УДК 338.2:65.01:658.5

ВІТЛІНСЬКИЙ Вальдемар Володимирович,
доктор економічних наук, професор, завідувач кафедри економіко-математичного моделювання,
ДВНЗ «Київський національний економічний університет імені Вадима Гетьмана»,
СКІЦЬКО Володимир Іванович,
кандидат економічних наук, доцент, докторант, доцент кафедри економіко-математичного моделювання,
ДВНЗ «Київський національний економічний університет імені Вадима Гетьмана»

РИЗИКИ В ІНДУСТРІЇ 4.0

Стаття є однієї із перших вітчизняних наукових робіт, яка присвячена Індустрії 4.0 (Четвертій промисловій революції). На засадах системного аналізу досліджуються деякі аспекти ризиків в Індустрії 4.0, зокрема, авторами окреслені ризики Індустрії 4.0 та дано авторські уточнення їх сутностей. Наведено авторське бачення класифікації ризиків Індустрії 4.0 за різними ознаками та критеріями.

Ключові слова: *ризик, Індустрія 4.0, Четверта промислова революція, кіберфізична система, Інтернет Речей*

Постановка проблеми. Багато вчених та фахівців характеризують сучасну стадію розвитку соціально-економічних систем низки розвинених країн як інформаційно-мережеве суспільство. Стосується це і промисловості. Так, зокрема, у квітні 2011 року на Ганноверській промисловій виставці-ярмарку (Hannover Messe) президент Німецької академії технічних наук Хеннінг Кагерманн (Henning Kagermann), представник Федерального міністерства освіти та наукових досліджень Вольф-Дітер Лукас (Wolf-Dieter Lukas) та голова правління Німецького науково-дослідного центру штучного інтелекту Вольфган Вальстер (Wolfgang Wahlster) озвучили новий термін «Індустрія 4.0» (анг. Industry 4.0, нім. Industrie 4.0) (або Четверта індустріальна революція), який узагальнює різні засоби та технології для підвищення конкурентоспроможності німецької промисловості шляхом імплементації кіберфізичних систем (Cyber-Physical Systems – CPS) у реальне виробництво [1]. На сьогодні для тлумачення суті Індустрії 4.0, окрім кіберфізичних систем, використовують й інші поняття. Дослідження, проведені авторами [2, с.8] показали, що станом на початок 2015 року найчастіше використовувалися такі поняття стосовно означень Індустрії 4.0: кіберфізичні системи, Інтернет Речей (Internet of Things – IoT), Розумна (Інтелектуальна) Фабрика (Smart Factory), Інтернет Послуг (Internet of Services – IoS), Розумна (Інтелектуальна) Продукція (Smart Product), взаємодія «Машина-Машина» (M2M), Великі Дані (Big Data), Хмара (Cloud) або хмарні обчислення. Пояснимо далі суть цих понять.

Кіберфізичні системи – це розумні (інтелектуальні) системи (smart systems), які складаються з фізичних та обчислювальних (апаратне та програмне забезпечення) компонент, що утворюють одне ціле в їх системній взаємодії та дозволяють відчути зміни стану реального світу [3]. Кіберфізичні системи містять розумні (інтелектуальні) машини (smart machines), системи зберігання та виробничі потужності, які здатні автономно обмінюватися інформацією, ініціювати дії та контролювати функціонування одне одного [4]. У кіберфізичних системах можна виокремити наступні компоненти (технології) [5]: блок кібернетичного управління (Cyber Control); кібернетичний моніторинг (Cyber Managing); Інтернет Речей; Хмара; засоби безпеки (Security); штучний інтелект (Intelligence); Великі дані та сервіс управління ними (Big Data and Services); цифровий моніторинг (Digital Monitoring); фізичний простір усього

«розумного», природа, соціальний та технічний простір (Physical Smart Everything, Nature, Social, and Tech World).

«Інтернет Речей – це концепція підключення до Інтернету побутових пристроїв, які завдяки цьому можуть взаємодіяти один з одним або з зовнішнім середовищем, збирати корисні дані та на їх основі самостійно здійснювати дії та операції, без участі людини» [6]. Інтернет Речей дозволяє «речам» та «об'єктам», наприклад, засобам радіочастотної ідентифікації RFID (Radio Frequency IDentification), датчикам, пристроям, мобільним телефонам тощо, взаємодіяти одне з одним для досягнення загальної мети [2, 7]. Оскільки концепція Індустрії 4.0 спрямована на перетворення в промисловості, то деякі науковці та фахівці у своїх роботах використовують поняття «Промисловий Інтернет Речей» (Industrial Internet of Things – IIoT [8] або Manufacturing Internet of Things – MIoT [9]), що передбачає використання технології Інтернету речей у промисловому виробництві для підвищення його (виробництва) ефективності та гнучкості [9]. Інтернет Речей повною мірою реалізує концепцію взаємодії «Машина-Машина» (Machine-to-Machine – M2M).

Інтернет Послуг (Internet of Services – IoS) – це мережа, за допомогою якої одна сторона (особа, установа, підприємство тощо) надає деякі послуги для іншої сторони. Наприклад, використовуючи різні мобільні додатки на своєму смартфоні людина може здійснити низку фінансових операції без відвідування установи банку, купити квитки до кінотеатрів, театрів чи на транспорт, відстежувати переміщення поштових відправлень тощо. Усе це можна віднести до Інтернету Послуг.

