порушення керованості державою, формування вигідного інформаційного порядку денного та обмеження доступу до об'єктивних даних. Події стали одним із перших прикладів комплексного поєднання військової агресії з координованими кібероперaціями, спрямованими на створення паніки, дезорганізацію управління, блокування економічної активності та маніпулювання міжнародною реакцією [15, с. 183].

Наслідки таких атак мали не лише політичний, а й відчутний економічний ефект: фінансові установи та підприємства малого бізнесу зазнавали збоїв у роботі, а інтернет-ресурси та провайдери втрачали прибутки. У зв'язку з цим виведення з ладу цифрової інфраструктури під час воєнних дій становить одну з найсерйозніших загроз економічній безпеці, оскільки здатне спричинити глибоку нестабільність економічних процесів і макроекономічні потрясіння.

Починаючи з 2007 року, Російська Федерація цілеспрямовано розвивала інструменти кібервпливу, що вперше яскраво проявилося під час атак на Естонію. Уже в 2008 році подібні дії супроводжували воєнні події в Грузії, а з 2014 року вони набули системного характеру щодо України. Напередодні повномасштабного вторгнення у 2022 році інтенсивність кібератак значно зросла, охоплюючи банківський сектор, державні інформаційні ресурси та телекомунікаційні системи. Зокрема, у

лютому 2022 року, за інформацією Державної служби спеціального зв'язку та захисту інформації України, на державні структури було здійснено близько 143 тисяч атак, тоді як уже в травні їх кількість зросла до десятків мільйонів (рис. 2.1) [15, с. 183-184].

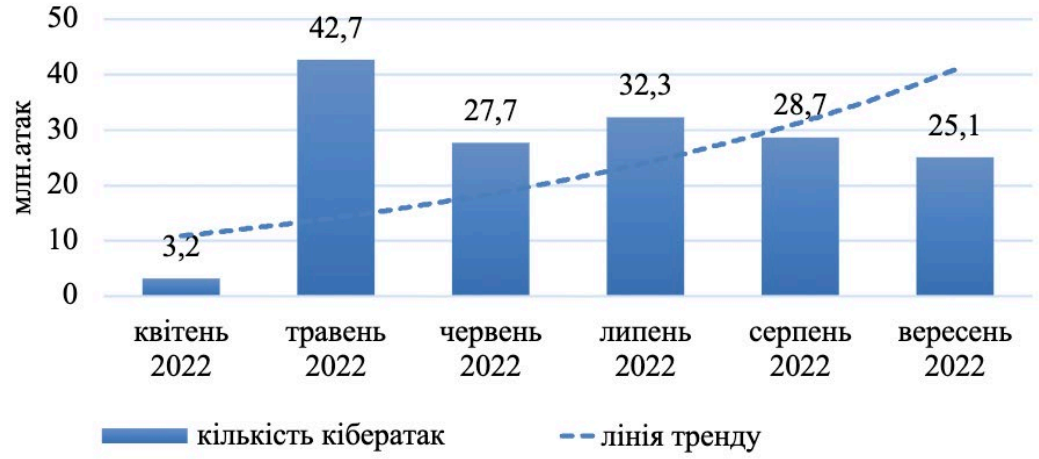

Рис. 2.1. Динаміка кількості кібератак на державний сектор України протягом квітня-вересня 2022 року

Джерело: [15, с. 186]

Кіберпротистояння між Україною та Росією у 2014–2022 роках стало складовою гібридної війни та невід'ємним елементом широкомасштабної агресії, розгорнутої у 2022 році за сценарієм, апробованим раніше в Грузії. Дії рф у цифровому середовищі були спрямовані на досягнення кількох ключових цілей: порушення енергетичної стабільності, що ускладнює ведення бойових операцій; отримання доступу до важливої фінансової, політичної та військової інформації з метою завдання економічних збитків і зниження інвестиційної привабливості країни; а також дестабілізацію внутрішньої ситуації через посилення соціальної напруги та провокування кризових явищ [15, с. 185].

Додаткову небезпеку становило використання програмних продуктів російського походження або таких, що мали вразливості. Частина з них була заздалегідь скомпрометована, містила приховані

недоліки або шкідливий код, що дозволяло отримувати несанкціонований доступ до інформаційних систем. Через тривале застосування такого програмного забезпечення в діяльності підприємств зловмисники отримували можливість проникати до баз даних різних установ. Окремі випадки стосувалися й вітчизняних, у тому числі військових програм, уразливість яких могла призводити до витоку даних про розташування українських сил.

Застосування недорогого, несертифікованого, піратського або технічно ненадійного програмного забезпечення спричинило виникнення значної кількості загроз для економічної безпеки України в цифровому середовищі, що значною мірою, пояснювалося як фінансовими обмеженнями, так і мовним бар'єром, адже якісні програмні продукти західного виробництва часто були дорогими або орієнтованими на англомовного користувача. Додатковим чинником ризику стало широке поширення російських соціальних мереж, зокрема «ВКонтакте» та «Одноклассники», а також антивірусних продуктів «Лабораторії Касперського» і «Doctor Web». Згодом такі джерела потенційної небезпеки були усунуті шляхом законодавчих обмежень і заборон, що стало одним із інструментів протидії кіберагресії [15, с. 185-186].

