DOI: 10.33498/louu-2021-07-013

Ніно Пацурія

докторка юридичних наук, професорка,
професорка кафедри господарського права
та господарського процесу
Інституту права Київського національного університету
імені Тараса Шевченка
(Київ, Україна)
ORCID ID: https://orcid.or/0000-0001-9974-3637
Researcher ID: http://www.researcherid.com/rid/T-8391-2019
nino_2005@ukr.net

Олег Заярний

доктор юридичних наук, доцент,
професор кафедри інтелектуальної власності
та інформаційного права
Інституту права Київського національного університету
імені Тараса Шевченка
(Київ, Україна)
ORCID ID: https://orcid.or/0000-0003-4549-7201
Researcher ID: http://www.researcherid.com/rid/S-3358-2018
oleganalitik.knu@gmail.com

УДК 336.7:340.5; 346.764,477

КІБЕРСТРАХУВАННЯ ЯК ЗАСІБ ЗАБЕЗПЕЧЕННЯ ГОСПОДАРСЬКОГО ПРАВОПОРЯДКУ В ІНФОРМАЦІЙНІЙ СФЕРІ: ПОНЯТТЯ, МЕХАНІЗМ ТА УМОВИ РЕАЛІЗАЦІЇ

Анотація. Актуальність проведеного дослідження обумовлена сучасним рівнем прояву негативних наслідків кіберзагроз у сфері господарювання, недостатнім функціональним потенціалом традиційних засобів забезпечення господарського правопорядку у подоланні кіберризиків.

Останніми роками в Україні аналогічно до більшості держав із розвиненою економікою для вирішення вказаних проблем активно почало застосовуватися кіберстрахування.

Відсутність належного правового регулювання в Україні діяльності з кіберстрахування поряд із непоодинокими спробами страховиків запровадити на ринок страхових послуг пропозиції зі страхування кіберризиків у межах інших, часто несумісних видів страхування, також посилюють актуальність обраної проблематики.

Метою статті є дослідження поняття, механізму й умов застосування кіберстрахування як засобу забезпечення господарського правопорядку в інформаційній сфері, формулювання окремих пропозицій щодо удосконалення законодавства України з відповідних питань, а також визначення напрямів подальших наукових досліджень цього виду страхування.

У межах статті авторами сформульовано визначення поняття "кіберстрахування", надано детальну характеристику завдань правового засобу, що ним позначається. На цій основі кіберстрахування проаналізовано як засіб правового та економічного захисту учасників відносин у сфері господарювання від кіберризиків та їх наслідків, а також у значенні виду господарської діяльності.

Виходячи з таких наукових і правових позицій, автори детально проаналізували елементи механізму кіберстрахування, визначили елементи страхових правовідносин у цій сфері, зокрема страховик, страхувальник, об'єкт і зміст кіберстрахування. Значну увагу приділено кіберзагрозам у значенні страхових випадків, розглянуто основні підходи до їх наукової класифікації, визначено основні види протиправних діянь, що спричиняють виникнення кіберризиків. Поряд із цим автори статті проаналізували зміст і сутність майнових інтересів страхувальників від кіберризиків, охарактеризували основні види збитків, які підлягають відшкодуванню за договорами кіберстрахування. Окрім цього, предметом окремої уваги в межах статті стали договори кіберстрахування, страхові програми як засоби реалізації механізму кіберстрахування, визначено їх істотні умови та вимоги до сторін.

У висновках за результатами проведеного дослідження визначені напрями подальшого удосконалення законодавства України у сфері кіберстрахування, охарактеризовані юридичні вимоги, яким повинні відповідати страховики за цим видом діяльності. Автори запропонували конкретні рекомендації щодо визначення розмірів страхового відшкодування за договорами кіберстрахування та шляхи посилення юридичного значення кіберстрахування у системі засобів забезпечення господарського правопорядку.

Ключові слова: господарський правопорядок; інформаційна сфера; кіберзагроза, кіберризик; кіберстрахування; страховик; страхувальник.

