DOI: https://doi.org/10.32782/2524-0072/2023-54-68

УДК 338.2:65.01:658.5

СУЧАСНІ ТЕНДЕНЦІЇ ТА СТРАТЕГІЧНІ РИЗИКИ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ ІНДУСТРІЇ 4.0 ТА ІНДУСТРІЇ 5.0[1]

CURRENT TRENDS AND STRATEGIC RISKS IN THE IMPLEMENTATION OF INDUSTRY 4.0 AND INDUSTRY 5.0 TECHNOLOGIES

Черніков Дмитро Ігорович
аспірант,
Харківський національний університет радіоелектроніки
ORCID: https://orcid.org/0009-0002-0647-5237

Гришко Світлана Валеріївна
кандидат економічних наук, доцент,
Харківський національний університет радіоелектроніки
ORCID: https://orcid.org/0000-0001-7286-413X

Chernikov Dmytro, Gryshko Svitlana
Kharkiv National University of Radio Electronics

Стаття присвячена аналізу особливостей впровадження технологій Індустрії 4.0 та Індустрії 5.0, а також формуванню системи стратегічних ризиків підприємств при реалізації проєктів цифровізації. Вплив цифрових технологій усе більше відчувається в усіх секторах економіки, включаючи ті, що є базовими для економіки України: металургія, нафтогаз, енергетика, агропромисловий комплекс. Метою статті є аналіз особливостей реалізації концепції Індустрії 5.0 та визначення класів стратегічних ризиків для підприємств при впровадженні цифрових технологій. Проаналізовані особливості Індустрії 4.0 та Індустрії 5.0, зазначені їх фактори розвитку. Авторами запропоновано підхід до систематизації стратегічних ризиків та описані вісім класів таких ризиків: технологічні ризики, ризики конкурентоспроможності, операційні ризики, ризики зв'язків із стейкхолдерами, фінансові ризики, ризики з людськими ресурсами, брендові ризики, ризики гібридних атак. Виділені особливості кожного класу ризиків при реалізації проєктів цифровізації.

Ключові слова: цифровізація, Індустрія 4.0, Індустрія 5.0, стратегічний ризик, клас ризиків.

The article is devoted to the analysis of the features of the implementation of Industry 4.0 and Industry 5.0 technologies, as well as the formation of a system of strategic risks of enterprises during the implementation of digitization projects. The influence of digital technologies is increasingly felt in all sectors of the economy, including those that are basic to the economy of Ukraine: metallurgy, oil and gas, energy, agro-industrial complex. This is what determined the relevance of the research topic. Despite significant achievements and the number of scientific publications on the implementation of digital technologies, a number of issues require constant attention and updating. Such issues include the actualization of risks that enterprises face due to the introduction of digital technologies. The purpose of the article is to analyze the peculiarities of the implementation of the concept of Industry 5.0 and to determine the classes of strategic risks for enterprises when implementing digital technologies. Research methods are analysis and synthesis. The features of Industry 4.0 and Industry 5.0 are analyzed, and their development and variability factors are indicated. Attention is drawn to hybrid threats and the response to them. It was noted that the principles of 5.0 are already relevant for Ukraine during the state of war and post-war recovery, because they will allow to direct efforts in the three most important directions: orientation to people, sustainability in the economy and ecological recovery. It is noted that Industry 4.0 and Industry 5.0 will not be able to use their full potential until all the risks of their implementation are well understood and clearly assessed.

[1] Дане дослідження проведено в межах реалізації наукових заходів і Міжнародних грантів кафедри економічної кібернетики та управління економічною безпекою Харківського національного університету радіоелектроніки, а саме: науково-дослідної роботи «Організаційно-економічне забезпечення інноваційного розвитку та економічної безпеки суб'єктів господарювання», 2022-2025 рр. (Державний реєстраційний номер 0122U000510); Міжнародного проєкту Еразмус+ «Academic Response to Hybrid Threats» (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP); Міжнародного проєкту Еразмус+ «Ukraine-EU: Digital innovations making connections 4 changes» (Erasmus Jean Monnet Module #101047751-EUDI4C).

