УДК 336:368 **DOI:10.32680/2409-9260-2023-9-310-98-106**

АКТУАЛІЗАЦІЯ КІБЕРСТРАХУВАННЯ В УМОВАХ ЦИФРОВІЗАЦІЇ ЕКОНОМІКИ

Шолойко А. С., доктор економічних наук, доцент, доцент кафедри страхування, банківської справи та ризик-менеджменту Київського національного університету імені Тараса Шевченка, м. Київ, Україна
e-mail: sholoiko@ukr.net
ORCID ID: 0000-0003-1239-4281

Анотація. *В умовах цифровізації економіки зростає рівень кіберризиків і актуалізується значення кіберстрахування. Проте під кіберстрахуванням часто розуміється лише страхування відповідальності перед третіми особами, що насправді є досить вузьким розумінням цього виду страхування та вимагає перегляду і уточнення визначення поняття «кіберстрахування». Метою статті є наукове обґрунтування визначення поняття «кіберстрахування». Цю мету досягнуто через виконання таких завдань: здійснити критичний аналіз існуючих дефініцій «кіберстрахування»; сформулювати власне визначення поняття «кіберстрахування»; довести практичну цінність запропонованого визначення. Реалізацію поставлених завдань здійснено на основі застосування методики конструювання дефініції поняття А. Старостіної та В. Кравченка. На основі критичного аналізу наявних дефініцій кіберстрахування виокремлено підходи до визначення його сутності, а саме, що кіберстрахування це:*
1) страховий продукт; 2) страховий поліс / контракт; 3) інструмент / метод. Сконструйовано авторську дефініцію кіберстрахування, яка містить три компоненти, а саме: це інструмент передачі (сутність) страховику на договірній основі несприятливих фінансових наслідків ризиків, що виникають у кіберпросторі з фізичними та юридичними особами (страхувальниками) (зміст), задля зміцнення їх фінансової безпеки шляхом виплати страхового відшкодування (результат). Доведено практичну цінність запропонованого визначення, яке має трикомпонентну структуру; конкретизує сторони кіберстрахування та договірний характер відносин між ними; уточнює сферу виникнення ризиків – кіберпростір і те, що кіберризики є непрямими фінансовими ризиками; підкреслює результат кіберстрахування – зміцнення фінансової безпеки юридичних і фізичних осіб. Одержані результати є основою для подальшого формування фреймворку з управління кіберризиками.
Ключові слова: *кіберризик, кіберпростір, кібербезпека, кібератака, цифрова економіка, страхування кібервідповідальності.*

ACTUALIZATION OF CYBER INSURANCE UNDER DIGITALIZATION OF THE ECONOMY

Sholoiko Antonina, Doctor of Economics, Associate Professor, Associate Professor of the Department of Insurance, Banking and Risk-management, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
e-mail: sholoiko@ukr.net
ORCID ID: 0000-0003-1239-4281

Abstract. *The level of cyber risks increases, and the importance of cyber insurance is rising under digitalization of the economy. However, cyber insurance is often understood only as third-party liability insurance, which is actually a rather narrow understanding of this type of insurance and requires a review and clarification of the definition of "cyber insurance". The purpose of the article is to scientifically ground the definition of the concept of "cyber insurance". This purpose was achieved through the following tasks: to carry out a critical analysis of existing definitions of "cyber insurance"; to formulate own definition of the concept of "cyber insurance"; to prove the practical value of the suggested definition. The achieving of the set tasks became possible due to the application of the method of construction of the definition of the concept by A. Starostina and V. Kravchenko. On the basis of a critical analysis of existing definitions of cyber insurance, approaches to defining its essence are singled out, namely, that cyber insurance is: 1) an insurance product; 2) insurance policy / contract; 3) tool / method. The constructed author's definition of cyber insurance contains three components, namely: it is a tool for transferring (essence) to the insurer on a contractual basis the adverse financial consequences of risks arising in cyberspace with individuals and legal entities (insureds) (content), in order to strengthen their financial security through insurance compensation payments (result). The practical value of the suggested definition is explained by: three-component structure; specification the parties to cyber insurance and the contractual nature of the relationship between them; clarification the scope of risks - cyberspace and the fact that cyber risks are indirect financial risks; emphasizing the result of cyber insurance - strengthening the financial security of legal entities and individuals. The obtained results are the basis for the further formation of the cyber risk management framework.*
Keywords*:cyber risk, cyberspace, cybersecurity, cyber-attack, digital economy, cyber liability insurance.*

JEL Classification: O310, G320.