Розвиток світової економіки на основі активного використання інформаційно-комунікаційних технологій і систем обумовлює глибоку цифрову трансформацію багатьох видів господарської діяльності. Разом із соціально-економічними результатами від цифрової трансформації, господарська діяльність піддається значним кіберризикам, які спрямовані передусім на дестабілізацію належного функціонування інформаційної інфраструктури національної економіки, окремих суб'єктів господарювання. За даними американської компанії *McAfee* та Центру стратегічних і міжнародних досліджень *(CSIS)*, протягом 2020 р. наслідки вчинення кіберзлочинів коштували світовій економіці понад 1 трлн доларів або 820 млрд євро, що становило понад 1 % світового внутрішнього валового продукту (далі – ВВП). Завдані у 2020 р. збитки від кіберзагроз і кіберінцидентів є на 50 % вищими, ніж у 2018 р.[1]. Згідно з дослідженн-

[1] 'Кіберзлочинці у 2020 році завдали у світі збитків на трильйон доларів: дослідження' <https://www.dw.com/uk/kiberzlochyny-u-2020-rotsi-zavdaly-svitu-zbytkiv-na-trylion-dolariv-doslidzhennia/a-55857766> (дата звернення: 15.06.2021).

ням оцінки якісних показників кіберризиків, проведеному у 2020 р. міжнародною аудиторською компанією "Делойт", удосконалення методів, які застосовуються кіберзлочинцями й істотне збільшення обсягів транзакцій в інтернеті, істотно ускладнює контроль за ризиками для інформаційної безпеки. Підтримання належного рівня безпеки вимагає інвестицій, які не завжди можливо виокремити у повному обсязі[2].

Існуючий стан господарського правопорядку в інформаційній сфері актуалізував перед державою та суб'єктами господарювання завдання з формування ефективного правового засобу протидії кіберризикам, запобігання прояву їх негативних наслідків. Таким правовим та економічним засобам, на думку дослідників проблем страхової діяльності, є кіберстрахування.

Одні з перших спроб надання послуг із кіберстрахування були зроблені у США у 2010 р.[3]. Однак інтерес до поняття "кіберстрахування" з боку вчених-правників та економістів істотно збільшився разом із набранням 24 травня 2016 р. чинності Регламентом Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 р. про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних)[4], а також проявом негативних наслідків міжнародної хакерської атаки з використанням комп'ютерного віруса "Петя" у 2017 р.[5].

Водночас відсутність в Україні спеціального правового регулювання відносин із кіберстрахування, поширена практика включення до страхових полісів зі страхування майна, транспортних засобів окремих кіберризиків, зумовило виникнення низки концептуальних проблем, які потребують наукового дослідження і законодавчого вирішення та закріплення.

Останніми роками різні аспекти проблематики кіберстрахування стали предметом дослідження багатьох учених – правників, економістів та фахівців із кібербезпеки.

Так, зокрема, В. Братюк у своєму дослідженні[6] приділяє значну увагу проблемам страхового захисту від кіберризиків, спричинених учиненням кіберзлочинів. У. Тихонько фокусує у своїх працях основну ува-

[2] 'Количественная оценка киберрисков' *(Deloitte Touche Tohmatsu Limited)* <https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/risk/russian/cyber-risk-quantification.pdf> (дата звернення: 15.06.2021).

[3] Leslie Scism, 'Insurers Creating a Consumer Ratings Service for Cybersecurity Industry' (*The Wall Street Journal,* 26.03.2019) <https://www.wsj.com/articles/insurers-creating-a-consumer-ratings-service-for-cybersecurity-industry-11553592600> (accessed: 15.06.2021).

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC *(General Data Protection Regulation)* <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679> (accessed: 15.06.2021).

[5] 'Розвиток кіберстрахування як сегменту глобального страхового ринку' <https://kon-insurance.mnau.edu.ua/files/work_2020/6.pdf> (дата звернення: 15.06.2021).

[6] В Братюк, 'Сутність кібер-злочинів та страховий захист від кібер-ризиків в Україні' (2015) 9 Актуальні проблеми економіки 421–7.

гу на сутності кіберризиків та перспективах запровадження в Україні кіберстрахування[7]. С. Перцева аналізує загальні аспекти застосування кіберстрахування в умовах розвитку цифрової економіки[8]. Г. Мамонова та Л. Позднякова аналізують загальні особливості страхування кіберризиків[9]. Н. Приказюк і Л. Гуменюк у своїх працях розглядають проблеми та перспективи запровадження у національну економіку кіберстрахування як нового страхового продукту на ринку страхових послуг[10].

Незважаючи на значний інтерес до проблематики кіберстрахування у вітчизняній та зарубіжній науковій літературі, малодослідженими, або такими, які потребують додаткового наукового обґрунтування, залишається низка проблем у цій сфері правового регулювання. Ідеться, зокрема, про визначення поняття "кіберстрахування" як інструменту забезпечення господарського правопорядку в інформаційній сфері, завдання та механізм реалізації цього правового й економічного засобу відновлення майнових інтересів страхувальників, визначення спеціальних вимог до страховика у правовідносинах кіберстрахування, формулювання істотних умов договору кіберстрахування, а також виокремлення напрямів подальшого удосконалення цього страхового продукту.

