DOI: https://doi.org/10.32782/2524-0072/2023-55-66

УДК 004:658 (477)

ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ СУТНОСТІ ЦИФРОВОЇ БЕЗПЕКИ

THEORETICAL BASIS OF STUDYING THE ESSENCE OF DIGITAL SECURITY

Дуляба Наталія Іванівна
кандидат економічних наук, доцент,
Національний університет «Львівська політехніка»
ORCID: https://orcid.org/0000-0002-4377-874X

Обрамич Орест Сергійович
аспірант,
Національний університет «Львівська політехніка»
ORCID: https://orcid.org/0009-0006-2280-5549

Duliaba Nataliia, Obramych Orest
Lviv Polytechnic National University

Стаття присвячена актуальним питанням визначення сутності цифрової безпеки підприємств. Визначено місце цифрової безпеки в сукупності безпеки підприємства. Наведено основні ризики та перешкоди розвитку підприємства, спричинені посилення цифровізації та зумовлені поширення інформації, застосуванням різноманітного програмного забезпечення і комп'ютерної техніки. Визначено, що такі ризики та загрози спричиняють необхідність формування цифрової безпеки підприємства. На основі проаналізованих досліджень науковців щодо визначення сутності цифрової безпеки, сформовано авторське бачення досліджуваного явища, яке передбачає поєднання інформаційної та кібербезпеки. Авторами доведено можливості забезпечення цифрової безпеки підприємства шляхом створення можливостей безпечного використання, зберігання та передавання інформації при застосуванні безпечних засобів її передачі, обробки та зчитування.

Ключові слова: цифровізація, ризики, загрози, безпека підприємства, цифрова безпека.

The article is devoted to the topical issues of defining the essence of digital security of enterprises. The place of digital security in the overall security of the enterprise is defined. In particular, it was determined that digital security is a separate type of security of the enterprise and occupies a prominent place in relation to the financial and information security of the enterprise, since it has a significant impact on the first and directly depends on the second. The main risks and obstacles to the development of the enterprise, caused by the strengthening of digitalization and caused by the spread of information, the use of various software and computer equipment, are presented. There are also risks of the internal environment, which arise under the negative influence of internal factors: organizational and managerial nature, personnel competencies, quality and capacity of internal networks and technical means. A special role among internal risks is assigned specifically to those that directly threaten the digital security of the enterprise. In the aggregate of risks and threats to digital security, enterprises will highlight risks of an external nature of interaction with the enterprise and influence, which are caused by receiving information from the outside, the need to communicate with external systems and networks, and the competence of users. It was determined that such risks and threats necessitate the formation of digital security of the enterprise. Taking into account the analyzed research of scientists regarding the definition of the essence of digital security, the author's vision of the studied phenomenon, which involves the combination of information and cyber security, was formed. The digital security of the enterprise reflects the security of information in all its forms and types, which belongs to the enterprise and is used by it, and the protection of technical means of processing, transmission and transfer of information and software used in the activities of the enterprise on a legal basis. Therefore, as part of digital security, it is appropriate to distinguish information security and cyber security, which closely interact with each other and are aimed at preventing the occurrence, countering risks and threats, as well as minimizing losses in the event of their occurrence in the field of information support for the enterprise's activities and technical and technological support for the use information

Keywords: digitalization, risks, threats, enterprise security, digital security.

Постановка проблеми. Розвиток інформаційних технологій прискорив можливості поширення та обробки інформації. Це в свою чергу стимулювало появу та розвиток нових сфер господарювання, зміну структуру національного виробництва та прискорило розвиток багатьох економік світу. Цифровізація охопила практично усі сфери суспільних відносин та стала важливою основою реалізації багатьох видів бізнесу. Це сприяло прискорення оборотності капіталів, обслуговування покупців, інтенсифікації бізнесу.

Разом з тим цифровізація всіх сфер суспільних відносин та бізнесу, зокрема, супроводжується суттєвими ризиками. Це ризики, пов'язані із поширенням та неправомірним використанням інформації, можливістю викрадення ресурсів (в тому числі фінансових) засобами електронної комунікації, виникнення проблем технічного характеру щодо роботи систем, мереж, приладів, які можуть спонукати зникнення інформації, її неякісну трансформацію, тощо. Ці та інші потенційні проблеми потребують забезпечення можливостей їх уникнення, що пов'язано із формуванням цифрової безпеки на всіх рівнях створення, обробки та використання інформації.