The authors proposed approach to systematization of strategic risks and described eight classes of such risks: technological risks, competitive risks, operational risks, stakeholder relations risks, financial risks, human resources risks, brand risks, risks of hybrid threats. The specifics of each class of risks during the implementation of digitization projects are highlighted. The proposed system of strategic risks will allow enterprises to further model the implementation of digitization projects and assess current risks. On the basis of the created model, the enterprise will be able to build a risk management system, including hybrid threats and cyber threats.

Key words: digitalization, Industry 4.0, Industry 5.0, strategic risk, risk class.

Постановка проблеми. На сучасному етапі розвитку вплив цифрових технологій усе більше відчувається в усіх секторах економіки. Цифровізація кардинально змінює традиційні галузі та сектори [2]. Відбувається зміна класичних бізнес-моделей, аналогові процеси та операції переходять в Інтернет, з'являється можливість формувати індивідуальні пропозиції для кожного окремого клієнта. Із розвитком Індустрії 4.0, що саме і базується на використанні цифрових технологій, кардинальні зміни відбуваються і в тих галузях, які вважаються базовими для української промисловості – металургія, нафтогаз, енергетика, агропромисловий комплекс тощо [1].

Проте криза пандемії COVID-19 виявила, що цифрові рішення не здатні зробити більш стійкими глобальні ланцюги постачань та екосистеми. Індустрія 5.0, також відома як п'ята промислова революція, – це нова фаза розвитку, що базується на кіберфізичних системах, коли люди працюють разом із передовими технологіями та роботами на основі штучного інтелекту, щоб покращити робочі процеси. Це поєднується з більшою орієнтацією на людину, а також підвищеною стійкістю та кращим акцентом на стійкість [5].

Ця нова фаза охоплює більше, ніж просто виробництво, і базується на Індустрії 4.0 і реалізується завдяки таким інструментам цифрових технологій, як штучний інтелект, хмарні обчислення, аналітика великих даних, Інтернет речей (IoT), машинне навчання, робототехніка, розумні системи та віртуалізація [5].

Оскільки багато галузей почали приймати або готуються впровадити цифрові технології у бізнес-процеси, це збільшує їх уразливість до потенційних ризиків безпеки, таких як крадіжка даних, зловмисне програмне забезпечення, відмова в обслуговуванні та злом пристроїв.

Таким чином, постає актуальним питання визначення ризиків впровадження цифрових рішень у бізнес-процеси.

Аналіз останніх досліджень і публікацій. Розвитку цифрових технологій присвячено багато праць вітчизняних та міжнародних науковців [2–4; 6; 7; 10], експертів у галузі цифровізації [1; 9], міжнародних агенцій [5; 8; 11]. У наукових працях, що присвячені дослідженню концепцій Індустрії 4.0 та 5.0, увага здебільшого приділена можливостям, які відкриваються перед суб'єктами господарювання від впровадження нових технологій. Багато публікацій розглядають теоретичні принципи реалізації технологій Індустрії 4.0 та Індустрії 5.0 [5; 8; 9; 11], аналізують практичні аспекти впровадження цифрових технологій [1–3; 7], порівнюють успіхи окремих країн у напрямку цифрового розвитку [4], роблять висновки про поширеність окремих цифрових інструментів [6; 10]. Однак впровадження цифрових технологій несе з собою не тільки можливості, але й реальні загрози та ризики. Система управління ризиками суб'єктів господарювання у таких умовах повинна враховувати нові ризики, які виникають у процесі цифрової трансформації.

Виділення невирішених раніше частин загальної проблеми. Незважаючи на значні напрацювання та кількість наукових публікацій щодо впровадження цифрових технологій ряд питань потребують постійної уваги та оновлення. До таких питань відносяться актуалізація ризиків, що виникають перед підприємствами через впровадження технологій Індустрії 4.0 та Індустрії 5.0, групування та класифікація таких ризиків, включаючи нові виклики, пов'язані з різкою зміною безпекового ландшафту. У сучасних умовах від швидкості реакції на нові неочікувані складні виклики залежить не лише ефективність діяльності, а й навіть можливість виживання бізнесів і цілих галузей.

