

DOI: <https://doi.org/10.32782/ecovis/2025-3-8>  
УДК 338.246.8:004.9

**Маслій Олександра Анатоліївна**

кандидат економічних наук, доцент,  
доцент кафедри фінансів, банківського бізнесу та оподаткування,  
Національний університет «Полтавська політехніка імені Юрія Кондратюка»  
ORCID: <https://orcid.org/0000-0003-2184-968X>

**Буряк Альона Анатоліївна**

кандидат економічних наук, доцент,  
доцент кафедри міжнародних економічних відносин та туризму,  
Національний університет «Полтавська політехніка імені Юрія Кондратюка»  
ORCID: <https://orcid.org/0000-0002-0814-7459>

**Науменко Олександр Андрійович**

аспірант кафедри фінансів, банківського бізнесу та оподаткування,  
Національний університет «Полтавська політехніка імені Юрія Кондратюка»  
ORCID: <https://orcid.org/0009-0006-9943-9460>

**ДЕТЕРМІНАНТИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ  
В УМОВАХ ІНДУСТРІЇ 4.0**

Стаття присвячена систематизації детермінант економічної безпеки держави в умовах четвертої промислової революції. З урахуванням багатовимірності впливу цифровізації на національну економіку запропоновано класифікацію детермінант економічної безпеки держави в умовах Індустрії 4.0, що охоплює шість груп чинників: економічні, технологічні, кібербезпекові, зовнішньоекономічні, соціально-кадрові та інституційно-правові. Обґрунтовано, що сучасна технологічна революція породжує фундаментальні виклики для економічної безпеки держави, оскільки традиційні механізми захисту національних економічних інтересів виявляються недостатньо ефективними в умовах цифровізації та глобалізації даних. Практичне значення результатів полягає у формуванні концептуальної основи для розробки національної стратегії забезпечення економічної безпеки в цифрову епоху.

**Ключові слова:** економічна безпека держави, Індустрія 4.0, цифрова трансформація, цифровізація економіки, детермінанти економічної безпеки, стратегічні орієнтири, безпекоорієнтоване інформаційне середовище, кібербезпека.

**Oleksandra Maslii**

PhD in Economics, Associate Professor,  
Associate Professor of the Department of Finance, Banking and Taxation,  
National University "Yuri Kondratyuk Poltava Polytechnic"

**Alona Buriak**

PhD in Economics, Associate Professor,  
Associate Professor of the Department of International Economic Relations and Tourism,  
National University "Yuri Kondratyuk Poltava Polytechnic"

**Oleksandr Naumenko**

Postgraduate Student of the Department of Finance, Banking and Taxation,  
National University "Yuri Kondratyuk Poltava Polytechnic"

**DETERMINANTS OF THE STATE ECONOMIC SECURITY IN THE  
CONTEXT OF INDUSTRY 4.0**

The contemporary global economy is undergoing fundamental transformation driven by the Fourth Industrial Revolution, or Industry 4.0, characterized by integration of cyber-physical systems, Internet of Things, cloud computing, artificial intelligence, Big Data analytics, and robotics. These technologies alter not only manufacturing processes but the entire economic architecture, generating unprecedented challenges and opportunities for national economic security. The purpose of this study is to systematize determinants of the state economic security under Industry 4.0 conditions to establish strategic guidelines for ensuring security in accelerated digital transformation. The research proposes a comprehensive classification of economic security determinants encompassing six dimensions: economic, technological, cybersecurity, foreign economic, social and human capital, and institutional-legal factors. The study



demonstrates that no country can achieve economic security without adequate cyberspace protection, as cyber threats have evolved into hybrid warfare instruments capable of destabilizing governance systems. This necessitates treating cybersecurity as an integral component of national defense and economic policy, requiring coordinated efforts across government, private sector, and international partners. The results suggest that institutional-legal determinants form the strategic architecture of digital transformation. Comparative analysis of international experience reveals distinct strategic orientations for ensuring state economic security under Industry 4.0 conditions. Particular attention is devoted to Ukraine, where despite substantial IT capabilities and successful initiatives like the Diia platform, analysis reveals a significant institutional gap characterized by absence of a holistic national strategy integrating economic security considerations within Industry 4.0 context. Practical significance of the research conducted lies in establishing a conceptual framework for developing national strategy of the state economic security that synchronize technological modernization with cybersecurity infrastructure development and institutional capacity building to counter emerging digital economic risks.

**Keywords:** state economic security, Industry 4.0, digital transformation, digitalization of economy, determinants of economic security, strategic guidelines, security-oriented information environment, cybersecurity.

