

Державний науково-дослідний інститут інформатизації та моделювання економіки

ФОРМУВАННЯ РИНКОВИХ ВІДНОСИН В УКРАЇНІ

**Збірник наукових праць
№6 (289)**

Київ 2025

**Формування ринкових відносин в Україні: Збірник наукових праць
Вип. 6 (289). – К., 2025. – 115 с.**

Рекомендовано Вченою радою ДНДІМЕ

Протокол №5 від 29.04.2025 р.

Збірник статей присвячено науковим здобуткам молодих науковців – аспірантів та здобувачів наукових ступенів кандидата та доктора економічних наук. Він охоплює широкий спектр проблем із таких напрямів:

- макроекономічні аспекти сучасної економіки;
- інноваційно–інвестиційна політика;
- економічні проблеми розвитку галузей та видів економічної діяльності;
- розвиток регіональної економіки;
- соціально–трудова проблеми.

Розраховано на науковців і спеціалістів, які займаються питаннями управління економікою та вивчають теорію та практику формування ринкових відносин в Україні.

Відповідно до Наказу Міністерства освіти і науки України від 28 грудня 2019 р. № 1643 даний збірник віднесено до Переліку наукових фахових видань України, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора і кандидата наук, категорія «Б».

РЕДАКЦІЙНА КОЛЕГІЯ

СТУДІНСЬКА Г.Я., доктор економічних наук (головний науковий редактор)
ХОДЖАЯН А.О доктор економічних наук, професор (заступник наукового редактора)
ПАСІЧНИК Ю.В. доктор економічних наук, професор (заступник наукового редактора)
ЗАХАРІН С.В., доктор економічних наук, с.н.с. (заступник наукового редактора)
АЛЕКСЄЄВ І.В., доктор економічних наук, професор
НЕБОТОВ П.Г., кандидат економічних наук, директор
ВАРНАЛІЙ З.С., доктор економічних наук, професор
ГУЖВА І.Ю., доктор економічних наук
КИЗИМ М.О., доктор економічних наук, професор, член–кор НАНУ
КУЛЬПІНСЬКИЙ С.В., доктор економічних наук
КОРНЄЄВ В.В., доктор економічних наук, професор
ВАСИЛЬЧАК С.В., доктор економічних наук, професор
ЛОПУШНЯК Г.С., доктор економічних наук, професор
КИЧКО І.І., доктор економічних наук, професор
ШОСТАК Л.Б., доктор економічних наук, професор
ГАРБАР Ж.В., доктор економічних наук, доцент, професор
ЧЕРКАШИНА К.Ф., кандидат економічних наук, доцент
ІВАНОВ Є.І., кандидат економічних наук (відповідальний секретар)

МІЖНАРОДНА РЕДАКЦІЙНА РАДА

АГНЄШКА ДЗЮБІНСЬКА, доктор філософії, Економічний університет м. Катовіце, Польща, професор кафедри менеджменту підприємства
АДАМ САМБОРСЬКІ, доктор філософії, Економічний університет м. Катовіце Польща, кафедра менеджменту підприємства
ВІРГНІЯ ЮРЕНІСНЕ, професор, доктор наук, завідувач кафедри філософії та культурології, Каунаський факультет, Вільнюський університет, Литва
ГОРБОВИЙ АРТУР ЮЛІАНОВИЧ, професор, доктор технічних наук, Словацька Академія аграрних наук, член відділення економіки та менеджменту, (Словацька республіка)
ДІАНА СПУЛБЕР, доктор філософії, Університет Генуї, асистент професора кафедри філософії суспільств, м. Генуя (Італія)
ІВАН ТЕНЕВ ДМІТРОВ, професор, доктор економічних наук, Університет «проф. д–р Асен Златаров», завідувач кафедри економіки і управління, м. Бургас (Болгарія)
МІТАР ЛУТОВАЦ, професор, доктор технічних наук, Університет Уніон ім. Миколи Тесла, факультет індустріального управління, завідувач кафедри технологій, м. Белград (Сербія)
ЮРАЙ СІПКО, професор, доктор економічних наук, Словацька Академія наук, директор інституту економічних досліджень, м. Братислава (Словацька республіка)
СОФІЯ ВИШКОВСЬКА, професор, доктор наук, зав. кафедри організації і управління (факультет управління) Технологічно–продюсний університет ім. Яна і Єнджея Снядецьких у Бидгощі, Бидгощ, Польща
СТЕФАН ДИРКА, доктор економічних наук, професор, Вища економічна школа, м. Катовіце, Польща, професор кафедри менеджменту і маркетингу. Міжнародний акредитор Міністерства науки і освіти Республіки Казахстан
ТОМАШ БЕРНАТ, професор, доктор наук, завідувач кафедри мікроекономіки, факультет економіки і менеджменту, Щецинський університет, Польща

Друковане періодичне видання «Формування ринкових відносин в Україні»
внесене в міжнародну базу даних періодичних видань:
ISSN 2522–1620

Key title: Formuvannâ rinkovih vidnosin v Ukraïni
Abbreviated key title: Form. rinkovih vidnosin Ukr.