Метою дослідження є вивчення поняття, механізму й умов застосування кіберстрахування як засобу забезпечення господарського правопорядку в інформаційній сфері, формулювання окремих пропозицій щодо удосконалення законодавства України з відповідних питань.

Закладаючи конституційні основи правопорядку у сфері господарювання, Господарський кодекс України (далі – ГК України) у ч. 1 ст. 5 закріпив норму, відповідно до якої:

> Правовий господарський порядок в Україні формується на основі оптимального поєднання ринкового саморегулювання економічних відносин суб'єктів господарювання та державного регулювання макроекономічних процесів, виходячи з конституційної вимоги відповідальності держави перед людиною за свою діяльність та визначення України як суверенної і незалежної, демократичної, соціальної, правової держави[11].

Разом із глибокими процесами цифрової трансформації національної економіки, господарська діяльність в Україні, аналогічно до більшості

[7] У Тихонька, 'Особливості страхування кібер-ризиків' (*Стратегічні орієнтири,* 13.04.2021) <http://libfor.com/index.php?newsid=3898> (дата звернення: 15.06.2021).

[8] С Перцева, 'Киберстрахование в цифровой экономике' в *Современное состояние и перспективы развития рынка страхования: Материалы III Международной научно-практической конференции* (2018) 60–4.

[9] Г Мамонова, 'Особливості страхування кібер-ризиків' *Матеріали конференцій МЦНД* (2020) 91–93.

[10] Н Приказюк, Л Гуменюк, 'Кібер-страхування як важливий інструмент захисту підприємств в умовах цифровізації економіки' (2020) 4 Ефективна економіка.

[11] Господарський кодекс України: Закон України від 16 січня 2003 р. № 436-IV <https://zakon.rada.gov.ua/laws/show/436-15> (дата звернення: 15.06.2021).

держав світу, опинилася під значним негативним впливом кіберризиків і кіберзагроз.

За даними міжнародної аудиторської компанії "Делойт", керівники суб'єктів господарювання готові виділяти кошти на рішення подібних завдань, проте вимагають обґрунтування витрат, чіткого розуміння того, які ризики будуть у результаті мінімізовані[12].

У зв'язку з цим забезпечення інформаційної безпеки, визначене у ч. 1 ст. 17 Конституції України основною функцією держави, справою всього українського народу[13], набуло особливого значення для учасників відносин у сфері господарювання і господарського правопорядку загалом.

За даними "Дослідження глобальних тенденцій інформаційної безпеки за 2018 рік: основні висновки", опублікованого міжнародною аудиторською компанією "ПрайсвотерхаусКуперс" (далі – *PWC*):

> Не дивлячись на зростаючу обізнаність та публічний розголос подій та наслідків кібератак, багато компаній дотепер не підготовлені до реальної протидії загрозам. З 9 500 топ-менеджерів у 122 країнах світу, які були опитані в рамках згаданого дослідження, 44 % відповіли, що у них відсутня цілісна стратегія забезпечення кібербезпеки. Ще 48 % повідомили, що не мають програми навчання співробітників та підвищення їх обізнаності у питаннях захисту інформації, а 54 % заявили, що у них не передбачена політика реагування на надзвичайні ситуації[14].

Багато традиційних засобів забезпечення господарського правопорядку (зокрема, господарсько-правова відповідальність, засоби забезпечення господарських зобов'язань та засоби державного регулювання економіки) виявилися нездатними попередити виникнення кіберризиків, захистити від їх прояву учасників відносин у сфері господарювання.

Одним із сучасних правових засобів протидії кіберризикам, який в останнє десятиліття активно застосовується у сфері господарювання, є кіберстрахування.

У теорії страхового права й економічній теорії поняття "кіберстрахування" розглядається в різних аспектах: як метод управління економічними ризиками та захисту від кіберзагроз у сфері електронної комерції[15]; як засіб відшкодування (покриття) збитків, завданих страхувальнику

[12] Количественная оценка киберрисков (н 2).

[13] Конституція України: Закон України від 28 червня 1996 р. № 254к/96-ВР <https://zakon.rada.gov.ua/laws/show/254к/96-вр> (дата звернення: 15.06.2021).

