

*Електронний журнал «Ефективна економіка» включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України № 975 від 11.07.2019). Спеціальності – 051, 071, 072, 073, 075, 076, 292.*  
*Ефективна економіка. 2024. № 12.*

**DOI: <http://doi.org/10.32702/2307-2105.2024.12.76>**

**УДК 338.2**

*С. О. Дегтярьов,  
аспірант кафедри фінансів, банківської справи та страхування,  
Державний біотехнологічний університет  
ORCID ID: <https://orcid.org/0009-0008-5403-3306>*

## **СТРАТЕГІЧНІ ПРІОРИТЕТИ ДЕРЖАВНОЇ ПОЛІТИКИ ЩОДО ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ В УМОВАХ ІНДУСТРІЇ 4.0**

*S. Degtyarev,  
Postgraduate student of the Department of Finance, Banking and Insurance,  
State Biotechnological University*

## **STRATEGIC PRIORITIES OF STATE POLICY TO ENSURE ECONOMIC SECURITY IN THE CONTEXT OF INDUSTRY 4.0**

*Об'єктом дослідження є економічна безпека держави в умовах трансформаційних процесів, зумовлених впровадженням технологій Індустрії 4.0. Предметом дослідження є стратегічні аспекти державної політики, спрямованої на забезпечення економічної безпеки в умовах Індустрії 4.0, зокрема механізми управління ризиками, розвиток технологічної бази, удосконалення кіберзахисту, реформування ринку праці та диверсифікація економіки. Визначено ключові виклики, такі як кіберзагрози, технологічна залежність, структурні зміни ринку праці та економічна нерівність. Обґрунтовано необхідність розвитку національної технологічної бази,*

зміцнення кібербезпеки, реформування ринку праці, диверсифікації економіки та посилення міжнародної співпраці. Підкреслено значення інноваційної інфраструктури, цифрової грамотності та інтеграції передових технологій у ключові галузі. Запропоновані підходи спрямовані на підвищення конкурентоспроможності держави, технологічну незалежність та соціально-економічну стабільність у контексті глобальної цифрової трансформації.

The development of Industry 4.0 is driving fundamental changes in economic, technological and social processes that create new opportunities for economic growth but also increase the level of threats to economic security. Digitalization, automation, and integration of cyber-physical systems are becoming key factors in the competitiveness of countries, but they also pose risks of cyber threats, technological dependence, unequal access to innovative resources, and structural shifts in the labor market.

The problem of ensuring economic security in the face of these challenges is gaining strategic importance for both research and public policy development. Successful resolution of these issues is the basis for maintaining technological independence, economic stability, and sustainable social development in the context of global digital transformation. The scientific aspect includes the study of the impact of digitalization and automation on key parameters of economic security, the development of risk management models and forecasting of cyber threats, as well as the identification of ways to adapt the labor market to new conditions. The practical significance of the problem lies in the development and implementation of innovative approaches to the formation of public policy aimed at strengthening technological independence, increasing the cyber resilience of critical infrastructure, supporting innovative entrepreneurship, and diversifying the economy. Solving this problem will help ensure the competitiveness of the state, the resilience of its economy to modern challenges and threats, and harmonious development in the global digital space.

An analysis of the strategic priorities of state policy to ensure economic security in the context of Industry 4.0 leads to several important conclusions. First, successful

*economic security in the context of digital transformation requires a comprehensive approach that includes the development of national technologies, strengthening cybersecurity, economic diversification, and labor market reform. Secondly, it is crucial to adapt educational and professional programs to the requirements of the digital economy, which will reduce the risks of socioeconomic inequality and ensure the sustainable development of national labor resources. Thirdly, it is necessary to promote international cooperation in the field of cybersecurity and innovation, which will allow the country to remain competitive on a global level.*

**Ключові слова:** *економічна безпека, Індустрія 4.0, державна політика, кібербезпека, цифровізація, інноваційна інфраструктура, технологічна незалежність.*

**Keywords:** *economic security, Industry 4.0, public policy, cybersecurity, digitalization, innovative infrastructure, technological independence.*

**Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями.** Розвиток Індустрії 4.0 зумовлює фундаментальні зміни в економічних, технологічних та соціальних процесах, які створюють нові можливості для економічного зростання, але водночас підвищують рівень загроз економічній безпеці. Цифровізація, автоматизація та інтеграція кіберфізичних систем стають ключовими факторами конкурентоспроможності країн, проте породжують ризики кіберзагроз, технологічної залежності, нерівності доступу до інноваційних ресурсів та структурних зрушень на ринку праці.