**Постановка проблеми.** Четверта промислова революція, що характеризується цифровізацією виробничих процесів, інтеграцією кіберфізичних систем, технологій штучного інтелекту, Інтернету речей, блокчейну й хмарних обчислень, докорінно трансформує виробничі відносини, традиційні бізнес-моделі та фундаментально змінює архітектуру світової економічної системи. З одного боку, стрімкий розвиток цифрових технологій генерує можливості для економічного зростання, а з іншого – виступає каталізатором принципово нових викликів та загроз економічній безпеці держави, зокрема технологічної залежності, цифрової нерівності, кіберзлочинності, масштабних кібератак, що можуть паралізувати критичну інфраструктуру та дестабілізувати фінансові системи.

В умовах геополітичної турбулентності та гібридних конфліктів виклики цифровізації вимагають перегляду традиційних методів забезпечення економічної безпеки держави та врахування безпекових аспектів економічного розвитку. Основна проблема полягає у відсутності дієвих механізмів та стратегічних орієнтирів забезпечення економічної безпеки держави в умовах цифровізації. Актуальність проблематики дослідження детермінант економічної безпеки держави в умовах Індустрії 4.0 посилюється необхідністю синхронізації темпів технологічної модернізації з розбудовою надійної системи кібербезпеки та формуванням інституційної спроможності держави протидіяти новітнім ризикам цифрової економіки.

**Аналіз останніх досліджень та публікацій.** Дослідження ґрунтується на аналізі наукових публікацій та офіційних стратегічних документів, що висвітлюють вплив Індустрії 4.0 на економічну безпеку держави. Значна увага приділяється дослідженням Стендера С. [1], Шкодіної І. [2], Зелінської Д. [3] та інших, які визначають Індустрію 4.0 як новий етап соціально-економічного розвитку, заснований на кіберфізичних системах. У роботах Онищенко С. [4] Копитко М. [5], Пушака Я. [6], Чайкіної А. [7] та інших розкрито особливості забезпечення економічної безпеки держави в умовах цифрової трансформації. Значна кількість наукових праць, зокрема Гонтаренко Ю. [8], Шпанель-Юхти О. [9] та інших

науковців, присвячена дослідженню соціально-економічних наслідків цифровізації, як-от небезпеки структурного безробіття, зростання цифрової нерівності, прийняття нерелевантних рішень та необхідності забезпечення кібербезпеки. Утім, незважаючи на значний науковий доробок, недостатньо дослідженими залишаються питання систематизації детермінант економічної безпеки держави в умовах Індустрії 4.0 для визначення стратегічних векторів формування безпекоорієнтованого цифрового економічного простору.

**Мета статті** полягає у систематизації детермінант економічної безпеки держави в умовах Індустрії 4.0 для формування стратегічних орієнтирів її забезпечення у контексті прискореної цифровізації економіки.

**Виклад основного матеріалу дослідження.** Сучасний етап техніко-економічного розвитку характеризується безпрецедентною швидкістю й масштабом трансформаційних процесів внаслідок об'єднання фізичних і цифрових систем, впровадження ІТ-технологій, робототехніки, хмарних обчислень, Big Data, штучного інтелекту (ШІ) та інших інтелектуальних виробничих систем, здатних до самоорганізації, автономного прийняття рішень й адаптації до мінливих умов функціонування [10]. На відміну від попередніх промислових революцій, що відбувалися лійно та послідовно, четверта промислова революція розгортається експоненціально, охоплюючи одночасно всі сектори економіки та сфери суспільного життя.

Розвиток Індустрії 4.0 та пов'язаних з нею цифрових технологій призвів до кардинальних змін у соціально-економічній системі: економічні відносини цифровізуються, бізнес-операції здійснюються переважно в цифровому форматі, фінансові ринки функціонують у режимі реального часу, а біржова торгівля трансформувалася у високотехнологічну галузь із миттєвим глобальним зв'язком [2, 3]. Це значно прискорило та збільшило обсяги капіталообігу, що є визначальним детермінантом економічного розвитку, а зростання електронної комерції та стрімінгових платформ наочно демонструє тренд до зміни споживчих звичок та ринкових стратегій.

Інтеграція цифрових технологій у діяльність суб'єктів господарювання та органів влади є потужним чинником підвищення економічної безпеки на макро-, мікро- та нанорівні. Для прикладу, впровадження «розумних» систем безпеки та управління у критичну інфраструктуру, таку як енергетика чи транспорт, дозволяє підвищити її надійність та стійкість в умовах зростаючої кількості цифрових ризиків і загроз завдяки ризик-орієнтованим системам управління [8].

Зазначені трансформації зумовлюють необхідність переосмислення ключових факторів, що визначають стан, динаміку й ефективність системи захисту національних економічних інтересів та забезпечення економічної безпеки держави в умовах Індустрії 4.0. Вважаємо, що під детермінантами економічної безпеки держави варто розуміти сукупність соціально-економічних, фінансових, інституційних та політичних чинників, взаємодія яких формує параметри безпечного функціонування національної економіки та визначає рівень її адаптивності до внутрішніх і зовнішніх ризиків.

