УДК 330.131.7:658

РИЗИК-МЕНЕДЖМЕНТ ЛАНЦЮГІВ ПОСТАЧАННЯ В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ

©2018 ВІТЛІНСЬКИЙ В. В., СКІЦЬКО В. І.

УДК 330.131.7:658

Вітлінський В. В., Скіцько В. І. Ризик-менеджмент ланцюгів постачання в умовах цифрової економіки

Проаналізувавши низку сучасних публікацій щодо досліджуваної проблеми, автори статті сформулювали основні поняття ризик-менеджменту та описали основні кроки ризик-менеджменту ланцюгів постачання фізичної, фізично-цифрової та цифрової продукції в умовах цифрової економіки. Ризик ланцюга постачання фізичної продукції в умовах цифрової економіки – це економічна категорія, яка відображає особливості сприйняття менеджментом підприємств – учасників ланцюга постачання об'єктивно існуючих небезпек і загроз, ненадійності різних засобів та технологій, рівня знань, невизначеності та конфліктності, відсутності вичерпної інформації на момент прийняття рішень у процесах перебігу матеріального та супроводжуючих його інформаційних потоків в усьому ланцюзі постачання. Для ланцюгів постачання цифрової та фізично-цифрової продукції зазначене означення ризику буде аналогічним з уточненням, що матеріальний потік буде мати відповідно цифрове та фізично-цифрове представлення. У статті окреслені також джерела ризику, визначено суб'єкт та об'єкт ризику; суб'єкт і об'єкт ризик-менеджменту ланцюгів постачання фізичної, фізично-цифрової, цифрової продукції. Отримані результати досліджень можуть бути використані під час розробки та впровадження системи ризик-менеджменту ланцюга постачання або адаптації існуючої з метою підвищення ефективності здійснення управління ризиками та врахування сучасного тренду розвитку економіки.

Ключові слова: *цифрова економіка, ланцюг постачання, ризик, штучний інтелект, когнітивні технології.*
Табл.: *1.* ***Бібл.:*** *32.*

Вітлінський Вальдемар Володимирович *– доктор економічних наук, професор, завідувач кафедри економіко-математичного моделювання, Київський національний економічний університет ім. В. Гетьмана (просп. Перемоги, 54/1, Київ, 03057, Україна)*
E-mail: *wite101@meta.ua*
Скіцько Володимир Іванович *– кандидат економічних наук, доцент, доцент кафедри економіко-математичного моделювання, Київський національний економічний університет ім. В. Гетьмана (просп. Перемоги, 54/1, Київ, 03057, Україна)*
E-mail: *skitsko.kneu@gmail.com*

УДК 330.131.7:658

Витлинский В. В., Скицко В. И. Риск-менеджмент цепей поставок в условиях цифровой экономики

Проанализировав ряд современных публикаций по исследуемой проблеме, авторы статьи сформулировали основные понятия риск-менеджмента и описали основные шаги риск-менеджмента цепей поставок физической, физически-цифровой и цифровой продукции в условиях цифровой экономики. Риск цепи поставки физической продукции в условиях цифровой экономики – это экономическая категория, которая отражает особенности восприятия менеджментом предприятий – участников цепи поставок объективно существующих опасностей и угроз, ненадежности различных средств и технологий, уровня знаний, неопределенности и конфликтности, отсутствия исчерпывающей информации на момент принятия решений в процессах течения материального и сопровождающих его информационных потоков во всей цепи поставки. Для цепей поставок цифровой и физически-цифровой продукции указанное определение риска будет аналогичным с уточнением, что материальный поток будет иметь соответственно цифровое и физически-цифровое представление. В статье обозначены также источники риска, определены субъект и объект риска; субъект и объект риск-менеджмента цепей поставок физической, физически-цифровой, цифровой продукции. Полученные результаты исследований могут быть использованы при разработке и внедрении системы риск-менеджмента цепи поставок или адаптации существующей с целью повышения эффективности осуществления управления рисками и учета современного тренда развития экономики.

Ключевые слова: *цифровая экономика, цепь поставок, риск, искусственный интеллект, когнитивные технологии.*
Табл.: *1.* ***Библ.:*** *32.*

Витлинский Вальдемар Владимирович *– доктор экономических наук, профессор, заведующий кафедрой экономико-математического моделирования, Киевский национальный экономический университет им. В. Гетьмана (просп. Победы, 54/1, Киев, 03057, Украина)*
E-mail: *wite101@meta.ua*
Скицко Владимир Иванович *– кандидат экономических наук, доцент, доцент кафедры экономико-математического моделирования, Киевский национальный экономический университет им. В. Гетьмана (просп. Победы, 54/1, Киев, 03057, Украина)*
E-mail: *skitsko.kneu@gmail.com*

UDC 330.131.7:658

Vitlinskyi V. V., Skitsko V. I. The Risk-Management of Supply Chains in the Conditions of Digital Economy

Having analyzed a number of recent publications on the researched problem, authors of the article have formulated the basic concepts of risk-management and have described the basic steps of risk-management of supply chains of physical, physical-digital and digital production in conditions of digital economy. The risk of the supply chain of physical products in the conditions of digital economy is an economic category that reflects the features of management of enterprises – participants in the supply chain of objectively existing hazards and threats, unreliability of various means and technologies, level of knowledge, uncertainty and conflict, absence of comprehensive information at the moment of decision-making in the processes of material flow and accompanying its information flows throughout the chain of supply. For the supply chains of digital and physical-digital products, the indicated definition of risk will be similar, specifying that the material flow will have a digital and physical-digital representation, respectively. The article also identifies the sources of risk, defines the subject and the object of risk; subject and object of risk-management of supply chains of physical, physical-digital, and digital products. The obtained results of researches can be used at development and introduction of system of risk-management of supply chains or adaptation of an existing one for the purpose of increase of efficiency of implementation of risk management and consideration of modern trend of economy development.

