DOI 10.52363/2414-5866-2024-1-6
УДК 004:35

Степанов В.Ю., *д.держ.упр., проф., ХДАК, м. Харків,*
ORCID: https://orcid.org/0000-0001-5892-4239

Stepanov V., *Doctor of Sciences in Public Administration, Full Professor,*
Kharkiv State Academy of Culture, Kharkiv,
ORCID: https://orcid.org/0000-0001-5892-4239

ЦИФРОВІЗАЦІЯ ТА РИЗИКИ ЦИФРОВОЇ БЕЗПЕКИ

DIGITALIZATION AND DIGITAL SECURITY RISKS

У статті концептуально розглянуто сутність ризику цифрової безпеки в умовах цифровізації суспільства. Показано, що цифровізація – це загальний термін, що означає цифрову трансформацію нашого суспільства та економіки. Обґрунтовується думка, що ризик цифрової безпеки має динамічний характер та може бути наслідком поєднання загроз і вразливостей у цифровому середовищі. Зроблено висновок, що управління ризиками цифрової безпеки – це процес, за допомогою якого особи, які приймають рішення, враховують у плануванні та здійсненні своєї діяльності фактори, які можуть вплинути на досягнення їхніх цілей.

Ключові слова*: цифровізація, ризики, цифрова безпека, суспільство, цифрові стратегії.*

The article conceptually examines the essence of digital security risk in the context of digitalization of society. It is shown that digitalization is a general term that refers to the digital transformation of our society and economy. The author argues that digital security risk is dynamic and may result from a combination of threats and vulnerabilities in the digital environment. It is concluded that digital security risk management is a process by which decision makers take into account factors that may affect the achievement of their goals in planning and carrying out their activities.

Keywords*: digitalization, risks, digital security, society, digital strategies.*

Постановка проблеми. Цифрову трансформацію нашого суспільства та економіки можна висловити через загальний термін «Цифровізація». У ньому описується перехід від індустріальної епохи до епохи творчих знань, що характеризується цифровими технологіями та цифровими бізнес-інноваціями. Тобто цифровізація, як розвиток цифрових інновацій, є однією з найважливіших бізнес-тенденцій для майбутнього економіки.

Цифровізація – це радикальні зміни в економіці та суспільстві. По-перше, підприємствам доводиться зацифровувати свої внутрішні процеси та

ISSN 2414-5858 (Print)
ISSN 2414-5866 (Online)

процедури. По-друге, підприємствам доводиться розробляти нові послуги та цифрові бізнес-моделі. При цьому підприємствам необхідно розробляти цифрові стратегії та зосередитись на ключових факторах цифрової трансформації. У будь-якому випадку їм доведеться стикатися з ризиками, що пов'язані з використанням, розвитком та керуванням цифрового середовища під час будь-якої діяльності.

Аналіз останніх досліджень та публікацій. Питання аспектів цифровізації в Україні досліджували науковці: Голюк В. Я.[4], Грінчук І. О. [5], Гавриленко Н. Г. [3], Дергачова В. В. [4], Двуліт З. П. [5], Завербний А. С. [5], Завдовєва Ю. М. [10], Карінцева О. І.[10], Котелевець Д. О. [7], Краус К. М. [6], Краус К. М. [6], Кубатко О. В. [10], Лапін А. В. [8], Любохинець Л. С. [9], Манжура О. В. [6], Мельник Л. Г. [10], Оленюк Д.О. [8], Романюк А. О. [5], Сотник І. М. [10], Тарасенко І. О. [3], Шпуляр Є. М. [9] й ін. У різнопланових працях науковці розглядали ключові ознаки цифровізації, використання інформації, цифровізацію економічного сектору, цифрові бізнес-моделі, цифрову ідентифікацію, цифровізацію соціального життя та управління, цифрові канали зв’язку, штучний інтелект тощо. Проте, основні тенденції та ризики цифрової безпеки в Україні не були детально розглянуті.