Проблема забезпечення економічної безпеки в умовах цих викликів набуває стратегічного значення як для наукових досліджень, так і для розробки державної політики. Успішне вирішення цих питань є основою для збереження технологічної незалежності, стабільності економіки та стійкого соціального розвитку в умовах глобальної цифрової трансформації. Науковий аспект включає дослідження впливу цифровізації та автоматизації на ключові

параметри економічної безпеки, розробку моделей управління ризиками та прогнозування кіберзагроз, а також визначення шляхів адаптації ринку праці до нових умов. Практична значущість проблеми полягає у розробці та впровадженні інноваційних підходів до формування державної політики, спрямованої на зміцнення технологічної незалежності, підвищення кіберстійкості критичної інфраструктури, підтримку інноваційного підприємництва та диверсифікацію економіки. Рішення цієї проблеми сприятиме забезпеченню конкурентоспроможності держави, стійкості її економіки до сучасних викликів та загроз, а також гармонійному розвитку у глобальному цифровому просторі.

***Аналіз останніх досліджень і публікацій.*** Проблеми економічної безпеки держави в умовах Індустрії 4.0 є об'єктом дослідження багатьох вітчизняних науковців, зокрема Микитася А.В., Мандич О.В., Гіржевої О.М., Рижикової Н.І., Савченко М.В., Носалюк Н.І., Заверухи Д.А., Занори В.О., Ганзюк С.М., Драй О.О., Гонтаренко Ю.Д., Зачосової Н.В., Копитко М.І., Кошикова Д.О., Правдивець О., Скоробогатової Н.Є., Товкачової А.С., Федоренко К.В. та багатьох інших. Однак, дана проблематика має ряд дискусійних моментів, особливо у контексті визначення стратегічних пріоритетів державної політики та розробки дієвого інструментарію, а отже потребує детального аналізу і подальших досліджень.

***Формулювання цілей статті (постановка завдання).*** Завданням дослідження є обґрунтування стратегічних пріоритетів державної політики, спрямованої на забезпечення економічної безпеки в умовах Індустрії 4.0, шляхом аналізу основних викликів і загроз, а також визначення ефективних підходів до їх подолання.

***Виклад основного матеріалу дослідження.*** Індустрія 4.0, яка характеризується глибокою цифровізацією, автоматизацією виробництва, інтеграцією кіберфізичних систем і штучного інтелекту, відкриває нові можливості для економічного зростання. Водночас вона породжує низку ризиків для економічної безпеки, зокрема кіберзагрози, структурні зрушення в

ринку праці та технологічну залежність від зовнішніх постачальників. У цих умовах державна політика має забезпечити комплексний підхід до управління економічною безпекою, враховуючи стратегічні виклики та можливості Індустрії 4.0.

Основними викликами економічної безпеки в умовах Індустрії 4.0 є [1, с. 100-103; 2, с. 50-55]:

1. Кібербезпека – широке впровадження цифрових технологій збільшує вразливість до кіберзлочинів, що може призводити до економічних втрат і порушення функціонування критичної інфраструктури.

2. Технологічна залежність – нерівномірний доступ до передових технологій створює ризики для національної технологічної незалежності.

3. Зміни на ринку праці – автоматизація загрожує скороченням робочих місць у традиційних секторах і вимагає перепідготовки кадрів для роботи в умовах цифрової економіки.

4. Економічна нерівність – диспропорції у розвитку регіонів і доступі до цифрових ресурсів можуть поглиблювати соціально-економічну нерівність.

Основними стратегічними пріоритетами державної політики в умовах Індустрії 4.0, за нашими переконаннями, мають бути:

1. Розвиток національної технологічної бази [4, с. 29-32; 6, с. 167-170]:

- створення стимулів для досліджень і розробок у сфері передових технологій;
- підтримка виробництва високотехнологічної продукції в рамках державних програм;
- розвиток інноваційної інфраструктури (технопарки, інкубатори стартапів).

Наприклад, в Україні програму «Horizon Europe» було адаптовано для підтримки наукових досліджень, що дозволяє отримувати фінансування для інноваційних проєктів у сфері ІТ, біотехнологій, робототехніки та інших високотехнологічних галузей. Це стимулює вітчизняні компанії до розробки новітніх технологій та впровадження їх на ринку.

В рамках державної програми «Індустріальна модернізація України», уряд надає субсидії та податкові пільги для підприємств, які впроваджують нові технології в виробництво. Вона включає в себе підтримку виробництва електричних автомобілів, роботизованих систем та іншої продукції, що базується на високих технологіях.