[14] 'Посилення цифрового середовища проти кібер-загроз. Дослідження глобальних тенденцій інформаційної безпеки за 2018 рік: основні висновки' <https://www.pwc.com/ua/uk/survey/2018/pwc-2018-gsiss-strengthening-digital-society-against-cyber-shocks-ukr.pdf> (дата звернення: 15.06.2021).

[15] Л Селіверстова, Д Трухан, 'Підходи до розвитку кіберстрахування як сегменту глобального страхового ринку' (2020) 1 Економіка та держава 25.

внаслідок прояву кіберінцидентів, кіберзлочинів і кібератак[16]; як інструмент управління кіберризикам у цифровій економіці[17].

Незважаючи на існування у науковій літературі відмінностей у підходах до розуміння сутності і призначення кіберстрахування, існуючі наукові погляди на це поняття збігаються у визначенні основних завдань господарської діяльності, які ним позначаються. Серед цих завдань у науковій літературі й актах правозастосування називаються захист від масштабних хакерських атак[18], протидія кіберризикам і кіберінцедентам, а також забезпечення відшкодування страхувальнику збитків, завданих проявом вказаних факторів[19].

Аналіз цих завдань через призму визначеного у ст. 1 Закону України "Про страхування" (з наступними змінами та доповненнями)[20] загального поняття "страхування" означає, що як вид господарської діяльності кіберстрахування повинно бути передусім спрямованим на захист від наслідків кіберризиків майнових інтересів страхувальників як фізичних, так і юридичних осіб.

На цій основі поняття "кіберстрахування" можна визначити як вид господарської діяльності, що здійснюється спеціальними суб'єктами господарювання (страховиками) на основі договору кіберстрахування з метою захисту інтересів фізичних та/або юридичних осіб (власників інформаційно-комунікаційних технологій, систем, баз даних) від можливих або потенційних кіберризиків негативного прояву їхніх наслідків для страхувальника чи третіх осіб.

У наведеному значенні кіберстрахування набуває властивостей особливого засобу забезпечення господарського правопорядку в інформаційній сфері, нерозривно пов'язаного із забезпеченням кібербезпеки держави, суспільства, суб'єктів господарювання та людини.

Для України, як загального суб'єкта забезпечення господарського правопорядку, зобов'язання з легалізації механізму кіберстрахування випливають із положень ст. 8 Конвенції про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних[21], Конвенції про кіберзлочинність[22], а також ст. 15 Угоди про асоціацію між Україною, з од-

[16] Братюк (н 6) 422–3.
[17] Н Нагайчук, Н Третяк, О Ткаленко, 'Страхування в системі управління кібер-ризиками підприємства в умовах цифрової економіки' (2019) 1 Фінансовий простір 98–9.
[18] Мамонова (н 9) 91.
[19] Нагайчук, Третяк, Ткаленко (н 17) 101–2.
[20] Про страхування: Закон України від 7 березня 1996 р. № 85/96-ВР <https://zakon.rada.gov.ua/laws/show/85/96-%D0%B2%D1%80> (дата звернення: 15.06.2021).
[21] Конвенція про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 р. № 108 <https://zakon.rada.gov.ua/laws/show/994_326> (дата звернення: 15.06.2021).
[22] Конвенція про кіберзлочинність від 21 листопада 2001 р. <https://zakon.rada.gov.ua/go/994_575> (дата звернення: 15.06.2021).

нієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони[23].

За своєю суттю зміст цих зобов'язань охоплює законодавче визначення вимог до страхувальників і страховиків у відносинах кіберстрахування, об'єкта кіберстрахування, критеріїв визначення кіберризиків, на які може спрямовуватися захист, вимог до здійснення відповідного виду страхування тощо.

За загальним правилом, закріпленим у ч. 1 ст. 5 Закону України "Про захист інформації в інформаційно-телекомунікаційних системах", якщо інше прямо не передбачено законом, обов'язок щодо забезпечення захисту інформації в інформаційно-телекомунікаційних системах покладається на їх власників, у порядку та на умовах, визначених у договорі, який укладається ними з володільцями інформації[24].

Наведена норма має важливе значення для вирішення питання про визначення страхувальника за договором кіберстрахування, оскільки вона проводить чітку лінію розмежування обов'язків щодо захисту інформаційно-телекомунікаційних систем та інформації, яка в них обробляється чи зберігається між власниками таких систем і володільцями інформації.