Виділення невирішених проблем. Надумку фахівців, цифровізація має наслідки для будь-яких підприємств. З одного боку, підприємствам доводиться проходити цифрову трансформацію, з іншого боку, їм доводиться розробляти нові послуги та враховувати нові ризики. Ризик цифрової безпеки, який ще недостатньо досліджений, є однією з багатьох інших категорій ризиків, з якими стикаються зацікавлені сторони та може бути наслідком поєднання загроз і вразливостей у цифровому середовищі.

Постановка завдання. Концептуально розглянути сутність ризику цифрової безпеки в умовах цифровізації суспільства.

Виклад основного матеріалу. В останні роки двадцятого століття різні цифрові технології (мобільний Інтернет, штучний інтелект тощо) отримали подальший розвиток та перейшли від експертного застосування до повсякденного життя людей. Поряд з інноваціями в бізнесі цифровізація, як цифрова трансформація суспільства, стала однією з найважливіших бізнес-тенденцій для майбутнього економіки. За твердженням фахівців, до 2030 року бізнес-інновації та цифровізація змінять ринки швидше ніж у попередні десять років [3, 9, 10, 12, 15].

Починаючи з 2020 року швидкість цифрової трансформації у суспільстві постійно прискорюється. Тенденції бізнесу вказують напрямок, у якому підприємствам необхідно розвивати інноваційні та цифрові стратегії [2, 11–13]. При цьому технологічні прориви стануть мейнстримом бізнес-тенденцій.

Очікується, що штучний інтелект та блокчейн, як технології, у цьому десятилітті з'являться в спеціалізованих підрозділах підприємств [7, 9, 12].

Зокрема, технології, які п'ять років тому були доступні лише фахівцям, будуть доступні практично кожному. Тобто однією з основних бізнес-тенденцій підприємств у найближчі роки стане полегшення доступу співробітників та менеджерів до цих нових технологій.

Цифровізація потребує нового підходу до стратегічного планування – розробки цифрової стратегії. Окрім бачення ролі, яку підприємства планують грати на цифрових ринках майбутнього, цифрова стратегія включає конкретні заходи та проєкти цифрової трансформації, це план дій щодо реалізації цифрової трансформації для підприємства. Вона включає розвиток цифрових бізнес-процесів, цифрового маркетингу, цифрових продажів, а також розробку цифрових бізнес-моделей. Зокрема, в розробці цифрової стратегії беруть участь усі відділи підприємства.

Слід зазначити, що реалізація цифрової стратегії часто дотримується принципів гнучкого управління проєктами. Замість статичного плану дій, проєкти цифровізації регулярно оцінюються. При цьому, через високий рівень невизначеності, що пов'язана з цифровізацією, необхідно регулярно переглядати проєкти, змінювати їх або навіть припиняти.

Усвідомлення того, що деякі проєкти можуть зазнати невдачі, стає важливою передумовою для визначення ризику цифрової безпеки. Термін «ризик цифрової безпеки» використовується для опису категорії ризику, пов’язаного з використанням, розвитком і управлінням цифрового середовища під час будь-якої діяльності. Цей ризик може підірвати досягнення економічних та соціальних цілей, порушуючи конфіденційність, цілісність та доступність діяльності чи навколишнього середовища [14].

Ризик цифрової безпеки, маючи динамічний характер, концептуально включає аспекти, що пов'язані з цифровим і фізичним середовищем та людьми, які беруть участь у діяльності й підтримують її організаційними процесами. Тобто діяльність, що здійснюють зацікавлені сторони для досягнення своїх цілей, залежить від факторів, які можуть мати наслідки для ймовірності успіху [14].

На думку фахівців, «ризик» – це наслідки невизначеності щодо цілей, які переслідують зацікавлені сторони, тобто відхилення, яке реальність може накласти на те, що вони очікують [4, 13–15]. Цей підхід до ризику ґрунтується на стандартах ISO/IEC 31000:2009, серії ISO/IEC 27000 та ISO Guide 73 [13, 14]. Слід зауважити, що ризик цифрової безпеки не охоплює невизначеності, що пов’язані з порушенням прав інтелектуальної власності або поширенням невідповідної інформації у цифровому середовищі.