Особливо критичним виявився доступ зловмисників, як хакерських угруповань, так і пов'язаних із державою структур до енергетичної інфраструктури країни. У 2015 році було здійснено атаки на енергопостачальні компанії, серед яких «Прикарпаттяобленерго», «Чернівціобленерго» та «Київобленерго». У результаті відбувалося дистанційне вимкнення окремих систем, знищення та викрадення даних, а також блокування віддаленого управління. Навіть відсутність прямого підключення до мережі Інтернет не стала перешкодою, оскільки проникнення здійснювалося через внутрішні мережі, де зловмисники тривалий час закріплювалися, розширюючи контроль і отримуючи доступ до систем керування. Повномасштабним руйнуванням

інфраструктури завадили низка факторів, серед яких передчасність атаки, наявність альтернативного ручного управління, а також специфічні економіко-політичні обставини [16, с. 127].

З огляду на це, досягнення значного рівня проникнення у цифрову інфраструктуру національної економіки може дозволити противнику фактично паралізувати функціонування держави шляхом відключення енергомережі, що призведе до зупинення фінансових, адміністративних та інформаційних процесів. Водночас реалізація таких сценаріїв є технічно складною, тривалою у підготовці та частково нейтралізується завдяки можливості ручного управління. Саме тому у другій половині 2022 року Росія вдалася до прямих фізичних атак на енергетичні об'єкти із застосуванням ракет і безпілотників, не досягнувши бажаного ефекту виключно кіберзасобами.

Серед інших об'єктів потенційних і фактичних кібератак розглядалися інформаційні системи ключових фінансових установ держави, зокрема Міністерства фінансів України, Державної казначейської служби та Пенсійного фонду, що підтверджує спрямованість таких дій на підрив фінансової стабільності країни.

Подальша ескалація гібридної агресії протягом 2023–2026 років підтвердила перехід ворожих кіберпідрозділів до стратегії системного виснаження національної економіки через точкові удари по критичних вузлах зв'язку, енергетики та фінансового посередництва. Найбільш масштабним інцидентом за вказаний період стала нейтралізація мережі оператора мобільного зв'язку «Київстар» у грудні 2023 року. Внаслідок деструктивного втручання хакерського угруповання «Sandworm», котре пов'язують із російським ГРУ, відбувся параліч не лише комунікаційних сервісів, а й суміжних економічних інституцій. Атака призвела до блокування роботи понад 100 тисяч терміналів безготівкової оплати, припинення функціонування банкоматів та збоїв у системах внутрішньої безпеки промислових підприємств. Економічні збитки лише одного

оператора перевищили 3,6 мільярда гривень, проте сукупний негативний ефект для ВВП країни виявився значно глибшим через вимушену зупинку торговельних операцій та логістичних процесів у масштабах усієї держави [17, с. 44-45].

У січні 2024 року та протягом подальшого періоду 2025 року спостерігалися скоординовані атаки на ІТ-інфраструктуру НАК «Нафтогаз України» та національного поштового оператора «Укрпошта». Мета означених дій полягала у зриві механізмів оплати енергоносіїв та блокуванні логістичних ланцюгів доставки товарів. Характерною рисою вказаних інцидентів стало використання програм-шифрувальників нового покоління, спрямованих на тривале виведення з ладу серверного обладнання без можливості швидкого відновлення даних. Зупинка сервісів «Укрпошти» спричинила затримки у виплатах пенсій та соціальних допомог, що створило додаткове навантаження на державний бюджет та спровокувало соціальну напругу, послаблюючи внутрішню стійкість господарського комплексу, тобто цифрова агресія трансформується у фактор прямого тиску на фінансові зобов’язання держави перед громадянами [18, с. 90].

Окремим напрямом деструктивної діяльності протягом 2025 року став кіберсаботаж морської логістики в межах функціонування експортних коридорів. Ворожі хакери здійснювали спроби втручання в автоматизовані системи управління Одеського та Чорноморського портів з метою спотворення даних про рух суден та блокування процесів митного оформлення експорту агропродукції. Вказані дії безпосередньо загрожували валютним надходженням до державного бюджету, оскільки кожна година простою судна генерувала значні фінансові втрати для агрохолдингів та страхових компаній.

Протягом 2025 та початку 2026 року суттєво зросла інтенсивність атак на хмарні сервіси та державні реєстри. Зокрема, спроби несанкціонованого доступу до Єдиного державного реєстру юридичних

осіб та Реєстру речових прав на нерухоме майно мали на меті створення юридичного хаосу. Можливість підробки записів про власність або блокування доступу до означених баз даних несе фундаментальну загрозу економічній безпеці, адже унеможливлює здійснення легітимних господарських операцій, паралізує ринок нерухомості та блокує процеси кредитування під заставу майна [18, с. 90-91].