Науковий парк «Київська політехніка» (м. Київ) забезпечує стартапи в Україні не лише приміщеннями та обладнанням, але й підтримкою виведення інноваційних продуктів на ринок. Він надає фінансову підтримку, консалтинг, менторство та створюють середовище для розвитку нових технологічних підприємств.

## 2. Забезпечення кібербезпеки [7, с. 153-157]:

- розробка національної стратегії кібербезпеки з акцентом на захист критичної інфраструктури;
- створення системи моніторингу та реагування на кіберзагрози;
- підвищення рівня цифрової грамотності серед бізнесу та населення.

Ще у 2017 році Україна прийняла «Стратегію кібербезпеки України», яка визначає основні пріоритети для захисту критичної інфраструктури, таких як енергетичні системи, транспорт, комунікації та фінансові установи. В рамках цієї стратегії створено механізми для запобігання кібератакам на ці сектори, а також забезпечення стійкості державних і приватних установ до кіберзагроз. Крім того, в Україні функціонує «Національний координаційний центр кібербезпеки», який відповідає за моніторинг кіберзагроз і реагування на інциденти. Цей центр здійснює збір і аналіз даних про кіберзагрози, координує дії органів державної влади та підприємств щодо запобігання та нейтралізації атак. Також розроблені системи моніторингу інфраструктури в реальному часі, що дозволяють оперативно виявляти аномалії та загрози.

В Україні також активно реалізується ініціатива «Цифрова освіта», яка передбачає освітні програми для підприємців, державних службовців та населення щодо основ кібербезпеки; проводяться тренінги та курси для малих та середніх підприємств, спрямовані на підвищення їх здатності захищати свої

дані і працювати з сучасними технологіями безпеки (зокрема, програми для молоді та студентів сприяють розвитку цифрових компетенцій і захисту особистих даних).

### 3. Реформування ринку праці [9, с. 17-20]:

- запровадження програм перекваліфікації кадрів для роботи з цифровими технологіями;
- сприяння розвитку підприємництва в цифровій економіці;
- інтеграція цифрових компетенцій у освітні програми.

Наприклад, в межах програми «Технічна освіта для цифрової економіки» розроблено курси перекваліфікації для працівників різних галузей. Наприклад, програма «Цифровий лідер» націлена на підготовку спеціалістів з управління цифровими проєктами та бізнес-аналітики. Також активно функціонують ініціативи на базі державних центрів зайнятості, де пропонуються курси для людей, які хочуть перейти на професії, пов'язані з ІТ, кібербезпекою та аналітикою даних.

Для підтримки стартапів та малих підприємств, які працюють у сфері цифрових технологій, реалізуються програми фінансування через фонд «Український фонд стартапів» та «Фонд підтримки інновацій». Ці програми надають гранти, кредити з пільговими умовами та консультаційну підтримку для підприємців, що працюють у таких сферах, як штучний інтелект, блокчейн, електронна комерція та автоматизація бізнес-процесів.

Елементи програми «Цифрова освіта», про яку ми вже згадували, передбачають інтеграцію цифрових технологій і компетенцій у навчальні програми для шкіл, професійно-технічних навчальних закладів та університетів. Наприклад, у рамках програми «Нова українська школа» учні початкових класів отримують базові навички програмування та робототехніки, а в університетах створюються спеціалізовані курси з великих даних, штучного інтелекту та кібербезпеки для підготовки майбутніх спеціалістів для цифрової економіки.

### 4. Диверсифікація економіки [3, с. 62-65; 9, с. 17-21]:

- зменшення залежності від традиційних галузей шляхом розвитку нових секторів економіки;
- залучення інвестицій у сектори, пов'язані з Індустрією 4.0 (штучний інтелект, робототехніка, «зелені» технології).

На сьогоднішній день в Україні реалізуються ініціативи, спрямовані на розвиток ІТ-галузі та стартапів, що дозволяє зменшити залежність від традиційних секторів економіки, таких як важка промисловість. Одним із таких прикладів є створення інноваційних кластерів у Львові, Києві та Одесі, де активно розвиваються стартапи в сферах інформаційних технологій, програмного забезпечення та фінансових послуг. Програма «Цифрова трансформація України» також сприяє інтеграції цифрових технологій у різні сфери економіки, такі як сільське господарство (AgTech), енергетика (Smart Grid), а також розширення експортних можливостей для технологічних компаній.