У повсякденній мові «ризик» зазвичай охоплює лише шкідливі наслідки невизначеності, яка може підірвати досягнення економічних і соціальних цілей. Невизначеність є частиною людського життя. Зокрема, це наші знання, а розуміння різних факторів і того, як вони можуть вплинути на наші цілі, обмежені. Однак невизначеність також може мати позитивний вплив

і приносити користь діяльності. Відповідно, управління ризиками цифровізації розглядається як засіб захисту цінностей для найкращого досягнення економічних і соціальних цілей [14].

Сприятливий вплив невизначеності часто називають «можливістю», а не ризиком. Зв'язок між поняттями «ризик» і «можливість» є важливим, оскільки управління ризиками цифровізації також можна використовувати для створення цінності шляхом систематичного виявлення та використання невизначеності для стимулювання інновацій.

Ризик цифровізації залежність від цифрового середовища, потребує програмного та апаратного забезпечення. Зокрема, прямого чи непрямого втручання, чи взаємодії людини та аспектам, які можуть піддаватися загрозам, уразливостям та інцидентам. При цьому загрози, уразливості та інциденти можуть мати як цифровий, так і фізичний або людський вимір [13–15].

Вплив або наслідки цифрової невизначеності є економічними й соціальними та можуть впливати на матеріальні й нематеріальні активи. Таким чином ризик має бути сформульований в економічних і соціальних термінах: фінансові втрати, втрата конкурентоспроможності, втрата можливостей, шкода репутації, іміджу чи довірі тощо.

Ризик може виникнути внаслідок подій, коли загрози в поєднанні з вразливими місцями породжують економічні наслідки. Події, які можуть змінити очікуваний хід діяльності та цілі впливу, часто називають «інцидентами». Інцидент може бути наслідком дій людини, таких як ненавмисні помилки, або людей, що маніпулюванні методами соціальної інженерії [14]. Тривалість інцидентів може варіюватися від дуже короткої до надзвичайно тривалої (багаторічної), як у випадку таємного вторгнення в інформаційну систему з метою усунення компанії з ринку шляхом викрадення її комерційних секретів.

І загрози, і вразливі місця необхідні для створення наслідків для діяльності. Загрози без уразливостей або вразливості без загроз не збільшують ризик. Зокрема, в повсякденній мові термін «ризик» використовується у вільній формі.

Управління ризиками цифрової безпеки, однак, вимагає чіткого розмежування між причинами та їх наслідками та розглядає перші (загрози, вразливі місця та інциденти), щоб керувати останнім (ризиком). Щоб підкреслити цю різницю, загрози, уразливості та інциденти називаються «факторами ризику» [13–15].

Загрози, як правило, зовнішні стосовно діяльності, тоді як уразливості зазвичай є слабкими місцями в діяльності. Як наслідок, зацікавлені сторони часто мають обмежені можливості впливати на загрози, тоді як зазвичай вони можуть діяти більш безпосередньо на вразливості. У деяких випадках і загроза, і вразливість походять зсередини діяльності.

Таким чином управління ризиками цифрової безпеки «це набір скоординованих дій, що вживаються всередині організації та/або між організаціями для розв'язання проблеми цифрової безпеки, ризик безпеки при максимальному використанні можливостей. Це невіддільна частина процесу прийняття рішень і загальної основи управління ризиками для економічної та соціальної діяльності. Він спирається на цілісний, систематичний і гнучкий набір циклічних процесів, який є максимально прозорим і чітким. Цей набір процесів допомагає гарантувати, що заходи з управління ризиками цифрової безпеки («заходи безпеки») відповідають і співмірні з ризиком, економічними та соціальними цілями, які поставлені на карту…» [14].

Ризик цифрової безпеки не можна усунути, але ним можна керувати, сприяючи та захищаючи економічну та соціальну діяльність. Таким чином, управління ризиками цифрової безпеки має на меті сприяти досягненню економічних і соціальних цілей.