У фінансовому секторі протягом вказаного періоду фіксувалися перманентні DDoS-атаки потужністю понад 100 Гбіт/с на провідні банки, включаючи «Монобанк» та державний «ПриватБанк». Хоча більшість спроб дестабілізації вдалося нейтралізувати, сам факт постійного тиску вимагає від фінансових установ значних додаткових витрат на кіберзахист та підтримку резервних потужностей, які автоматично здійснили вплив на собівартість банківських послуг, що опосередковано здорожує кредитні ресурси для реального сектору економіки [18, с. 92].

Таким чином, слід констатувати остаточне формування кіберпростору як повноцінного нового місця для ведення воєнних дій, де успішна атака на програмний код за економічними наслідками прирівнюється до фізичного руйнування промислових потужностей. Використання ворогом методів «кібервиснаження» спрямоване на максимальне здорожчання функціонування української економіки та підрив довіри до державних інституцій. Економічна безпека України в умовах воєнного стану тепер неподільно пов’язана з технологічною незалежністю та стійкістю інформаційних систем до постійно оновлюваного арсеналу цифрових загроз.

РОЗДІЛ 3
ПЕРСПЕКТИВИ ТА СТРАТЕГІЇ РОЗВИТКУ ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ЦИФРОВИХ ТРАНСФОРМАЦІЙ

3.1. Напрями зміцнення економічної безпеки України в умовах цифрових загроз

Інтенсивне поширення та інтеграція цифрових технологій, сервісів і рішень, які формують новітнє економічне середовище, інструментарій діяльності та спектр сучасних викликів, зумовлюють необхідність їх цілеспрямованого регулювання, супроводу й осмислення у межах економічної безпекології. У такому контексті цифровізація характеризується низкою специфічних рис: здатністю до самовідтворення і розвитку за циклічним принципом, глобальним масштабом поширення, багаторівневою системністю, виходом за межі національних юрисдикцій, обмеженою результативністю прямих втручань, а також подвійним впливом на стан економічної безпеки.

Водночас структурні трансформації, спричинені цифровими змінами, мають не лише прямий, але й опосередкований негативний ефект. Зокрема, спостерігається зниження потенціалу традиційних галузей економіки, що супроводжується підвищенням їхньої вразливості до різноманітних загроз, від прихованих і гібридних до класичних форм впливу на цифрову та енергетичну інфраструктуру [19, с. 5-6].

За таких умов ефективне впровадження цифрових рішень потребує чітко продуманої державної політики, яка базується на визначених стратегічних орієнтирах розвитку та забезпечення економічної безпеки. Йдеться про формування цілісної стратегії, яка окреслює ключові завдання, пріоритети, інструменти реалізації та етапи досягнення результатів. Важливим етапом такого процесу виступає визначення пріоритетів, тобто ранжування напрямів діяльності, ресурсів і завдань

залежно від їх значущості з урахуванням обмеженості часу та можливостей, а також необхідності підвищення ефективності економічної політики.

Концептуально новий підхід до формування політики безпеки в умовах цифровізації, запропонований О. Тарасенко , передбачає зміщення акценту з максимального обмеження загроз і прагнення до автономності на їх мінімізацію через підвищення конкурентоспроможності та здатності до адаптації. Він, у свої моделі, відмовляється від надмірно амбітних орієнтирів і водночас сприяє зниженню витрат, дозволяючи зосередитися на досягненні більш реалістичних і практично досяжних результатів [20, с. 174-175].

Для України особливого значення набуває раціональне використання наявного ресурсного потенціалу, що зумовлює необхідність активного запозичення зарубіжного досвіду, урахування специфіки регіонального розвитку, використання напрацювань у сфері міжнародної безпеки та адаптації вже апробованих рішень до національних умов.

У зв’язку з цим доцільно звернутися до практики Європейського Союзу як впливового наднаціонального центру формування економічної, політичної та безпекової політики. Варто звернути увагу на ключові напрямам забезпечення безпеки, які закріплені у нормативно-правових актах міждержавного рівня.

Система економічної безпеки ЄС ґрунтується на трьох базових орієнтирах: підвищенні конкурентоспроможності, протидії ризикам і загрозам, а також розвитку міжнародного співробітництва. Досягнення конкурентних переваг забезпечується шляхом реалізації фінансових інструментів підтримки, активного впровадження екологічно орієнтованих трансформацій, розвитку високотехнологічних секторів і диверсифікації логістичних ланцюгів, що водночас сприяє зміцненню технологічної автономії та економічної стійкості об’єднання [21, с. 26-

27].

Попри відмінності між Україною як унітарною державою та Європейським Союзом як наддержавним утворенням, що ускладнює пряме порівняння за масштабами, варто враховувати, що країни-члени ЄС значною мірою делегують повноваження у сфері економічного регулювання та безпеки на спільний рівень. З огляду на це, стратегічні підходи, регуляторні механізми та визначені пріоритети ЄС, зокрема у сфері цифровізації, можуть розглядатися як орієнтир для формування ефективної політики у європейському просторі.