Keywords: *digital economy, supply chain, risk, artificial intelligence, cognitive technologies.*
Tbl.: *1.* ***Bibl.:*** *32.*

Vitlinskyi Valdemar V. *– D. Sc. (Economics), Professor, Head of the Department of economic and mathematical modeling, Kyiv National Economic University named after V. Hetman (54/1 Peremohy Ave., Kyiv, 03057, Ukraine)*
E-mail: *wite101@meta.ua*
Skitsko Volodymyr I. *– PhD (Economics), Associate Professor, Associate Professor of the Department of Economic and Mathematical Modeling, Kyiv National Economic University named after V. Hetman (54/1 Peremohy Ave., Kyiv, 03057, Ukraine)*
E-mail: *skitsko.kneu@gmail.com*

Урядом України 17 січня 2018 року було ухвалено Концепцію розвитку цифрової економіки та суспільства України впродовж 2018–2020 рр., згідно з якою «цифрова економіка» означає діяльність, в якій основними засобами (чинниками) виробництва є цифрові (електронні, віртуальні) дані – як числові, так і текстові» [1]. Цифрова економіка є економікою, підґрунтям функціонування якої є цифрові технології та сервіси, що створюються, впроваджуються та обслуговуються цифровою промисловістю, яку також називають ІТ-сектором або сферою інформаційно-комунікаційних технологій (ІКТ) [2, с. 38; 3]. Інколи цифрову економіку називають Інтернет-економікою, електронною економікою, веб-економікою, новою економікою [4]. Основою цифрової економіки є дані, знання, інформація в цифровому вигляді. Завдяки цифровій економіці процеси традиційної економіки, виконання яких пов'язано з генеруванням, обробкою, аналізом і зберіганням даних, стають більш ефективними, зокрема зменшується кількість помилок і час виконання таких процесів, вартість їх здійснення тощо. Цифрова економіка зумовлює структурні зрушення та розвиток як економіки загалом, так і різних ринків, зокрема логістики.

Завдяки логістиці учасники економічних відносин можуть ефективно взаємодіяти один з одним, узгоджуючи виробничі та збутові процеси через ланцюги постачання тощо. Використання ІКТ на різних етапах ланцюга постачання сприяє підвищенню ефективності переміщення готової продукції від виробника до кінцевого споживача, створює нові можливості щодо розвитку як такого ланцюга в цілому, так і його компонент окремо, дозволяє покращити якість логістичних послуг тощо.

Інновації в цифровій економіці зумовлюють виникнення нових і зміну сутності деяких існуючих ризиків, якими учасникам економічних відносин треба вміти управляти на різних економічних рівнях у межах відповідного ризик-менеджменту. Тобто, з метою збереження стійкості, покращання результатів функціонування ланцюгів постачання в умовах цифрової економіки необхідно також уміти ефективно управляти ризиками таких ланцюгів.

Джерела, використані у підготовці статті, можна розподілити на такі: 1) публікації, присвячені ризик-менеджменту ланцюгів постачання в умовах цифрової економіки, Індустрії 4.0, використання інноваційних цифрових технологій, а також кібер-ризику ланцюгів постачання як одного із основних ризиків нової економіки; 2) публікації, присвячені різним змінам у функціонуванні ланцюгів постачання внаслідок використання сучасних інновацій та перспективи їх (ланцюгів) розвитку; 3) публікації, присвячені ризик-менеджменту в цифровій економіці (без прив'язки до ланцюгів постачання); 4) публікації, присвячені цифровій економіці, Індустрії 4.0 у цілому. З іншого боку, джерела можна розподілити на: публікації науковців; публікації фахівців у різних видах діяльності; звіти міжнародних організацій та компаній, які відображають думки власних фахівців, та опитування фахівців із різних країн світу.

Катаріною Дідріх (*K. Diedrich*) у праці [5] було зроблено ґрунтовний аналіз публікацій, які присвячені різним аспектам ризик-менеджменту в ланцюгах постачання за період з 2000 р. по червень 2017 р. На її думку, усі досліджувані нею публікації можна розподілити на такі, в яких розглядаються: 1) різні аспекти ризик-менеджменту існуючих ланцюгів постачання, що орієнтуються на майбутнє; 2) аспекти управління майбутніми ризиками у випадках, коли учасники ланцюгів постачання приймають рішення щодо їх урахування у своїй роботі; 3) нові можливості ризик-менеджменту ланцюгів постачання в умовах цифрової економіки; 4) майбутні аспекти ризик-менеджменту ланцюгів постачання.

Проведений К. Дідріх аналіз робіт показав, що переважна більшість із них описує кроки процесу ризик-менеджменту ланцюгів постачання, які можна звести до ідентифікації та оцінювання ризиків, застосування заходів щодо зниження впливу негативних наслідків можливого прояву таких ризиків, і лише невелика частина публікацій присвячена використанню в ризик-менеджменті інноваційних засобів та технологій, завдяки яким і відбувається імплементація з цифровим світом. Наприклад, у праці [6] описані етапи управління ризиками ланцюгів постачання (ідентифікація, аналіз, оцінювання, обробка, моніторинг ризику) для різних стадій розвитку концепції «Індустрія 4.0» (комп'ютеризація, взаємозв'язок з використанням Інтернету, видимість у мережі, прозорість, передбачуваність подій, здатність пристосовуватись (адаптація). На основі узагальнення актуальних публікацій різних авторів щодо впливу технологій цифрової економіки на ризик-менеджмент ланцюгів постачання в [7] отримано такий висновок: завдяки цифровим даним, збільшенню їх обсягу (великі дані), сучасним інформаційно-комунікаційним засобам і технологіям, тісній взаємодії між учасниками ланцюга постачання ризик-менеджмент стає ефективнішим, що, зокрема, дозволяє підвищити видимість, гнучкість та прибутковість таких ланцюгів постачання.

У публікації [8] на підставі опитування респондентів із всього світу досліджуються фінансові ризики в цифровій економіці з метою визначення тенденцій розвитку ризик-менеджменту в цифрову еру, виокремлення критичних моментів з метою допомогти менеджменту установ фінансового сектора здійснювати перетворення більш ефективно. Низку аспектів, які висвітлено у праці [8], можна віднести й до інших економічних ризиків, зокрема ризиків ланцюгів постачання.

Автори [9] наголошують на актуальності проблеми ризик-менеджменту в ланцюгах постачання і на тому, що особливої уваги потребують кібер-ризики, що пов'язані з втручанням в апаратне забезпечення функціонування ланцюга постачання та використання шкідливого програмного забезпечення, яке здатне несанкціоновано передавати інформацію, змінювати існуючі реальні дані на фіктивні тощо. Проблемі управління кібер-ризиком у ланцюзі постачання присвячена також публікація [10].