Закладений у нормах Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" підхід одержав свій розвиток у спеціальних нормах окремих законів, якими регулюються конкретні види правовідносин. Зокрема, це стосується володільців персональних даних, на яких Законом України "Про захист персональних даних" покладені обов'язки щодо створення належних умов для правомірної обробки і захисту персональних даних[25].

Таким чином, для визначення учасників відносин у сфері господарювання, які можуть набувати статус страхувальника у відносинах кіберстрахування, першочергове значення має виконання ними обов'язків власника інформаційної системи, бази даних або реєстру чи функцій володільця інформації, на які спрямовується дія конкретних кіберризиків.

Як комплексний, інтегрований об'єкт права, що поєднує в собі поряд з інформацією також інформаційні ресурси, національну інформаційну інфраструктуру та суспільні відносини, які складаються у процесі створення, використання, обробки й оновлення[26], інформаційна сфера

[23] Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони від 27 червня 2014 р. <https://zakon.rada.gov.ua/laws/show/984_011> (дата звернення: 15.06.2021).

[24] Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 р. № 80/94-ВР <https://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80> (дата звернення: 15.06.2021).

[25] Про захист персональних даних: Закон України від 1 червня 2010 р. № 2297-VI <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення: 15.06.2021).

[26] О Заярний, 'Інформаційна сфера як об'єкт адміністративно-правової охорони: деякі доктринальні та нормативні аспекти' (2016) 22 Журнал східноєвропейського права.

охоплює діяльність, яка пов'язана не лише зі створенням інформаційних об'єктів, а й для конкретних потреб. У зв'язку з цим особливого значення набуває факт створення або використання інформаційних об'єктів, на які спрямовані кіберризики для здійснення господарської діяльності чи управління нею.

Відповідно, страхувальником за договором кіберстрахування у сфері господарювання може бути суб'єкт господарювання або орган державної влади або місцевого самоврядування, наділений господарською компетенцією, який здійснює функції власника інформаційної системи, а також обов'язки володільця інформації, що створюється або використовується в цілях здійснення господарської діяльності, управління нею.

Істотний вплив на визначення як кола суб'єктів кіберстрахування, так і з'ясування його місця в системі засобів забезпечення господарського правопорядку відіграє об'єкт цього виду господарської діяльності.

Закон України "Про страхування"[27], як і правова доктрина, пов'язують зміст цього елементу страхування з майновим інтересом страхувальника (об'єктом страхування).

На нашу думку, страховий інтерес – це потреба страхувальника (застрахованої особи, вигодонабувача, іншої третьої особи) у захисті своїх правомірних майнових інтересів, які є підставою для виникнення страхового правовідношення[28].

Визначення поняття "майновий інтерес" як об'єкта страхування через правомірні потреби страхування має важливе правове і методологічне значення. Його сутність виявляється у встановленні причинно-наслідкових зв'язків між інтересами власників інформаційних систем, реєстрів, баз даних, володільців інформації та збитками, обумовленими настанням страхових випадків – проявом кіберризиків.

Похідний характер майнових інтересів страхувальників від змісту кіберризиків, що проявляються в наш час у сфері господарювання, актуалізує перед юридичною наукою потребу у детальному аналізі останнього поняття з позицій призначення кіберстрахування у механізмі забезпечення господарського правопорядку.

У науковій літературі неодноразово зверталася увага на поширену в Україні та більшості держав світу практику поєднання кіберзагроз з іншими ризиками при визначенні кола страхових випадків (кіберстрахування як інструмент управління підприємствами). Така практика зазнає критики з огляду на кілька факторів, зокрема: 1) оцінку кіберзагроз як похідних ризиків від групи інших страхових випадків; 2) спробу звуження можливих наслідків кіберризиків; 3) неврахування широкої групи

[27] Про страхування (н 20).

[28] Н Пацурія, 'Страховий інтерес: теоретичне обґрунтування та проблеми правового закріплення' (2011) 88 Вісник Київського національного університету імені Тараса Шевченка. Юридичні науки 33.

кіберзагроз, які традиційно залишаються поза страховими полісами й іншими страховими продуктами, які пропонуються на відповідному ринку фінансових послуг.

За своєю суттю кіберризики пов'язані з використанням комп'ютерного обладнання та програмного забезпечення як у (локальних) мережах, так і у мережі Інтернет загалом; у розрахунково-платіжних системах, системах електронної торгівлі, промислових системах управління; а також ризики, пов'язані з накопиченням, зберіганням і використанням особистих даних[29].