Стратегічні документи України, розроблені у 2020 році разом із відповідною нормативно-правовою базою, у певних аспектах навіть випереджали регіональні орієнтири, відображаючи аналогічні складові, що пізніше були закріплені у підходах Європейського Союзу 2023–2024 років, тобто слід відзначити вагомість українського підходу в контексті загальноєвропейських безпекових тенденцій [21, с. 28].

Ключовими елементами зазначеної стратегії виступають забезпечення автономності, розвиток інституційної спроможності державних органів, визначення пріоритетних технологій і стратегічних партнерств, системний моніторинг загроз, а також посилення ролі провідних органів у сфері безпеки, зокрема Ради національної безпеки і оборони України та Кабінету Міністрів України. Водночас нормативно-правові акти, ухвалені до 2022 року, в умовах нових кризових викликів значною мірою втратили актуальність, що обумовлює необхідність переосмислення та визначення пріоритетних напрямів захисту економічних інтересів держави [21, с. 28-29].

Одним із ефективних інструментів визначення таких пріоритетів виступає методика RICE, яка дає змогу оцінити доцільність спрямування ресурсів, зосередитися на найбільш значущих напрямах і підвищити результативність управлінських рішень завдяки використанню простої математичної моделі.

$$RICE = (Reach * Impact * Cцoonfidence) / Effort \qquad (3.1)$$

де RICE – оцінка пріоритетності; Reach – охоплення змінами, цільовою аудиторією; Impact – рівень впливу від рішення, від 0,25 до 2; Confidence – рівень довіри припущенням, від 0,25 до 1; Effort – час на впровадження змін, відповідно до процесів, від 0,25 до 2 [22, с. 131].

Показник Reach у межах дослідження визначався з урахуванням чисельності населення України на рівні близько 32 мільйонів осіб, а також високого рівня проникнення інтернету, що становить приблизно 94%. Відповідно, напрями, які безпосередньо впливають на більшість користувачів, охоплюють близько 30 мільйонів осіб, тоді як інші оцінювалися пропорційно частці населення, на яку поширюється їхній вплив.

Для визначення таких параметрів, як Impact, Confidence та Effort, було проведено експертне оцінювання із залученням фахівців навчально-наукового інституту фінансів, економіки, управління та права Національного університету «Полтавська політехніка імені Юрія Кондратюка». У дослідженні взяли участь десять експертів – кандидатів і докторів економічних наук. Узагальнені результати опитування та відповідних розрахунків подано у табличній формі (табл. 3.1) [22, с. 132].

За підсумками проведених розрахунків найбільш перспективним слід визначити напрям інтеграції до регіонального безпекового простору, який отримав середній показник на рівні 22,9 бала. Такий результат пояснюється можливістю залучення широкого кола учасників, одночасним розвитком національних інституцій відповідно до європейських стандартів, а також запозиченням і адаптацією передового досвіду та технологій із відносно невеликими витратами ресурсів.

Водночас різниця між другим і третім за значущістю напрямами виявилася мінімальною — лише 0,2 бала. Основним їхнім обмеженням виступає потреба у тривалому та послідовному розвитку, який не може

бути забезпечений виключно за рахунок зовнішнього досвіду чи інтеграційних процесів, а потребує поступового формування всередині національної системи безпеки. Такий підхід передбачає значні витрати ресурсів і характеризується відкладеним у часі позитивним ефектом.

Таблиця 3.1

Пріоритезація напрямів захисту національних економічних інтересів України в умовах цифровізації методом RICE

Напрям	R,млн,ос.	I	C	E	RICE
Гармонізація та уніфікація нормативно-правового забезпечення					
Приведення нормативно-правової бази у відповідність до актуальних викликів	32	1,3	0,8	1,7	19,6
Модернізація законодавчого регулювання у сфері цифрових технологій	30	0,8	0,8	1,5	12,8
Розроблення цілісної та узгодженої політики цифрового розвитку	28	0,5	0,6	1	8,5
Оновлення підходів і методів оцінювання загроз економічній безпеці	27	0,5	0,8	0,5	21,3
Посилення та вдосконалення інструментів інформаційно-технологічного захисту					
Підвищення рівня цифрової грамотності населення	22	1,7	0,8	2	15,2
Розвиток професійних цифрових компетентностей фахівців ІКТ та перепідготовка ІТ-кадрів	14	1,3	0,6	1	11,2
Долучення до міжнародних механізмів захисту телекомунікаційної та інтернет-інфраструктури	30	1	0,7	1	21
Сприяння становленню цифрових форм участі громадян в управлінні	32	0,7	0,9	1,5	13,4
Включення до регіональних інституційних систем безпеки					
Участь у міжнародних ініціативах і проєктах у сфері економічної безпеки	32	1	0,9	0,8	36
Активізація залучення інвестицій та інноваційних ресурсів	14	1	0,9	1	13,0
Формування спільного цифрового простору у культурній, науковій та бізнес-сферах	22	0,9	0,8	0,8	19,6
Гармонізація законодавства та інституційної системи безпеки відповідно до європейських стандартів	32	1,8	0,8	2	23

Джерело: [22, с. 131]

З огляду на зазначене, доцільним є додаткове оцінювання ефективності визначених напрямів із застосуванням альтернативного інструменту — матриці «Value vs Effort» (рис. 1), що дозволяє більш комплексно зіставити очікувані результати та необхідні витрати.