В умовах Індустрії 4.0 новими, критично важливими складовими економічної безпеки держави є технологічна, інформаційна та кібербезпека [1, 5], які консолідують основні детермінанти національної стійкості у цифровому просторі. Попередній аналіз трансформаційних процесів, зумовлених Індустрією 4.0 [7, 13], дає змогу запропонувати авторську класифікацію детермінант економічної безпеки держави (рис. 1). В умовах Індустрії 4.0 детермінанти економічної безпеки держави набувають цифрового змісту, адже технологічна незалежність, кіберзахисність, інноваційна спроможність та людський капітал нового покоління формують умови сталого економічного розвитку.

Оптимізація виробництва з використанням сучасних цифрових технологій призводить до підвищення продуктивності, якості продукції з одночасним зниженням витрат, що сприяє економічному зростанню та підвищенню конкурентоспроможності. А глибокий аналіз даних, що стає можливим завдяки IoT та Big Data, дає змогу компаніям розробляти прогностичні моделі для проактивного контролю стану обладнання, уникнення простоїв та забезпечення оптимального використання активів у будь-який час [2, 6]. Ця ланцюгова реакція позитивних ефектів економічних та технологічних детермінант економічної безпеки держави в Індустрії 4.0 стимулює появу нових бізнес-моделей та створює значну додану вартість для споживачів, роблячи економіку більш гнучкою й адаптивною до змін.

Крім цього Індустрія 4.0 трансформує саму природу конкуренції. Замість традиційного протистояння, заснованого на низькій собівартості, з'являються нові форми, такі як «шерінгова економіка» та «спільні інновації», де виробник і споживач взаємодіють для створення нових продуктів і

послуг. Ця концепція дозволяє пропонувати індивідуальні рішення, що мають значну додану вартість для споживачів. Перехід від масового виробництва до гнучкої, індивідуалізованої моделі змінює вимоги до виробництва, адже інтеграція технологій штучного інтелекту у бізнес-процеси може динамічно адаптувати виробничі процеси до змінного продуктового асортименту, що дозволяє оптимізувати використання виробничих потужностей [5]. Цей зсув від масовості до персоналізації робить економіку більш стійкою до зовнішніх шоків, оскільки вона стає менш залежною від глобальних ланцюгів постачання і може швидше реагувати на локальні потреби, що посилює її внутрішню стійкість [6]. Таким чином, сучасні IT-технології визначають фінансово-ресурсну основу економічної безпеки держави у цифрову епоху.

Поряд із можливостями, Індустрія 4.0 породжує низку загроз, що можуть суттєво вплинути на економічну безпеку держави. Головними ризиками є прийняття нерелевантних рішень, питання безпеки даних та значна загроза залежності від іноземних технологій й енергоресурсів, необхідних для їх підтримки, що може призвести до технологічного розриву та підірвати економічний суверенітет.

Відсутність власної інноваційної екосистеми, наприклад, в Україні, що відзначається слабким внутрішнім попитом на інновації в Індустрії 4.0 та відсутністю дієвих стратегій цифрового розвитку, призводить до втрати контролю над стратегічно важливими галузями [2]. Це явище створює «стратегічну пастку» технологічної залежності, в якій національна економіка втрачає суб'єктність у глобальному цифровому просторі, стаючи об'єктом зовнішнього впливу технологічних гегемонів, що фундаментально обмежує можливості реалізації національних економічних інтересів та власного економічного потенціалу. Тому зовнішньоекономічні детермінанти економічної безпеки держави, пов'язані з інтеграцією у світову цифрову економіку, відіграють вагомий роль у забезпеченні довгострокового суверенного розвитку держави.

В умовах Індустрії 4.0 кіберпростір є не лише середовищем для економічної діяльності, а й зоною для потенційної злочинної активності: кібервтручань та кібершахрайства. Цифрова трансформація, збільшення кількості онлайн-операцій та залежність від цифрової інфраструктури генерує нові ризики і загрози, які постійно зростають і включають кібератаки, витоки персональних даних, шпигунство та діяльність шпигунського програмного забезпечення. Масштабні кібератаки, зокрема WannaCry та NotPetya, які завдали сукупних економічних збитків у мільярди доларів США та уразили критичну інфраструктуру IoT-систем, переконливо демонструють, що їхні наслідки виходять далеко за межі технологічних порушень. Ці інциденти засвідчують трансформацію кібер-

