3. Cherubini, U., Luciano, E., and Vecchiato, W. (2004), *Copula Methods in Finance*. Wiley, Chichester.
4. Hu L. (2006). Dependence patterns across financial markets: a mixed copula approach. *Applied Financial Economics* 16, 717–729.
5. Katsiampa, P. (2017), Volatility estimation for Bitcoin: A comparison of GARCH models, *Economics Letters* 158, 3-6.
6. Phillip, A., Chan, J., Peiris, S. (2018), A new look at Cryptocurrencies. *Economics Letters* 163, 6-9.
7. Urquhart, A. (2016), The inefficiency of Bitcoin. *Economics Letters* 148, 80–82.
8. Urquhart, A. (2017), Price clustering in Bitcoin. *Economics Letters* 159, 145-148.

В.В. Вітлінський,
д.е.н., професор;
В.І. Скіцько,
к.е.н., доцент,
ДВНЗ «Київський національний економічний університет ім. Вадима Гетьмана»

Ризик у цифровій економіці

Цифрову економіку можна трактувати як глобальний тренд, як необхідну умову, завдяки якій кожна галузь економіки, бізнесу залишається конкурентноздатною. Концептуальні засади цифрового суспільства й економіки вперше були сформульовані у 1995 р. американським ученим Ніколасом Негропонте (NicholasNegroponte) з Массачусетського технологічного інституту (Massachusetts Institute of Technology) та дістали подальший розвиток з остаточним формулюванням терміна «цифрова економіка» у роботі Дона Тепскотта (Don Tapscott) «Цифрова економіка: перспективи та ризики в епоху мережевої інформації» [1, 2]. Наразі цим терміном послуговуються учені-економісти, практики, політики, соціологи, психологи, фахівці сфери ІТ тощо. Вважається, що цифрова економіка, її модельна складова є віртуальним середовищем, яке щоразу більше органічно доповнює фізичну реальність, інтегрується з нею.

Сьогодення в глобальному масштабі характеризується стрімким розвитком нової економіки та суспільних відносин, основою якого є цифрові технології, поступ яких докорінно змінює як життя людей, так і бізнес-процеси. Уже стало повсякденністю використання смартфонів, планшетів, ноутбуків; спілкування з використанням не лише електронної пошти, а й соціальних мереж та месенджерів; Інтернет; зберігання інформації за допомогою хмар тощо. До сучасних світових цифрових трендів можна віднести віртуальну або доповнену реальність, гаджети, розумний будинок, під'єднані до глобальної мережі автомобілі, дрони, датчики та сенсори нового покоління, нанотехнології, аналітика Великих Даних [3]. Цифровими технологіями найближчого майбутнього, які частково використовуються вже наразі, є: технології імплантів, штучний інтелект, автономні роботи, блокчейн та криптовалюти, 3D-друк, розподілені обчислення, автономні електронні автомобілі, нові технології в енергетиці, економіка спільного користування тощо [3].

У низці наукових праць зазначається, що сутність цифрової економіки полягає в тому, щоб водночас з відомими традиційними фізичними продуктами, послугами, процесами та технологіями існувала й модельна (віртуальна) дійсність цих самих речей, процесів. Це дасть змогу проводити модельні комп'ютерні експерименти, модельний цифровий супровід у режимі реального часу, ефективно діяти.

Усі ці інновації зумовили широке впровадження цифрової економіки і, водночас, переосмислення усталених понять, зокрема, ризику. У контексті цифрової економіки доцільно говорити про цифровий ризик. Наразі, коли йдеться про цифрові технології, то згадують про кіберризик. У професійній колах використовують обидва поняття, які, по суті, означають одне й те саме. Можна припустити, що з плином часу буде одне поняття, проте кіберризик залишиться складовою цифрового ризику.

Кіберризик означає відповідний ризик фінансових втрат, втрати ділової репутації організації (підприємства) через деякі вади або несправності, які можуть мати місце в її системі інформаційних технологій (IT-системі), та зумовлені різними причинами [4]. Цифровий ризик охоплює процеси впровадження та використання цифрових технологій у діяльності підприємства, зокрема, й прийнятті рішень, які

передбачають комп'ютеризацію всіх процесів, застосування робототехніки, розширення аналітичних можливостей завдяки машинному навчанню та штучному інтелекту тощо [5]. По суті, цифровий ризик пов'язаний з узгодженим функціонуванням усіх процесів, генеруванням, передачею та зберіганням даних, аналітикою, ІТ, загальною системою менеджменту, знаннями й уміннями працівників [5].

Цифровий ризик – це проблема бізнесу, а не лише технологічна проблема [6]. Інакше кажучи, цифровий ризик відображає проблеми бізнесу загалом, а кіберризик – лише ІТ. Окрім того, існує думка, що цифровий ризик-менеджмент, як наступна сходинка еволюції управління ризиком та безпеки підприємства, що широко використовує у своїй діяльності цифрові технології, має стосуватися компетенції топ-менеджменту, а не лише відділу ІТ [6].