Зазначені вище види Інтернету по суті є етапами його розвитку, які сформувались у різні проміжки часу. На сьогодні виокремлюють такі кроки розвитку Інтернету [10]:

- Крок 1. «До інтернетівський» період (Pre-Internet). Людина з людиною спілкується за допомогою дротового чи бездротового зв'язку;
- Крок 2. Інтернет Змісту (Контенту, Наповнення) (Internet of Content). Перший етап появи Інтернету, коли комп'ютери стали інформаційно пов'язаними одне з одним, утворюючи Всесвітнє павутиння (World Wide Web – WWW), а користувачі (люди, підприємства) отримали можливість спілкуватися за допомогою електронної пошти, обмінюватися інформацією у простому вигляді тощо;
- Крок 3. Інтернет Послуг. Завдяки інформаційним технологіям Веб 2.0 (Web 2.0) користувачі (люди, підприємства) отримали можливість розміщувати у Всесвітній павутині власну інформацію у складному вигляді, з'являються Інтернет-магазини (основні представники електронної комерції), сайти підприємств зазнають змін щодо представлення інформації, можливостей її опрацювання тощо;
- Крок 4. Інтернет Людей (Internet of People). Цей крок характеризується бурхливим розвитком та широким розповсюдженням соціальних мереж та різних засобів, за допомогою яких люди за допомогою Інтернету мають можливість спілкуватися між собою;
- Крок 5. Інтернет Речей.

Інтернет Послуг з'явився раніше за Інтернет Речей і, на відміну від останнього, вже повністю ввійшов у наше життя.

Розумна фабрика (підприємство) – це фабрика, де кіберфізичні системи через Інтернет Речей здатні до спілкування між собою та з людьми з метою досягнення поставлених завдань [2]. Розумні фабрики здатні ефективно виробляти складну багатокомпонентну продукцію завдяки тісній взаємодії (спілкуванню) між людиною, машиною та ресурсами. Ця взаємодія стала такою ж природною як і просте спілкування людей між собою в соціальних мережах [4].

Розумна Продукція є виробом, який має однозначну ідентифікацію, містить свою історію (де, коли і як виріб був виготовлений; зміни, які відбулись під час експлуатації; поточний стан тощо) і здатний оцінювати альтернативні шляхи досягнення цілей експлуатації тощо [4].

«Великі Дані» – це процес пошуку у великому обсягу інформації необхідної та її подальша обробка [11]. Завдяки Хмарам (хмарним технологіям), така інформація може зберігатись, швидко оброблятись та бути миттєво доступною відповідному пристрою з різних точок доступу [12].

Отже, «Індустрія 4.0» є узагальнюючим терміном для технологій і концепцій організації ланцюга доданої вартості: на Розумних фабриках (яким властива модульна структура) кіберфізичні системи здійснюють та контролюють фізичні процеси виробництва, створюють віртуальні копії реальних виробничих процесів та приймають децентралізовані рішення; «спілкування» кіберфізичних систем одна з одною та людиною здійснюється за допомогою Інтернету Речей; завдяки Інтернету Послуг учасниками ланцюга доданої вартості пропонуються та надаються внутрішні та загальні послуги [2].

Індустрія 4.0 є інноваційним промисловим виробництвом, за яким майбутнє. Як Індустрії 4.0 притаманна невизначеність, яка породжує ризик, так і інноваціям властиві різні види та типи ризиків, які необхідно вміти ідентифікувати аналізувати, моделювати та управляти ними.

Аналіз останніх досліджень і публікацій. Наразі ґрунтовних наукових чи практичних робіт, в яких системно досліджувалися б проблеми притаманних Індустрії 4.0 ризиків, опубліковано небагато. Проте існують зарубіжні роботи, в яких розглядаються окремі аспекти ризик-менеджменту в Індустрії 4.0. Розглянемо далі деякі із них.

Сандіп Пател (Sandip Patel) у своєму повідомленні [13] зауважує, що ризики в Індустрії 4.0 є взаємопов'язаними, та виокремлює наступні із них: 1) кібер-ризик (віртуальний ризик) (cyber risk). Він є основним ризиком Індустрії 4.0. і виникає у разі виходу з ладу сучасних технологій, порушення інформаційної безпеки, порушення процесу виробництва та постачання та має каскадний ефект; 2) ризик збою у бізнесі (risk of business disruption), що пов'язаний з віртуалізацією ланцюга доданої вартості; 3) ризики довкілля на макро рівні (macro environment risks), що проявляються в різних глобальних стихійних лихах тощо; 4) репутаційний ризик (reputation risk), який може виникнути у результаті виникнення попередніх ризиків; 5) кадровий ризик (talent risk), що пов'язаний з новими компетенціями та знаннями, якими мають володіти працівники, задіяні в Індустрії 4.0. У повідомленні [14] Сандіп Пател наводить приклади та методи зниження деяких зазначених вище ризиків, якими користується низка світових виробників. Проте він наголошує що ці рішення є точковими, а не системними. Окрім того, він зауважує, що страхові компанії мають активно включитись у страхування таких ризиків.