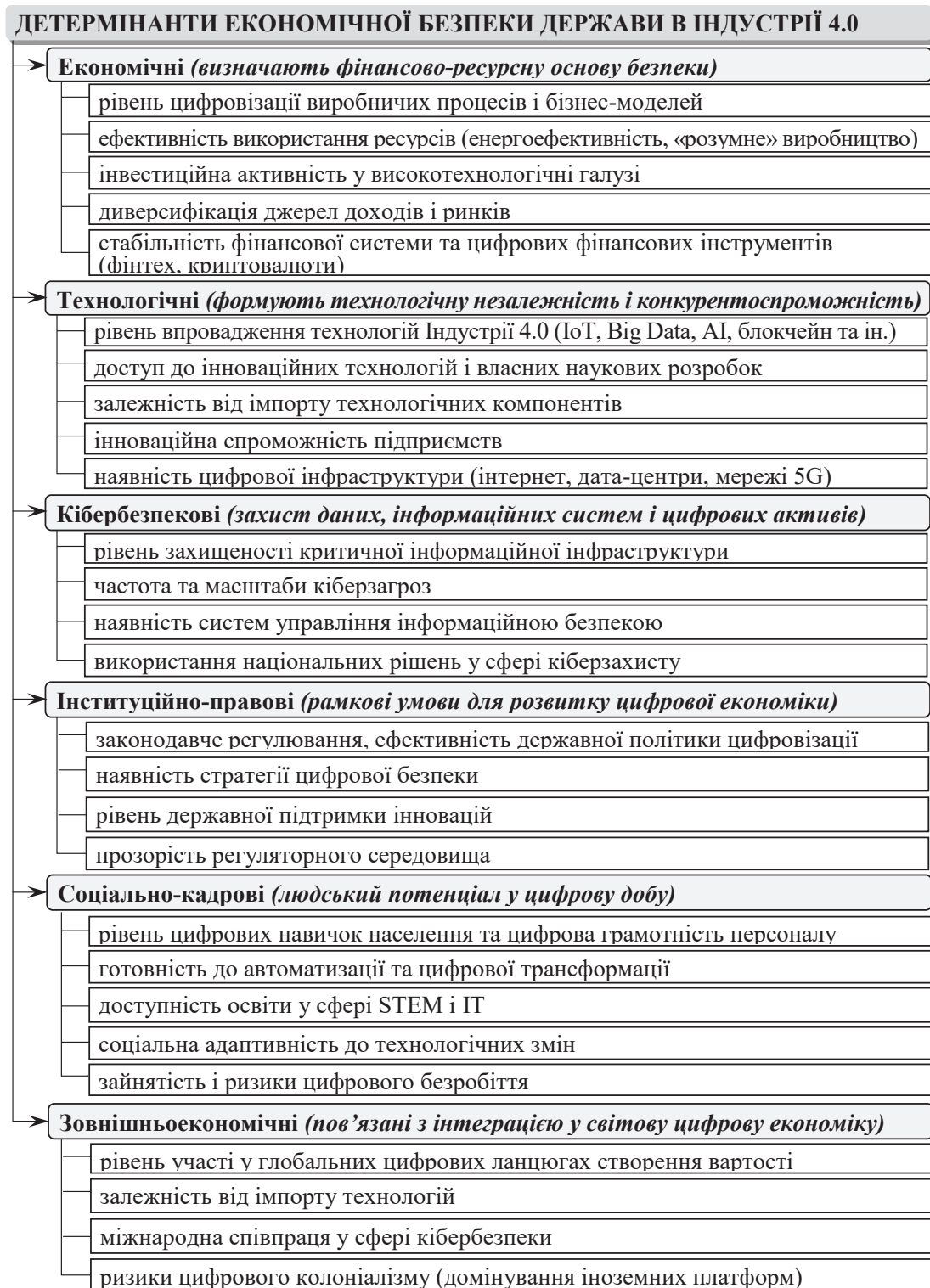


Рис. 1. Класифікація детермінант забезпечення економічної безпеки держави в умовах Індустрії 4.0

Джерело: побудовано авторами на основі [5–11]

загроз у інструмент гібридної війни, спрямований на дестабілізацію системи державного управління та послаблення національної безпеки [1]. Тому надійність цифрової екосистеми, що обслуговує фінансові потоки й соціально-економічні відносини у цифровому просторі, переносить проблему

кіберзахисту з площини технічних збоїв у площину кібербезпекових детермінант економічної безпеки держави [4, 13], що вимагає системного підходу до захисту інформаційних ресурсів [12] та формування безпекоорієнтованого інформаційного середовища національної економіки [18].

Відсутність власної кіберстійкості та технологічного суверенітету робить економіку «мішенню», що створює екзистенційну загрозу економічній безпеці держави [19]. Автоматизація та роботизація, що є основними рисами Індустрії 4.0, змінюють структуру ринку праці. Прогнозується, що на кінець 2025 року частка людської праці в промисловості може впасти з 71% до 58%. Це породжує ризик структурного безробіття та знецінення людської праці перед технологіями. Хоча очікується, що нові технології створять додаткові 133 мільйони робочих місць, вони вимагатимуть інших, більш високих кваліфікаційних вимог [11]. На основі цих даних здійснено узагальнення дуального впливу основних технологій Індустрії 4.0 на економічну безпеку держави (табл. 1).