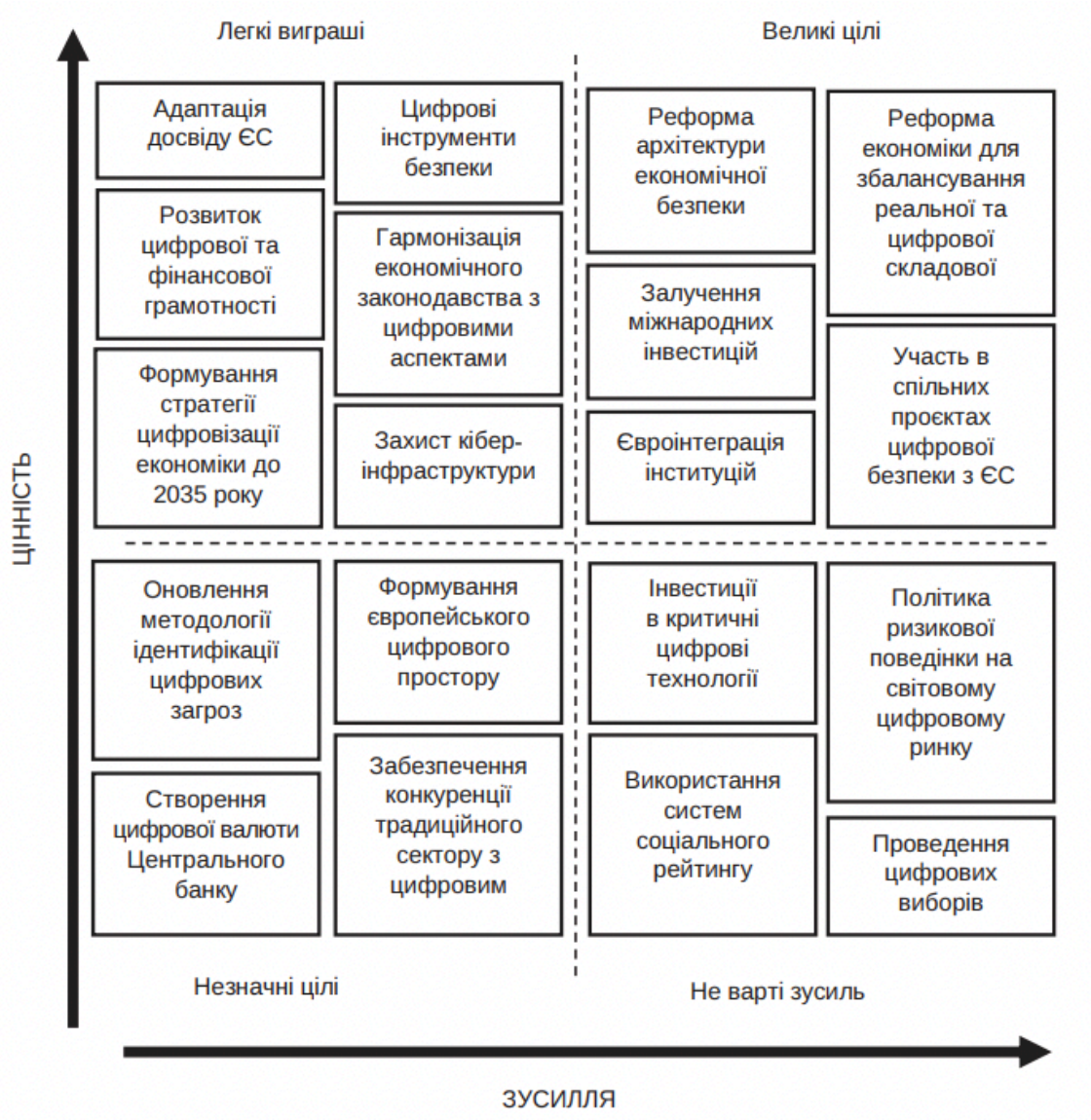

Рис. 3.1. Матриця «Value vs Effort» пріоритезації напрямів захисту національних економічних інтересів України від цифрових загроз

Джерело: [22, с. 132]

Отже, проаналізувавши наведені положення є підстави стверджувати, що найбільший вплив і водночас найвищу ресурсну затратність мають процеси економічних перетворень та інтеграції до європейського простору, які слід розглядати як пріоритетні напрями зміцнення економічної безпеки України в умовах цифрової трансформації. Водночас реалізація таких завдань, як проведення реформ, залучення зовнішніх інвестицій і участь у міжнародних безпекових ініціативах, потребує значних зусиль і координації, тому їх доцільно

впроваджувати поетапно, з урахуванням складності та взаємозалежності зазначених процесів.