Сучасні тренди та майбутні зміни в ланцюгах постачання в умовах цифрової економіки досліджують такі автори, як В. Лехмачер (*W. Lehmacher*), Ф. Бетті (*F. Betti*), П. Бічер (*P. Beecher*), К. Гротемеєр (*C. Grotemeier*), М. Лорензен (*M. Lorenzen*) [11], П. Алкантара (*P. Alcantara*), Г. Ріглієтті (*G. Riglietti*), Л. Агуада (*L. Aguada*) [12], В. Керстен (*W. Kersten*), М. Сейтер (*M. Seiter*), Б. фон Зее (*B. von See*), Н. Хакіус (*N. Hackius*), Т Маурер (*T. Maurer*) [13], С. Шрауф (*S. Schrauf*), Ф. Бертрам (*P. Berttram*) [14], А. Мусомелі (*A. Mussomeli*), Д. Гіш (*D. Gish*), С. Лаапер (*S. Laaper*) [15], К. Аліке (*K. Alicke*), Д. Рексхаузен (*D. Rexhausen*), А. Сейферт (*A. Seyfert*) [16], проте вони приділяють недостатньо уваги проблемі управління ризиками ланцюгів постачання.

Опрацювавши різні джерела за тематикою статті, можна дійти висновку, що наразі публікацій, в яких системно досліджували б ризик-менеджмент ланцюгів постачання в умовах цифрової економіки, обмаль, а в Україні публікацій з даної проблеми майже немає. Зауважимо, що багатогранність, перспективність та актуальність проблеми управління ризиками ланцюгів постачання цифрової економіки містить велику кількість аспектів, які потребують ретельних досліджень.

Мета статті полягає в аналізі та уточненні існуючих засад ризик-менеджменту ланцюгів постачання в умовах цифрової економіки та формулювання власного бачення щодо даної проблеми.

Ризики ланцюгів постачання займають перше місце серед ділових ризиків уже кілька років поспіль за версією щорічних досліджень *Allianz Risk Barometer* [17–22] (*табл. 1*). Ризик, який пов'язаний з різними кібер-подіями, (кібер-ризик), упевнено рухається вгору в топ-10 ділових ризиків і посідає друге місце згідно з останніми дослідженнями (див. табл. 1), що відповідає тенденції практично повсюдного використання інформаційно-мережних засобів і технологій у бізнесі. З кібер-ризиком у контексті цифрової економіки тісно пов'язаний ризик нових технологій, який також рухається вгору в рейтингу ділових ризиків. На нашу думку, така тенденція буде зберігатися ще деякий час, і в найближчі роки ці три ризики будуть складати топ-3 ділових ризиків. Окрім того, вже наразі існує потреба в уточненні поняття ризику ланцюгів постачання в умовах нової економіки, що зумовлено існуючими та майбутніми змінами в ланцюгах постачання.

Основна трансформація ланцюгів постачання, котра є характерною для цифрової економіки та відбувається вже зараз, пов'язана з переходом від лінійних ланцюгів постачання до динамічних взаємопов'язаних відкритих систем постачання, які називаються цифровими мережами постачання (*Digital Supply Network – DSN*) і в яких центральне місце займають цифрові дані [15; 16]. До основних характеристик ланцюга постачання цифрової економіки (або цифрової мережі постачання) можна віднести такі [15; 16]:

- гнучкість процесів доставки буде полягати в тому, що навіть у процесі здійснення доставки буде можлива оперативна зміна параметрів такої доставки (наприклад, місця та часу доставки);
- взаємопов'язана спільнота учасників (спілкування учасників один з одним відбувається безпосередньо);
- інтелектуальна оптимізація (у прийнятті рішень уміння людей посилюються штучним інтелектом. Системи управління, які здатні самостійно навчатися, зможуть без залучення людини визначати ризикові ситуації в роботі ланцюга постачання та змінювати процеси з метою зниження відповідних ризиків);
- цілковита прозорість (зацікавлені учасники мереж мають доступ до повної, актуальної, оперативної інформації щодо різних аспектів постачання в мережі. Перебіг інформаційних потоків є безперервним і водночас доступним для усіх зацікавлених учасників мережі. Це дає змогу частково уникнути різних проблем і затримок у роботі, які притаманні традиційним ланцюгам постачання);
- комплексне прийняття обґрунтованих оперативних рішень (усі учасники ланцюга постачання під час прийняття рішень можуть мати актуальну, оперативну та достовірну інформацію щодо всього ланцюга постачання. Це повинно сприяти підвищенню ефективності таких рішень і досягнути, зокрема, підвищення балансу між пропозицією та попитом);
- скорочення терміну доставки за допомогою більш ефективного розподілу споживчих товарів. Це досягається завдяки зростанню точності прогнозів попиту споживачів з урахуванням різних чинників. Завдяки раціональним і надійним ланцюгам постачання значно зростуть продажі товарів;
- перехід від надання стандартних послуг доставки продукції до задоволення індивідуальних потреб окремого споживача;
- широке використання роботів тощо;
- зменшення експлуатаційних витрат та обсягів запасів товарів, зростання маневреності ланцюгів.

Таблиця 1

Місце глобальних ділових ризиків згідно з Allianz Risk Barometer у рейтингах за 2013–2018 рр.

Ризик	Рік					
	2013	2014	2015	2016	2017	2018
Ризик переривання бізнес-процесів, у т. ч. логістичних ланцюгів постачання	1	1	1	1	1	1
Кібер-ризики, які пов'язані з кіберзлочинністю, збоями в роботі інформаційних систем та технологій апаратного та програмного характеру, шпигунство, збій даних тощо		8	5	3	3	2
Природні катастрофи (шторм, повінь, землетрус)	2	2	2	4	4	3
Розвиток ринку (волатильність, зростання конкуренції, стагнація ринку)				2	2	4
Зміни законодавства та регулюючих нормативних документів (економічні санкції, протекціонізм і т. п.)	4	4	4	5	5	5
Пожежа, вибух	3	3	3	8	7	6
Новітні технології				11	10	7
Втрата репутації підприємства (компанії, корпорації тощо) або вартості бренда	10	6	6	7	9	8
Політичні ризики (війна, тероризм, політичні та соціальні перевороти тощо)			9	9	8	9
Зміна клімату / зростання мінливості погоди						10
Макроекономічні події (програми жорсткої економії, зростання цін, інфляція/дефляція)				6	6	
Крадіжка, шахрайство, корупція		9	10	10		
Застій чи занепад ринку	8	5	7			
Посилення конкуренції	5	7	8			
Недоліки в якості продукції, можливі дефекти і т. п.	6	10				
Ринкові коливання (курс обміну валют, відсоткові ставки тощо)	7					
Можливість порушення Єврозони	9					

Джерело: побудовано за даними [17–22].