Зважаючи на дуальний вплив цифровізації технологічний прогрес без належної соціальної адаптації може стати джерелом внутрішньої соціальної нестабільності через нерівномірний доступ до базових цифрових послуг та інформації [9], що є реальною загрозою економічній безпеці держави в умовах Індустрії 4.0. Тому соціально-кадрові детермінанти економічної безпеки держави набувають стратегічного значення для збалансованого переходу до цифрової економіки, забезпечуючи синхронізацію технологічного прогресу з розвитком людського капіталу та збереженням соціальної стабільності.

Важливе значення мають також інституційно-правові детермінанти економічної безпеки держави, які формують стратегічну архітектуру цифрової трансформації. Провідні країни світу розглядають цифрову трансформацію як стратегічний імператив, що інтегрується в їхню національну безпекову та економічну політику. Так, німецька концепція «Industrie 4.0» (2011) орієнтована на посилення конкурентоспроможності обробної промисловості через кіберфізичні системи, мультистейкхолдерну коорди-

націю та цільову підтримку малих і середніх підприємств через фінансування й створення «єдиних вікон» для спрощення переходу до цифрових технологій [14, 15]. Національні стратегії кібербезпеки країн Європейського Союзу, розроблені під егідою European Union Agency for Cybersecurity (ENISA), формують європейську рамку політики кіберстійкості, визначаючи базові принципи, цілі та механізми захисту цифрового простору як ключового елемента економічної безпеки [16]. Китайська програма «Made in China 2025» (2015) передбачає комплексну технологічну модернізацію десяти пріоритетних секторів з метою досягнення інноваційної автономії та реалізації національних економічних інтересів в умовах Індустрії 4.0 [17]. Аналіз зазначених стратегій підтверджує зміщення стратегічних орієнтирів забезпечення економічної безпеки держави у сферу технологічно-інституційного розвитку (табл. 2).

Україна володіє значними конкурентними перевагами, які потенційно можуть забезпечити успішність цифрової трансформації економіки. До таких переваг належать розвинута ІТ-галузь та сформований сегмент компаній-інтеграторів і розробників цифрових рішень, а також унікальний досвід цифровізації державних послуг, втілений у платформі «Дія». Водночас проведений аналіз засвідчує наявність суттєвого інституційного розриву між технологічними можливостями та системою забезпечення економічної безпеки держави. У чинній структурі національної безпеки питанням економічної безпеки в контексті Індустрії 4.0 не приділено належної уваги. Нормативно-правова база характеризується фрагментарністю, а методичний інструментарій оцінювання рівня економічної стійкості та безпеки не адаптований до реалій цифрової економіки.

**Висновки.** Проведене дослідження дало змогу систематизувати детермінанти економічної

Таблиця 1

Дуальний вплив технологій Індустрії 4.0 на економічну безпеку держави

Технологія	Можливості	Загрози
Інтернет речей (IoT)	Оптимальне використання активів, збір глибоких даних, прогнози моделі, підвищення продуктивності	Вразливість до кібератак, злом IoT-систем у виробництві, використання як інструменту гібридної війни
Штучний інтелект (ШІ)	Автоматизація процесів, створення нових продуктів, покращення виробничих процесів, оптимізація	Залежність від рішень, що приймає ШІ, ризик прийняття нерелевантних рішень, несанкціонований доступ до даних
Хмарні обчислення та Big Data	Ефективний збір та аналіз даних, підвищена швидкість, масштабованість, нові бізнес-моделі	Загроза безпеці даних, витік конфіденційної інформації, залежність від постачальників хмарних послуг
Роботизація та автоматизація	Зменшення взаємодії людини у виробництві, підвищення ефективності, конкурентоспроможності, створення нових робочих місць	Знецінення людської праці, структурне безробіття, підвищення кваліфікаційних вимог, соціальні наслідки
Кіберфізичні системи	Інтеграція виробництва з ІТ-технологіями, самоконтрольовані системи, підвищення гнучкості виробництва	Складність захисту даних, ризик кібервтручання в операційні процеси, підвищена кількість інтерфейсів та обсягу даних

Джерело: сформовано авторами на основі [7–11, 13]

Таблиця 2

Стратегічні орієнтири забезпечення економічної безпеки держави в умовах Індустрії 4.0