Постановка проблеми. З поступовим розвитком концепції «метавсесвіт» проявилася тенденція до тестування компаніями взаємодії зі своїми клієнтами через нові платформи (наприклад, платформа віртуальної нерухомості Decentraland, метавсесвіт Skodaverse, цифрове місто Gucci у метавсесвіті Roblox тощо). Отже, в умовах цифровізації економіки дистанційна взаємодія поступово нарощує оберти і, як наслідок, зростає кількість кіберзагроз. Уряди країн реагують на таку ситуацію. Так, в Україні є «Стратегія кібербезпеки України» [1] та Закон «Про основні засади забезпечення кібербезпеки України» [2]. У країнах Європейського Союзу (ЄС) діють Директива про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу [3] і Загальний регламент захисту даних (General Data Protection Regulation, GDPR) [4]. GDPR встановлює, що органи державного нагляду у країнах ЄС можуть накладати штрафи у розмірі до 20 млн. євро або до 4% від загального річного обороту компанії за попередній фінансовий рік залежно від того, яка сума є вищою [4]. Відповідно, актуальність кіберстрахування як інструменту фінансування негативних наслідків у разі реалізації кіберризиків лише зростає.

Аналіз останніх досліджень і публікацій. Передумовою появи кіберстрахування є кіберризик, значну увагу якому приділили К. Авізцуз, Т. Кніспел, І. Пеннер, Г. Свідленд, А. Вос, С.Вебер у частині вдосконалення типологізації кіберризиків, виділивши ідіосинкратичні, систематичні та системні кіберризики [5]. С. Волосович, Л. Клапків і Ю. Клапків окреслили кримінальні та некримінальні джерела кіберризиків та методи ідентифікації кіберризиків [6, 7]. Проблематика кримінальної відповідальності за кримінальні правопорушення у кіберпросторі відображена у монографії М. Думчикова [8].

Через підвищення рівня кіберризиків в умовах цифровізації економіки зростає і актуальність їх страхування, що потребує формування більш усталеного визначення поняття «кіберстрахування». Спроби дати дефініції робили як вітчизняні, так і зарубіжні вчені. Серед них: Р. Пікус і Ю. Бабенко, Н. Приказюк та Л. Гуменюк, Н. Нагайчук, Н. Третяк і О. Ткаленко, Р. Бьоме і Г. Шварц, С. Романовський, Л. Аблон, А. Куен і Т. Джонс та інші.

Відокремлення невирішених раніше частин загальної проблеми. Однак наявні визначення містять певні упущення, що потребує їх перегляду та точнішого конструювання дефініції кіберстрахування.

Мета дослідження. Метою дослідження є наукове обґрунтування визначення поняття «кіберстрахування».

Цю мету досягнуто через виконання таких завдань:

– здійснити критичний аналіз існуючих дефініцій «кіберстрахування»;

– сформулювати власне визначення поняття «кіберстрахування»;

– довести практичну цінність запропонованого визначення.

Реалізацію поставлених завдань здійснено на основі застосування методики А. Старостіної та В. Кравченка. Основні етапи цієї методики такі:

1) формування переліку визначень поняття, що досліджується;
2) розбір існуючих категорій за трьома компонентами: суть явища, його зміст та результат;
3) узагальнення існуючих в літературі підходів до визначення поняття;
4) класифікація існуючих підходів до визначення поняття;
5) проведення критичного аналізу виявлених підходів;
6) конструювання власного визначення поняття;
7) окреслення практичного використання поняття [9].