Майке Шрьодер (Meike Schröder), Маріус Індорф (Marius Indorf), Вольфганг Керстен (Wolfgang Kersten) досліджують різні аспекти управління ризиками логістичного ланцюга поставок (supply chain) в умовах функціонування Індустрії 4.0. Вони зазначають, що складові «класичного» управління ризиками (ідентифікація, аналіз, зниження, контроль) залишаються актуальними і для ризик-менеджменту в Індустрії 4.0, та запропонували наступну класифікацію ризиків логістичного ланцюга поставок в умовах Індустрії 4.0: 1) ризики постачання (втрата постачальників; різні стандарти безпеки уздовж ланцюга); 2) ризики процесу (стабільність зв'язку; виникнення подій внаслідок порушення норм експлуатації; залежність від постачальників інформаційних технологій; втрата здатності обладнання виконувати нові завдання; недоліки інфраструктури; проблеми IT-інтерфейсу; зовнішнє втручання; несумісність компонент, що призводить до підвищення часу та збільшення обсягу коштів на обслуговування у системі постачання; впровадження інновацій; втрата кваліфікації та компетенцій працівниками; саботаж працівників); 3) ризики управління (відсутність логіки у прийнятті управлінських рішень; некоректні дані, на основі яких приймаються управлінські рішення); 4) ризики попиту (вимоги постійних споживачів; вимоги до гнучкості логістичного ланцюга поставок); 5) ризики зовнішнього середовища (відсутність стандартів; низький рівень захисту даних; промислове шпигунство; рівень технологічного розвитку) [15].

У звіті [16] групи професійних ризик-менеджерів окреслені проблеми управління ризиками на Розумних фабриках, трудність вирішення яких зумовлена, зокрема, складністю та взаємною залежністю виробничих процесів. Основні проблеми, які можуть мати місце у роботі таких фабрик, пов'язані з встановленням відповідальності за можливі збитки, протіканням та зберіганням інформаційних потоків, підвищеною вразливістю до кібернетичних атак, можливими зупинками чи затримками виробничого процесу і ланцюга поставок тощо.

У праці [17] також зазначено значимість в Індустрії 4.0 проблеми кібернетичних атак. Окрім того, на сьогодні глобальний кібер-ризик за версією щорічника «Allianz Risk Barometer» займає третє місце серед глобальних бізнес-ризиків, переміщуючись у рейтингу лише догори, зокрема, в 2014р. він посідав 8 місце, а у 2015р. – уже 5 місце [18, 19].

Фрідріх Волльмар (Friedrich Vollmar) досліджує ризики, які пов'язані з виникненням, розвитком та впровадженням концепції «Індустрія 4.0» у життя [20]. Зокрема, він виокремлює ризики, які пов'язані з такими ситуаціями: партнери не можуть дійти згоди щодо загального прийнятих стандартів для Індустрії 4.0, або ця узгодженість займе надто багато часу; стан технологій ще не дозволяє їх використовувати у масовому виробництві; час настання Четвертої промислової революції ще не настав; прибутковість інвестованого капіталу в Індустрію 4.0 є під питанням [20].

Вітчизняних робіт з досліджуваної проблеми фактично не має, а тому даною роботою хотілось би деякою мірою заповнити цю прогалину вітчизняного наукового середовища.

Мета статті полягає у визначенні, на засадах системного аналізу, основних ризиків Індустрії 4.0, уточнення їх тлумачень та формулювання власного бачення щодо їх класифікації.

Виклад основного матеріалу. Застосування системного аналізу дозволяє дійти висновку, що у тлумаченні ризику в Індустрії 4.0 для загального випадку цілком актуальним є означення, яке наведено в [21]: «ризик – це економічна категорія, яка відображає особливості сприйняття заінтересованими суб'єктами економічних відносин об'єктивно існуючих невизначеності та конфліктності, які притаманні процесам цілепокладання, управління, прийняття рішень, оцінювання, що обтяжені можливими загрозами щодо понесення збитків, втрат іміджу та невикористаними можливостями». Це визначення може бути підґрунтям для ідентифікації конкретних видів ризиків в Індустрії 4.0. Опишемо далі ризики, які можуть мати місце в Індустрії 4.0.

Нинішній етап Індустрії 4.0 можна вважати підготовчим до безпосередньої Четвертої промислової революції. Наразі відбуваються різні заходи (форуми, промислові виставки-ярмарки, круглі столи, конференції і т.п.), на яких фахівці обговорюють різні аспекти Індустрії 4.0 та формують бачення майбутнього світової економіки та суспільства; світовими промисловими виробниками та науково-дослідними центрами створюються прототипи майбутніх Розумних Фабрик, автономні роботи тощо; урядами розвинутих країн формуються державні програми досліджень в контексті Індустрії 4.0 тощо. Характерними для даного етапу, на наш погляд є наступні основні ризики:

1) інвестиційні ризики. Розвиток та провадження у реальне життя концепції Індустрії 4.0 потребує значного фінансування – інвестицій. Здійснення інвестицій у проекти в межах Індустрії 4.0, які наразі не є швидко поверненими, а тому на кінцевий результат таких інвестицій може вплинути велика кількість негативних чинників, які можуть посилити ступінь відповідних ризиків. Існує досить велика кількість видів інвестиційних ризиків, з якими можна детально ознайомитися, наприклад у [21];

2) ризики інноваційної діяльності. Індустрія 4.0 за своєю суттю є сукупністю інновацій у промисловість – результатів науко-дослідних та проектно-конструкторських робіт, економічна ефективність яких може виявитися неприйнятною для окремого підприємства;

3) ризики промислового шпигунства та конкурентної розвідки. На різних заходах фахівці обмінюються інформацією та представляють готові рішення в рамках Індустрії 4.0, які вони можуть публічно оприлюднити. Проте частина інформації, яка є комерційною таємницею через її цінність, залишається закритою для сторонніх. І можлива втрата такої інформації й зумовлює відповідні ризики втрати комерційної таємниці;