Індексування і реферування: Україніка Наукова, Джерело

Міжнародні інформаційні та наукометричні бази даних: Google Scholar, Index Copernicus International (ICI), Національна бібліотека України імені В.І. Вернадського.

Формування ринкових відносин в Україні, 2025. Свідоцтво про державну реєстрацію друкованого засобу масової інформації Серія КВ 22545–12445ГПР від 20.02.2017 року

© Державний науково–дослідний інститут інформатизації та моделювання економіки, 2025

Цифрова трансформація та кіберстійкість енергетичної інфраструктури України в умовах воєнних загроз

Актуальність теми дослідження. Умови воєнних загроз в Україні актуалізували питання енергетичної безпеки та стійкості критичної інфраструктури. Зростання кіберзагроз у поєднанні з необхідністю цифрової трансформації енергетичного сектору вимагає пошуку нових стратегічних та управлінських рішень для забезпечення його надійного функціонування.

Мета дослідження – оцінка викликів і перспектив цифрової трансформації енергетичної інфраструктури України та визначення механізмів підвищення її кіберстійкості в умовах воєнних дій.

Методи дослідження. Використано системний та ризик–орієнтований підходи, методи аналізу загроз, порівняльний аналіз міжнародного досвіду кіберзахисту енергетичних систем, а також елементи сценарного моделювання.

Результати роботи. Обґрунтовано напрями цифрової трансформації енергетичного сектору України, визначено ключові вектори підвищення кіберстійкості інфраструктури, окреслено роль державної політики та міжнародного співробітництва у сфері кіберзахисту. Запропоновано концептуальні підходи до формування стратегії кіберстійкості енергетики у воєнний та післявоєнний період.

Галузь застосування результатів. Результати можуть бути використані у сфері державного управління енергетичною безпекою, при розробці національних стратегій цифрової трансформації та у діяльності енергетичних компаній для удосконалення систем кіберзахисту.

Висновки. Поглиблення цифрової трансформації та розвиток кіберстійкості енергетичної інфраструктури є ключовими передумовами забезпечення енергетичної безпеки України в умовах війни. Це дозволить знизити ризики кібератак, зміцнити національну енергетичну систему та створити базу для сталого розвитку у післявоєнний період.

Ключові слова: енергетична інфраструктура, цифрова трансформація, кіберстійкість, енергетична безпека, воєнні загрози, ризик–орієнтований підхід.

TETIANA MELNYK
YANA KOVAL

Digital transformation and cyber resilience of Ukraine's energy infrastructure in the context of military threats

The relevance of the research. The conditions of military threats in Ukraine have brought the issues of energy security and critical infrastructure resilience to the forefront. The growth of cyber threats, combined with the need for digital transformation of the energy sector, requires the search for new strategic and managerial solutions to ensure its reliable functioning.

The purpose of the study is to assess the challenges and prospects of the digital transformation of Ukraine's energy infrastructure and to identify mechanisms for increasing its cyber resilience in the context of military operations.

Research methods. Systemic and risk-oriented approaches, threat analysis methods, comparative analysis of international experience in cyber protection of energy systems, as well as elements of scenario modeling were used.

Results of the work. The directions of digital transformation of Ukraine's energy sector are substantiated, key vectors for increasing the cyber resilience of infrastructure are identified, and the role of state policy and international cooperation in the field of cyber protection is outlined. Conceptual approaches to the formation of a cyber resilience strategy for the energy sector in the war and post-war periods are proposed.