Основний матеріал. Нижче наведено перелік дефініцій кіберстрахування, що були розкладені на три компоненти (табл. 1).

Таблиця 1

Перелік визначень поняття «кіберстрахування»

№	Автор, рік, вид публікації	Суть явища	Зміст явища	Результат явища

1.	Пікус Р., Бабенко Ю., 2022, стаття [10]	страховий продукт,	який пов'язаний з передачею фінансового ризику третій стороні, тобто страховій компанії для того, щоб допомогти державі, суспільству, суб'єктам господарювання та фізичній особі зменшити вплив ризику шляхом компенсації витрат, пов'язаних із потенційно руйнівними наслідками кіберзлочинів,	забезпечити захист від збитків, що виникають внаслідок порушення безпеки та конфіденційності
2.	Нагайчук Н., Третяк Н. і Ткаленко О., 2019, стаття [11]	це страховий продукт	від ризиків, пов'язаних з використанням мережі Інтернет, а також із ризиками, що належать до інформаційних технологій, ІТ-інфраструктури та діяльності підприємства у кібер-просторі,	що захищає компанію
3.	Приказюк Н., Гуменюк Л., 2020, стаття [12]	є не просто інструментом з мінімізації наслідків, а й ефективним механізмом попередження їх настання,	оскільки забезпечує співпрацю зі спеціалізованими організаціями, експертами з захисту систем та конфіденційної інформації (партнерські програми) та попередній моніторинг стану клієнта	
4.	Бьоме Р. і Шварц Г., 2010, матеріали конференції [13]	інструмент передачі фінансового ризику,	пов’язаного з мережевими та комп’ютерними інцидентами, третій стороні	
5.	Hiscox, 2023, запитання-відповіді [14]	форма покриття	від загроз цифрової епохи, таких як витік даних або зловмисні кібер-зломи робочих комп’ютерних систем	призначена для захисту бізнесу
6.	Романовський С., Аблон Л., Куен А., Джонс Т., 2019, дослідницька стаття [15]	страхові поліси,	які стосуються збитків першої та третьої сторони в результаті комп’ютерної атаки або несправності систем інформаційних технологій фірми	
7.	Мажука Р.П., Юрсік У., Кесан Дж. П., 2006, стаття [16]	є потужним інструментом	для вирівнювання ринкових стимулів	для підвищення безпеки в Інтернеті
8.	Баер В. С., Паркінсон А., 2007, стаття [17]	інструмент управління ризиками,	стимул для інвестицій у безпеку, які зменшують ризик	для покриття збитків і зобов’язань від порушення безпеки мережі чи інформації
9.	TechTarget, 2021, огляд [18]	відноситься до контракту,	який підприємства можуть придбати,	щоб зменшити фінансові ризики, пов’язані з веденням онлайн-бізнесу

10.	Селіверстова Л. С., Трухан Д. А., 2020, стаття [19]	метод захисту	від кібератак і негативних наслідків	забезпечує фінансовий механізм відновлення після великих збитків, допомагаючи підприємствам повернутися до нормального функціонування, збереження стабільності, платоспроможності і зниження втрат у результаті перерви у виробництві, викликаної різного роду кіберзагрозами

Джерело: складено автором за матеріалами [10-19]

На наступному етапі було здійснено класифікацію існуючих підходів до визначення поняття «кіберстрахування» (табл. 2).

Таблиця 2

Класифікація існуючих підходів до визначення поняття «кіберстрахування»

№	Автор, рік, вид публікації	Сутність явища					Наявність змісту	Наявність результату
		Страховий продукт	Інструмент	Форма покриття	Страховий поліс / контракт	Метод захисту		
1	Пікус Р., Бабенко Ю., 2022, стаття [10]	+					+	+
2	Нагайчук Н., Третяк Н. і Ткаленко О., 2019, стаття [11]	+					+	+
3	Приказюк Н., Гуменюк Л., 2020, стаття [12]		+				+	-
4	Бьоме Р. і Шварц Г., 2010, матеріали конференції [13]	+				+	-	
5	Hiscox, 2023, запитання-відповіді [14]			+			+	+
6	Романовський С., Аблон Л., Куен А., Джонс Т., 2019, дослідницька стаття [15]			+		+	-	
7	Мажука Р.П., Юрсік У., Кесан Дж. П., 2006, стаття [16]	+				+	+	
8	Баер В.С., Паркінсон А., 2007, стаття [17]		+				+	+