Формулювання цілей статті (постановка завдання). Метою статті є аналіз сучасних тенденцій та визначення стратегічних ризиків впровадження технологій Індустрії 4.0 й Індустрії 5.0.

Виклад основного матеріалу дослідження. Індустрія 5.0 описується Європейським Союзом як така, що забезпечує «…бачення промисловості, яке спрямоване за межі ефективності та продуктивності як єдиних цілей, і посилює роль і внесок промисловості в суспільство…» [5].

Таблиця 1

Головні риси Індустрії 4.0 та Індустрії 5.0

Особливості Індустрії 4.0	Особливості Індустрії 5.0
1. Центрована навколо виробничої ефективності шляхом кращої цифрової інтеграції та використання штучного інтелекту. 2. Присутня оптимізація бізнес моделей в рамках існуючих ринків капіталу та економічних моделей, які, наприклад, автоматично фокусуються на скороченні витрат та максимізації прибутку. 3. Немає фокусу на напрямах повторного використання ресурсів та матеріалів, щоб мінімізувати кліматичні та соціальні ризики	1. Забезпечує галузеві фреймворки (рамки розвитку – framework), які комбінують завдання конкурентоспроможності та сталості. 2. Фокусується на впливі альтернативних (крім технологій) режимів керування моделями, що ведуть до сталості та стійкості. 3. Робить працівників більш значимими через використання цифрових пристроїв, й уособлює, таким чином, людино-центричний підхід до використання технологій. 4. Будує шлях по переходу до сталої економіки. 5. Вводить індикатори, що показують для кожної галузі прогрес в досягненні стійкості, процвітання та сталості

Джерело: складено авторами на основі [5]

У звіті Європейської комісії [5] акцентується увага на таких недоліках Індустрії 4.0 як не відповідність новим викликам кліматичних змін, пандемічних та інших криз, які ведуть до нестабільності й викликають значні соціальні напруження. У таблиці 1 наведено головні відмінні риси між Індустрією 4.0 та 5.0.

На думку Європейської Комісії, Індустрія 5.0 є необхідним еволюційним кроком Індустрії 4.0 через такі суттєві проблеми, характерні для Індустрії 4.0 [5]:

Індустрія 4.0 не є правильною основою для досягнення цілей Європи до 2030 року, оскільки створює технологічну монополію та гігантську нерівність у багатстві;

Індустрія 5.0 – це не технологічний стрибок вперед, а спосіб побачити підхід Індустрії 4.0 у ширшому контексті, забезпечуючи досягнення сталого розвитку, з акцентом на безпеку та соціальний вимір [5].

В аналітичному центрі Industry4Ukraine [1] стверджують, що принципи 5.0 вже є актуальними для України за низкою важливих напрямів, й це стосується навіть воєнного стану, а тим більше післявоєнного. До таких напрямів автори відносять: формування стійких ланцюгів створення вартості та їх децентралізацію, сталість відносин в екосистемах. Як можливий інструмент реалізації цих напрямів автори бачать створення кластерів для організації взаємодії, координації зусиль, обміну досвідом, даними між економічними суб'єктами, а також державними, безпековими, соціальними, неприбутковими інституціями [1].

У роботі [7] проаналізований успішний досвід українських компаній по впровадженню технологій Індустрії 4.0/5.0, зокрема – штучного інтелекту. Авторами проаналізований поточний стан та динаміка розвитку Індустрії 4.0 в Україні. Значна увага присвячена успішним прикладам впровадження цифрових технологій в бізнес-процеси українських підприємств [7].

В. Терзіян, С. Гришко та М.Голов'янко у своєму дослідженні також роблять наголос на використанні штучного інтелекту на роблять висновок про невизначеність ролі людини у нинішніх умовах індустрії, яка розвивається в напрямку вищого рівня автономії, самоуправління, використання штучного інтелекту, зокрема в області глибокого навчання [10].