Можна припустити, що в умовах цифрової економіки будуть існувати:

- класичні (традиційні) ланцюги постачання фізичної продукції від джерела сировини до кінцевого споживача, в яких будуть широкого використовуватись різні інноваційні засоби та технології.

Це ланцюги постачання, в яких матеріальний потік має фізичне представлення на усьому шляху його руху від сировини до готової продукції, а в ланках такого ланцюга здійснюються традиційні логістичні та інші операції. Наприклад, постачальник сировини постачає матеріальну (фізичну) сировину від джерел появи чи зберігання сировини до виробника, який здійснює фізичне виготовлення продукції, котра спрямовується оптовиками, дистриб'юторами, логістичними центрами до місць продажу продукції, де кінцевий споживач може безпосередньо її придбати. У такому ланцюзі інформація набуде цифрового вигляду, а регламентований доступ до неї зможуть мати всі учасники ланцюга постачання. Використання інновацій дозволяє пришвидшити різні логістичні процеси насамперед завдяки зменшенню помилок під час обробки інформації;

- ланцюги постачання цифрової продукції, завдяки яким буде відбуватися доступ споживачів до готової цифрової продукції або доставка від місць зберігання готової цифрової продукції (деякі каталоги, бази даних тощо) до електронного пристрою споживача (ноутбук, смартфон, телевізор тощо) чи до місця, яке вкаже споживач (наприклад, електронна пошта споживача чи інше сховище власних даних споживача).

У цьому разі можна говорити про електронний (цифровий) матеріальний потік, під яким можна розуміти сукупність продукції в електронному вигляді, до якої застосовуються різні логістичні операції (зберігання, передача, розповсюдження тощо) електронної логістики, зокрема й операції кіберзахисту, в заданому часовому інтервалі [23];

- нові ланцюги постачання фізичної продукції, в яких матеріальний потік буде мати деякі особливості, пов'язані з технологічними процесами виготовлення готової продукції з використанням інноваційних засобів, зокрема 3D-принтерів.

У цьому випадку ланцюг постачання можна описати таким чином. Сировина доставляється безпосередньо до місця розташування 3D-принтера в деякому спеціальному місці або в кінцевого споживача, здійснюється передача до друкарки за запитом споживача файлу, котрий є цифровим відображенням готової продукції, та відбувається друк (виготовлення) готової продукції у фізичному вигляді. Тут можна говорити про гібридний фізично-цифровий матеріальний потік.

Попри різноманітність ланцюгів постачання, функціонування кожного із них буде сприяти досягненню основної мети логістики, що полягає у доставці потрібної продукції в будь-якій формі (фізичній чи цифровій) у потрібному обсязі, належної якості, за узгодженою ціною, в узгоджене місце (в реальному чи цифровому світі) та в замовлений споживачем час. Можна припустити, що основні поняття ризик-менеджменту також будуть мати спільні риси. Спираючись на існуючі тлумачення понять ризику в загальному випадку, ризику ланцюгів постачання, логістичного ризику, ризик-менеджменту, наведемо далі авторське бачення щодо основних понять ризик-менеджменту різних ланцюгів постачання в цифровій економіці.

Ризик ланцюга постачання фізичної продукції в умовах цифрової економіки – це економічна категорія, яка відображає особливості сприйняття менеджментом підприємств – учасників ланцюга постачання об'єктивно існуючих небезпек і загроз, ненадійності різних засобів і технологій (зокрема, й цифрових інформаційно-комунікаційних), рівня знань, невизначеності та конфліктності, відсутності повної (вичерпної) інформації на момент прийняття рішень у процесах перебігу матеріального та супроводжуючих його інформаційних потоків у всьому ланцюзі постачання.

Для ланцюгів постачання цифрової та фізично-цифрової продукції надане вище означення ризику буде аналогічним з уточненням, що матеріальний потік буде мати відповідно цифрове та фізично-цифрове представлення.

Об'єктом ризику для усіх зазначених ланцюгів постачання буде ланцюг постачання, а *суб'єктом ризику* – менеджмент підприємств – учасників ланцюга постачання.

Ланцюг постачання можна розглядати як узгоджену взаємодію різних його ланок, тобто підприємств, які є окремими суб'єктами господарювання та виконують певні основні функції в ланцюзі постачання. Ці функції можуть у різних підприємствах не співпадати. Наприклад, у ланцюзі постачання фізичної продукції виробник відповідає виключно за виробництво продукції, а логістична компанії – за доставку продукції; у ланцюзі постачання цифрової продукції також може існувати виробник, тобто деяка компанія, яка буде створювати таку продукцію, а доставка такої продукції буде компетенцію низки компаній, що надають послуги доступу та передачі інформації (Інтернет-провайдери). Тому об'єктом ризику в ланцюзі постачання може бути як ланцюг постачання в цілому, так і окрема його ланка, тобто деяке підприємство.

Джерелами ризику ланцюга постачання фізичної (цифрової та фізично-цифрової) продукції в умовах цифрової економіки є чинники (процеси, явища), які зумовлюють виникнення небезпек і загроз ефективного функціонування ланцюга постачання, ненадійність цифрових технологій (що пов'язана, зокрема, з генеруванням, збереженням і передачею інформації, її коректністю тощо), невизначеність результатів прийняття рішень та конфліктність між учасниками ланцюга постачання та підприємствами, які не є учасниками досліджуваного ланцюга постачання, але можуть певним чином взаємодіяти з його учасниками, окремі особи (групи осіб), котрі схильні нашкодити з тих чи інших причин, або й без причин.

Можна висунути гіпотезу, що в умовах цифрової економіки сутність ризику ланцюгів постачання під впливом розвитку та використання інноваційних технологій та засобів буде змінюватися. Зокрема, наразі ризик насамперед пов'язаний зі ставленням осіб, що приймають рішення, до можливого його прояву, а суб'єктом ризику є менеджмент підприємства, проте в умовах цифрової економіки, Індустрії 4.0 значна кількість логістичних операцій будуть здійснюватися без втручання людини, зокрема й прості управлінські дії. Тому в умовах цифрової економіки доречно ризик пов'язувати як з особами, які приймають рішення, так і з системами штучного інтелекту, які можуть приймати рішення без втручання людини, а їх основою є, зокрема, машинне навчання, когнітивне обчислення, інтелектуальний аналіз даних тощо.