3.2. Формування ефективної державної політики та стратегічні механізми забезпечення економічної безпеки в умовах цифрової трансформації

Трансформація глобального економічного простору під впливом масштабної діджиталізації актуалізує питання перегляду фундаментальних засад державного управління у сфері захисту національних інтересів. Побудова дієвої моделі забезпечення економічної безпеки вимагає відходу від фрагментарних регуляторних актів на користь цілісної державної стратегії, спроможної адаптуватися до динамічних цифрових викликів. Означений процес передбачає імплементацію багаторівневих механізмів, де поєднуються міжнародна інтеграція, інституційне оновлення та розвиток автономних ринкових систем саморегуляції.

Пріоритетним вектором формування безпекової політики виступає поглиблення інтеграції України у міжнародні, зокрема європейські, структури модерації цифрових процесів. Синхронізація національного законодавства із загальноєвропейськими стратегіями розвитку цифрового ринку дозволяє не лише масштабувати захист господарюючих суб’єктів, а й залучити потужний інструментарій колективної безпеки. Спільні заходи у межах партнерства з Європейським Союзом створюють підґрунтя для вироблення єдиних стандартів кіберзахисту фінансових установ, промислових комплексів та логістичних мереж. Участь у транскордонних ініціативах забезпечує доступ до передових технологій моніторингу загроз, що мінімізує вразливість вітчизняного виробника перед зовнішніми деструктивними впливами і дозволить перенести акцент із локального реагування на глобальну превенцію, де національна

економічна безпека розглядається як невід'ємна частина загальноєвропейської стабільності [23, с. 132-133].

Ефективність безпекозабезпечувальних заходів безпосередньо залежить від глибини структурних та інституційних реформ, спрямованих на оновлення нормативно-правового базису. Застарілі регуляторні норми часто виступають бар'єром для інноваційного розвитку, створюючи правовий вакуум у критично важливих сегментах цифрової економіки. Відповідно, формування державної політики має ґрунтуватися на принципах випереджального нормотворення, котре враховує появу новітніх технологій штучного інтелекту, хмарних обчислень та блокчейн-платформ. Насичення законодавчого поля чіткими юридичними дефініціями та механізмами відповідальності у віртуальному середовищі створює прогнозовані умови для бізнесу та підвищує рівень довіри споживачів до цифрових послуг. Водночас підтримка загальнонаукового дискурсу у межах безпекології виступає інтелектуальним фундаментом для розробки методологічного апарату оцінювання ризиків, що дозволяє державним органам приймати обґрунтовані управлінські рішення на основі математичних моделей та прогнозних сценаріїв [23, с. 133-134].

Захищеність телекомунікаційних мереж, енергетичних контурів та банківських систем становить ядро економічної стійкості держави, тому важливим компонентом стратегічних механізмів захисту національних інтересів є модернізація та забезпечення стійкості існуючої інфраструктури. Замість прямого директивного втручання та надмірної централізації управління, державна політика повинна стимулювати інституційно-правову саморегуляцію ринку. Створення автономного середовища, де суб'єкти господарювання зацікавлені у самостійному впровадженні високих стандартів безпеки, дозволяє знизити адміністративне навантаження та підвищити адаптивність економіки. Держава за вказаних умов перебирає на себе роль арбітра та

координатора, встановлюючи рамкові вимоги та забезпечуючи підтримку критичних вузлів інфраструктури, тоді як ринкові механізми забезпечують гнучкість та інноваційність засобів захисту [24].

Реалізація окресленої моделі вимагає посилення інституційної спроможності органів виконавчої влади та координації зусиль під егідою Ради національної безпеки і оборони України. Стратегічне планування має включати регулярний моніторинг технологічних трендів та оперативне корегування пріоритетів залежно від зміни ландшафту загроз. Важливо забезпечити синергію між державним сектором, науковими установами та приватним IT-бізнесом, оскільки тільки такий симбіоз здатний згенерувати ефективні відповіді на кібертероризм та цифрові маніпуляції. Фінансові інструменти підтримки цифрових трансформацій повинні спрямовуватися не лише на закупівлю закордонного обладнання, а й на стимулювання розробки вітчизняних криптографічних рішень та підготовку кадрів нової генерації, здатних оперувати у складному цифровому ландшафті.

Особливе значення має формування культури цифрової гігієни та грамотності серед усіх бенефіціарів безпеки – від рядових громадян до керівників великих корпорацій. Соціальний вимір державної політики передбачає створення доступних освітніх програм, спрямованих на мінімізацію ризиків соціальної інженерії та підвищення обізнаності щодо прав і обов'язків у мережі. Зниження рівня вразливості людського фактору автоматично підвищує загальну стійкість економічної системи, оскільки значна частина інцидентів виникає саме через необізнаність користувачів [25, с. 136-137].