9	TechTarget, 2021, огляд [18]				+		+	+
10	Селіверстова Л. С., Трухан Д. А., 2020, стаття [19]					+	+	+

Джерело: складено автором за матеріалами [10-19]

Аналізуючи підходи до визначення сутності кіберстрахування, що наведені у табл. 1, можна виокремити три підходи до трактування його сутності, а саме, що це є: 1) страховий продукт; 2) страховий поліс / контракт; 3) інструмент / метод.

Варто зауважити, що на сучасному етапі цифровізації економіки кіберстрахування вже виокремилося із простого страхового продукту до окремого виду страхування за такою ознакою, як рід небезпеки (зокрема небезпека у кіберпросторі) і за різноманіттям кіберризиків у межах кіберстрахування можлива варіація страхових продуктів. Цей підхід узгоджується з уже виокремленими за родом небезпеки таких видів страхування, як автострахування, сільськогосподарське страхування, космічне страхування тощо, у межах яких можливе як майнове страхування, так і страхування відповідальності за шкоду третім особам. Аналогічним чином і при кіберстрахуванні можливе виокремлення страхування кібервідповідальності та майнового страхування, що підтверджує дослідження Р. Пікус та Ю. Бабенко [10, с. 135].

Страховий поліс / контракт більше характеризує юридичну природу будь-якого виду страхування, оскільки страхові послуги належать до фінансових послуг, що вимагає дотримання договірних засад їх надання.

Складно не погодитися, що кіберстрахування – це інструмент, зокрема управління ризиками в частині трансферу кіберризиків третій стороні (страховику) для фінансування негативних наслідків від їх реалізації.

Щодо результату явища, то більшість визначень наголошують на такому ефекті як захист і безпека. Тут необхідно конкретизувати, що йдеться саме про фінансову безпеку (яка є ширшим поняттям, ніж платоспроможність і стабільність з погляду довгострокового горизонту), оскільки власники полісів кіберстрахування або треті особи у випадку страхування кібервідповідальності отримують грошове відшкодування втрат від настання кіберризиків, що дозволяє відновити і продовжити функціонування.

Наступним етапом конструювання дефініції кіберстрахування є оцінювання наявних підходів за п'ятибальною шкалою, де 1 – мінімальний бал, а 5 – максимальний за такими критеріями як: наявність трьох компонентів у визначенні, поширеність визначення у наукових джерелах, теоретична обґрунтованість поняття, доступність для практичного використання [8]. Результати представлено у таблиці 3.

Таблиця 3

Оцінка існуючих підходів до визначення поняття «кіберстрахування»

№	Автор, рік, вид публікації	Оцінка (бали)				
		наявність компонентів	поширеність визначення	теоретична обґрунтованість	практична доступність	сумарна оцінка
1	Пікус Р., Бабенко Ю., 2022, стаття [10]	5	3	3	3	14
2	Нагайчук Н., Третяк Н. і Ткаленко О., 2019, стаття [11]	5	3	3	2	13

3	Приказюк Н., Гуменюк Л., 2020, стаття [12]	3	4	3	2	12
4	Бьоме Р. і Шварц Г., 2010, матеріали конференції [13]	3	4	3	3	13
5	Hiscox, 2023, запитання-відповіді [14]	5	2	3	2	12
6	Романовський С., Аблон Л., Куен А., Джонс Т., 2019, дослідницька стаття [15]	3	2	2	2	9
7	Мажука Р. П., Юрсік У., Кесан Дж. П., 2006, стаття [16]	5	1	1	2	9
8	Баер В. С., Паркінсон А., 2007, стаття [17]	5	3	3	2	13
9	TechTarget, 2021, огляд [18]	5	2	2	2	11
10	Селіверстова Л. С., Трухан Д. А., 2020, стаття [19]	5	3	3	2	13