Країна Критерій	Німеччина	Країни ЄС	Китай	Україна
Назва стратегії	“Industrie 4.0”	Національні стратегії кібербезпеки	«Зроблено в Китаї 2025»	Відсутня цілісна Стратегія економічної безпеки в умовах Індустрії 4.0
Ключові цілі	Зміцнення промисловості, інновації, конкурентоспроможність	Захист критичної інфраструктури, кіберстійкості	Зростання як світового лідера у високотехнологічних галузях, зменшення залежності від іноземних технологій	Фрагментовані ініціативи, відсутність системного бачення
Основні напрями	Стандартизація, підтримка МСП, кластеризація	Захист інфраструктури, протидія загрозам, міжнародна співпраця	Інноваційний розвиток, інтеграція R&D та виробництва	Розвинена ІТ-галузь, але відсутність дієвих промислових стратегій
Інституційна підтримка	“Platform Industrie 4.0”, фінансування досліджень	European Union Agency for Cybersecurity	Центральний народний уряд КНР	Асоціації, окремі відомства
Фокус на безпеці	Стандарти, ІТ-безпека, захист даних	Захист від кіберзагроз, відповідальність розробників	Захист національної безпеки через посилення виробничої могутності	Не приділено належної уваги забезпеченню економічної безпеки держави

Джерело: складено авторами на основі [12, 14–17]

безпеки держави в умовах Індустрії 4.0, виокремивши економічні, технологічні, кібербезпекові, зовнішньоекономічні, соціально-кадрові та інституційно-правові групи чинників. Встановлено дуальний характер впливу цифрових технологій на економічну безпеку держави: поряд із можливостями підвищення продуктивності, конкурентоспроможності та створення нових бізнес-моделей виникають загрози технологічної залежності, кібервразливості та структурних диспропорцій на ринку

праці. Виявлено, що відсутність цілісної державної стратегії цифрової трансформації створює «стратегічну пастку», яка обмежує можливості реалізації національних економічних інтересів на наявного економічного потенціалу. Обґрунтовано необхідність формування безпекоорієнтованого підходу до цифровізації економіки через синхронізацію технологічної модернізації з розбудовою інституційної спроможності держави протидіяти новітнім ризикам цифрової економіки.

СПИСОК ЛІТЕРАТУРИ

1. Стендер С. В., Фротер О. С., Снітко Ю. М. Цифрова інтеграція та кіберзахист економіки України: правові аспекти та інноваційні стратегії. *Академічні візії*. 2023. Вип. 26. URL: <https://academy-vision.org/index.php/av/article/view/799/725>
2. Шкодін І. В., Кондратенко Н. В., Щукіна А. М. Креативна індустрія 4.0: тенденції та трансформації в епоху цифровізації. *Вісник Харківського національного університету імені В. Н. Каразіна*. 2023. № 18. С. 22–30. DOI: <https://doi.org/10.26565/2310-9513-2023-18-03>
3. Зелінська Д. Індустрія 4.0 та її вплив на країни світу в контексті досягнення цілей сталого розвитку-2030. *Галицький економічний вісник*. 2024. Том 91. № 6. С. 133–141. DOI: [https://doi.org/10.33108/galicianvisnyk\\_tntu2024.06.133](https://doi.org/10.33108/galicianvisnyk_tntu2024.06.133)
4. Onyshchenko S., Maslii O., Hlushko A. Digital and Economic Security of the State Under Global Threats. *Lecture Notes in Networks and Systems*. 2025. Vol. 1338. DOI: [https://doi.org/10.1007/978-3-031-89296-7\\_29](https://doi.org/10.1007/978-3-031-89296-7_29)
5. Копитко М. І., Заверуха Д. А. Ключові аспекти впливу Індустрії 4.0 на економічну безпеку держави. *Соціально-правові студії*. 2021. Вип. 4 (14). С. 117–122. URL: <https://dspace.lvduvs.edu.ua/bitstream/1234567890/4285/1/17.pdf>
6. Пушак Я. Я., Трушкіна Н. В. Механізм стратегічного управління економічною безпекою держави в умовах індустрії 4.0. *Ефективна економіка*. 2023. № 8. С. 37–61. DOI: <https://doi.org/10.32702/2307-2105.2023.8.3>
7. Чайкіна А., Маслій О., Черв'як А. Сучасні драйвери підвищення економічної безпеки країни в умовах цифрової трансформації. *Сталий розвиток економіки*. 2024. № 2 (49). С. 307–313. DOI: <https://doi.org/10.32782/2308-1988/2024-49-49>
8. Гонтаренко Ю. Д., Зачосов Н. В. Стратегії управління економічними ризиками об'єктів критичної інфраструктури для стабілізації їх економічної безпеки умовах Vani World та індустрії 4.0. *Цифрова економіка та економічна безпека*. 2023. Вип. 7 (07). С. 165–171. DOI: <https://doi.org/10.32782/dees.7-27>
9. Шпанель-Юхта О. І. Цифрова нерівність та її вплив на нерівномірність доходів у регіонах України. *Цифрова економіка та економічна безпека*. 2024. Вип. 4 (13). С. 130–134. DOI: <https://doi.org/10.32782/dees.13-19>
10. Dodd P. What is Industry 4.0? Everything you need to know. *Fiberroad*. 2022. URL: <https://fiberroad.com/resources/new-trends/what-is-industry-4-0/> (дата звернення: 20.09.2025)