Поряд з тим позитивним, що привносять Індустрія 4.0 та Індустрія 5.0, вони також привносить нові ризики, які потребують відповідного реагування від керівництва підприємств. Глибоке розуміння того, які перешкоди постають перед суб'єктами господарювання на шляху цифровізації, формує основу життєздатності проєкту цифрової трансформації і тим самим дає змогу реалізувати потенціал довгострокового зростання.

У роботі О. І. Гринюк [2] визначені бар'єри впровадження технологій Індустрії 4.0: невідповідність навичок керівництва; відсутність розуміння перспективних процесів; відсутність цілісного бачення; потреба вкладення значних фінансових ресурсів та складнощі в оцінюванні майбутніх економічних вигод; відсутність або ж невідповідність інфраструктури; низький рівень інтеграції ланцюга формування вартості; дефіцит необхідних навичок у працівників; супротив змінам з боку менеджменту та персоналу. Автором також виокремлено такі ризики реалізації проєкту цифрової трансфор-

мації: інвестиційні, інноваційні, інформаційні ризики, ризики законодавчо-адміністративного характеру, людського капіталу [2].

В. Г Гуцуляк та В. М. Гуцуляк у своєму дослідженні [3] визначили ключові аспекти та ризики, які привносить Індустрія 4.0 для малих і середніх підприємств, а саме: технологічні ризики, що виникають в результаті технічної складності; сильна залежність від технологій та програмного забезпечення, а також кіберзагрози (інформаційна атака).

Кіберзагрозам також приділена особлива увага у звіті Всесвітнього економічного форуму «Глобальні ризики – 2022» [11]. Автори звіту вказують на взаємозв'язок між подальшою діджиталізацією та зростанням кіберзагроз. У контексті повсюдної залежності від дедалі складніших цифрових систем зростання кіберзагроз випереджає спроможність суспільства ефективно запобігати їм і управляти ними. Так, наприклад, у 2021 році шахрайство в Інтернет-банкінгу у Великій Британії зросло на 117% за обсягом і на 43% за вартістю порівняно з рівнем 2020 року, оскільки люди витрачали більше часу на покупки онлайн [8]. Окрема увага у звіті приділена геополітичним ризикам та гібридним загрозам [11].

Група виконавців міжнародного проєкту протидії гібридним загрозам (Countering Hybrid Warfare Project) [8] розглядають гібридну загрозу як «…це синхронне використання кількох інструментів влади, адаптованої до конкретних вразливостей у всьому спектрі суспільних функцій для досягнення синергічного ефекту…» [8]. Серед інструментів влади авторами виділені п'ять категорій: військовий, політичний, економічний, цивільний та інформаційний. Вразливості автори також поділяють на декілька категорій, в залежності від цілі гібридної загрози: політична, військова, економічна, соціальна та інформаційна сфери країни, що є об'єктом гібридної атаки, а також інфраструктура [8]. Цифрові інструменти можуть служити зброєю при гібридних атаках на інфраструктуру, банківські, урядові, соціальні (медичні, освітні) установи, при розповсюдженні недостовірної інформації.

О. Каікова, В. Терзіян та інші у дослідженні [7] стверджують, що інструменти гібридної атаки («отруєної» атаки) може бути засто-