Джерело: складено автором за матеріалами [10-19]

За даними табл. 3 найбільшу кількість балів одержало визначення, запропоноване Р. Пікус і Ю. Бабенко. Це визначення вирізняється тим, що наголошує на значенні кіберстрахування не лише для держави і бізнесу, тобто юридичних осіб, а й для фізичних осіб. До того ж, як вже зазначалося, кіберстрахування передбачає надання покриття як у разі виникнення відповідальності за шкоду третім особам, так і у разі спричинення майнової шкоди тримачам полісу кіберстрахування.

Визначивши сильні та слабкі сторони досліджуваних дефініцій поняття кіберстрахування, можна запропонувати власне визначення. Так, кіберстрахування – це інструмент передачі страховику на договірній основі несприятливих фінансових наслідків ризиків, що виникають у кіберпросторі з фізичними та юридичними особами (страхувальниками), задля зміцнення їх фінансової безпеки шляхом виплати страхового відшкодування.

Це визначення має низку характеристик, які доводять його практичну цінність:

– трикомпонентна структура: визначення містить сутність, зміст і результат;

– конкретизуються сторони кіберстрахування – страховики і страхувальники та договірний характер відносин між ними, що є обов'язковим для страхової послуги, як фінансової послуги. До того ж, у межах такого страхового договору можливе застосування правової та фінансової превенцій, що робить наголос на попереджувальному характері кіберстрахування;

– уточнено сферу виникнення ризиків – кіберпростір і підкреслено спричинення ними несприятливих фінансових наслідків, що є більш точним, оскільки кіберризики не є прямими фінансовими ризиками, а більше – непрямими;

– підкреслено результат кіберстрахування, а саме зміцнення фінансової безпеки юридичних і фізичних осіб для забезпечення їх безперервної діяльності у довгостроковій перспективі шляхом виплати їм або постраждалим третім особам (у разі страхування кібервідповідальності) страхового відшкодування страховиками.

Висновки. У статті було здійснено наукове обґрунтування визначення поняття «кіберстрахування». У результаті критичного аналізу наявних дефініцій кіберстрахування виокремлено підходи до визначення його сутності, а саме, що кіберстрахування це: 1) страховий продукт; 2) страховий поліс / контракт; 3) інструмент / метод.

Запропоновано авторську дефініцію кіберстрахування, яка містить три компоненти, а саме: це інструмент передачі (сутність) страховику на договірній основі несприятливих фінансових наслідків ризиків, що виникають у кіберпросторі з фізичними та юридичними особами (страхувальниками) (зміст), задля зміцнення їх фінансової безпеки шляхом виплати страхового відшкодування (результат).

Доведено практичну цінність сконструйованого визначення, яке має трикомпонентну структуру; конкретизує сторони кіберстрахування та договірний характер відносин між ними; уточнює сферу виникнення ризиків – кіберпростір і те, що кіберризики є непрямими фінансовими ризиками; підкреслює результат кіберстрахування – зміцнення фінансової безпеки юридичних і фізичних осіб.

Перспективи подальших досліджень полягають у формуванні фреймворку з управління кіберризиками.

Список літератури

1. Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення 15.08.2023).

2. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 15.08.2023).

3. Directive (eu) 2016/1148 of the European parliament and of the council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Official Journal of the European Union. L 194/1. 19.7.2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L-1148&from=EN (дата звернення 15.08.2023).

4. General Data Protection Regulation: Regulation (EU)2016/679 in the current version of the OJ L 127, 23.5.2018. URL: https://gdpr-info.eu/ (дата звернення 15.08.2023).

5. Awiszus K., Knispel T., Penner I., Svindland G., Voß A., Weber S. Modeling and pricing cyber insurance. European Actuarial Journal. 2023. 13.