Аналіз останніх досліджень і публікацій. Питання цифровізації всіх суспільних відносин та їх вплив на розвиток світової економіки та її трансформації стало особливо актуальним в останнє десятиліття як за кордоном, так і в Україні. Особливу увагу дослідники приділяють розгляду змісту цифровізації, її перевагам та перспективам розвитку економіки під впливом цифровізації. Зокрема, вчені Д. Тапскотт, М. Кастельс, Т. Месенбург, В. Апальков, О. Гудзь, В. Компанієць, С. Кубів, В. Ляшенко, О. Вишневський, І. Тушканов, К. Шваб та інші активно досліджують питання запровадження інформаційних технологій у всі сфери життєдіяльності країн, а особливо в окремі галузі суспільної діяльності (державне управління, промисловість, банківську сферу) та на рівні окремих підприємств. При цьому першочергове значення відводиться дослідженню сутності цифровізації, її складу, змісту та значенню для розвитку економіки та її місця в сучасних трендах суспільно-економічних формацій.

Виділення невирішених раніше частин загальної проблеми. Цифрова безпека, яка повинна стати незмінною складовою реалізації процесу цифровізації суспільства та економіки, досі вивчена не достатньо. Проте, питання безпеки в умовах цифровізації досліджувались такими вченими, як Г. Мельничук та В. Мамалига [1], Г. Ткачук [2], Ю. Самойленко та ін. [3], С. Співаковський [4]. У своїх працях Т. Передерій [5] приділяє важливу роль розгляду сутності, складу, механізму реалізації цифрової безпеки підприємства, як підґрунтя для формування дієвої стратегії цифрової безпеки. Також в працях К. Краус, Н. Краус [6; 7] досліджується питання кібербезпеки та рекомендуються напрями її забезпечення для підприємств в умовах воєнного стану.

Недостатнім залишається дослідження сутності та складу цифрової безпеки, її значення для забезпечення безперебійної та безперешкодної діяльності підприємств в умовах тотальної цифровізації всіх суспільно економічних відносин.

Формулювання цілей статті (постановка завдання). Зважаючи на викладене вище, метою даної статті є дослідження сутності та змісту цифрової безпеки підприємства.

Виклад основного матеріалу дослідження. Будь-яке підприємство в сучасних умовах прагне свого позитивного розвитку, який передбачає зростання соціально-економічних показників (результатів) діяльності та зростання стійкості в мінливому середовищі функціонування, в сукупності факторів зовнішнього та внутрішнього впливу. Зміцнення зростання опору негативним факторам зовнішнього та внутрішнього середовища підприємства забезпечує посилення безпеки підприємства. В свою чергу, безпечне функціонування підприємства передбачає формування високого рівня опірності можливим негативним явищам і в залежності від системи, яка більшій мірі підлягає реалізації (активації), виділяють ринкову, соціальну, економічну, фінансову, екологічну, політичну, правову, пожежну, інформаційну, цифрову безпеки (рис. 1). Зважаючи на цілісність функціонування підприємства як системи, наведені види безпеки не реалізуються у відокремленому вигляді, а взаємодіють в сукупності з іншими, часто пов'язаними функціонально. Відтак, розглядають та управлять такими видами безпеки підприємства: соціально-економічна безпека, фінансово-економічна, політико-правова, інформаційно-цифрова, тощо.

Стрімкий розвиток інформаційних технологій спонукав виникнення нових ризиків, насамперед, пов'язаних із поширенням інформації, використання програмного забезпечення та технічних засобів обробки та передачі інформації. Всі ці ризики виникають внаслідок неправового використання, передачі

Рис. 1. Місце цифрової безпеки в загальній безпеці підприємства

Джерело: сформовано авторами

та спотворення інформації, порушення умов використання програмного забезпечення та виникнення несправностей чи несумісності різноманітних програм, поширення шкідливих програм та загроза виведення з ладу комп'ютерної техніки. Узагальнену та деталізовану характеристику ризиків та загроз, які виникають від цифровізації суспільно-економічних процесів наведено колективом авторів [3], до яких віднесено:

«Ризики на вході:

– ризики та загрози правового характеру;

– зовнішні інформаційні ризики, зумовлені політичними та соціально-економічними ситуаціями в країні;

– ризики, пов'язані з використанням технологій цифрової економіки (технологічний ризик): Інтернет речей, ризики технології блокчейн, ризики використання штучного інтелекту та технологій робототехніки та автоматизації на його основі, ризики та загрози використання імпортних апаратних компонентів та запозичення нових цифрових технологій; ризики та загрози до використання хмарних та розподілених обчислень; ризики та загрози, пов'язані зі стабільністю Інтернету;

– високотехнологічні фізичні загрози;

– ризики низьких цифрових компетенцій потенційних працівників.

Ризики у внутрішньому середовищі:

– організаційно-управлінські ризики;

– внутрішні інформаційні ризики, які безпосередньо пов'язані з діяльністю підприємства та його персоналу і залежать від таких факторів , як виробничі та кадрові ресурси, рівень техніко-технологічної оснащеності та розвитку інформаційної інфраструктури, організація цифрової безпеки;

– ризики цифрової безпеки: втрата інформаційних ресурсів, втрата доступу до інформаційних ресурсів, порушення їх цілісності, доступності внаслідок свідомого впливу; викрадення інформації та даних у цифровому форматі; навмисне спотворення інформації, збої технічного та програмного забезпечення автоматизованих систем управління та інформаційних систем, а також несправності програмного забезпечення та засобів захисту в наслідок навмисного впливу; поширення шкідливого програмного забезпечення та закладок; шпигунське програмне забезпечення; несанкціонований доступ; порушення авторських прав;

– використання третіх осіб для управління процесами.

Ризики на вході:

– ризики, пов'язані з інтеграцією цифрових технологій між основними зацікавленими сторонами (постачальниками,

– перевізниками, споживачами);

– зниження рівня фінансово-економічної безпеки підприємства у цілому та цифрової безпеки зокрема;

– вразливість до шкідливих впливів;

– радикальна зміна бізнес-моделей та «злиття» економічних, правових та інформаційних загроз, набуваючи складної цифрової технологічної ознаки».

Забезпечення цифрової безпеки підприємства направлено на запобігання та протидію існуючим ризикам та загрозам. Боднар О. А. Розглядає цифрову безпеку, як «стан цифровізації в економічній науці, що забезпечує економічні та інформаційні інтереси підприємства в поточному періоді та його стратегічну фінансово-економічну безпеку в довгостроковій перспективі з використанням відповідних технологій» [8, с. 236]. Безперечним є вплив цифрової безпеки підприємства на його фінансовий стан, проте не є основною стратегічною метою, враховуючи існуючі ризики та загрози.

Якщо розглядати цифрову безпеку в стратегічному плані та її зв'язок зі стратегією розвитку підприємства, доцільно погодитись із точкою зору Т. С. Передерій, в якій визначено, що «Розробка стратегії підприємства необхідна для адаптації бізнесу до трансформації економіки, що не є можливим саме без забезпечення цифрової безпеки підприємства» [5, с. 202]. При цьому науковець зазначає, що головною метою цифрової безпеки підприємства є « забезпечення стабільного функціонування бізнесу з подальшим розвитком у майбутньому, що ґрунтується на структурі її функціональних складових [5, с. 202]. Відтак, під цифровою безпекою Т. С. Передерій розглядає «захищеність функціональних складових підприємства під час здійснення господарської діяльності в умовах цифровізації і конкуренції; заходи і методи, що спрямовані на мінімізацію зовнішніх і внутрішніх ризиків е-бізнесу, а також забезпечення безпеки функціональних складових [5, с. 202].