Державна програма «Green Deal Ukraine» сприяє залученню інвестицій у проекти, пов'язані з екологічно чистими технологіями, такими як відновлювальна енергетика, енергозбереження та переробка відходів. Зокрема, великий інтерес викликають проекти з використання сонячної та вітрової енергетики. Також для підтримки розвитку високотехнологічних стартапів в Україні створено «Фонд розвитку інновацій», який фінансує інвестиції в робототехніку, штучний інтелект і блокчейн-проекти. Наприклад, українська компанія SoftServe активно залучає інвестиції для створення рішень у сфері штучного інтелекту, а також активно працює в галузі автоматизації бізнес-процесів.

#### 5. Міжнародна співпраця [5, с. 30-32; 8, с. 69-70]:

- участь у міжнародних проєктах з розвитку цифрових технологій;
- налагодження партнерств у сфері кібербезпеки та обміну інноваціями;
- гармонізація національного законодавства з міжнародними стандартами цифрової економіки.

Україна активно бере участь у міжнародних проєктах з розвитку цифрових технологій, зокрема компанія «Miratech» бере участь у проєктах по автоматизації бізнес-процесів та розвитку цифрових рішень для міжнародних клієнтів. Також наша держава активно співпрацює з міжнародними організаціями та країнами у сфері кібербезпеки. Одним із прикладів є участь у програмі НАТО щодо розвитку спільних стандартів кібербезпеки, а також співпраця з Європейським Союзом у рамках ініціативи «EU Cybersecurity Strategy», що передбачає спільне реагування на кіберзагрози. Крім того, Україна має партнерства з міжнародними компаніями, такими як Microsoft та Cisco, для обміну передовими технологіями в галузі кіберзахисту та розвитку інноваційних рішень для національних і приватних секторів.

Україна працює над гармонізацією національного законодавства з міжнародними стандартами цифрової економіки через ініціативи, як-от адаптація законів до стандартів ЄС щодо захисту даних (GDPR). Одним із таких кроків стало прийняття Закону України «Про захист персональних даних», який сприяє інтеграції країни в європейський цифровий простір. Також Україна активно працює над імплементацією стандартів е-урядування та цифрових послуг, що відповідають вимогам міжнародних організацій, зокрема ООН та ЄС, для розвитку безпечної та прозорої цифрової економіки.

Отже, в умовах Індустрії 4.0 економічна безпека стає ключовим елементом державної політики, що вимагає комплексного і проактивного підходу. Реалізація стратегічних пріоритетів, спрямованих на зміцнення технологічної незалежності, забезпечення кібербезпеки, підтримку інновацій та реформування ринку праці, дозволить державам зберегти стабільність і підвищити конкурентоспроможність в умовах глобальної цифрової трансформації.

***Висновки та перспективи подальших розвідок у даному напрямі.*** Аналіз стратегічних пріоритетів державної політики щодо забезпечення економічної безпеки в умовах Індустрії 4.0 дозволяє зробити кілька важливих висновків. По-перше, успішне забезпечення економічної безпеки в умовах цифрової

трансформації вимагає комплексного підходу, що охоплює як розвиток національних технологій, так і зміцнення кібербезпеки, диверсифікацію економіки та реформування ринку праці. По-друге, вкрай важливою є адаптація освітніх і професійних програм до вимог цифрової економіки, що дозволить знизити ризики соціально-економічної нерівності та забезпечити стійкий розвиток національних трудових ресурсів. По-третє, необхідно сприяти міжнародній співпраці у сфері кібербезпеки та інновацій, що дозволить країні залишатися конкурентоспроможною на глобальному рівні.

Перспективи подальших досліджень у даному напрямі включають вивчення механізмів інтеграції передових цифрових технологій в національну економіку, розробку моделей адаптації малого та середнього бізнесу до умов Індустрії 4.0, а також оцінку ефективності державних програм кіберзахисту та інноваційної підтримки. Крім того, важливим є розвиток міждержавних ініціатив, спрямованих на гармонізацію нормативно-правових актів у сфері цифрової економіки та технологій, що дозволить забезпечити більш високу стабільність та безпеку в глобальному цифровому середовищі.

### Література

1. Mandych O., Mykytas A., Girzhev O., Ryzhikova N. Management strategies for companies in conditions of development and digital adaptation with AI. *Scientific research in modern conditions of instability*. 2023. Pp. 98-105.
2. Savchenko M., Nosaliuk N. Розвиток індустрії 4.0 та її вплив на економічну безпеку країн. *Actual Problems in Economics*. 2024. С. 48-60.
3. Заверуха Д. Основна характеристика сутності механізму забезпечення економічної безпеки держави в умовах Індустрії 4.0. *Актуальні питання у сучасній науці*. 2023. № 1(7). С. 61-68.
4. Занора В.О. Інноваційний розвиток підприємств в Україні: особливості та проблемні аспекти за умов Індустрії 4.0. *Вісник Черкаського університету. Економічні науки*. 2019. № 2. С. 27-33.