За такого підходу до розуміння сутності кіберризиків, на нашу думку, у значенні предмета кіберстрахування можуть розглядатися інформаційно-телекомунікаційні системи, технології, реєстри чи бази даних, а також інформація, включаючи конфіденційну, що перебуває у володінні суб'єктів господарювання або органів, наділених господарською компетенцією щодо управління цими об'єктами.

Таке уточнення має важливе методологічне значення для формування механізму кіберстрахування. Воно виявляється у конкретизації предмета й об'єкта кіберстрахування, виключенні з відповідних категорій тих інформаційно-телекомунікаційних систем і технологій, які не використовуються у господарській діяльності, а отже, не пов'язані з інтересами учасників відносин у сфері господарювання.

Нині у нормах законодавства України відсутнє визначення поняття "кіберризик".

Закон України "Про основні засади забезпечення кібербезпеки України" для позначення негативних обставин, явищ і процесів, які проявляються у межах кіберпростору, у ст. 1 сформулював визначення поняття "кіберзагроза". Згідно з нормативним визначенням це поняття визначається як:

> Наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів[30].

Через категорію "загроза кібербезпеки" цей Закон визначає поняття "кіберінцидент", під яким розуміється:

> Подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потен-

[29] Розвиток кіберстрахування як сегменту глобального страхового ринку (н 5).
[30] Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII <https://zakon.rada.gov.ua/go/2163-19> (дата звернення: 15.06.2021).

ційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів[31].

Із системного тлумачення змісту наведених визначень випливає, що поняттям "кіберзагрози" охоплюються як умисні, так і необережні дії чи бездіяльність, обставини природного і техногенного характеру, що проявляються у кіберпросторі внаслідок втручання в роботу інформаційно-телекомунікаційних систем, реєстрів, баз даних, блокування їх належного функціонування або доступу до них, чим фактично створюється небезпека для життєво важливих інтересів держави, суспільства, фізичних і юридичних осіб у кіберпросторі.

Отже, поняття "кіберзагроза" може розглядатись як видова категорія стосовно родового поняття "кіберризик". Адже, на відміну від кіберзагроз, кіберризики можуть виникати не лише внаслідок прояву кіберінцидентів, а й будь-яких інших обставин, факторів, процесів та явищ, настання яких у кіберпросторі може спричинити негативні наслідки для їх адресатів, а часто й усіх інших суб'єктів правовідносин, які реалізуються у відповідному сегменті кіберпростору.

Нині в юридичній літературі не було сформовано єдиного підходу до класифікації кіберризиків.

У дослідженні глобальних тенденцій інформаційної безпеки, станом на 2018 р., зазначено:

<…> керівники організацій, які використовують автоматизовані та роботизовані системи, відмітили усвідомлення значимості потенційних негативних наслідків кіберзагроз. У якості основного можливого результату кіберзагрози 40 % учасників опитування у світі назвали порушення операційної діяльності, 39 % – витік конфіденційних даних, 32 % – завдання шкоди якості продукції, 29 % – завдання фізичної шкоди майну та 22 % – завдання шкоди людському життю[32].

Згідно з іншим дослідженням уся система кіберризиків, які підпадають під кіберстрахування за сутнісними ознаками, поділена на такі види:

1. Втрата інформації або пошкодження інформаційно-комунікаційних систем. Цей ризик зазвичай проявляється при зламі пароля доступу або внаслідок *DDoS*-атаки.

[31] Про основні засади забезпечення кібербезпеки України (н 30).
[32] Посилення цифрового середовища проти кібер-загроз. Дослідження глобальних тенденцій інформаційної безпеки за 2018 рік: основні висновки (н 14).

2. Втрата вигоди в офлайн-страхуванні у зв'язку з незаконним втручанням у роботу комп'ютерних мереж.

3. Втрати від регрес-позовів власників даних при викраденні, розголошенні та використанні кіберзлочинцями їх персональних даних.

4. Кібервимагання через примушення до сплати (наприклад, *SMS*) за розблокування інформаційних систем або інформації. Цей вид ризику проявляється через блокування належної роботи комп'ютерних мереж унаслідок використання комп'ютерних вірусів.

5. Пошкодження програмного забезпечення або цілісності інформації[33].

Поряд із наведеною класифікацією, деякі дослідники запропонували поділ кіберризиків (кіберзагроз) за іншими критеріями.

Згідно з цим підходом виокремлюють такі види кіберризиків:

1. Ризик втрати інформації під час злому паролю доступу або внаслідок *DDoS*-атаки.

2. Ризик фінансових втрат від фішингових атак.