Зважаючи на те, що не існує правового визначення цифрової безпеки, яке б забезпечило єдиний погляд предмет захисту, суб'єктів захисту та створило юридичне підґрунтя для формування захисту майнових інтересів щодо інформації та засобів її обробки і зберігання, розглянемо існуючі в економічній науці точки зори щодо досліджуваного явища. Зокрема, Т. Ткачук визначає цифрову безпеку як «безпеку об'єкта від інформаційних загроз або негативних впливів, які пов'язані з інформацією, та нерозголошення даних про той чи інший об'єкт, що є комерційною таємницею» [2, с. 45]. М. Саврук зазначає, що «цифрова безпека – це стан захищеності інформації, яка забезпечує життєво важливі інтереси підприємства та суспільства в цілому» [9, с. 78]. Н. В. Касьянова, досліджуючи цифрову безпеку на різних рівнях суспільно-економічних відносин, визначає, цифрову безпеку підприємства як «стан захищеності цифрової інформації підприємства, який дозволяє забезпечити існування та інноваційний розвиток підприємства незалежно від наявності внутрішніх і зовнішніх цифрових загроз» [10, с. 56].

Також в наукових дослідженнях зустрічаються ототожнення цифрової безпеки з інформаційною безпекою та кібербезпекою. Зокрема, І. М. Сопілко, що «…інформаційна безпека – це набір інструментів і методик, розроблених і тих, що використовуються для захисту конфіденційної інформації від зміни, порушення, знищення і перевірки» [10, с. 111]. О. І. Ткаченко та К. О. Ткаченко, під кібербезпекою розглядають «…захист інформаційної системи що входять до складу кіберпростору, від нападів, забезпечення конфіденційності, цілісності та доступності інформації, яка обробляється в цьому просторі, виявлення та протидія атакам і кіберінцидентам» [3, с. 77]. Розглядаючи кібербезпеку як основний інструмент забезпечення цифрової безпеки, та через застосування процесного підходу, Н. Краус та К. Краус визначають основні завдання кібербезпеки, які полягають у: «виявленні потенційних загроз кібербезпеки підприємств і вразливостей; попередженні кіберінцидентів; нейтралізації або мінімізації загроз інформаційної безпеки підприємства» [6, с. 29].

Висновки. Розглядаючи сутність та значення цифрової безпеки підприємства, автори дотримуються думки, що цифрову безпеку не можливо ототожнювати із інформаційною та кібербезпекою. Цифрова безпека підприємства відображає захищеність інформації в усіх її формах та видах, яка належить підприємству і використовується ним та захист технічних засобів обробки, передачі та передачі інформації та програмного забезпечення,

використовуваного в діяльності підприємства на законних засадах. Відтак, в складі цифрової безпеки доцільно виділити інформаційну безпеку та кібербезпеку, які тісно взаємодіють між собою та направлені на запобігання виникненню, протидію ризикам та загрозам, а також на мінімізацію втрат в разі їх виникнення в сфері інформаційного забезпечення діяльності підприємства та технікотехнологічного забезпечення використання інформації.

Перспективи подальших досліджень полягають в деталізації складу цифрової безпеки та визначенні функціональних і процесних напрямів, дієвих інструментів забезпечення цифрової безпеки підприємства. На загальнодержавному рівні необхідно визначити сутність цифрової безпеки підприємства та механізм державного забезпечення дотримання прав юридичних осіб щодо формування цифрової безпеки в умовах зростання ризиків та загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Мельничук Г. С., Мамалига В. С. Цифровізація економіки: можливості та загрози для ефективного функціонування підприємств. *Приазовський економічний вісник.* 2020. № 2 (19). С. 125–130.

2. Ткачук Г. О. «Цифрові» трансформації: взаємозв'язок із системою економічної безпеки підприємства. *Економіка харчової промисловості*. 2019. Том 11. № 4. С. 42–50.

3. Samoilenko Y., Britchenko I., Levchenko I., Lošonczi P., Bilichenko O., Bodnar O. Economic Security of the Enterprise Within the Conditions of Digital Transformation. *Economic Affairs.* 2022. Vol. 67. № 4. P. 619–629.

4. Spivakovskyy S., Kochubei O., Shebanina O., Yaroshenko I., Nych T. The impact of digital transformation on the economic security of Ukraine. *Estudios de Economia Aplicada.* 2021. Vol. 39.

5. Передерій Т. Стратегія цифрової безпеки підприємства як драйвер цифрової трансформації економіки України. *Вісник економічної науки України.* 2019. № 2 (37). С. 201–204.

6. Краус К., Краус Н., Штепа О. Цифрова трансформація кібербезпеки на мікрорівні в умовах воєнного стану. *Innovation and Sustainability.* 2022. № 3. С. 26–37.