4) ризики інтелектуально-трудових ресурсів пов'язані, зокрема, з відсутністю потрібних фахівців, недостатнім рівнем знань та компетенцій у існуючих фахівців для виконання поставлених завдань тощо;

5) адміністративно-законодавчі ризики. Повна або часткова відсутність необхідних для реалізації у життя Індустрії 4.0 нормативних та законодавчих документів зумовлює відповідні ризики, які пов'язані насамперед з низькою законодавчою підтримкою з боку держави інноваційної діяльності підприємств, університетів, науково-дослідних установ тощо у межах Індустрії 4.0. Окрім того, до цих ризиків можна віднести й такі [22]: ризики недостатнього обсягу патентування усіх видів рішень, що застосовуються для створення інновацій, ризики опротестування патентів, ризики незабезпечення патентної чистоти, ризики, пов'язані з паралельним патентуванням і нелегальною імітацією інноваційних рішень тощо;

6) ризики стандартів. В Індустрії 4.0 виробництво є гнучким (здатним випускати поштучно товар серійного виробництва), а це вимагає повної уніфікації виробничих процесів, наявності відповідних стандартів, інакше швидке переналаштування буде утруднене. Отже потрібно вже зараз, на початковому етапі Індустрії 4.0, це враховувати;

7) ризики неузгодженості, пов'язані з невідповідністю окремих аспектів концепції Індустрії 4.0 існуючим інформаційно-комунікаційними засобам та технологіям. Може виявитись, що окремі задуми чи методичні положення Індустрії 4.0 на деякому етапі не можуть бути втілені в життя через «відставання» реальних технологій від задумів фахівців та науковців, а тому потрібний деякий час щоб вони були відпрацьовані та реалізовані у житті.

Наступний етап реалізації Індустрії 4.0 передбачає втілення у реальне виробництво прототипів. За успішної реалізації цього етапу можна буде вважати, що Четверта промислова революція настала. У такому разі, всі ризики, які існують зараз, будуть з меншими чи більшими модифікаціями притаманні й Індустрії 4.0. Окрім того, з'явиться низка нових ризиків, які пов'язані з перебігом науково-технічного прогресу та змінами в організації виробництва. Отже, до ризиків Індустрії 4.0 також необхідно віднести наступні:

1) ризики кіберфізичних систем, що пов'язані з різними небажаними ситуаціями у роботі компонент таких систем, зокрема: звичайні фізичні поломки механізмів устаткування; збої в управлінні кібернетичними компонентами фізичних процесів; некоректне переналаштування виробничих процесів; помилки у виборі комплектуючих, які необхідні для виробництва продукції; вибір неправильної програми виробництва продукції; помилки, які можуть статись на різних ділянках фізичного виробництва продукції (некоректна обробка інформаційних компонент, неправильне компонування комплектуючих тощо); моральне «старіння» устаткування та його вузлів тощо;

2) ризики Інтернету Речей (або Промислового Інтернету Речей), що пов'язані з проблемами у роботі устаткування інформаційно-комунікаційних мереж, які забезпечують стійкість та якість зв'язку, пропускну здатність каналів зв'язку тощо;

3) ризики Розумної Продукції. Кожна готова продукція загалом та її компоненти в Індустрії 4.0 будуть мати так звані «електронні паспорти» [24], в яких мають зазначатись усі операції з ними: виробництво, ремонт, обслуговування, відмови, заміни частин, фізичне та інформаційне оновлення тощо. Похибки в

заповненні цих відомостей також можуть зумовити відповідні ризики. Окрім того, кожна продукція буде мати свій унікальний радіочастотний ідентифікатор (RFID), який повинен відповідати продукції, на якій він знаходиться, і в цьому випадку віртуальна (цифрова) копія продукції буде повністю відповідати фізичній продукції і навпаки. Можлива невідповідність зумовить відповідні ризики, які у свою чергу можуть генерувати інші ризики, що пов'язані, наприклад, з сервісним обслуговуванням такої продукції;

4) ризики Великих Даних пов'язані із небажаними ситуаціями, які можуть виникнути в процесах пошуку цінної аналітичної інформації серед постійно зростаючого обсягу даних та використання її у прийнятті рішень як роботами, так і людиною: задання таких критеріїв пошуку, які не можуть привести до задовільного результату; некоректна обробка отриманої інформації; проміжок часу отримання інформації є більшим за проміжок часу, за який потрібно прийняти рішення тощо;

5) ризики Хмар або хмарних обчислень пов'язані з нездатністю провайдерів хмарних рішень надати спектр необхідних послуг в цілому або частково;

6) ризики управління підприємством. В Індустрії 4.0 «речі» та людина будуть функціонувати в єдиному інформаційному просторі. Межі між ними в інформаційному аспекті фактично будуть розмиті за рахунок, зокрема, того, що «речі» будуть наділені інтелектом та приймати певні локальні самостійні рішення. Окрім того, разом з вертикальними інформаційними зв'язками будуть розвинуті й горизонтальні. Інтеграція між підприємствами буде фактично на рівні виробничих систем, що зумовить певне розмиття інформаційних меж між підприємствами [23] та, відповідно. змінить центри прийняття управлінських рішень. Все це зумовить виникнення відповідних видів ризиків;