В умовах цифрової економіки прийняття будь-яких рішень може відбуватися з використанням великого обсягу оперативної, достовірної та більш повної інформації, що може сприяти зниженню невизначеності та відповідних ризиків. Усе обладнання на виробництві та складах, автомобілі, пристрої, які нас оточують в побуті та використовуються в бізнесі, індивідуальні комунікаційні засоби тощо будуть підключені до Інтернету Речей для миттєвого обміну інформацією між ними. Це буде сприяти, зокрема, зростанню швидкості прийняття відповідних рішень. Наприклад, здійснюючи постійний моніторинг ситуації на дорогах, система може обрати оптимальний маршрут переміщення продукції, що значно скоро-

тить час і вартість її доставки, відповідно, знизиться транспортний ризик.

Можна припустити, що в цифровій економіці невизначеність, пов'язана з інформацією, що використовується у прийнятті рішень, з одного боку, буде зведена до допустимих меж, а з іншого – зростатиме внаслідок ущільнення потоку змін, збурень, конфліктності. Проте наявність великого обсягу даних не гарантує якості прийнятих рішень. Це пов'язано, зокрема, з тим, що інформація може бути неструктурованою чи слабо структурованою, не уніфікованою, неадекватною, суперечливою тощо. Тому тут доречно використовувати заходи Видобутку даних (*Data Mining*). Невизначеність буде пов'язана в основному з майбутнім, в якому буде отримано результат прийнятого наразі рішення, бо мінливість майбутнього буде притаманна й цифровій економіці.

У цифровій економіці в усьому ланцюзі (мережі) постачання людина може бути відсутня взагалі, окрім першого етапу (формування замовлення) та останнього (отримання продукції та користування нею). Проте можуть бути ситуації, коли замовлення здійснюється автоматично, без втручання людини, але на останньому етапі людина все ж таки має бути присутня, щоб підтвердити виконання замовлення, якість продукції та надання послуги тощо. Необхідно враховувати також і ризик зміни цілей у процесі виконання замовлень.

Ризик-менеджмент в ланцюгах постачання цифрової економіки – це система управління ризиками як окремого підприємства – учасника ланцюга постачання, так і ланцюга в цілому, яка затверджується, організовується, контролюється вищим керівництвом підприємств, функціонує безперервно в координації з іншими сферами діяльності підприємств з метою сприяння стійкості функціонування та життєздатності такого ланцюга в реальному (фізичному) просторі та віртуальному (цифровому, кібер-) просторі одночасно.

Об'єктом управління є об'єкт ризику ланцюга постачання, а суб'єктом управління – суб'єкт ризику ланцюга постачання. В умовах цифрової економіки для різних ланцюгів постачання справедливими також будуть загальноприйняті такі кроки процесу ризик-менеджменту (які наведено, зокрема, в стандарті [24]): 1) визначення оточення або контексту ризиків; 2) оцінювання ризиків (ідентифікація, аналіз та кількісне оцінювання ризиків); 3) обробка ризиків з метою зниження їх ступеня; 4) моніторинг ризиків.

Перший крок ризик-менеджменту «Визначення оточення або контексту ризиків» для усіх описаних вище ланцюгів постачання цифрової економіки, по суті, буде однаковим. На цьому кроці формулюються основні засади системи ризик-менеджменту, його стратегічні (глобальні), тактичні (конкретні завдання) та оперативні (щоденні або такі, що відносяться до кожної окремої поставки продукції) цілі; визначаються чинники можливих ризиків; вивчається попередній досвід підприємств – учасників ланцюга постачання щодо управління ризиками тощо.

Сутність ідентифікації ризиків для ланцюгів постачання фізичної, фізично-цифрової, цифрової продукції є подібною, проте перелік ризиків, які входять до сфери впливу ризик-менеджменту в ланцюгу постачання, є різним. Зокрема, у ланцюзі постачання фізичної продукції цифровізація стосується насамперед процесів генерування, передачі та зберігання інформації, супроводжуючої поставку продукції. Тому в такому ланцюзі ризики, пов'язані безпосередньо з фізичною продукцією, є первинними, а ризики, пов'язані з цифровою інформацією, – вторинними. У ланцюзі постачання фізично-цифрової продукції однаково важливими будуть традиційні ризики (ризики фізичного світу) та цифрові ризики. Для ланцюга постачання цифрової продукції можна постулювати, що цифрові ризики будуть первинними, а ризики фізичного світу будуть вторинними, і пов'язані вони будуть, насамперед, з апаратним забезпеченням переміщення цифрового матеріального та інформаційного потоків. Аналіз ризиків по суті також буде однаковим для всіх ланцюгів постачання, результатом проведення якого буде отримання всебічного опису ризиків. Для оцінювання ризиків усіх ланцюгів постачання можуть використовуватися як традиційні методи та моделі, так і нові, які здатні враховувати швидко та надійно великі обсяги оперативної актуальної цифрової інформації, що побудовані, зокрема, з використанням алгоритмів колективного штучного інтелекту.

Колективний (ройовий) штучний інтелект (англ. – *Swarm Intelligence*) – це формалізація комплексного колективного поводження децентралізованої системи, яка здатна до самоорганізації, у вигляді відповідних алгоритмів, які називаються також поведінковими, метаевристичними, натхненними (інспірованими) природою, багатоагентними, популяційними [25; 26]. До алгоритмів колективного штучного інтелекту відносять метод рою часток, алгоритм косяка риб, бджолиний алгоритм, алгоритм мурах, алгоритм кажанів тощо. Використання таких алгоритмів в оцінюванні ризиків наразі має значні перспективи, зокрема тому, що за прийнятний для дослідника час вони спроможні надати задовільний результат і повною мірою відображають одну із особливостей цифрової економіки – її мережевість. Із деякими концептуальними засадами використання алгоритмів колективного штучного інтелекту в моделюванні логістичного ризику можна ознайомитися, зокрема, в дослідженнях авторів статті [27].