На нашу думку, цифровий ризик потрібно розглядати як трансформаційний розвиток традиційного поняття ризику. Проте можна припустити, що в цифровій економіці поняття звичайного ризику не зникне, зокрема, завдяки існуванню процесів фізичного світу, в яких використання цифрових технологій буде лише сприяти їхньому функціонуванню, а не заміщати їх, інтегруватися в нові прояви буття.

Цифровий ризик в умовах цифрової економіки – це економічна категорія, яка відображає особливості сприйняття суб'єктами економічних відносин об'єктивно існуючих невизначеності та конфліктності в процесах функціонування та управління компанією (організацією, підприємством тощо), що зумовлені можливими збоями у функціонуванні цифрових засобів і технологій, які використовуються компанією. *Об'єкт і суб'єкт цифрового ризику* будуть такі самі, як і для звичайного ризику, які наведено, зокрема, в монографії [7].

Джерелами цифрового ризику є цифрові технології, які можна класифікувати так: пристрої та апаратне забезпечення; програмне забезпечення та інноваційні технології генерування, зберігання, передача та обробка інформації; мережі (локальні, глобальні, зокрема Інтернет); штучний інтелект.

Система управління цифровими ризиками має стати складовою загальної системи ризик-менеджменту організації (підприємства), та може бути побудована, зокрема, на основі використання методології та інструментарію, що викладені в [8, 9]. Залишаються актуальними для

цифрового ризику, проте з уточненнями та змінами сутності, традиційні кроки ризик-менеджменту: 1) встановлення оточення; 2) загальне оцінювання ризику (ідентифікація, аналіз та оцінювання ризику); 3) обробка ризику; 4) моніторинг ризику [8]. Остаточною метою управління цифровими ризиками є досягнення цифрової стійкості організації, за якої негативний вплив на діяльність організації можливих цифрових загроз зведено до мінімуму [6].

У цифровій економіці можна виокремити декілька видів ризиків, які конфліктують між собою [10]. Знижуючи ступінь ризику одного виду, можна зумовити підвищення ступеня ризику іншого. Тому, на нашу думку, важливою є розбудова ігрових моделей та методів штучного інтелекту, які б адекватно моделювали зазначені колізії, пов'язані з цифровою економікою, та забезпечували б обґрунтування раціональних рішень [10, 11].

Фахівці з управління цифровим ризиком мають однаковою мірою володіти знаннями як з економіки, так і з сфери IT. Це, своєю чергою, потребує зміни чинних навчальних планів і програм підготовки відповідних фахівців, упровадження нових, які відображають тенденції розвитку економіки та суспільства найближчого майбутнього.

Список використаних джерел

1. NegroponteN. BitsandAtoms // Wiredmagazine. 1995.
2. TapscottD.Thedigitaleconomy : promiseandperilintheageofnetworkedintelligence. NewYork: McGraw-Hill. 1997.
3. 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/
4. Cyberriskandriskmanagement // InstituteofRiskManagement. – URL : https://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk/
5. Ganguly S., Harreis H., Margolis B., Rowshankish K. Digital risk: Transforming risk management for the 2020. –February 2017. – URL : https://www.mckinsey.com/business-functions/risk/our-insights/digital-risk-transforming-risk-management-for-the-2020s.
6. WhatisDigitalRiskManagement?– URL: http://www.drminstitute.org/what-is-digital-risk-management/
7. Вітлінський В.В. Аналіз, оцінка й моделювання ризику: монографія / В.В. Вітлінський. – К. : ДЕМІУР. – 1996. – 212 с.
8. «Riskmanagement – Riskassessmenttechniques». International Standard. IEC/ISO 31010, 2009.

9. COBIT 5 forRisk. ISACA, 2013.
10. Вітлінський В.В., Скіцько В.І. Ризики в Індустрії 4.0 // Вісник Черкаського університету. Серія «Економічні науки». – 2016. – № 3. – С. 17 – 26.
11. 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.

Т.І. Городиський,
к.е.н., доцент,
Дрогобицький державний педагогічний
університет ім. Івана Франка

Особливості побудови системи фінансово-економічної безпеки підприємства

В умовах розвитку сучасної економіки щоразу більшого значення для підприємства набуває такий внутрішній чинник, як фінансова безпека, що безпосередньо забезпечує його економічну безпеку.

На думку В.І. Бокія [1], механізм забезпечення фінансово-економічної безпеки підприємства в практичній діяльності варто розглядати як систему організаційних, фінансових та правових засобів впливу, які мають на меті своєчасне виявлення, попередження, нейтралізацію та ліквідацію загроз його фінансово-економічній безпеці.

На думку С.В. Цюцюпи [7], механізм забезпечення фінансово-економічної безпеки підприємства має формуватися через систему управління фінансовими відносинами шляхом використання певних принципів, фінансових важелів, інструментів, фінансових методів, правового й інформаційного забезпечення, за допомогою фінансових досліджень, що уможливить досягнути основних цілей підприємства.

Під механізмом системи фінансово-економічної безпеки підприємства слід визнати взаємодію у динаміці між елементами (підсистемами або власниками процесів) та суб'єктом системи на основі руху інформації від елементів (підсистем або власників процесів) до суб'єкта системи і у зворотному напрямі, за результатами якої ухвалюються та виконуються дії щодо функціонування системи економічної безпеки підприємства та управління нею. Саме рух