7) ризики віртуальної реальності та моделювання. В Індустрії 4.0 водночас з реальним фізичним виробництвом має існувати його детальна віртуальна модель (копія). Відповідність між ними буде однозначна: зміни в реальному світі миттєво будуть відображатись у віртуальному, і навпаки. Проте використання віртуальної реальності може зумовити низку ризиків, які будуть пов'язані, зокрема, з наступним: неврахування деяких ознак реального світу у віртуальному; порушення взаємних зв'язків між реальністю та віртуальністю; поводження моделюючого об'єкту в реальному світі може відрізнятись від його поводження у віртуальному світі; можливий вплив віртуальної реальності на психоемоційний та фізіологічний стан людини, котра зобов'язана аналізувати та приймати управлінські рішення тощо;

8) ризики адитивного виробництва пов'язані з несприятливими ситуаціями, які можуть трапитися під час випуску продукції за допомогою 3-D принтерів: відсутність потрібного виду вільного принтеру, повна або часткова відсутність необхідних матеріалів для друку; низька якість матеріалів для друку; зношення вузлів принтеру тощо. Використання 3-D принтерів змінює логістичний ланцюг постачання, в якому центр виробництва продукції буде переміщено або безпосередньо до споживача (або близько до нього), що безумовно вплине на весь виробничий процес від сировини до готової продукції як на фізичному, так і на інформаційному (віртуальному) рівні. Окрім того, на промисловому виробництві постійно діють процеси перевірки якості та безпечності продукції, проте за умови використання 3-D принтерів у специфічних умовах досить важко перевірити якість «надрукованої» готової продукції. Усе це зумовить виникнення, наприклад, ризиків постачання сировини та матеріалів; ризиків зв'язку; ризиків якості та безпеки виробленої продукції тощо;

9) ризики інформаційної безпеки та кібербезпеки. Дедалі більшу частину свого життя ми переносимо в «цифру», що зумовлює оновлення відомих понять, до яких додається прикметник «електронний» або «цифровий»: електронна пошта, електронний бізнес, цифровий маркетинг, а також аналітичний цифровий маркетинг тощо. З кожним роком зростає кількість різних функцій та операцій у бізнесі, що

мають цифрове відображення без обов'язкового паперового їх підтвердження. В Індустрії 4.0. взагалі постулюється, що вся інформація буде цифровою. Все це зумовлює підвищений інтерес до проблеми інформаційної безпеки та кібербезпеки, сутність якої полягає у захисті інформації (насамперед, цінної для підприємства) шляхом боротьби з різними можливими загрозами: несанкціоноване встановлення шкідливого програмного забезпечення, несанкціоновані злочинні зміни в існуючому програмному забезпеченні, можливе спотворення або знищення інформації на різних етапах її існування недобросовісними працівниками підприємства або несанкціоноване втручання ззовні тощо;

10) ризики інтелектуально-трудових ресурсів є актуальними для Індустрії 4.0. Окрім згаданих вище ризиків, виникне загроза масштабного безробіття, що може спричинити скорочення робочих місць на підприємствах нового зразка. Проте виникне потреба у великій кількості ІТ-фахівців різних напрямків;

11) екологічні ризики – ризики, які пов'язані з завданням шкоди довкіллю внаслідок діяльності підприємств Індустрії 4.0;

12) ризики ресурсного забезпечення інноваційного виробництва пов'язані з суттєвими змінами, що відбудуться у використанні ресурсів виробництва, де одні із вагомих змін будуть стосуватись енергетичних ресурсів та, зокрема, їх ефективного використання (енергозбереження).

Зазначені вище ризики, на нашу думку, можна розподілити на:

1) ультра нові (які виникнуть лише під час впровадження концепції промислового виробництва «Індустрія 4.0» у реальне життя, і які взагалі не притаманні нинішній економіці): ризики кіберфізичних систем, ризики Інтернету Речей (або Промислового Інтернету Речей), ризики Розумної Продукції;

2) нові ризики (що лише почали виникати на теперішньому етапі розвитку світової економіки, і проявляться повною мірою в Індустрії 4.0): ризики Великих Даних, ризики Хмар або хмарних обчислень, ризики віртуальної реальності та моделювання, ризики адитивного виробництва, ризики інформаційної безпеки та кібербезпеки;

3) традиційні (або класичні) ризики (які були, є та будуть притаманні розвитку світової економіки та суспільства): інвестиційні ризики, ризики інноваційної діяльності, ризики промислового шпигунства та конкурентної розвідки, ризики інтелектуально-трудових ресурсів, адміністративно-законодавчі ризики, ризики стандартів, ризики управління підприємством, екологічні ризики, ризики ресурсного забезпечення.

З погляду основних учасників Індустрії 4.0 та сфер, яких вона торкнеться, ризики в Індустрії 4.0 можна класифікувати за «центрами» їх виникнення: соціальні ризики (пов'язані насамперед зі змінами зайнятості населення у виробництві, його соціальними гарантіями); ризики інноваційних засобів та технологій (пов'язані з результатами науково-технічного прогресу); економічні ризики (пов'язані з економічними результатами діяльності інноваційних підприємств Індустрії 4.0); адміністративно-законодавчі ризики; екологічні ризики. Водночас ризики інформаційної безпеки та кібербезпеки в Індустрії 4.0 стануть ключовими ризиками, які будуть притаманні усім процесам та об'єктам бізнесу.

Висновки і перспективи подальших досліджень. Інновації в Індустрії 4.0 зумовлюють виникнення низки різноманітних ризиків, які необхідно всебічно досліджувати та враховувати у прийнятті рішень. У даній статті нами запропоновано авторське бачення класифікації ризиків в Індустрії 4.0 та наведені уточнюючі тлумачення таких ризиків. У подальшому вбачаємо за доцільне зосередитися на системних дослідженнях кожного із зазначених у роботі ризиків: визначення їх суб'єктів, об'єктів, джерел, проведення детальної їх класифікації, визначення показників та методів оцінювання, побудова відповідних економіко-математичних моделей, розробка концептуальних засад та інструментарію управління ризиками.