Отже, можна констатувати, що формування державної політики забезпечення економічної безпеки в умовах цифрової трансформації являє собою складний процес балансування між контролем та свободою інновацій. Ключ до успіху полягає у створенні гнучкої нормативно-правової архітектури, здатної інтегруватися у міжнародний безпековий

простір, підтримуючи при цьому внутрішню автономність та конкурентоспроможність національної економіки. Тільки поєднання міжнародного співробітництва, глибоких інституційних перетворень та інфраструктурного розвитку дозволить Україні нівелювати вплив цифрових загроз і забезпечити сталий розвиток у довгостроковій перспективі. Сформовані стратегічні механізми повинні стати надійним щитом для національних економічних інтересів, гарантуючи суверенітет держави у віртуальному та реальному вимірах

ВИСНОВКИ

Проведене дослідження дозволило встановити, що економічна безпека держави у сучасних умовах трансформувалася у динамічну систему технологічної та інституційної стійкості, де захищеність національних інтересів безпосередньо залежить від рівня адаптивності до цифрових трансформацій. Встановлено, що цифровізація виступає водночас каталізатором економічного розвитку та джерелом принципово нових деструктивних впливів, котрі нівелюють традиційні методи державного регулювання. Сутність механізму забезпечення економічної безпеки за даних обставин полягає у формуванні випереджальних заходів протидії загрозам, що виникають у віртуальному просторі та мають пряму проекцію на реальний сектор господарювання.

Під час аналізу виявлено появу якісно нових чинників ризику, серед яких особливу небезпеку становлять синтетичне шахрайство з ідентифікацією, професіоналізація криптоджекінгу та використання генеративного штучного інтелекту для дестабілізації фінансових ринків. Окреслені явища призводять до розмивання податкової бази, втрати контролю над транскордонним рухом капіталу та підриву інвестиційної привабливості держави. Доведено, що джерелом небезпеки стає сама логіка функціонування сучасних інформаційних екосистем, де вразливість програмних інтерфейсів та ланцюгів постачання цифрових послуг дозволяє зловмисникам здійснювати масштабне промислове шпигунство та блокувати роботу суб'єктів критичної інфраструктури.

Особливого значення набули результати оцінювання впливу збройної агресії та кібератак протягом 2023–2026 років. Встановлено, що ворожа стратегія еволюціонувала у бік системного кібервиснаження національної економіки через точкові удари по вузлах зв’язку, енергетиці та логістиці. Масштабні інциденти, пов'язані з нейтралізацією мереж мобільних операторів та втручанням у роботу державних реєстрів,

підтвердили здатність цифрової зброї паралізувати безготівкові розрахунки, припиняти експортні операції та створювати умови для юридичного хаосу.

На основі застосування методики RICE визначено пріоритетні напрями зміцнення економічної безпеки України. Найбільш ефективним вектором розвитку встановлено інтеграцію до європейського безпекового простору та гармонізацію нормативно-правового забезпечення відповідно до міжнародних стандартів. Доведено, що залучення до колективних механізмів захисту та спільних ініціатив Європейського Союзу дозволяє значно підвищити рівень стійкості інформаційних мереж при раціональному використанні обмежених внутрішніх ресурсів. Крім того, виявлено необхідність стимулювання інституційно-правової саморегуляції ринку, де державне втручання замінюється створенням автономного середовища, здатного до самостійного нівелювання загроз через впровадження високих технологічних регламентів.