11. What impact does the Industrial Revolution 4.0 have on the labor market? *Athena.blog*. URL: <https://atena.sk/blog/en/what-impact-does-the-industrial-revolution-4-0-on-the-labor-market/> (дата звернення: 20.09.2025).
12. Яковенко Я. Ю., Доманецький І.В. Нормативно-правове регулювання економічної безпеки країни: сучасний стан та перспективи розвитку. *Цифрова економіка та економічна безпека*. 2024. Вип. 6 (15). С. 86–93. DOI: <https://doi.org/10.32782/dees.15-13>
13. Onyshchenko S., Hlushko A., Maslii O., Chumak O. Digital transformation of the national economy in the context of information environment development in Ukraine. *Transformations of national economies under conditions of instability : monograph*. Tallinn : Scientific Route OÜ, 2024. Pp. 169–197. DOI: <https://doi.org/10.21303/978-9916-9850-6-9.ch6>
14. Industrie 4.0. *Federal Ministry for Economic Affairs and Energy*. URL: <https://www.bundeswirtschaftsministerium.de/Redaktion/EN/Dossier/industrie-40.html> (дата звернення: 25.09.2025).
15. Germany – Industry 4.0. European Monitor of Industrial Ecosystems. *European Commission*. URL: <https://monitor-industrial-ecosystems.ec.europa.eu/reports/other-reports/germany-industry-40> (дата звернення: 25.09.2025).
16. National Cyber Security Strategies. *European Union Agency for Cybersecurity*. URL: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies> (дата звернення: 25.09.2025).
17. Notice of the State Council on Strategy “Made in China 2025”. *Official website of the Central People's Government of the PRC*. URL: [https://www.gov.cn/zhengce/content/2015-05/19/content\\_9784.htm](https://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm) (дата звернення: 25.09.2025).
18. Maslii O., Buriak A., Chaikina A., Cherviak A. Improving conceptual approaches to ensuring state economic security under conditions of digitalization. *Eastern-European Journal of Enterprise Technologies*. 2025. Vol 133. Issue 13. Pp. 35–45. DOI: <https://doi.org/10.15587/1729-4061.2025.319256>
19. Завербний А. С., Сало К. Р. Проблеми та перспективи розвитку Індустрії 4.0 в Україні за умов євроінтегрування. *Менеджмент та підприємництво в Україні: етапи становлення та проблеми розвитку*. 2022. № 2 (8). С. 374–382. DOI: <https://doi.org/10.23939/smeu2022.02.374>