Scope of application of the results. *The results can be used in the field of state management of energy security, in the development of national digital transformation strategies, and in the activities of energy companies to improve cyber defense systems.*

Conclusions. *Deepening digital transformation and developing cyber resilience in energy infrastructure are key prerequisites for ensuring Ukraine's energy security in wartime. This will reduce the risk of cyberattacks, strengthen the national energy system, and lay the foundation for sustainable development in the post-war period.*

Keywords: *energy infrastructure, digital transformation, cyber resilience, energy security, military threats, risk-based approach.*

Постановка проблеми. Сучасна війна проти України наочно продемонструвала критичну вразливість енергетичної інфраструктури до комплексних загроз, які поєднують фізичне руйнування об'єктів із масштабними кібератаками на системи управління. Енергетичний сектор став однією з основних цілей агресора, адже його дестабілізація має прямий вплив на економічну, соціальну та військову спроможність держави. У цих умовах процес цифрової трансформації енергетики, який є невід'ємною складовою модернізації та інтеграції до європейського енергетичного простору, супроводжується новими ризиками. З одного боку, цифровізація створює передумови для підвищення ефективності управління, розвитку «розумних» мереж і застосування інноваційних технологій. З іншого — вона посилює вразливість інфраструктури до кібератак, які можуть паралізувати роботу систем та завдати значної шкоди національній безпеці. Наявні нормативно-правові та організаційні механізми в Україні лише частково враховують специфіку захисту енергетики від кіберзагроз, що обмежує здатність системи протистояти сучасним викликам. Крім того, кадровий дефіцит і брак фінансування унеможливають реалізацію масштабних цифрових та кіберзахисних проєктів.

Таким чином, виникає об'єктивна потреба у формуванні комплексної стратегії цифрової трансформації та кіберстійкості енергетичного сектору України, яка б поєднувала технологічні, організаційні та правові рішення, враховувала міжнародний досвід і відповідала умовам воєнних загроз.

Аналіз останніх досліджень і публікацій. В умовах повномасштабної війни Росії проти України енергетична інфраструктура країни зазнає значних викликів. Одним із ключових напрямів забезпечення її стійкості є цифрова трансформація та посилення кібербезпеки. Однак, попри

численні дослідження, ця тема залишається недостатньо висвітленою в науковій літературі.

Наприклад, Когут–Ференс, О. І. [1] зазначив, що загрози об'єктам критичної інфраструктури в умовах воєнного стану потребують розробки нових класифікацій та підходів до їх оцінки та захисту. Євтушенко Н., Стеценко Д. [2] проаналізував вплив воєнних загроз на енергетичну інфраструктуру та можливості держави ефективно реагувати на них за допомогою існуючих механізмів. На думку, Дугінець Г., Генералов О., Ніжейко К. [3] зазначають, що роль та місце об'єктів критичної інфраструктури в структурі національної безпеки України, детально описавши фактори, які впливають на їх захищеність. Тульчинська С. О., Солосіч О. С. [4] дослідили трансформаційний вплив цифрових технологій на європейський енергетичний сектор в контексті геополітичної нестабільності та викликів сталого розвитку. Боліла С. [5] дослідила сучасні виклики та тенденції у сфері інформаційної та кібербезпеки в державних структурах України в умовах повномасштабної війни.

Незважаючи на значну кількість досліджень у сфері цифрової трансформації та кіберстійкості енергетичної інфраструктури України, існує потреба в подальшому розвитку цієї теми. Зокрема, необхідно поглибити аналіз специфічних загроз та розробити ефективні стратегії захисту в умовах воєнного часу.

Метою статті є оцінка викликів і перспектив цифрової трансформації енергетичної інфраструктури України та визначення механізмів підвищення її кіберстійкості в умовах воєнних дій.

Виклад основних результатів дослідження. Війна в Україні кардинально змінила уявлення про безпеку критичної інфраструктури. Енергетичний сектор став однією з основних цілей гібридних атак, що поєднують фізичне знищення об'єктів із кібератаками на інформаційно-керуючі системи. У таких умовах цифрова трансформація енерге-

тики набуває подвійного значення: з одного боку, вона створює нові можливості для підвищення ефективності та прозорості управління, з іншого – збільшує вразливість до кіберзагроз. Тому формування комплексної політики кіберстійкості та цифрового розвитку енергетичної інфраструктури є ключовим завданням держави.

Цифрова трансформація енергетичного сектору передбачає інтеграцію цифрових технологій у всі процеси виробництва, передачі та споживання енергії. Йдеться про впровадження «розумних мереж» (smart grids), інтелектуальних систем обліку, автоматизованих платформ управління попитом, а також використання технологій big data, IoT та хмарних рішень [6].

Кіберстійкість у цьому контексті розглядається як здатність енергетичних систем протистояти кіберзагрозам, мінімізувати наслідки атак та швидко відновлюватися після них. Методологічною основою виступає ризик–орієнтований підхід, що дозволяє визначати пріоритети захисту залежно від критичності об'єктів та рівня загроз. Дослідження цифрової трансформації та кіберстійкості енергетики України в умовах воєнних загроз є надзвичайно актуальним, оскільки від стабільності функціонування енергетичного сектору залежить не лише економічна безпека, а й здатність держави протистояти агресії та забезпечувати життєдіяльність суспільства.