Завершальним положенням дослідження виступає обґрунтування стратегічних механізмів державної політики, котрі мають базуватися на принципах технологічної незалежності та проактивного моделювання ризиків. Встановлено, що гарантування економічної безпеки вимагає синергії між державним сектором, науковими установами та приватним IT-бізнесом для розробки вітчизняних криптографічних стандартів та програмних продуктів. Оновлення методологічного апарату оцінювання загроз та розвиток цифрових компетентностей персоналу визначено як базові передумови збереження фінансового суверенітету. Сформована у роботі комплексна модель захисту національних інтересів дозволяє Україні мінімізувати деструктивний вплив цифрових трансформацій та забезпечити стабільний розвиток господарського комплексу у довгостроковій перспективі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Живка З. та ін. Економічна безпека держави : навчально-методичний посібник. Черкаси : видавець Чабаненко Ю.А., 2019. 240 с.
2. Варналій З. С. Економічна та фінансова безпека України в умовах глобалізації. Київ : Знання України. 2020. 423 с
3. Про Стратегію економічної безпеки України на період до 2025 року: Рішення від 11.08.2021 року n0048525-21 / *РНБО*. URL: https://zakon.rada.gov.ua/laws/show/n0048525-21#Text (дата звернення: 26.03.2026)
4. Економічна безпека держави: навчально-методичний посібник / Живко З.Б., Черевко О.В., Копитко М.І., Зачосова Н.В., Живко М.О., Середа В.В., Занора В.О., Бієвець А.В.; за ред. Живко З.Б. Черкаси : видавець Чабаненко Ю.А., 2019. 240 с.
5. Денисов О.Є. Сутність поняття економічної безпеки та її вплив на розвиток державності. *Економіка та держава*. 2016. № 7. С. 52-57;
6. Гнатенко В. Основні складові економічної безпеки держави. *Науковий вісник: Державне управління*. 2021. №1 (7). С. 66-82
7. Реслер М., Лінтур І., Цигак О. Цифрова економіка: виклики та можливості. *Економіка та суспільство*. 2024. № 64. URL: https://doi.org/10.32782/2524-0072/2024-64-117 (дата звернення: 29.03.2026)
8. Сторчак С.В. Вплив розвитку цифрової економіки на економічну безпеку держави. *Економіка та суспільство*. 2025. Вип. 71. URL: https://economyandsociety.in.ua/index.php/journal/article/view/5526/5464 (дата звернення: 30.03.2026)
9. Кириленко С.В. Система економічної безпеки в умовах цифрової економіки. *Журнал стратегічних економічних досліджень*. 2024. № 1(18). С. 40-47;
10. Пустовойт О. В. Цифрова економіка України: окремі підходи до

вимірювання та аналізу. *Економіка України*. 2025. № 68(8(765). С. 3–25;

11. Уткіна М.С. Цифровізація та вплив на фінансову безпеку в Україні: виклики та перспективи. *Наукові перспективи*. 2023. № 11(43). С. 1075-1083;
12. Калініченко О.В. Зовнішні та внутрішні загрози економічній безпеці України. *Інтелект XXI*. 2024. № 2. С. 25-35;
13. Безп'ятко О.А., Стопчак С.Г., Лавров Р.В. Концепційні підходи до формування моделі економічної безпеки держави в умовах диджиталізації. *Агросвіт*. 2024. № 8. С. 49-57;
14. Машненков К., Деркаченко Ю. Вплив гібридних загроз на економічну безпеку держави: механізми адаптації публічного управління в контексті цифрової трансформації. *Scientific journal Herald of Khmelnytskyi National University. Economic sciences*. 2026, № 1. С. 55-60;
15. Максименко А.П., Маслій О.А. Ризики та загрози економічній безпеці України у цифровій сфері в умовах війни. *Ринкова економіка: сучасна теорія і практика управління*. 2022. Том 21. Вип. 3(52). С. 179-199;
16. Маслій О.А., Глушко А.Д. Державне фінансове регулювання як інструмент мінімізації загроз економічній безпеці України в умовах воєнного стану. *Цифрова економіка та економічна безпека*. 2022. Вип. 2 (02). С. 125–130.
17. Максименко А.П. Реальні та потенційні загрози цифрової економіки в умовах війни. *Економічний простір*. 2023. № 188. С. 41-49;
18. Пікуліна О.В., Чаркіна Т.Ю. Специфіка забезпечення економічної безпеки в умовах воєнного стану. *Економічна наука*. Інвестиції: практика та досвід. 2025. № 22. С. 87-94;
19. Бередд Д., Цаль-Цалко Ю. Формування економічних індикаторів національної безпеки в умовах цифровізації бізнесу та змін в економіці. *Суспільство та безпека*. 2024. № 1(2). С. 3-13;

20. Шевчук І., Депутат Б., Тарасенко О. Цифровізація та її вплив на економіку України: переваги, виклики, загрози й ризики. *Причорноморські економічні студії*. 2019. Випуск 47-2. С.173-77.
21. Милашко О.Г., Дем'яненко Д.М. Цифрові технології та їх вплив на розвиток економіки України. *Науковий вісник Одеського національного економічного університету*. 2025. № 12 (337). С. 24-30;
22. Максименко А.П. Пріоритетні напрями запобігання загрозам економічної безпеки України в умовах цифровізації. *Цифрова економіка та економічна безпека*. 2025. Вип. 2(17). С. 128-135;
23. Череп О. Г., Дашко І. М., Бехтер Л. А., Підлісний Р. О. Переваги та виклики цифровізації економіки України. *Український журнал прикладної економіки та техніки*. 2024. Том 9. № 1. С. 131-135.
24. Варламова М. Л., Любасюк В. Е. Економічна безпека України: виклики та перспективи. *Мультидисциплінарний Міжнародний науковий журнал «Інтернаука»*. Серія: «Економічні науки». 2024 №11/166. URL: https://doi.org/10.25313/2520-2057-2024-11-10443 (дата звернення: 12.04.2026)
25. Папирін Д.О. Механізми забезпечення економічної безпеки України в умовах формування ринкової економіки: стратегічні виклики та перспективи. *Актуальні проблеми державного управління*. 2024. № 2 (65). С. 130-148.