#### REFERENCES

1. Stander S. V., Frother O. S., Snitko Y. M. (2023) Tsyfrova intehratsiia ta kiberzakhyst ekonomiky Ukrainy: pravovi aspekty ta innovatsiini stratehii [Digital integration and cyber protection of the economy of Ukraine: legal aspects and innovative strategies]. *Academy Visions*, vol. 26. Available at: <https://academy-vision.org/index.php/av/article/view/799/725> (accessed October 11, 2025)
2. Shkodina I., Kondratenko N., Shchukina A. (2023) Kreatyvna industriia 4.0: tendentsii ta transformatsii v epokhu tsyfrovizatsii [Creative industry 4.0: trends and transformations in the era of digitalization]. *The Journal of V. N. Karazin Kharkiv National University*, is. 18, pp. 22–30. DOI: <https://doi.org/10.26565/2310-9513-2023-18-03>
3. Zelinska D. (2024) Industriia 4.0 ta yii vplyv na krainy svitu v konteksti dosiahnennia tsilei staloho rozvytku-2030 [Industry 4.0 and its impact on world countries in the context of achieving the 2030 sustainable development goals]. *Halytskyi ekonomichnyi visnyk – Galician economic journal*, vol. 91, no 6, pp. 133–141. DOI: [https://doi.org/10.33108/galicianvisnyk\\_tntu2024.06.133](https://doi.org/10.33108/galicianvisnyk_tntu2024.06.133)
4. Onyshchenko S., Maslii O., Hlushko A. (2025) Digital and Economic Security of the State Under Global Threats. *Lecture Notes in Networks and Systems*, vol. 1338. DOI: [https://doi.org/10.1007/978-3-031-89296-7\\_29](https://doi.org/10.1007/978-3-031-89296-7_29)
5. Kopytko M. I., Zaverukha D. A. (2021) Kliuchovi aspekty vplyvu Industrii 4.0 na ekonomichnu bezpeku derzhavy [Key aspects of the impact of Industry 4.0 on the economic security of the state]. *Social & Legal Studios*, is. 4 (14), pp. 117–122. Available at: <https://dspace.lvduvs.edu.ua/bitstream/1234567890/4285/1/17.pdf> (accessed October 11, 2025)
6. Pushak Ya. Ya., Trushkina N. V. (2023) Mekhanizm stratehichnoho upravlinnia ekonomichnoiu bezpekoiu derzhavy v umovakh industrii 4.0 [The mechanism of strategic management of the economic security of the state in the conditions of Industry 4.0]. *Efficient Economy*, is. 8. DOI: <https://doi.org/10.32702/2307-2105.2023.8.3>
7. Chaykina A., Maslii O., Chervyak A. (2024). Suchasni drayvery pidvyshchennya ekonomichnoyi bezpeky krayiny v umovakh tsyfrovoyi transformatsiyi [Modern drivers of increasing the country's economic security in the context of digital transformation]. *Sustainable Development of Economy*, vol. 2 (49), pp. 307–313. DOI: <https://doi.org/10.32782/2308-1988/2024-49-49>
8. Yakovenko Ya. Yu., Domanetsky I.V. (2024) Normatyvno-pravove rehuliuвання економічної безпеки країни: suchasnyi stan ta perspektyvy rozvytku [Regulatory and legal regulation of the country's economic security: current state and development prospects]. *Tsyfrova ekonomika ta ekonomichna bezpeka – Digital Economy and Economic Security*, no. 6 (15), pp. 86–93. DOI: <https://doi.org/10.32782/dees.15-13>
9. Gontarenko Yu. D., Zachosov N. V. (2023) Stratehii upravlinnia ekonomichnymy ryzykamy ob'ektiv krytychnoi infrastruktury dlia stabilizatsii yikh ekonomichnoi bezpeky umovakh Bani World ta industrii 4.0 [Strategies for managing economic risks of critical infrastructure facilities to stabilize their economic security in the context of bani world and industry 4.0]. *Tsyfrova ekonomika ta ekonomichna bezpeka – Digital Economy and Economic Security*, no. 7 (07), pp. 165–171. DOI: <https://doi.org/10.32782/dees.7-27>
10. Dodd P. (2022) What is Industry 4.0? Everything you need to know. *Fiberroad*. Available at: <https://fiberroad.com/resources/new-trends/what-is-industry-4-0/> (accessed September 20, 2025)
11. What impact does the Industrial Revolution 4.0 have on the labor market? *Athena.blog*. Available at: <https://atena.sk/blog/en/what-impact-does-the-industrial-revolution-4-0-on-the-labor-market/> (accessed September 20, 2025)
12. Onyshchenko S., Hlushko A., Maslii O., Chumak O. (2024). Digital transformation of the national economy in the context of information environment development in Ukraine. *Transformations of national economies under conditions of instability : monograph*. Tallinn : Scientific Route OÜ, pp. 169–197. DOI: <https://doi.org/10.21303/978-9916-9850-6-9.ch6>

13. Shpanel-Yukhta O. I. (2024) Tsyfrova nerivnist ta yii vplyv na nerivnomirnist dokhodiv u rehionakh Ukrainy [Digital inequality and its impact on income inequality in the regions of Ukraine]. *Tsyfrova ekonomika ta ekonomichna bezpeka – Digital Economy and Economic Security*, no. 4 (13), pp. 130–134. DOI: <https://doi.org/10.32782/dees.13-19>
14. Industrie 4.0. *Federal Ministry for Economic Affairs and Energy*. Available at: <https://www.bundeswirtschaftsministerium.de/Redaktion/EN/Dossier/industrie-40.html> (accessed September 25, 2025)
15. Germany – Industry 4.0. European Monitor of Industrial Ecosystems. *European Commission*. Available at: <https://monitor-industrial-ecosystems.ec.europa.eu/reports/other-reports/germany-industry-40> (accessed September 25, 2025)
16. National Cyber Security Strategies. *European Union Agency for Cybersecurity*. Available at: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies> (accessed September 25, 2025)
17. Notice of the State Council on Strategy “Made in China 2025”. *Official website of the Central People's Government of the PRC*. Available at: [https://www.gov.cn/zhengce/content/2015-05/19/content\\_9784.htm](https://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm) (accessed September 25, 2025)
18. Maslii O., Buriak A., Chaikina A., Cherviak A. (2025) Improving conceptual approaches to ensuring state economic security under conditions of digitalization. *Eastern-European Journal of Enterprise Technologies*, vol. 133, is. 13, pp. 35–45. DOI: <https://doi.org/10.15587/1729-4061.2025.319256>
19. Zaverbnyi A. S., Salo K. R. (2022) Problemy ta perspektyvy rozvytku Industriii 4.0 v Ukraini za umov yevrointehruvannia [Problems and prospects of the development of Industry 4.0 in Ukraine under the conditions of European integration]. *Menedzhment ta pidpriemnytstvo v Ukraini: etapy stanovlennia ta problemy rozvytku – Management and Entrepreneurship in Ukraine: the Stages of Formation and Problems of Development*, vol. 4, no. 8, pp. 374–382. DOI: <https://doi.org/10.23939/smeu2022.02.374>

Стаття надійшла: 14.10.2025  
Стаття прийнята: 03.11.2025  
Стаття опублікована: 28.11.2025