Тому основними викликами та проблемами цифрової трансформації в умовах війни можна виокремити:

1. Зростання кількості кібератак. За час війни кількість спроб несанкціонованого доступу до систем енергетики зросла у декілька разів, що підтверджує стратегічну вразливість галузі.

2. Фізичне пошкодження об'єктів. Руйнування електропідстанцій та ліній електропередач поєднується з атаками на їхні цифрові системи управління.

3. Недостатність нормативно–правової бази. Українське законодавство лише частково враховує потреби кіберзахисту енергетики, відсутні комплексні стандарти, гармонізовані з європейськими.

4. Кадровий дефіцит. Недостатня кількість висококваліфікованих фахівців у сфері кіберзахисту енергетики стримує реалізацію стратегічних завдань.

5. Обмежене фінансування. Значна частина ресурсів спрямовується на відновлення зруйно–

ваних об'єктів, що зменшує можливості інвестування у цифрові рішення [7].

Аналіз викликів засвідчує, що цифрова трансформація енергетики України відбувається в умовах безпрецедентного тиску. Поєднання фізичних атак із кібератаками формує багаторівневі загрози, які вимагають комплексного підходу до кіберстійкості. Основними бар'єрами залишаються недостатність нормативно–правового забезпечення, кадровий дефіцит та обмежені фінансові ресурси. Подолання цих проблем є критично важливим для збереження працездатності енергетичної системи, забезпечення стійкості держави у воєнний час та створення основи для післявоєнного відновлення на нових технологічних засадах.

Зважаючи на виявлені проблеми та бар'єри цифрової трансформації енергетичної інфраструктури України в умовах війни, постає потреба у вивченні зарубіжних підходів до організації кіберзахисту. Саме міжнародний досвід може слугувати орієнтиром для формування дієвої моделі кіберстійкості, яка відповідатиме сучасним викликам та інтегруватиме Україну у глобальний простір безпеки [8].

Крім того, у світі активно розробляються моделі кіберстійкості критичної інфраструктури. Зокрема:

ЄС впровадив Директиву NIS2, яка посилює вимоги до кіберзахисту енергетичних компаній та встановлює механізми моніторингу інцидентів.

США застосовують Національну стратегію кібербезпеки, де енергетика визначена серед критичних секторів, для яких діють спеціальні стандарти (NERC CIP).

Ізраїль інтегрував кіберзахист енергетики у військову стратегію, створивши кіберкомандування з функціями швидкого реагування на інциденти.

Україна може адаптувати ці практики, зокрема уніфікувати стандарти з європейськими, запровадити обов'язкове тестування кіберстійкості об'єктів енергетики та розвивати співпрацю з міжнародними центрами реагування на кіберінциденти. Аналіз світових практик засвідчує, що успішні стратегії кіберзахисту енергетики базуються на поєднанні трьох ключових чинників: нормативної уніфікації, інституційної координації та оперативного реагування на загрози. Для України критично важливо гармонізувати національне законодавство з європейськими вимогами, розбудувати систему обов'язкового аудиту та тестування кіберстійкості об'єктів, а також

розширити міжнародну співпрацю. Це дозволить не лише посилити захист у воєнний час, але й закласти основу для післявоєнного відновлення енергетичного сектору на принципах стійкості та інтеграції у світовий безпековий простір [9].

Враховуючи результати проведеного дослідження, доцільно сформувавши ряд пропозицій, які є актуальними для України в сучасних умовах:

1. Формування національної стратегії кіберстійкості енергетики – вона має поєднувати завдання цифрової трансформації з комплексними механізмами захисту інформаційних систем.

2. Впровадження системи багаторівневого кіберзахисту – використання криптографічних протоколів, сегментації мереж, засобів моніторингу та штучного інтелекту для виявлення атак у режимі реального часу.

3. Розвиток людського капіталу – підготовка та перепідготовка кадрів у сфері кібербезпеки енергетики, створення спеціалізованих навчальних програм у вишах.

4. Державна та приватна взаємодія – запровадження партнерств між державними інституціями та енергетичними компаніями у сфері обміну даними про кіберзагрози.

5. Сценарне планування – розробка моделей реагування на різні типи воєнних та кіберзагроз із визначенням алгоритмів відновлення.

Цифрова трансформація енергетичної інфраструктури України є неминучим процесом, який відкриває нові можливості для підвищення ефективності та прозорості управління, але водночас створює додаткові ризики. Кіберстійкість стає ключовим чинником енергетичної безпеки, особливо в умовах воєнних загроз. Для України стратегічним завданням є поєднання процесів цифрової модернізації із системними заходами кіберзахисту, гармонізація стандартів із європейськими, розвиток людського капіталу та активна міжнародна співпраця [10].