7. Краус Н., Краус К. Цифровізація в умовах інституційної трансформації економіки: базові складові та інструменти цифрових технологій. Інтелект XXI століття. 2018. 1. С. 211–214.

8. Боднар О. А. Модернізація фінансово-економічної безпеки підприємства в умовах цифровізації. *Наукові перспективи*. 2023. № 2. С. 234–246.

9. Саврук М. В. Актуальність проблеми забезпечення інформаційної безпеки України та шляхи її розв'язання системи обробки інформації. *Системи обробки інформації.* 2010. № 3 (84). С. 77–79.

10. Сопілко І.М. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. *Юридичний вісник*, 2021. Вип. 2 (59).

REFERENCES:

1. Melnychuk, H. & Mamalyha V. (2020). Tsyfrovizatsiia ekonomiky: mozhlyvosti ta zahrozy dlia efektyvnoho funktsionuvannia pidpryiemstv [Digitization of the economy: opportunities and threats for the effective functioning of enterprises]. *Pryazovsky Economic Bulletin*. 2 (19). 125–130. Retrieved from: http://pev.kpu.zp.ua/journals/2020/2_19_ukr/23.pdf [in Ukrainian].

2. Tkachuk, H., Tkachuk H. O. (2019). «Tsyfrovi» transformatsii: vzaiemozviazok iz systemoiu ekonomichnoi bezpeky pidpryiemstva ["Digital" transformations: relationship with the economic security system of the enterprise]. *Ekonomika kharchovoi promyslovosti – Economics of the food industry.* 11 (4). 42–50. [in Ukrainian].

3. Samoilenko, Y., Britchenko, I., Levchenko, I., Lošonczi, P., Bilichenko, O. & Bodnar O. (2022). Economic Security of the Enterprise Within the Conditions of Digital Transformation. *Economic Affairs.* 67 (4), 619–629.

4. Spivakovskyy, S., Kochubei, O., Shebanina, O., Yaroshenko, I. & Nych, T. (2021). The impact of digital transformation on the economic security of Ukraine. *Estudios de Economia Aplicada*. 39 (5).

5. Perederij, T. (2019). Stratehiia tsyfrovoi bezpeky pidpryiemstva yak draiver tsyfrovoi transformatsii ekonomiky Ukrainy [The digital security strategy of the enterprise as a driver of the digital transformation of the economy of Ukraine]. *Herald of economic science of Ukraine.* 2 (37). 201–204. [in Ukrainian].

6. Kraus, K., Kraus, N. & Shtepa, O. (2022). Tsyfrova transformatsiia kiberbezpeky na mikrorivni v umovakh voiennoho stanu [Digital transformation of cyber security at the micro level in martial law]. *Innovation and Sustainability*. 3. 26–37. [in Ukrainian].

7. Kraus, N. M. and Kraus, K. M. (2018) Tsyfrovizatsiia v umovakh instytutsiinoi transformatsii ekonomiky: bazovi skladovi ta instrumenty tsyfrovykh tekhnolohii [Digitalization in the conditions of institutional transformation of economy: basic components and tools of digital technologies]. *Intelekt XXI stolittia,* vol. 1, pp. 211–214. [in Ukrainian].

8. Bodnar O.A. (2023) Modernizatsiia finansovo-ekonomichnoi bezpeky pidpryiemstva v umovakh tsyfrovizatsii [Modernization of the financial and economic security of the enterprise in the conditions of digitalization]. *Naukovi perspektyvy*. № 2, pp. 234–246. [in Ukrainian].

9. Savruk M. V. (2010) Aktualnist problemy zabezpechennia informatsiinoi bezpeky Ukrainy ta shliakhy yii rozviazannia systemy obrobky informatsii [The relevance of the problem of ensuring information security of Ukraine and ways of solving it in the information processing system]. *Systemy obrobky informatsii.* № 3 (84), pp. 77–79. [in Ukrainian].

10. Sopilko I. M. (2021). Informatsiina bezpeka ta kiberbezpeka: porivnialno-pravovyi aspekt [Information security and cyber security: a comparative legal aspect]. *Yurydychnyi visnyk.* Vyp. 2 (59). [in Ukrainian].