Таблиця 2

Класи стратегічних ризиків

Клас	Зміст
1. Галузь	Основним ризиком є скорочення прибутковості у галузі, що обумовлено впливом негативних факторів: подорожчання досліджень та розробок для високотехнологічних компаній, підвищення вартості капітальних витрат по галузі загалом, відмова постачальників від послуг посередників та прямий вихід на кінцевого споживача, мінливість бізнес-циклів. За таких умов галузь може виявитися економічно непривабливою
2. Технології	Технологічні зміни пов'язані з моральним старінням технологій, виробничого обладнання, продукції та послуг, закінченням дії патенту. В умовах цифрових трансформацій зміна технологій відбувається дуже швидко і компаніям доводиться приймати рішення у короткі терміни
3. Бренд	Основним ризиком є ерозія та втрата бренду. Існує безліч негативних факторів, здатних підірвати цінність бренду. Загрози, що раптово виникають, можуть поставити торгову марку на межу загибелі
4. Конкуренти	Основний ризик – поява нового конкурента, який швидше виявляє та якісніше задовольняє потреби потенційних клієнтів. В умовах розвитку цифровізації конкурентом може стати будь-яка компанія, що реалізує продукцію онлайн, незважаючи на її географічне розташування та розміри
5. Споживачі	Основний ризик – зміна вподобань споживачів. Прискорення темпів науково-технічного прогресу змушує клієнтів змінювати свої вподобання. Підприємство з вузькою спеціалізацією, ризикує втратити своїх основних споживачів через зміни їхніх переваг
6. Проєкт	Основний ризик – провал нового проєкту. В умовах великої невизначеності будь-які прогнози мають похибку, тому розраховані показники їх ефективності є достовірними з певною часткою ймовірності
7. Стагнація	Основний ризик пов'язаний зі стагнацією бізнесу (застій бізнесу) через неспроможність підприємств знайти нові джерела зростання

Джерело: складено авторами на основі [9]

сований як проти людей, так і проти інструментів штучного інтелекту та машинного навчання AI/ML, тобто він включає виявлення вразливого підпростору в просторі прийняття рішень потенційною жертвою та вплив на нього уразливість через неправильно позначені зразки даних («отрута»). У відповідь автори пропонують абстрактну концепцію «імунітету» проти гібридних загроз за допомогою спеціальної техніки «когнітивної вакцинації», коли на виявлений уразливий підпростір прийняття рішень впливають специфічними методами проактивного захисту за технологією генеративних змагальних мереж (англ. Generative adversarial networks, GANs) [7].

Т. В. Полозова та І. В. Колупаєва у [4] визначили групу специфічних міжнародних рейтингів та індексів, що характеризують систему забезпечення економічної безпеки країни. Побудовано матрицю відповідності міжнародних рейтингів складовим економічної безпеки України. Авторами відмічено погіршення деяких позицій України у світових рейтингах, що є передумовою погіршення конкурентоспроможності та загрозою зниження рівня її економічної безпеки [4].

Авторами у роботі [9] визначено класи стратегічних ризиків, що наведено у таблиці 2.

Впровадження цифрових інновацій може вносити значні зміни в бізнес-середовище, і це може призвести до різних видів стратегічних ризиків. На основі проведеного аналізу теоретичних підходів у даному дослідженні запропоновано виокремити класи стратегічних ризиків впровадження цифрових інновацій (рис. 1).

До класу технологічних ризиків слід віднести: неспроможність виявити і впровадити потрібні технологічні рішення; проблеми зі скасуванням або старінням технологій, що були використані раніше; кібербезпека та ризики щодо захисту цифрових активів від кібератак.

До класу ризиків конкурентоспроможності запропоновано віднести: неспроможність адаптувати бізнес-модель до нових цифрових реалій; втрата конкурентної переваги через швидке розвиток технологій та конкуренцію; ризики втрати клієнтів через недостатню інноваційність.

Клас операційних ризиків передбачає врахування таких аспектів: порушення бізнес-процесів при впровадженні нових технологій;