Формування ефективної стратегії кіберстійкості енергетики України в умовах воєнних загроз вимагає застосування комплексних та взаємопов'язаних підходів. Вони повинні враховувати як специфіку воєнного часу, так і перспективи післявоєнного відновлення, інтеграції у європейський енергетичний простір та глобальну систему кібербезпеки (рис. 1).

Варто розглянути концептуальні підходи до формування стратегії кіберстійкості енергетики

у воєнний та післявоєнний період більш детально [14]:

1. Системний підхід – кіберстійкість має розглядатися як інтегрована складова енергетичної безпеки, що поєднує технічні, організаційні, управлінські та правові механізми. Це передбачає взаємопов'язаність політики кіберзахисту з іншими аспектами безпеки: фізичною охороною об'єктів, захистом інформаційних систем та відновлювальною інфраструктурою.

Обґрунтування: в умовах гібридної війни ізольовані заходи не дають належного ефекту, тому потрібна цілісна стратегія, що враховує всі рівні загроз.

2. Ризик–орієнтований підхід – розробка та реалізація заходів кіберзахисту має ґрунтуватися на оцінці ризиків для кожного елементу енергетичної системи залежно від його критичності. Це дозволяє концентрувати ресурси на захисті найбільш вразливих і стратегічно важливих об'єктів.

Обґрунтування: обмежені ресурси в умовах війни вимагають раціонального розподілу зусиль і фінансування.

3. Адаптивний підхід – стратегія кіберстійкості повинна передбачати гнучкість і здатність швидко адаптуватися до нових типів загроз. Це означає постійний моніторинг кібератак, створення механізмів оперативного реагування та відновлення роботи після інцидентів.

Обґрунтування: у динамічних умовах воєнних дій та швидкої еволюції кіберзагроз статичні моделі стають неефективними.

4. Міжнародно–інтеграційний підхід – розбудова кіберстійкості повинна спиратися на гармонізацію українських стандартів із європейськими (зокрема, NIS2), участь у глобальних мережах обміну інформацією про кіберінциденти, співпрацю з міжнародними центрами реагування.

Обґрунтування: енергетичні мережі інтегровані у європейський простір, тому забезпечення їхнього захисту потребує єдиних правил та спільної координації.

5. Інноваційно–технологічний підхід – у центрі стратегії має бути впровадження сучасних цифрових рішень: «розумних мереж», систем прогнозування кібератак на основі штучного інтелекту, блокчейн–рішень для захисту даних, автоматизованих платформ кібермоніторингу.

Обґрунтування: технологічний прогрес дає можливість не лише захищати, а й проактивно запобігати загрозам.



Рисунок 1. Концептуальні підходи до формування стратегії кіберстійкості енергетики у воєнний та післявоєнний період

Джерело: сформовано автором на основі даних [11–13]

6. Людиноцентричний підхід – кадрове забезпечення є ключовим елементом кіберстійкості. Необхідно розвивати систему підготовки фахівців з кіберзахисту енергетики, підвищувати рівень культури безпеки серед працівників галузі, створювати спеціалізовані навчальні програми та симуляційні центри.

Обґрунтування: навіть найсучасніші технології є неефективними без належної підготовки персоналу та людського фактору.

Формування стратегії кіберстійкості енергетики у воєнний та післявоєнний період має ґрунтуватися на поєднанні системного, ризик-орієнтованого, адаптивного, міжнародно-інтеграційного, інноваційно-технологічного та людиноцентричного підходів. Така стратегія дозволить не лише ефективно протидіяти сучасним кібератакам, але й створити фундамент для довгострокового розвитку енергетичної інфраструктури України як складової європейського та глобального безпекового простору.

Висновки

Енергетична інфраструктура України є однією з головних цілей гібридних атак, що поєднують фізичне руйнування об'єктів та кібератаки на цифрові системи управління. Це створює подвійний виклик: необхідність одночасно відновлювати

зруйновані об'єкти та посилювати їхній кіберзахист. Цифрова трансформація енергетики є неминучим процесом, адже вона відкриває можливості для підвищення ефективності, інтеграції до європейського енергетичного простору та розвитку «розумних» мереж. Водночас вона підвищує вразливість систем до кібератак, що вимагає комплексних заходів кіберстійкості.

Основні виклики для цифрової трансформації в умовах війни полягають у зростанні кількості кібератак, фізичному пошкодженні об'єктів, недосконалості нормативно-правової бази, кадровому дефіциті та обмеженому фінансуванні. Ці чинники значно ускладнюють розвиток та модернізацію галузі.