Зниження ступеня ризиків ланцюгів постачання будь-якої продукції може здійснюватися різними способами, наприклад: страхування; розподілення ризику між підприємствами – учасниками ланцюга поста-

чання; формування резервів та запасів матеріальних і фінансових ресурсів; захист фізичних матеріальних ресурсів та продукції; кіберзахист цифрових ресурсів та продукції, який є «сукупністю організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості та надійності функціонування комунікаційних, технологічних систем» [28]; підвищення надійності збереження цифрової інформації за допомогою використання хмарних технологій та технології блокчейн тощо. Важливою є також розробка нових методів прогнозування.

Процеси моніторингу ризиків для ланцюгів постачання фізичної, фізично-цифрової та цифрової продукції, по суті, будуть подібними та полягатимуть у постійному спостереженні за процесами ризик-менеджменту та аналізі їхніх результатів, зокрема з використанням когнітивних обчислень, які, на думку фахівців, є дієвим засобом в обґрунтуванні рішень та збільшенні кількості спостережень, а також знаходження відомих і невідомих ризиків [29]; здійснення коригувань у системі управління ризиками з метою підвищення її ефективності; дослідження економічного середовища, в якому функціонує ланцюг постачання, щодо структурних зрушень, впровадження нових технологій, які можуть зумовити появу нових ризиків та вплинути на існуючі.

У цифровій економіці передбачається використання різноманітних сенсорів та датчиків для збору різної інформації, яка може оперативно оброблятись та аналізуватись, що дозволить здійснювати моніторинг ризику в таких умовах за деякими аспектами досить швидко (майже миттєво) та ефективно. З іншого боку, широке розповсюдження різних засобів здобування та обробки інформації може зумовити деяке зниження невизначеності в контексті доступності, повноти, актуальності та достовірності інформації у прийнятті рішень, що зумовить трансформацію сформульованого раніше у статті поняття ризику. Можна висунути гіпотезу, що акцент зміститься від невизначеності та конфліктності в бік загроз, можливих збитків, відхилення від цілей та нормального функціонування ланцюга постачання, зниження рівня безпеки. Але майбутнє завжди залишатиметься невизначеним.

Згідно з концепцією розвитку економіки Індустрії 4.0 однією зі складових частин нової економіки є кіберфізичні системи, в яких здійснюється поєднання «розумних деталей (компонент)» і «розумного виробництва», де кожен робочий пристрій самостійно визначає дії, які йому необхідно здійснити у процесі виробництва [30; 31]. Можна стверджувати, що кіберфізичні системи будуть присутні також у ланцюгах постачання, що зумовить заміщення людей у більшості логістичних процесів, зокрема й у прийнятті рішень.

Широке застосування кіберфізичних систем у цифровій економіці може зумовити потребу в уточненні поняття ризику в контексті сприйняття ними (кіберфізичними системами) ризику. Чи все ж таки поняття ризику пов'язане виключно з людьми? Залишимо це дискусійне питання відкритим.

ВИСНОВКИ

Цифрова економіка є незворотним майбутнім, яке твориться вже сьогодні й ігнорувати яке не доцільно, щоб не втратити конкурентні переваги. Це підтверджує і той факт, що у світі частка традиційної економіки скорочується, натомість зростає частка цифрової економіки [32]. Однією із основних складових функціонування як традиційної, так і цифрової економіки є ланцюги постачання, ризики переривання яких займають перше місце не один рік поспіль за версією щорічних звітів [17–22]. Тому в контексті цифрової економіки дослідження різних аспектів ризик-менеджменту в ланцюгах постачання є актуальним і перспективним напрямком.

У даній статті нами окреслено зміни ланцюгів постачання, представлено власне бачення щодо сутності поняття ризику ланцюга постачання в цифровій економці, його об'єкта та суб'єкта, а також описані основні кроки відповідного ризик-менеджменту, показано вплив інноваційних цифрових технологій на основні поняття ризик-менеджменту.

Вбачаємо доцільним у подальшому аналізувати (відслідковувати) ситуацію щодо використання цифрових технологій у ланцюгах постачання з метою своєчасного та адекватного уточнення джерел ризику, об'єктів і суб'єктів ризику, кроків управління ризиком тощо.

На нашу думку, доречно зосередитись на використанні алгоритмів колективного штучного інтелекту та когнітивних обчислень в оцінюванні ризиків і прийняття рішень в ланцюгу постачання, які обтяжені ризиком. ■

ЛІТЕРАТУРА

1. Розпорядження Кабінету міністрів України «Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації» від 17 січня 2018 р. № 67-р. URL: http://zakon3.rada.gov.ua/laws/show/67-2018-р

2. Цифрова адженда України – 2020. Проект // Офіційний сайт Торгово-промислової палати України. URL: https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf

3. Фіщук В. Цифрова економіка – це реально. Новое время. Бізнес. 18 квітня 2017р. URL: https://biz.nv.ua/ukr/experts/fichuk/tsifrova-ekonomika-tse-realno-1001102.html

4. Цифрова економіка // Вільна енциклопедія «Вікіпедія». URL: https://uk.wikipedia.org/wiki/Цифрова_економіка

5. Diedrich K. Framework for Digitalized Proactive Supply Chain Risk Management. Proceedings of the Hamburg International Conference of Logistics (HICL). Digitalization in

Supply Chain Management and Logistics. 2017. P. 381–403. URL: https://tubdok.tub.tuhh.de/bitstream/11420/1459/1/diedrich_framework_digitalized_supply_chain_hicl_2017.pdf

6. Schlüter F., Henke M. Smart Supply Chain Risk Management – A Conceptual Framework. Proceedings of the Hamburg International Conference of Logistics (HICL). Digitalization in Supply Chain Management and Logistics. 2017. P. 361–380. URL: https://tubdok.tub.tuhh.de/bitstream/11420/1469/1/schl%c3%bcter_henke_smart_supply_chain_risk_hicl_2017.pdf

7. Schlüter F., Diedrich K., Güller M. Analyzing the Impact of Digitalization on Supply Chain Risk Management // 26th IPSERA Conference. 2017. URL: https://www.researchgate.net/publication/315619880_Analyzing_the_Impact_of_Digitalization_on_Supply_Chain_Risk_Management

8. The Future of Risk Management in the Digital Era. October 2017 / Portilla A., Vazquez J., Harreis H. at al. Editor: M. Staples. URL: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/The%20future%20of%20risk%20management%20in%20the%20digital%20era/Future-of-risk-management-in-the-digital-era-IIF-and-McKinsey.ashx