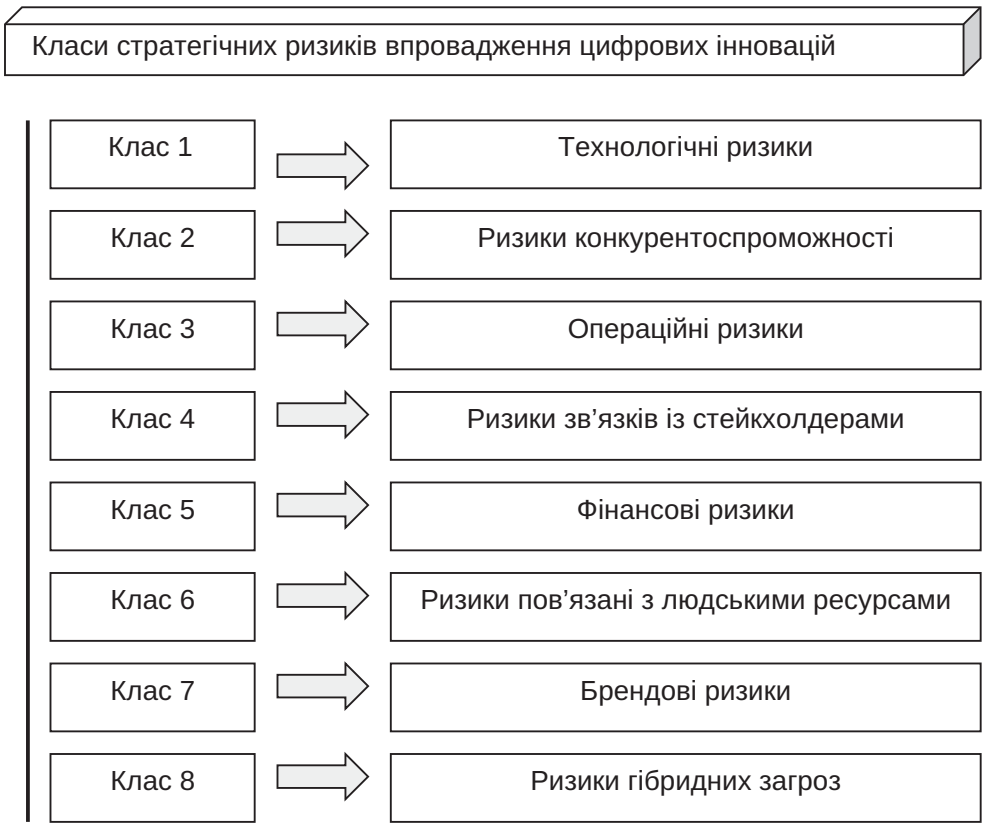

Рис. 1. Класи стратегічних ризиків впровадження цифрових інновацій

Джерело: складено авторами

проблеми з інтеграцією нових цифрових систем з існуючими інфраструктурами; ризики зниження продуктивності або якості під час переходу до цифрових процесів.

Ризики зв'язків із стейкхолдерами містять: негативні реакції клієнтів, інвесторів або регуляторів на цифрові зміни; ризики з погляду дотримання законодавства та регуляторних вимог в сфері цифрових технологій; втрата довіри або репутаційних ризиків у разі неспроможності ефективно управляти даними або захищати конфіденційну інформацію.

Ризики, що входять до класу фінансових ризиків, передбачають врахування таких аспектів: великі витрати на розробку та впровадження цифрових інновацій; ризики фінансової нестабільності в разі невдачі проєктів з цифрової трансформації; негативний вплив на прибутковість підприємства під час переходу до нових бізнес-моделей.

До класу ризиків з людськими ресурсами пропонується віднести такі аспекти: проблеми зі здатністю працівників адаптуватися до нових технологій; ризики зв'язані з браком кваліфікованого персоналу для розробки та підтримки цифрових ініціатив; можливість конфліктів або опору з боку персоналу при впровадженні змін.

При аналізі брендових ризиків необхідно враховувати: ризики зниження цінності бренду; ризики недоброчесної конкуренції; ризики, пов'язані з неефективним управлінням інвестиціями.

Ризики гібридних загроз носять комплексний характер. Гібридні загрози можуть бути націлені на широкий спектр цілей на підприємстві (створення проблем з регуляторними та судовими органами, розрив ланцюгів постачань або взаємовідносин з покупцями, розповсюдження негативної інформації про підприємство) і можуть вживатися, щоб послабити конкурентну позицію, взаємовідносини з контрагентами, знизити ринкову вартість фірми.