3. Ризик фінансових втрат через порушення роботи комп'ютерних систем.

4. Ризик фінансових втрат від кібершантажу або вірусного блокування комп'ютерних систем.

5. Ризик фінансових втрат через викрадення і розголошення персональних даних та інформації[34].

Існування в інформаційній сфері широкої групи кіберризиків, які супроводжують процедури здійснення господарської діяльності й управління нею, обумовлено характером протиправних дій чи бездіяльності, якими вони спричиняються, а також наслідками їх прояву для страхувальників.

Загальний підхід до визначення видів протиправних діянь, які можуть спричинити негативні наслідків для власників інформаційних систем і володільців інформації, закладений у ст. 1 Закону України "Про захист інформації в інформаційно-телекомунікаційних системах". Згідно з цим Законом до протиправних дій, що можуть викликати негативні наслідки для власників інформаційно-телекомунікаційних систем та володільців інформації, належать:

1. Блокування інформації в системі – дії, внаслідок яких унеможливлюється доступ до інформації в системі.

2. Виток інформації – результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї.

[33] Розвиток кіберстрахування як сегменту глобального страхового ринку (н 5).

[34] 'Страхування кіберризиків підприємств в умовах інтернету речей' <https://kon-insurance.mnau.edu.ua/files/work_2019/20.pdf> (дата звернення: 15.06.2021).

3. Знищення інформації в системі – дії, внаслідок яких інформація в системі зникає.

4. Несанкціоновані дії щодо інформації в системі – дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства.

5. Порушення цілісності інформації в системі – несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст[35].

На думку дослідників проблематики кіберстрахування:

> Кіберризики реалізують внаслідок настання таких подій:
> 1) Нецільові атаки (фішинг, кардинг, *sms*-шахрайство);
> 2) Цільові атаки (фінансове шахрайство, розкрадання баз даних, промислове шпигунство, *DDoS* атаки, вимагання);
> 3) Атаки зсередини (розкрадання, знищення інформації, сприяння цільовій атаці)[36].

Аналіз існуючих нормативних і доктринальних підходів до характеристики кіберризиків та протиправних діянь, які обумовлюють їхнє виникнення з позицій інтересів страхувальника, дає змогу нам констатувати, що їхній зміст не завжди охоплюється майновою сутністю, як це передбачено у ст. 1 Закону України "Про страхування"[37].

Це пов'язано з тим, що як предмет кіберстрахування, інформація, інформаційно-телекомунікаційні системи, технології, бази даних є немайновими об'єктами права власності[38].

У зв'язку з цим майновий інтерес страхувальника щодо предмету кіберстрахування зводиться лише до витрат, пов'язаних із розробленням, придбанням, експлуатацією та технічним захистом інформації, інформаційно-телекомунікаційних систем і баз даних. Натомість комерційна, історична, управлінська, мистецька, науково-освітня цінність предмета кіберстрахування залишається поза змістом інтересу страхувальника.

Окреслена проблема породжує окремі концептуальні труднощі при визначенні видів та розмірів страхового покриття за договорами кіберстрахування, які відповідають майновим інтересам страхувальників.

Закладаючи у главі 25 правові засади відшкодування збитків, ГК України у ч. 2 ст. 224 закріпив загальне правило, згідно з яким:

> Під збитками розуміються витрати, зроблені управненою стороною, втрата або пошкодження її майна, а також не одержані нею доходи, які

[35] Про захист інформації в інформаційно-телекомунікаційних системах (н 24).
[36] Страхування кіберризиків підприємств в умовах інтернету речей (н 34).
[37] Про страхування (н 20).
[38] О Заярний, 'Класифікація адміністративних інформаційних правопорушень, як метод наукового дослідження адміністративної деліктності та інструмент удосконалення адміністративно-деліктного законодавства' [2014] 4 (10) Адміністративне право і процес 93.

управнена сторона одержала б у разі належного виконання зобов'язання або додержання правил здійснення господарської діяльності другою стороною[39].

Виходячи зі змісту наведеної норми ГК України, кіберстрахуванням повинні охоплюватися як реальні втрати суб'єкта господарської діяльності чи органу наділеного господарською компетенцією, так і неодержані доходи, якщо їх одержання від використання інформаційно-телекомунікаційних систем, реєстрів чи технологій прямо випливає з мети діяльності таких суб'єктів, або прийнятих ними зобов'язань.