Міжнародний досвід (ЄС, США, Ізраїль) демонструє ефективність стратегій кіберстійкості, що базуються на поєднанні нормативної уніфікації, інституційної координації та оперативного реагування. Україна може адаптувати ці підходи через гармонізацію стандартів, створення механізмів аудиту кіберзахисту та посилення міжнародної співпраці. Концептуальні підходи до формування стратегії кіберстійкості енергетики повинні включати системний, ризик-орієнтований, адаптивний, міжнародно-інтеграційний, інноваційно-технологічний та людиноцентричний виміри. Лише їхнє поєднання дозволить створити дієву й

гнучку стратегію, здатну відповідати викликам як воєнного, так і післявоєнного періоду.

Таким чином, цифрова трансформація та кіберстійкість мають розглядатися не лише як інструменти захисту від сучасних загроз, а як стратегічні напрями розвитку української енергетики, здатні гарантувати її безпеку та конкурентоспроможність у майбутньому.

Подальші дослідження можуть зосередитися на розробці методів оцінки кіберризиків для енергетичної інфраструктури, інтеграції цифрових технологій та штучного інтелекту для підвищення стійкості систем, оцінці ефективності державної політики у сфері кібербезпеки, адаптації міжнародного досвіду та розробці стратегій цифрової трансформації для відновлення енергетики після воєнних руйнувань.

Список використаних джерел:

1. Когут–Ференс, О. І. Сучасний стан розвитку та функціонування світового ринку енергетики та торгівлі енергоресурсами. *Scientific notes of Lviv University of Business and Law*, 2022. №32. С. 265–272. URL: <https://nzlubp.org.ua/index.php/journal/article/view/585>

2. Євтушенко Н., Стеценко Д. Цифрова трансформація бізнесу в умовах війни в Україні виклики та можливості. *Економічний простір*, 2024. № 191. С. 211–216. DOI: <https://doi.org/10.32782/2224-6282/191-34>.

3. Дугінець Г., Генералов О., Ніжейко К. Цифрова трансформація європейського енергетичного сектору: виклики сталого розвитку під час геополітичних криз. *Економіка та суспільство*, 2025. Вип. 76. DOI: <https://doi.org/10.32782/2524-0072/2025-76-108>.

4. Тульчинська С. О., Солосіч О. С. Концептуальні засади забезпечення економічної безпеки підприємництва в умовах воєнного стану. *Економіка та управління підприємством. Науковий погляд: економіка та управління*, 2022. № 3 (79). С. 97–102. DOI: [10.51369/3083-5917-2024-1-10](https://doi.org/10.51369/3083-5917-2024-1-10).

5. Боліла С. Роль інформаційних технологій та цифрових інструментів в умовах викликів війни та післявоєнного відновлення економіки України. *Таврійський науковий вісник. Серія: Економіка*, 2023. №(16), 265–275. <https://doi.org/10.32782/2708-0366/2023.16.35>.

6. Панченко О. А., Гнатенко В. С. Економічна кібербезпека в державній системі національної безпеки. *Публічне урядування*, 2021. № 2 (27). С. 22–31. DOI: [https://doi.org/10.32689/2617-2224-2021-2\(27\)-3](https://doi.org/10.32689/2617-2224-2021-2(27)-3).

7. Цифрова трансформація економіки України в умовах війни. URL: <https://niss.gov.ua/news/komentariekspertiv/tsyfrova-transformatsiya-ekonomiky-ukrayiny-v-umovakh-viynyzhovten-2023>

8. Тилігульська ВЕС — символ незламності та еко–трансформації. Україна OSS. 2024. URL: <https://ukraine-oss.com/tyligulska-ves-symvolnezlamnosti-i-ekotransformacziyi-v-diyi>.

9. Семенченко А. І., Мялковський Д. В., Станіславський Т. В. Науково–методологічні підходи до проведення огляду кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури. *Інвестиції: практика та досвід*, 2018. № 18. С. 87–94. URL: <http://www.investplan.com.ua/?op=1&z=6303&i=16>.

10. Томах В., Сігаєва Т., Мартиненко М. Цифрова трансформація управління підприємствами України у контексті сталого розвитку: інноваційні рішення, креативні технології. *Академічні візії*, 2023. Вип. 18. URL: <https://academy-vision.org/index.php/av/article/view/315/277>.

11. Енергетика України 2024–2025 років: у тумані невизначеності. Центр Разумкова. 2024. URL: <https://razumkov.org.ua/statti/energetykaukrainy-20242025-rokiv-u-tumani-nevyznachenosti>.