Управління цими стратегічними ризиками є ключовим аспектом успішної цифрової трансформації. Підприємства мають ретельно аналізувати, ідентифікувати та враховувати ці ризики в процесі розробки та впровадження своїх цифрових стратегій.

Висновки. Таким чином, кожне підприємство, окрім класичних ризиків стратегічного розвитку буде стикатися в тому числі с ризиками, які обумовлюються як існуючими, вже відомими загрозами, так і новими викликами, що утворюються внаслідок переходу розвинутих країн до концепції Індустрії 5.0. Тому для реалізації цифрових трансформацій також необхідний систематичний моніторинг ризиків.

Індустрія 5.0 дозволяє підприємствам і промисловості активно пропонувати суспільству рішення для збереження ресурсів, забезпечення соціальної стабільності та вирішення кліматичних цілей.

Однак існує дуже висока ймовірність виникнення нових ризиків, що негативно впливають на багато аспектів в організаціях. Індустрія 4.0 та Індустрія 5.0 не зможуть використовувати весь свій потенціал доти, доки всі їх ризики не будуть добре зрозумілі та чітко оцінені. Ця ситуація вимагає активізації наукового пошуку та практичних розробок у цій галузі, що є перспективами подальших досліджень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Аналітичний центр Industry4Ukraine. Про Індустрію 5.0 – чому це стає актуальним для України. URL: https://www.industry4ukraine.net/publications/pro-industriyu-5-0-chomu-cze-staye-aktualnym-dlya-ukrayiny/ (дата звернення: 04.09.2023).

2. Гринюк О. І. Цифрова трансформація суб'єктів господарювання у контексті концепції Індустрії 4.0: Сучасні тенденції, бар'єри та ризики впровадження. *Ефективна економіка*. 2021. № 5. DOI: 10.32702/2307-2105-2021.5.97

3. Гуцуляк В. Р., Гуцуляк В. М. Основні ризики Індустрії 4.0 для підприємств у сучасних умовах розвитку. *Проблеми системного підходу в економіці.* 2021. № 1 (87). С. 49–53. DOI: https://doi.org/10.32782/2520-2200/2022-1-7. (дата звернення: 04.09.2023).

4. Полозова Т. В., Колупаєва І. В. Аналіз міжнародних рейтингів України в контексті забезпечення економічної безпеки. *Механізм регулювання економіки.* 2022. № 1–2 (95–96). С. 103–113.

5. European Commission Industry 5.0: A Transformative Vision for Europe. ESIR Policy Brief No. 3. December 2021. URL: https://op.europa.eu/en/web/eu-law-and-publications/publication-detail/-/publication/38a2fa08-728e-11ec-9136-01aa75ed71a1 (дата звернення: 04.09.2023).

6. Golovianko M., Gryshko S., Titova L., Filatov V. Good practices of Industry 4.0 in Ukraine. Kharkiv: Kharkiv National University of Radio Electronics. 2022. 38 p. URL: https://openarchive.nure.ua/server/api/core/bitstreams/714c09ab-3e31-48f2-a930-63a2c1e8f58d/content. (дата звернення: 15.09.2023).

7. Kaikova, O., Terziyan, V., Tiihonen, T., Golovianko, M., Gryshko, S., & Titova, L. (2022). Hybrid threats against Industry 4.0: adversarial training of resilience. In E3S Web of Conferences, № 353. 2022. DOI: https://doi.org/10.1051/e3sconf/202235303004. URL: https://www.e3s-conferences.org/articles/e3sconf/pdf/2022/20/e3sconf_evf2021_03004.pdf (дата звернення: 15.09.2023).

8. Multinational Capability Development Campaign (MCDC) Countering Hybrid Warfare Project: Understanding Hybrid Warfare. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf (дата звернення: 07.09.2023).

9. Slywotzky A., Drzik J. Countering the biggest risk of all. *Harvard Business Review*. 2005. Apr; 83(4). 78–88. URL: https://hbr.org/2005/04/countering-the-biggest-risk-of-all (дата звернення: 04.09.2023).