9. Camillo M., Overton M. Cyber Risks and Your Supply Chain. 03/29/2017. URL: https://www.aig.com/knowledge-and-insights/k-and-i-article-cyber-supply-chain

10. Moss C. Cybersecurity in the Digital Supply Chain: Managing Third-Party Risk Through Verified Trust. URL: http://www.digitalistmag.com/digital-supply-networks/2017/03/14/cybersecurity-in-digital-supply-chain-managing-third-party-risk-through-verified-trust-04958505

11. Lehmacher W., Betti F., Beecher P., Grotemeier C., Lorenzen M. Impact of the Fourth Industrial Revolution on Supply Chains. October 2017. URL: http://www3.weforum.org/docs/WEF_Impact_of_the_Fourth_Industrial_Revolution_on_Supply_Chains_.pdf

12. Alcantara P., Riglietti G., Aguada L. BCI Supply Chain Resilience Report 2017 / Business Continuity Institute. Nov 2017. URL: https://www.thebci.org/news/bci-supply-chain-resilience-report-2017.html

13. Kersten W., Seiter M., von See B., Hackius N., Maurer T. Trends and Strategies in Logistics and Supply Chain Management. BVL Study on Digital Transformation Opportunities. DVV Media Group GmbH, Bremen. 2017. 71 p. URL: https://logistiktrends.bvl.de/en

14. Schrauf S., Berttram P. Industry 4.0: How digitization makes the supply chain more efficient, agile, and customer-focused. PwC Strategy&. September 7, 2016. URL: https://www.strategyand.pwc.com/reports/industry4.0

15. Mussomeli A., Gish D., Laaper S. The rise of the digital supply network. December 01, 2016. URL: https://www2.deloitte.com/insights/us/en/focus/industry-4-0/digital-transformation-in-supply-chain.html

16. Alicke K., Rexhausen D., Seyfert A. Supply Chain 4.0 in consumer goods. Operations as a competitive advantage in a disruptive environment. McKinsey & Company. 2017. P. 41–51. URL: https://www.mckinsey.com/industries/consumer-packaged-goods/our-insights/supply-chain-4-0-in-consumer-goods

17. Allianz Risk Pulse: Focus on Business Risks 2013. URL: http://www.agcs.allianz.com/assets/PDFs/Reports/Allianz-RP-Risk%20Barometer%20Jan2013.pdf

18. Allianz Risk Barometer on Business Risks 2014. URL: http://www.agcs.allianz.com/assets/PDFs/Reports/Allianz-Risk-Barometer-2014_EN.pdf

19. Allianz Risk Barometer: Top Business Risks 2015. URL: http://www.agcs.allianz.com/assets/PDFs/Reports/Allianz-Risk-Barometer-2015_EN.pdf

20. Allianz Risk Barometer: Top Business Risks 2016. URL: http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRisk-Barometer2016.pdf

21. Allianz Risk Barometer: Top Business Risks 2017. URL: http://www.agcs.allianz.com/assets/PDFs/Reports/Allianz_Risk_Barometer_2017_EN.pdf

22. Allianz Risk Barometer: Top Business Risks For 2018. URL: http://www.agcs.allianz.com/assets/PDFs/Reports/Allianz_Risk_Barometer_2018_EN.pdf

23. Скіцько В. І. Аспекти функціонування логістики в умовах Четвертої промислової революції // Маркетинг та логістика в системі менеджменту : тези доповідей XI Міжнародної науково-практичної конференції. Львів : Видавництво НУ «Львівська політехніка». 2016. С. 267–268.

24. Risk management – Risk assessment techniques. International Standard. IEC/ISO 31010, 2009.

25. Карпенко А. П. Популяционные алгоритмы глобальной поисковой оптимизации. *Обзор новых и малоизвестних алгоритмов. Информационные технологии*. 2012. № 7. Приложение. С. 1–32.

26. Колективний інтелект // Вільна енциклопедія «Вікіпедія». URL: https://uk.wikipedia.org/wiki/Колективний_інтелект

27. Вітлінський В. В., Скіцько В. І. Концептуальні аспекти моделювання логістичного ризику інформаційно-мережної економіки з використанням інструментарію природних обчислень. *Проблеми економіки*. 2016. № 4. С. 231–237.

28. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII. URL: http://zakon5.rada.gov.ua/laws/show/2163-19

29. Why cognitive computing is a game changer for risk management. URL: https://www2.deloitte.com/global/en/pages/risk/articles/cognitive-computing.html

30. Жемлиханов Т. «Индустрия 4.0»: революция без потерь? *Электротехнический рынок*. 2015. № 5-6. С. 32–36.

31. Индустрия 4.0: производственные процессы будущего. Интервью с профессором Вольфгангом Вальстером. Тенденции в автоматизации. 15 апреля 2014 г. URL: http://www.up-pro.ru/library/opinion/industriya-4.0.html

32. Риженко О., Фіщук В. Як цифрова економіка змінить Україну. Економічна правда. 2018. 16 січня. URL: https://www.epravda.com.ua/columns/2018/01/16/633057/

REFERENCES

Alcantara, P., Riglietti, G., and Aguada, L. "BCI Supply Chain Resilience Report 2017" Business Continuity Institute. Nov 2017. https://www.thebci.org/news/bci-supply-chain-resilience-report-2017.html

"Allianz Risk Pulse: Focus on Business Risks 2013". http://www.agcs.allianz.com/assets/PDFs/Reports/Allianz-RP-Risk%20Barometer%20Jan2013.pdf

"Allianz Risk Barometer on Business Risks 2014". http://www.agcs.allianz.com/assets/PDFs/Reports/Allianz-Risk-Barometer-2014_EN.pdf

"Allianz Risk Barometer: Top Business Risks 2015". http://www.agcs.allianz.com/assets/PDFs/Reports/Allianz-Risk-Barometer-2015_EN.pdf

"Allianz Risk Barometer: Top Business Risks 2016". http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometer2016.pdf

"Allianz Risk Barometer: Top Business Risks 2017". http://www.agcs.allianz.com/assets/PDFs/Reports/Allianz_Risk_Barometer_2017_EN.pdf