Висновки. Розвиток цифровізації сприяє появі безлічі інтеграційних можливостей. Зокрема: створення нових викликів для шкіл та освіти; навчання та подальшої освіти; державного управління; удосконалення вітчизняного нормативно-правого регулювання цифровізації тощо.

Управління ризиками цифрової безпеки – це процес, за допомогою якого особи, які приймають рішення, враховують у плануванні та здійсненні своєї діяльності фактори, які можуть вплинути на досягнення їхніх цілей. Оскільки їхня економічна та соціальна діяльність прямо чи опосередковано залежить від цифрового середовища, управління ризиками цифрової безпеки має бути невіддільною частиною процесу прийняття рішень і розглядатися разом із їхніми стратегіями для максимізації можливостей.

Керівники підприємств повинні розглядати управління ризиками цифрової безпеки як економічну та соціальну, а не суто технічну проблему. Вони повинні співпрацювати з іншими зацікавленими сторонами, такими як ті, хто відповідає за експлуатацію та підтримку цифрового середовища, щоб краще зрозуміти ключові фактори ризику. Подібним чином лише керівники та особи, які приймають рішення, можуть враховувати ризики цифрової безпеки в головних стратегічних цілях і планах підприємств, що є перспективним напрямком та потребує подальших досліджень.

Список використаних джерел:

1. Про стимулювання розвитку цифрової економіки в Україні, Закон України, (Відомості Верховної Ради України (ВВР), 2023, № 6-7, ст.18) із змінами, (дата звернення: 15.05.2024).

2. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації. Розпорядження Кабінету Міністрів України від 24.12.2018 № 67-р. URL: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80., (дата звернення: 15.05.2024).

3. Гавриленко Н. Г., Тарасенко І. О. Сучасні тенденції цифровізації еконо-

міки: проблеми та перспективи розвитку. *Міжнародний науковий журнал «Інтернаука». Серія: «Економічні науки»*, 2021. № 3 (47). Т. 1. С. 36-46.

4. Дергачова В. В., Голюк В. Я. Цифрова термінологія у стратегіях. Сутність, місце та роль діджитал менеджменту. *Економічний вісник НТУУ «Київський політехнічний інституту»*, 2022. № 22. С. 114−117. DOI: https://doi.org/10.20535/2307-5651.22.2022.260165.

5. Двуліт З. П., Завербний А. С., Романюк А. О. Диджиталізація – дієвий інструмент антикризового розвитку бізнесу в умовах пандемії. *Ефективна економіка*, 2021. № 1. URL: http://www.economy.nayka.com. ua/?op=1&z=85571-8. (дата звернення: 30.11.2022).

6. Краус К. М., Краус Н. М., Манжура О. В. Електронна комерція та Інтернет-торгівля: навчально-метод. посібник. Київ : Аграр Медіа Груп, 2021. 454 с.

7. Котелевець Д. О. Тенденції розвитку цифрової економіки в Україні. *Проблеми сучасних трансформацій. Серія: «Економіка та управління»*, 2022. № 5. DOI: https://doi.org/10.54929/2786-5738-2022-5-03-01.

8. Лапін А. В., Грінчук І. О., Оленюк Д.О. Діджиталізація економіки в Україні: сучасний стан та перспективи. *Електронний журнал «Ефективна економіка»*. 2022. № 7. DOI: https://doi.org/10.32702/2307-2105.2022.7.22.

9. Любохинець Л. С., Шпуляр Є. М. Цифрова трансформація національної економіки: сучасний стан та тренди майбутнього. *Вісник Хмельницького національного університету. Економічні науки,* 2019. № 4. С. 213–128.

10. Мельник Л. Г., Карінцева О. І., Кубатко О. В., Сотник І. М., Завдовєва Ю. М. Цифровізація економічних систем та людський капітал: підприємство, регіон, народне господарство. *Механізм регулювання економіки*, 2020. № 2. С. 9–28.

11. Світовий рейтинг цифрової конкурентоспроможності – IMD. URL: https://www.imd.org/centers/worldcompetitiveness-center/rankings/world-digital-competitiveness, (дата звернення: 15.05.2024).