10. Terziyan V., Gryshko S., Golovianko M. Patented intelligence: Cloning human decision models for Industry 4.0. *Journal of manufacturing systems*. 2018. №48. 204-217.

11.World Economic Forum. The Global Risks Report. 2022. URL: https://www.weforum.org/reports/global-risks-report-2022/ (дата звернення: 07.09.2023).

REFERENCES:

1. Industry4Ukraine. *Pro Industriiu 5.0 – chomu tse staie aktualnym dlia Ukrainy* [About Industry 5.0 – why it is becoming relevant for Ukraine]. Retrieved from https://www.industry4ukraine.net/publications/pro-industriyu-5-0-chomu-cze-staye-aktualnym-dlya-ukrayiny/ [In Ukrainian]

2. Hryniuk O. I. (2021) Tsyfrova transformatsiia subiektiv hospodariuvannia u konteksti kontseptsii Industrii 4.0: Suchasni tendentsii, bariery ta ryzyky vprovadzhennia [Digital transformation of business entities in the context of the concept of Industry 4.0: Modern trends, barriers and risks of implementation]. *Efektyvna ekonomika – Efficient economy*, № 5. DOI: 10.32702/2307-2105-2021.5.97 [In Ukrainian]

3. Hutsuliak V. R., Hutsuliak V. M. (2021) Osnovni ryzyky Industrii 4.0 dlia pidpryiemstv u suchasnykh umovakh rozvytku [The main risks of Industry 4.0 for enterprises in modern conditions of development]. *Problemy systemnoho pidkhodu v ekonomitsi – Problems of the systemic approach in economics*, № 1(87), 49–53. DOI: https://doi.org/10.32782/2520-2200/2022-1-7 [In Ukrainian]

4. Polozova T. V., Kolupaieva I. V. (2022) Analiz mizhnarodnykh reitynhiv Ukrainy v konteksti zabezpechennia ekonomichnoi bezpeky [Analysis of international ratings of Ukraine in the context of ensuring economic security]. *Mekhanizm rehuliuvannia ekonomiky*. № 1–2 (95–96). P. 103113. [In Ukrainian]

5. European Commission (2021) Industry 5.0: A Transformative Vision for Europe. *ESIR Policy Brief.* No. 3. December 2021. Retrieved from https://op.europa.eu/en/web/eu-law-and-publications/publication-detail/-/publication/38a2fa08-728e-11ec-9136-01aa75ed71a1

6. Golovianko, M., Gryshko, S., Titova, L., & Filatov, V. (2022). Good practices of Industry 4.0 in Ukraine. Kharkiv: Kharkiv National University of Radio Electronics. 38 p. URL: https://openarchive.nure.ua/server/api/core/bitstreams/714c09ab-3e31-48f2-a930-63a2c1e8f58d/content

7. Kaikova, O., Terziyan, V., Tiihonen, T., Golovianko, M., Gryshko, S., & Titova, L. (2022). Hybrid threats against Industry 4.0: adversarial training of resilience. In E3S Web of Conferences, № 353. 2022. DOI: https://doi.org/10.1051/e3sconf/202235303004. URL: https://www.e3s-conferences.org/articles/e3sconf/pdf/2022/20/e3sconf_evf2021_03004.pdf.

8. Multinational Capability Development Campaign (MCDC) (2017) *Countering Hybrid Warfare Project: Understanding Hybrid Warfare*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf

9. Slywotzky A., Drzik J. (2005) Countering the biggest risk of all. *Harvard Business Review*, 83(4), 7888. Retrieved from https://hbr.org/2005/04/countering-the-biggest-risk-of-all

10. Terziyan V., Gryshko S., & Golovianko M. (2018). Patented intelligence: Cloning human decision models for Industry 4.0. *Journal of manufacturing systems*, 48, 204217.

11. World Economic Forum (2022). *The Global Risks Report*. Retrieved from https://www.weforum.org/reports/global-risks-report-2022/