12. Енергетична безпека України: перспективна модель управління ризиками : монографія / О. М. Суходоля, Ю. М. Харазішвілі, Г. Л. Рязцев; за ред. О. М. Суходолі. Київ : НІСД, 2023. 152с.

13. Перерва П. Г., Ткачова Н. П., Шаульська Л. В. Рефлексивне управління підприємствами в умовах діджиталізації бізнес–процесів в промисловій та аграрній сферах. *Енергозбереження. Енергетика. Енергоаудит*, 2024. №1 (191). С. 87–101.

14. Левчинський Д., Ступнікер Г., Каширнікова І., Зозуля Н. Підприємництво України в умовах воєнного стану. *Економічний простір*, 2022. № 181. С. 110–114.

References:

1. Kohut–Ferens, O. I. (2022) Suchasnyy stan rozvytku ta funktsionuvannya svitovoho rynku enerhetyky ta torhivli enerhoresursamy. *Scientific notes of Lviv University of Business and Law*, №32. S. 265–272. URL: <https://nzlubp.org.ua/index.php/journal/article/view/585>.

2. Yevtushenko, N. & Stetsenko, D. (2024) Tsyfrova transformatsiya biznesu v umovakh viyny v Ukrayini vyklyky ta mozhlyvosti. *Ekonomichnyy prostir*, № 191. С. 211–216. DOI: <https://doi.org/10.32782/2224-6282/191-34>.

3. Duhinets, H., Heneralov, O. & Nizheiko K. (2025) Tsyfrova transformatsiia yevropeiskoho enerhetychno–

ho sektoru: vyklyky staloho rozvytku pid chas heopolitychnykh kryz. Ekonomika ta suspilstvo, Vyp. 76. DOI: <https://doi.org/10.32782/2524-0072/2025-76-108>.

4. Tul'chyns'ka, S. O. & Solosich, O. S. (2022) Kontseptual'ni zasady zabezpechennya ekonomichnoyi bezpeky pidpryyemnytstva v umovakh voyennoho stanu. Ekonomika ta upravlinnya pidpryyemstvom. Naukovy pohlyad: ekonomika ta upravlinnya, № 3 (79). S. 97–102. DOI: [10.51369/3083-5917-2024-1-10](https://doi.org/10.51369/3083-5917-2024-1-10).

5. Bolila, S. (2023) Rol' informatsiynykh tekhnolohiy ta tsyfrovyykh instrumentiv v umovakh vyklykiv viyny ta pislyavoyennoho vidnovlennya ekonomiky Ukrainy. Tavriys'kyi naukovy visnyk. Seriya: Ekonomika, №(16), 265–275. DOI: <https://doi.org/10.32782/2708-0366/2023.16.35>.

6. Panchenko, O. A. & Hnatenko, V. S. (2021) Ekonomichna kiberbezpeka v derzhavniy systemi natsional'noyi bezpeky. Publichne uryaduvannya, № 2 (27). S. 22–31. DOI: [https://doi.org/10.32689/2617-2224-2021-2\(27\)-3](https://doi.org/10.32689/2617-2224-2021-2(27)-3).

7. Tsyfrova transformatsiya ekonomiky Ukrainy v umovakh viyny. URL: <https://niss.gov.ua/news/komentariekspertiv/tsyfrova-transformatsiya-ekonomiky-ukrainy-v-umovakh-viynyzhovten-2023>

8. Tylihul's'ka VES — symbol nezlamnosti ta ekotransformatsiyi. Ukraina OSS. 2024. URL: <https://ukraine-oss.com/tyligulska-ves-symbolnezlamnosti-ekotransformatsiyi-v-diyi>.

9. Semenchenko, A. I., Myalkovs'kyi D. V., Stanislavs'kyi, T. V. (2018) Naukovo-metodolohichni pidkhody do provedennya ohlyadu kiberzakhystu derzhavnykh informatsiynykh resursiv ta krytychnoyi informatsiynoyi infrastruktury. Investytsiyi: praktyka ta dosvid, 2018. №18. S. 87–94. URL: <http://www.investplan.com.ua/?op=1&z=6303&i=16>.

10. Tomakh, V. and Sihayeva, T., Martynenko, M. (2023) Tsyfrova transformatsiya upravlinnya pidpryyemstvamy Ukrainy u konteksti staloho rozvytku: innovatsiyni rishennya, kreatyvni tekhnolohiyi. Akademichni viziyi, Vyp. 18. URL: <https://academy-vision.org/index.php/av/article/view/315/277>.