12. Україна 2030Е – країна з розвинутою цифровою економікою. Український інститут майбутнього, 2018. URL: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html., (дата звернення: 15.05.2024)

13. ENISA (European Union Agency for Network and Information Security), National Cyber Security Strategies in the World. www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world.

14. OECD (2015), "Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document". OECD Publishing, Paris.

15. Piper, A. (2014), "Risk-informed innovation. Harnessing risk management in the service of innovation". URL: www.economistinsights.com/technologyinnovation/analysis/risk-informed-innovation.

References:

1. On Stimulating the Development of the Digital Economy in Ukraine, Law of Ukraine, (Bulletin of the Verkhovna Rada of Ukraine (VVR), 2023, No. 6-7, Article 18) as amended, (accessed on May 15, 2024).

2. Cabinet of Ministers of Ukraine (2018), "About the conceptualization of the development of the digital economy for Ukraine and Ukraine for 2018-2020 and the hardening of the plan for entry into the project", available at: http://zakon.rada.gov.ua/laws/ show/67-2018-%D1%80 (accessed on May 15, 2024).

3. Havrylenko N. H., Tarasenko I. O. (2021) Current trends in the digitalization of the economy: problems and prospects for development. *International scientific journal "Internauka". Series: "Economic Sciences*", No. 3 (47). V. 1. P. 36 46.

4. Derhachova V. V., Goliuk V. Ya. (2022) Digital terminology in strategies. The essence, place and role of digital management. *Economic Bulletin of NTUU "Kyiv Polytechnic Institute"*, No. 22. P. 114-117.
DOI: https://doi.org/10.20535/2307-5651.22.2022.260165.

5. Dvulit Z. P., Zaverbnyi A. S., Romaniuk A. O. (2021) Digitalization is an effective tool for anti-crisis business development in a pandemic. *Efficient economy*, No. 1. URL: http://www.economy.nayka.com. ua/?op=1&z=85571-8. (accessed on November 30, 2022).

6. Kraus K. M., Kraus N. M., Manzhura O. V. (2021) E-commerce and Internet trade: a study guide. Kyiv: Agrarian Media Group. 454 p.

7. Kotelevets D. O. (2022) Trends in the development of the digital economy in Ukraine. *Problems of modern transformations. Series: «Economics and management»*, No. 5. DOI: https://doi.org/10.54929/2786-5738-2022-5-03-01.

8. Lapin A. V., Hrinchuk I. O., Oleniuk D.O. (2022) Digitalization of the Economy in Ukraine: Current Status and Prospects. *Electronic journal "Effective Economy"*, No. 7. DOI: https://doi.org/10.32702/2307-2105.2022.7.22.

9. Liubokhynets L. S., Shpuliar Ye. M. (2019) Digital transformation of the national economy: current state and future trends. *Bulletin of Khmelnytsky National University. Economic Sciences*, No. 4. P. 213-128.

10. Melnyk L. H., Karintseva O. I., Kubatko O. V., Sotnyk I. M., Zavdovieva Yu. M. (2020) Digitalization of economic systems and human capital: enterprise, region, economy. *Mechanism of economic regulation*, No. 2. P. 9-28.

11. IMD World Digital Competitiveness Index. URL: URL: https://www.imd.org/centers/worldcompetitiveness-center/rankings/world-digital-competitiveness/ (accessed on May 15, 2024).

12. Ukraine 2030E is a country with a developed digital economy. Ukrainian Institute of the Future, 2018. URL: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html. (accessed on May 15, 2024).

13. ENISA (European Union Agency for Network and Information Security), National Cyber Security Strategies in the World. www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world.

14. OECD (2015), “Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document”. OECD Publishing, Paris.

15. Piper, A. (2014), “Risk-informed innovation. Harnessing risk management in the service of innovation”. URL: ww.economistinsights.com/technologyinnovation/analysis/risk-informed-innovation.

дата надходження статті: 07.05.2024
дата прийняття статті: 16.05.2024
дата публікації: 28.06.2024