5. Ганзюк С.М., Драї О.О. Загрози фінансовій безпеці України. *Modern Economics*. 2023. № 38. С. 28-33.

6. Гонтаренко Ю.Д., Зачосова Н.В. Стратегії управління економічними ризиками об'єктів критичної інфраструктури для стабілізації їх економічної безпеки умовах BANI WORLD та Індустрії 4.0. *Цифрова економіка та економічна безпека*. 2023. № 7 (07). С. 165-171.

7. Копитко М.І., Заверуха Д.А. Характеристика основних складових забезпечення економічної безпеки держави. *Вчені записки Університету «КРОК»*. № 3 (63). 2021. С. 155-160.

8. Кошиков Д. О. Поняття та класифікація функцій державної політики у сфері забезпечення економічної безпеки держави. *Право і безпека*. 2020. № 1 (76). С. 67-73.

9. Правдивець О. Аналіз результатів вітчизняних наукових досліджень у напрямку інноваційного розвитку системи економічної безпеки підприємства на основі цифрових технологій. *Вчені записки Університету «КРОК»*. 2023. № 1 (69). С. 15-28.

10. Скоробогатова Н.Є., Товкачова А.С., Федоренко К.В. Методи управління економічними ризиками в умовах військового стану. *Матер. III Міжнар. наук.-практ. конф. «Бізнес, інновації, менеджмент: проблеми та перспективи»*. КПІ імені Ігоря Сікорського. 2023. № 7. С. 195-196.

## References

1. Mandych, O. Mykytas, A. Girzhev, O. and Ryzhikova, N. (2023), "Management strategies for companies in conditions of development and digital adaptation with AI", *Scientific research in modern conditions of instability*, pp. 98-105.

2. Savchenko, M. and Nosaliuk, N. (2024), "Development of Industry 4.0 and its impact on the economic security of countries", *Actual Problems in Economics*, pp. 48-60.

3. Zaverukha, D. (2023), "The main characteristics of the essence of the mechanism for ensuring the economic security of the state in the conditions of Industry 4.0", Aktual'ni pytannia u suchasnij nautsi, vol. 1 (7), pp. 61-68.
4. Zanora, V.O. (2019), "Innovative development of enterprises in Ukraine: peculiarities and problematic aspects under the conditions of Industry 4.0", Visnyk Cherkas'koho universytetu. Ekonomichni nauky, vol. 2, pp. 27-33.
5. Hanzhuk, S.M. and Draj, O.O. (2023), "Threats to the financial security of Ukraine", Modern Economics, vol. 38, pp. 28-33.
6. Hontarenko, Yu.D. and Zachosova, N.V. (2023), "Strategies for managing economic risks of critical infrastructure objects to stabilize their economic security under the conditions of BANI WORLD and Industry 4.0", Tsyfrova ekonomika ta ekonomichna bezpeka, vol. 7 (07), pp. 165-171.
7. Kopytko, M.I. and Zaverukha, D.A. (2021), "Characteristics of the main components of ensuring the economic security of the state", Vcheni zapysky Universytetu «KROK», vol. 3 (63), pp. 155-160
8. Koshykov, D.O. (2020), "The concept and classification of the functions of state policy in the sphere of ensuring the economic security of the state", Pravo i bezpeka, vol. 1 (76), pp. 67-73.
9. Pravdyvets', O. (2023), "Analysis of the results of domestic scientific research in the direction of innovative development of the economic security system of the enterprise based on digital technologies", Vcheni zapysky Universytetu «KROK», vol. 1 (69), pp. 15-28.
10. Skorobohatova, N.Ye. Tovkachova, A.S. and Fedorenko, K.V. (2023), "Methods of managing economic risks under martial law", Mater. III Mizhnar. nauk.-prakt. konf. «Biznes, innovatsii, menedzhment: problemy ta perspektyvy» [Materials of the 3rd International Scientific and Practical Conference "Business, Innovations, Management: Problems and Prospects"], KPI imeni Ihoria Sikors'koho, Kyiv, Ukraine, vol. 7, pp. 195-196.

*Стаття надійшла до редакції 17.11.2024 р.*