11. Enerhetyka Ukrainy 2024–2025 rokiv: u tumani nevyznachenosti. Tsentrazumkova. URL: <https://razumkov.org.ua/statti/enerhetykaurainy-20242025-rokiv-u-tumani-nevyznachenosti>.

zumkov.org.ua/statti/enerhetykaurainy-20242025-rokiv-u-tumani-nevyznachenosti.

12. Enerhetychna bezpeka Ukrainy: perspektyvna model' upravlinnya ryzykamy: monohrafiya / O. M. Sukhodolya, Yu. M. Kharazishvili, H. L. Ryabtsev; za red. O. M. Sukhodoli. Kyiv: NISD. 152c.

13. Pererva, P. H., Tkachova, N. P. & Shaul's'ka, L. V. (2024) Refleksyvne upravlinnya pidpryyemstvamy v umovakh didzhytalizatsiyi biznes-protsesiv v promysloviy ta ahraryniy sferakh. Enerhozberezhennya. Enerhetyka. Enerhoaudyt, №1 (191). S. 87–101.

14. Levchyns'kyi, D., Stupniker, H., Kashyrynikova, I. & Zozulya, N. (2022) Pidpryyemnytstvo Ukrainy v umovakh voyennoho stanu. Ekonomichnyy prostir, № 181. S. 110–114.

Дані про авторів

Мельник Тетяна Миколаївна,

доктор економічних наук, професор, завідувач кафедри міжнародного менеджменту, Державний торговельно-економічний університет

<https://orcid.org/0000-0002-3839-6018>

e-mail: t.melnyk@knute.edu.ua

Коваль Яна Сергіївна,

кандидат наук з державного управління, доцент, доцент кафедри міжнародного менеджменту, Державний торговельно-економічний університет

<https://orcid.org/0000-0001-6578-2996>

e-mail: y.koval@knute.edu.ua

Data about the authors

Tetiana Melnyk,

Doctor of Sciences (Economics), Professor, Head of the Department of International Management, State University of Trade and Economics

<https://orcid.org/0000-0002-3839-6018>

e-mail: t.melnyk@knute.edu.ua

Yana Koval,

PhD (Public administration), associate professor, associate professor of the department of international management, State University of Trade and Economics

<https://orcid.org/0000-0001-6578-2996>

e-mail: y.koval@knute.edu.ua

ЗМІСТ

Макроекономічні аспекти сучасної економіки

ВАСИЛЬЧАК С. В. Венчурне фінансування інноваційних технологій в підприємствах в умовах цифровізації та циркулярної економіки.....	5
КОЛОДЯЖНИЙ О. В. Глобальні ризики як фактор трансформації моделей розвитку страхового ринку.....	13
ВІСЯГІН О. О. Цифровізація як чинник формування інклюзивності фінансових послуг.....	21
ПАЛІЙ Н. Р., СЕЛЕПЕЙ Ю. Я. Мінімізація впливу тіньової економіки як стратегічний напрям забезпечення фінансово–економічної безпеки України.....	28

Інноваційно–інвестиційна політика

СТУДІНСЬКА Г. Я. Аналіз досвіду впровадження проєктів у контексті інноваційного розвитку аграрної сфери України.....	35
УСАЧОВ А. І. Користувацький досвід як чинник ефективності цифрової фіскальної політики: аналіз міжнародних практик та українських перспектив.....	48

Економічні проблеми розвитку галузей та видів економічної діяльності

ЧУПРИНА Ю. А., ЧУПРИНА Х. М. Концептуальне обґрунтування диференційованої оцінки ризиків при виборі моделі реалізації державних цільових програм на основі кластерно–інтегративного механізму в будівельному секторі.....	56
МОЛНАР О. С., БАЛОГА П. В. Макроекономічна стабілізація в Україні в умовах воєнного часу.....	70
КУДИРКО Л. П., МАКАРОВА Т. Л. Розвиток ІКТ–сектору у вимірі цифрової трансформації та конкурентоспроможності національних економік.....	75
ПОПРОЗМАН О. І., ПОСТОВА А. В. Вплив стратегії менеджменту персоналу на діяльність підприємства в сучасних умовах.....	81
КРУПСЬКИЙ В. С. Легальна оптимізація як елемент виживання в неконкурентному середовищі сільськогосподарських підприємств.....	89

Соціально–трудова проблема

ШЕДЯКОВ В. Є. Участь у міжнародному поділі праці як напрям економічних відносин.....	94
МЕЛЬНИК Т. М., КОВАЛЬ Я. С. Цифрова трансформація та кіберстійкість енергетичної інфраструктури України в умовах воєнних загроз.....	103