Список використаної літератури

1. Kagermann H. Industrie 4.0: Mit dem Internet der Dinge auf dem Weg zur 4. industriellen Revolution [Електронний ресурс] / H. Kagermann, W.-D. Lukas, W. Wahlster // VDI nachrichten. – 2011. – №13. – Режим доступу: http://www.vdi-nachrichten.com/Technik-Gesellschaft/Industrie-40-Mit-Internet-Dinge-Weg-4-industriellen-Revolution
2. Hermann M. Design Principles for Industrie 4.0 Scenarios: A Literature Review [Електронний ресурс] / M. Hermann, T. Pentek, B. Otto // Working Paper. – Technical University of Dortmund. – 2015. – №1. – 16p. – Режим доступу: http://www.snom.mb.tu-dortmund.de/cms/de/forschung/Arbeitsberichte/Design-Principles-for-Industrie-4_0-Scenarios.pdf
3. Foundations for Innovation in Cyber-Physical Systems. Workshop Report [Електронний ресурс] // National Institute of Standards and Technology – January 2013. – Режим доступу: http://www.nist.gov/el/upload/CPS-WorkshopReport-1-30-13-Final.pdf
4. Securing the future of German manufacturing industry. Recommendations for implementing the strategic initiative Industrie 4.0. Final report of the Industrie 4.0 working group [Електронний ресурс] // Federal Ministry of education and research. – April 2013. – Режим доступу: http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Material_fuer_Sonderseiten/Industrie_4.0/Final_report__Industrie_4.0_accessible.pdf
5. Хаханов В. И. Киберфизические системы как технологии киберуправления (аналитический обзор) [Електронний ресурс] / В. И. Хаханов, В. И. Обризан, А. С. Мищенко, И. В. Филиппенко // Радиоэлектроника и информатика. – ХНУРЭ. – январь-март 2014. – № 1 (64). – С. 39-45. – Режим доступу: http://www.ewdtest.com/ri/no-164-январь-март-2014/
6. Что нужно знать об Индустрии 4.0 и Интернете вещей [Електронний ресурс]. – 2015. – Режим доступу: http://www.therunet.com/articles/4826-chto-nuzhno-znat-ob-industrii-4-0-i-internete-veschey
7. Atzori L. The Internet of Things / L. Atzori, D. Giusto, A. Iera, and G. Morabito. (Editors). – Springer-Verlag New York, 2010. – 442p.
8. Жемлиханов Т. «Индустрия 4.0»: революция без потерь? / Т. Жемлиханов // Электротехнический рынок. – 2015. – №5-6 (65-66). – С. 32-36.
9. Лайдон Б. Промышленный Интернет Вещей [Електронний ресурс] / Б. Лайдон. – Режим доступу: http://ua.automation.com/content/promyshlennyj-internet-veshhej
10. Elloumi O. Smart M2M/OneM2M Architecture And Principle Overview [Електронний ресурс] / O. Elloumi, E. Scarrone // DG Connect/ETSI Smart Appliances Workshop. – Brussels, 27-28 May 2014. – Режим доступу: https://docbox.etsi.org/workshop/2014/201405_smartappliancesworkshop/s02_m2marchitecture_elloumi.ppt
11. Компанії беруться за «Великі дані» – дослідження Microsoft [Електронний ресурс]. 2013. – Режим доступу: http://microsoftblog.azurewebsites.net/2013/02/12/kompaniyi-berut-sya-za-veliki-dani-doslidzhennya-microsoft/
12. Rüßmann M. Industry 4.0: The Future of Productivity and Growth in Manufacturing Industries [Електронний ресурс] / M. Rüßmann, M. Lorenz, P. Gerbert, M. Waldner, J. Justus, P. Engel, M.Harnisch. – 2015. – Режим доступу: https://www.bcgperspectives.com/content/articles/engineered_products_project_business_industry_40_future_productivity_growth_manufacturing_industries/
13. Sandip Patel. Industry 4.0 and Risk – Part 1 [Електронний ресурс] / Sandip Patel // The IBM Insurance industry blog «Insights on Business». – October 19, 2015. – Режим доступу: http://insights-on-business.com/insurance/industry-4-0-and-risk-part-1-2/
14. Sandip Patel. Industry 4.0 and Risk – Part 2 [Електронний ресурс] / Sandip Patel // The IBM Insurance industry blog «Insights on Business». – October 26, 2015. – Режим доступу: http://insights-on-business.com/insurance/industry-4-0-and-risk-part-2/
15. Schröder M. Industry 4.0 And Its Impact On Supply Chain Risk Management [Електронний ресурс] / M. Schröder, M. Indorf, W. Kersten // 14th International Conference «Reliability and Statistics in Transportation and Communication (RelStat)». – Riga, 15–18 October 2014. – Режим доступу: http://www.tsi.lv/sites/default/files/editor/science/Conferences/RelStat14/schroeder_indorf_kersten.pdf
16. The Smart Factory – Risk Management Perspectives [Електронний ресурс] // Chief Risk Officer (CRO) Forum. – December 2015. – Режим доступу: http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CROF-ERI-2015-The-Smart-Factory.pdf
17. Hader M. Cyber-Security – Managing threat scenarios in manufacturing companies [Електронний ресурс] / M. Hader, C. Rossbach//. Think Act. – Roland Berger Strategy Consultants, March 2015. – Режим доступу: https://www.rolandberger.de/media/pdf/Roland_Berger_TAB_Cyber_Security_20150305.pdf
18. Allianz Risk Barometer 2016 [Електронний ресурс] . – Режим доступу: http://www.agcs.allianz.com/insights/white-papers-and-case-studies/allianz-risk-barometer-2016/
19. Allianz Risk Barometer 2015: Businesses exposed to increasing number of disruptive scenarios [Електронний ресурс] . – Режим доступу: http://www.agcs.allianz.com/about-us/news/press-riskbarometer2015/