P. 1-53. DOI: 10.1007/s13385-023-00341-9

6. Волосович С., Клапків Л. Детермінанти виникнення та реалізації кіберризиків. Зовнішня торгівля: економіка, фінанси, право. 2018. № 3.

С. 101-115.

7. Klapkiv L., Klapkiv Yu. Methods for the Identification of Cyber Risks: an Analysis Based on Patent Data. CBU International Conference Proceedings 2018. 2018. Vol. 6. DOI: https://doi.org/10.12955/cbup.v6.1163

8. Думчиков М. О. Концептуальні засади кримінально-правової охорони кіберпростору в Україні : монографія. Суми : Сумський державний університет. 2023. 413 с.

9. Старостіна А., Кравченко В. Сутність та практичне застосування методики конструювання категоріального апарату економічної науки (на прикладі понять «глобалізацація» та «підприємницький ризик»). Вісник Київського національного університету імені Тараса Шевченка. Економіка. 2011. № 128. С. 5-10.

10. Пікус Р. В., Бабенко Ю. Л. Кіберстрахування: нові можливості для страхового ринку України. Економіка та держава. 2022. № 2. С. 134-140. DOI: 10.32702/2306-6806.2022.2.134

11. Нагайчук Н., Третяк Н., Ткаленко О. Страхування в системі управління кібер-ризиками підприємства в умовах цифрової економіки. Міжнародний науково-практичний журнал «Фінансовий простір». 2019.
№ 1(33). С. 97-111. DOI: 10.18371/fp.1(33).2019.177102

12. Приказюк Н. В., Гуменюк Л. С. Передумови розвитку
кібер-страхування. Інвестиції: практика та досвід. 2020. № 15-16. С. 28-34. DOI: 10.32702/2306-6814.2020.15-16.28

13. Bohme R., Schwartz G. Modeling Cyber-Insurance: Towards A Unifying Framework. Workshop on the Economics of Information Security (WEIS), Harvard, June 2010. URL: http://www.icsi.berkeley.edu/pubs/ networking/modelingcyber10.pdf.

14. Hiscox. What is cyber insurance? URL: https://www.hiscox.co.uk/ business-insurance/cyber-and-data-insurance/faq/what-is-cyber-insurance

15. Romanosky S., Ablon L., Kuehn A., Jones T. Content analysis of cyber insurance policies: how do carriers price cyber risk? Journal of Cybersecurity. 2019. 1-19. DOI: 10.1093/cybsec/tyz002

16. Majuca R. P., Yurcik W., Kesan J. P. The Evolution of Cyberinsurance. 2006. URL: https://arxiv.org/abs/cs/0601020

17. Baer W. S., Parkinson A. Cyber insurance in IT security management. IEEE Security&Privacy. 2007. 5. P. 50-56. URL: https://sites.pitt.edu/ ~dtipper/2825/CIn.pdf (дата звернення 15.08.2023).

18. TechTarget. What is cybersecurity insurance (cybersecurity liability insurance)? URL: https://www.techtarget.com/searchsecurity/definition/ cybersecurity-insurance-cybersecurity-liability-insurance (дата звернення 16.08.2023).

19. Селіверстова Л. С., Трухан Д. А. Підходи до розвитку кіберстрахування як сегменту глобального страхового ринку. Економіка та держава. 2020. № 1. С. 23–26. DOI: 10.32702/2306-6806.2020.1.23

References

1. The cyber security strategy of Ukraine, approved by the Decree of the President of Ukraine dated August 26, 2021 No. 447/2021. Retrieved from https://zakon.rada.gov.ua/laws/show/447/2021#Text [In Ukrainian].

2. On the main principles of ensuring cyber security of Ukraine: Law of Ukraine dated October 5, 2017 No. 2163-VIII. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text [In Ukrainian].