"Allianz Risk Barometer: Top Business Risks For 2018". http://www.agcs.allianz.com/assets/PDFs/Reports/Allianz_Risk_Barometer_2018_EN.pdf

Alicke, K., Rexhausen, D., and Seyfert, A. "Supply Chain 4. 0 in consumer goods. Operations as a competitive advantage in a disruptive environment. McKinsey & Company. 2017". https://www.mckinsey.com/industries/consumer-packaged-goods/our-insights/supply-chain-4-0-in-consumer-goods

Camillo, M., and Overton, M. "Cyber Risks and Your Supply Chain. 03/29/2017". https://www.aig.com/knowledge-and-insights/k-and-i-article-cyber-supply-chain

Diedrich, K. "Framework for Digitalized Proactive Supply Chain Risk Management" Proceedings of the Hamburg International Conference of Logistics (HICL). Digitalization in Supply Chain Management and Logistics. 2017. https://tubdok.tub.tuhh.de/bitstream/11420/1459/1/diedrich_framework_digitalized_supply_chain_hicl_2017.pdf

Fishchuk, V. "Tsyfrova ekonomika – tse realno" [The digital economy is real]. Novoye vremya. Biznes. https://biz.nv.ua/ukr/experts/fichuk/tsifrova-ekonomika-tse-realno-1001102.html

"Industriya 4. 0: proizvodstvennyye protsessy budushchego. Intervyu s professorom Volfgangom Valsterom" [Industry 4. 0: the production processes of the future. Interview with Professor Wolfgang Wahlster]. Tendentsii v avtomatizatsii. 15 aprelya 2014 g. http://www.up-pro.ru/library/opinion/industriya-4.0.html

"Kolektyvnyi intelekt" [Collective intelligence]. Vilna entsyklopediia «Vikipediia». https://uk.wikipedia.org/wiki/Колективний_інтелект

Karpenko, A. P. "Populyatsionnyye algoritmy globalnoy poiskovoy optimizatsii. Obzor novykh i maloizvestnykh algoritmov" [Population algorithms of global search engine optimization. Review of new and little-known algorithms]. *Informatsionnyye tekhnologii,* no. 7. Attachment (2012): 1-32.

Kersten, W. et al. "Trends and Strategies in Logistics and Supply Chain Management". BVL Study on Digital Transformation Opportunities. DVV Media Group GmbH, Bremen. 2017. https://logistiktrends.bvl.de/en

[Legal Act of Ukraine] (2017). http://zakon5.rada.gov.ua/laws/show/2163-19

[Legal Act of Ukraine] (2018). http://zakon3.rada.gov.ua/laws/show/67-2018-p

Lehmacher, W. et al. "Impact of the Fourth Industrial Revolution on Supply Chains. October 2017". http://www3.weforum.org/docs/WEF_Impact_of_the_Fourth_Industrial_Revolution_on_Supply_Chains_.pdf

Moss, C. "Cybersecurity in the Digital Supply Chain: Managing Third-Party Risk Through Verified Trust". http://www.digitalistmag.com/digital-supply-networks/2017/03/14/cybersecurity-in-digital-supply-chain-managing-third-party-risk-through-verified-trust-04958505

Mussomeli, A., Gish, D., and Laaper, S. "The rise of the digital supply network. December 01, 2016". https://www2.deloitte.com/insights/us/en/focus/industry-4-0/digital-transformation-in-supply-chain.html

Portilla, A. et al. "The Future of Risk Management in the Digital Era. October 2017". https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/The%20future%20of%20risk%20management%20in%20the%20digital%20era/Future-of-risk-management-in-the-digital-era-IIF-and-McKinsey.ashx

Risk management – Risk assessment techniques. International Standard. IEC/ISO 31010, 2009.

Ryzhenko, O., and Fishchuk, V. "Yak tsyfrova ekonomika zminyt Ukrainu" [How the digital economy will change Ukraine]. Ekonomichna pravda. 2018. https://www.epravda.com.ua/columns/2018/01/16/633057/

Schluter, F., Diedrich, K., and Guller, M. "Analyzing the Impact of Digitalization on Supply Chain Risk Management" 26th IPSERA Conference. 2017. https://www.researchgate.net/publication/315619880_Analyzing_the_Impact_of_Digitalization_on_Supply_Chain_Risk_Management

Schluter, F., and Henke, M. "Smart Supply Chain Risk Management - A Conceptual Framework" Proceedings of the Hamburg International Conference of Logistics (HICL). Digitalization in Supply Chain Management and Logistics. 2017. https://tubdok.tub.tuhh.de/bitstream/11420/1469/1/schl%c3%bcter_henke_smart_supply_chain_risk_hicl_2017.pdf

Skitsko, V. I. "Aspekty funktsionuvannia lohistyky v umovakh Chetvertoi promyslovoi revoliutsii" [Aspects of the operation of logistics in the conditions of the Fourth Industrial Revolution]. *Marketynh ta lohistyka v systemi menedzhmentu*. Lviv: Vyd-vo NU «Lvivska politekhnika», 2016. 267-268.

Schrauf, S., and Berttram, P. "Industry 4.0: How digitization makes the supply chain more efficient, agile, and customer-focused" PwC Strategy&. September 7, 2016. https://www.strategyand.pwc.com/reports/industry4.0

"Tsyfrova adzhenda Ukrainy – 2020. Proekt" [Digital Advent Ukraine – 2020. Project]. Ofitsiinyi sait Torhovo-promyslovoi palaty Ukrainy. https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf

"Tsyfrova ekonomika" [Digital economy]. Vilna entsyklopediia «Vikipediia». https://uk.wikipedia.org/wiki/Цифрова_економіка

Vitlinskyi, V. V., and Skitsko, V. I. "Kontseptualni aspekty modeliuvannia lohistychnoho ryzyku informatsiino-merezhnoi ekonomiky z vykorystanniam instrumentariiu pryrodnykh obchyslen" [Conceptual aspects of modeling the logistic risk of information-network economy using the tools of natural calculations]. *Problemy ekonomiky,* no. 4 (2016): 231-237.

"Why cognitive computing is a game changer for risk management". https://www2.deloitte.com/global/en/pages/risk/articles/cognitive-computing.html

Zhemlikhanov, T. "«Industriya 4. 0»: revolyutsiya bez poter?" ["Industry 4. 0": a revolution without losses?]. *Elektrotekhnicheskiy rynok*, no. 5-6 (2015): 32-36.