20. Industrie 4.0 – From Vision to Reality. Challenges and Opportunities // IBM Architektentage. – Nov 12-2013 https://www-304.ibm.com/events/wwe/grp/grp006.nsf/vLookupPDFs/11-13-IBM-Architektentage_Industrie-4.0_V1/$file/11-13-IBM-Architektentage_Industrie-4.0_V1.pdf
21. Вітлінський В. В., Ризикологія в економіці та підприємництві : Монографія. / В. В. Вітлінський., Г. І. Великоіваненко – К. : КНЕУ. – 2004. – 480 с.
22. Клименко С. М. Обгрунтування господарських рішень та оцінка ризиків: навч. посібник / С. М. Клименко, О. С. Дуброва. – К. : КНЕУ, 2005. – 252 с.
23. Югринова Н. Машинный междусобой [Електронний ресурс]/ Н. Югринова // Бизнес-журнал. – 29 февраля 2016. – №3. – Режим доступу: http://b-mag.ru/2016/industriya-4-0/mashinnyiy-mezhdusoboy/

References

1. Kagermann, H. Lukas, W.-D., Wahlster W. (2011). *Industrie 4.0: Mit dem Internet der Dinge auf dem Weg zur 4. industriellen Revolution*. VDI nachrichten, 13. Retrieved from: http://www.vdi-nachrichten.com/Technik-Gesellschaft/Industrie-40-Mit-Internet-Dinge-Weg-4-industriellen-Revolution
2. Hermann, M., Pentek, T., Otto, B. (2015). *Design Principles for Industrie 4.0 Scenarios: A Literature Review.* (Working Paper). Technical University of Dortmund, 1. Retrieved from: http://www.snom.mb.tu-dortmund.de/cms/de/forschung/Arbeitsberichte/Design-Principles-for-Industrie-4_0-Scenarios.pdf
3. National Institute of Standards and Technology. (2013, January). *Foundations for Innovation in Cyber-Physical Systems. Workshop Report.* Retrieved from: http://www.nist.gov/el/upload/CPS-WorkshopReport-1-30-13-Final.pdf
4. Federal Ministry of education and research. (2013, April). *Securing the future of German manufacturing industry. Recommendations for implementing the strategic initiative Industrie 4.0. Final report of the Industrie 4.0 working group*. Retrieved from: http://www.acatech.de/fileadmin/user_upload /Baumstruktur_nach_Website/Acatech/root/de/Material_fuer_Sonderseiten/Industrie_4.0/Final_report__ Industrie_4.0_accessible.pdf
5. Hahanov, V.I., Obrizan, V.I., Mishchenko, A.S., Filippenko. I.V. (2014, January-March). *Cyber-physical systems as cyber-technology management (analytical review).* RadioElectronics & Informatics Journal, 1(64), 39-45. Retrieved from: http://www.ewdtest.com/ri/no-164-январь-март-2014/ (in Rus.)
6. TheRunet. (2015). *What you need to know about the Industry 4.0 and the Internet of things.* Retrieved from: http://www.therunet.com/articles/4826-chto-nuzhno-znat-ob-industrii-4-0-i-internete-veschey (in Rus.)
7. Atzori, L., Giusto, D., Iera, A., Morabito, G. (2010). *The Internet of Things.* Springer-Verlag New York
8. Zhemlihanov T. (2015). *«Industry 4.0»: a revolution without a loss.* Electrical market, 5-6(65-66), 32-36 (in Rus.)
9. Lydon B. *Industrial Internet of Things.* Retrieved from: http://ua.automation.com/content/promyshlennyj-internet-veshhej (in Rus.)
10. Elloumi, O., Scarrone, E. (2014, May). *Smart M2M/OneM2M Architecture And Principle Overview.* DG Connect/ETSI Smart Appliances Workshop. Brussels. Retrieved from: https://docbox.etsi.org/workshop/2014/201405_smartappliancesworkshop/s02_m2marchitecture_elloumi.ppt
11. Microsoft. (2013). Companies set to «Big Data» – Microsoft study. Retrieved from: http://microsoftblog.azurewebsites.net/2013/02/12/kompaniyi-berut-sya-za-veliki-dani-doslidzhennya-microsoft/ (in Ukr.)
12. Rüßmann, M., Lorenz, M., Gerbert, P., Waldner, M., Justus, J., Engel, P. Harnisch, M. (2015). *Industry 4.0: The Future of Productivity and Growth in Manufacturing Industries*. 2015. Retrieved from: https://www.bcgperspectives.com/content/articles/engineered_products_project_business_industry_40_future_ productivity_growth_manufacturing_industries/
13. Sandip Patel. (2015, October 19). *Industry 4.0 and Risk – Part 1*. The IBM Insurance industry blog «Insights on Business». Retrieved from: http://insights-on-business.com/insurance/industry-4-0-and-risk-part-1-2/
14. Sandip Patel. (2015, October 26). *Industry 4.0 and Risk – Part 2*. The IBM Insurance industry blog «Insights on Business». Retrieved from: http://insights-on-business.com/insurance/industry-4-0-and-risk-part-2/
15. Schröder, M., Indorf, M., Kersten, W. (2014, October 15–18). *Industry 4.0 And Its Impact On Supply Chain Risk Management*. 14th International Conference «Reliability and Statistics in Transportation and Communication (RelStat)». Riga. Retrieved from: http://www.tsi.lv/sites/default/files/editor/science/ Conferences/RelStat14/schroeder_indorf_kersten.pdf
16. Chief Risk Officer (CRO) Forum. (2015, December). *The Smart Factory – Risk Management Perspectives.* Retrieved from: http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CROF-ERI-2015-The-Smart-Factory.pdf
17. Hader, M., Rossbach, C. (2015, March). *Cyber-Security – Managing threat scenarios in manufacturing companies*. Think Act. Roland Berger Strategy Consultants. Retrieved from: https://www.rolandberger.de/media/pdf/Roland_Berger_TAB_Cyber_Security_20150305.pdf
18. Allianz. (2016). *Allianz Risk Barometer 2016.* Retrieved from: http://www.agcs.allianz.com/insights/white-papers-and-case-studies/allianz-risk-barometer-2016/