3. Directive (eu) 2016/1148 of the European parliament and of the council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Official Journal of the European Union. L 194/1. 19.7.2016. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L-1148&from=EN

4. General Data Protection Regulation: Regulation (EU)2016/679 in the current version of the OJ L 127, 23.5.2018. Retrieved from https://gdpr-info.eu/

5. Awiszus, K., Knispel, T., Penner, I., Svindland, G., Voß, A., and Weber, S. (2023). Modeling and pricing cyber insurance. European Actuarial Journal. 13. 1-53. DOI: 10.1007/s13385-023-00341-9

6. Volosovych, S., Klapkiv, L. (2018). Determinants of the occurrence and implementation of cyber risks. Foreign trade: economy, finance, law. 3, 101-115. Retrieved from: http://zt.knute.edu.ua/files/2018/03(98)/10.pdf [In Ukrainian].

7. Klapkiv, L., Klapkiv, Yu. (2018). Methods for the Identification of Cyber Risks: an Analysis Based on Patent Data. CBU International Conference Proceedings l., 6. DOI: https://doi.

org/10.12955/cbup.v6.1163

8. Dumchykov, M. O. (2023). Conceptual principles of criminal and legal protection of cyberspace in Ukraine: monograph. Sumy: Sumy State University. [In Ukrainian].

9. Starostina, A., & Kravchenko, V. (2011). The essence and practical application of the method of construction of the categorical apparatus of economic science (on the example of the concepts "globalization" and "entrepreneurial risk"). Bulletin of Taras Shevchenko National University of Kyiv. Economics. 128, 5-10 [In Ukrainian].

10. Pikus, R., and Babenko, Y. (2022). Cyber insurance: new opportunities for the insurance market of Ukraine. Ekonomika ta derzhava. 2,. 134-140. DOI: 10.32702/2306-6806.2022.2.134 [In Ukrainian].

11. Nagaichuk, N., Tretiak, N., and Tkalenko O. (2019). Insurance in the cyber risk management system of the enterprise under the digital economy. International scientific and practical journal "Financial Space". 1(33), 97-111 DOI: 10.18371/fp.1(33).2019.177102 [In Ukrainian].

12. Prykaziuk, N., and Gumenyuk, L. (2020). Prerequisites for the development of cyber insurance. Investytsiyi: praktyka ta dosvid. 15-16., 28-34. DOI: 10.32702/2306-6814.2020.15-16.28 [In Ukrainian].

13. Bohme, R., and Schwartz, G. (2010). Modeling Cyber-Insurance: Towards A Unifying Framework. Workshop on the Economics of Information Security (WEIS), Harvard. Retrieved from: http://www.icsi.berkeley.edu/ pubs/networking/modelingcyber10.pdf.

14. Hiscox (2023). What is cyber insurance? Retrieved from https://www.hiscox.co.uk/business-insurance/cyber-and-data-insurance/faq/what-is-cyber-insurance

15. Romanosky, S., Ablon, L., Kuehn, A., and Jones, T. (2019). Content analysis of cyber insurance policies: how do carriers price cyber risk? Journal of Cybersecurity. Pp. 1-19. DOI: 10.1093/cybsec/tyz002

16. Majuca, R. P., Yurcik, W., Kesan, J. P. (2006). The Evolution of Cyberinsurance. Retrieved from https://arxiv.org/abs/cs/0601020

17. Baer, W. S., and Parkinson, A. (2007). Cyber insurance in IT security management. IEEE Security&Privacy, 5, 50-56. Retrieved from https://sites.pitt.edu/~dtipper/2825/CIn.pdf

18. TechTarget (2021). What is cybersecurity insurance (cybersecurity liability insurance)? Retrieved from https://www.techtarget.com/
searchsecurity/definition/cybersecurity-insurance-cybersecurity-liability-insurance

19. Seliverstova, L., Truhan, D. (2020). Approaches to the development of cyber insurance as a segment of the global insurance market. Ekonomika ta derzhava. 1 23-26. DOI: 10.32702/2306-6806.2020.1.23 [In Ukrainian].

Стаття надійшла до редакції 19.10.2023
Прийнята до публікації 23.10.2023