19. Allianz. (2015). *Allianz Risk Barometer 2015: Businesses exposed to increasing number of disruptive scenarios.* Retrieved from: http://www.agcs.allianz.com/about-us/news/press-riskbarometer2015/
20. IBM. (2013, November 12). *Industrie 4.0 – From Vision to Reality. Challenges and Opportunities*. Retrieved from: https://www-304.ibm.com/events/wwe/grp/grp006.nsf/vLookupPDFs/11-13-IBM-Architektentage_Industrie-4.0_V1/$file/11-13-IBM-Architektentage_Industrie-4.0_V1.pdf
21. Vitlinskyy, V.V., Velykoivanenko, G.I. (2004). Ryzykolohiya in economics and entrepreneurship: Monograph. Kyiv: KNEU (in Ukr.)
22. Klimenko, S.M., Dubrova, A.S. (2005). Justification business decisions and risk assessment: teach. manual, Kyiv: KNEU (in Ukr.)
23. Yugrinova N. (2016, February 29). *Machine interconnected.* Business Magazine, 3. Retrieved from: http://b-mag.ru/2016/industriya-4-0/mashinnyiy-mezhdusoboy/ (in Rus.)

VITLINSKYY Valdemar Volodymyrovych,
Doctor of Economics Sciences, Professor,
Head of Department of Economic and Mathematical Modeling,
State Higher Educational Establishment
«Kyiv National Economic University named after Vadym Hetman»
SKITSKO Volodymyr Ivanovych,
PhD (Economics), Associate Professor,
Postdoctoral Fellow of Department of Economic and Mathematical
Modeling, State Higher Educational Establishment
«Kyiv National Economic University named after Vadym Hetman»

RISKS IN INDUSTRY 4.0

Abstract. ***Introduction***. *Industry 4.0 is an innovative industrial production of the future, to which uncertainty is inherent that gives rise to various risks that need to be analyzed, modeled and managed. Currently, there are not enough fundamental scientific or practical works that would systematically investigate the problem of risks of Industry 4.0. However, there are foreign works which cover some aspects of risk management in the industry 4.0. There are practically no domestic works on the problem under investigation, therefore we would like to some extent to fill this gap of domestic scientific achievements.* ***Purpose***. *The purpose is to identify the main risks of Industry 4.0, based on system analysis and refinement of their interpretations and to formulate our own vision of their classification.* ***Materials***. *In the process of writing the work the available public Internet materials on various aspects of Industry 4.0 were used.* ***Results***. *The current phase of Industry 4.0 can be considered preparatory to actually the Fourth Industrial Revolution, which is characterized by the following risks: investment; innovation activity; industrial espionage and competitive intelligence; intellectual and human resources; administrative and legislative; standards; inconsistencies related to the discrepancy of the concept of Industry 4.0 to the existing information and communication tools and technologies. The next phase of Industry 4.0 implementation stipulates the actual production of prototypes. In case of successful implementation of this phase it can be considered that the Fourth Industrial Revolution has occurred. In this case, all the risks that already exist with some changes will be typical of Industry 4.0 as well. In addition a number of new risks will appear. That is, the risks of Industry 4.0 will be the following: risks of Cyber-Physical Systems, risks of the Internet of Things (or the Industrial Internet of Things), Smart Products risks, Big Data risks, risks of cloud or cloud computing, risk of management, risks of virtual reality and modeling, risks of additive production, risks of information security and cyber security, risks of intellectual and human resources, environmental risks, risks of resource provision of innovative production. In addition, the work also specifies other risk classifications of Industry 4.0.* ***Originality***. *The authors define risks of Industry 4.0, provide author clarifications of their eesences and propose the author vision of risk classification of Industry 4.0 based on various properties and criteria.* ***Conclusion***. *This work can be a starting point for further research on the risks inherent to the Industry 4.0 based on various areas, including Industry 4.0 risk modeling.*

Keywords: *risk, Industry 4.0, the Fourth Industrial Revolution, Cyber-Physical Systems (CPS), Internet of Things (IoT).*

Одержано редакцією: 12.01.2016
Прийнято до публікації: 19.01.2016