Ґрунтуючись на цій авторській позиції та спираючись на дію норми, закріпленої у ч. 1 ст. 225 ГК України, можна запропонувати таку систему збитків, які охоплюються страховим покриттям і відповідають змісту поняття "об'єкт кіберстрахування":

1. Вартість втраченого або пошкодженого, знищеного внаслідок прояву кіберризиків майна (телекомунікаційного обладнання, комп'ютерної техніки, матеріальних носіїв інформації, засобів технічно захисту інформації).

2. Операційні витрати, пов'язані з розробленням та експлуатацією інформаційно-телекомунікаційних систем, технологій і реєстрів, які внаслідок кіберзагроз були виведені з експлуатації, а також витрати, пов'язані з відновленням їхнього належного функціонування.

3. Витрати страхувальника, пов'язані з використанням програмного забезпечення для технічного захисту інформації в інформаційно-телекомунікаційних системах і реєстрах, а також технічного захисту вказаних об'єктів від хакерських чи будь-яких інших кібератак.

4. Штрафні санкції, сплачені страхувальником іншим суб'єктам у зв'язку з невиконанням або неналежним виконанням господарських зобов'язань у зв'язку з проявом негативних наслідків кіберризиків.

5. Витрати понесені страхувальником у зв'язку з наданням технічної, правової або іншої допомоги з відновлення нормальної експлуатації інформаційно-телекомунікаційних систем, реєстрів чи технологій, що є предметом кіберстрахування.

6. Неодержаний прибуток (втрачена вигода), на який страхувальник міг розраховувати за нормальної експлуатації інформаційно-телекомунікаційних систем, реєстрів, технологій чи комп'ютерного обладнання, так само як і від правомірних інформаційних обмінів.

7. Матеріальна компенсація моральної шкоди, пов'язаної з репутаційними втратами страхувальника.

Таким чином, враховуючи характер кіберризиків, що проявляються у наш час у сфері господарювання, на нашу думку, обґрунтованим вба-

[39] Господарський кодекс України (н 11).

чається включення до майнових втрат страхувальника не лише фінансових витрат, пов'язаних із відновленням функціонування інформаційно-телекомунікаційних систем чи технологій, а й витрати, пов'язані з їхньою оцінкою як немайнових об'єктів інтелектуальної власності.

Вироблені у науковій літературі особливості кіберстрахування дають підстави розглядати його як окремий вид страхування, що виключає можливість страхування кіберризиків як похідної складової інших категорій страхових ризиків, визначених Законом України "Про страхування".

З позицій формування механізму реалізації в Україні цього виду страхової діяльності необхідним є визначення у нормах Закону України "Про страхування" спеціальних вимог до страховиків за договорами кіберстрахування.

Враховуючи характер і масштабність прояву наслідків кіберризиків, як правило, значні розміри страхового покриття за наслідками їх прояву, на наше переконання, законодавчі вимоги до страховиків за цим видом страхування мають бути аналогічними вимогам до страховиків життя і здоров'я людини. Поряд із цими вимогами, важливими умовами для надання страховим компаніям права здійснювати кіберстрахування є їхня здатність до забезпечення проведення незалежної фахової експертизи кіберризиків, включаючи оцінку стану технічного захисту інформації та заходів із забезпечення кібербезпеки у діяльності страхувальника. Оскільки кіберризики часто мають транснаціональний прояв, важливо, щоб страховик мав міжнародне підтвердження власної фінансової спроможності до покриття страхового відшкодування, а також належну ділову репутацію на відповідному ринку страхових послуг.

Вироблені теорією страхового права правові, економічні та методологічні передумови для виділення кіберстрахування в окремий вид страхової діяльності вимагають визначення напрямів подальшого розвитку цього виду діяльності.

Висновки. Проведене дослідження поняття та механізму реалізації кіберстрахування дає підстави констатувати, що нині в Україні сформувалися необхідні передумови для виокремлення відповідного виду страхування в окремий вид господарської діяльності в межах видового поняття страхування. За результатами дослідження можна сформулювати такі основні науково-теоретичні висновки та практичні рекомендації:

1. Як засіб забезпечення господарського правопорядку, кіберстрахування виступає особливим механізмом захисту інтересів власників інформаційно-телекомунікаційних систем, реєстрів чи технологій, володільців інформації від кіберризиків, відновлення їхнього майнового стану та репутації у зв'язку з їх проявом.

2. За своєю суттю кіберризики в господарській діяльності проявляються через конкретні процеси, дії та явища, які спрямовані на несанкціонований доступ до інформації або інформаційних ресурсів, блокування доступу чи їх знищення, зміну вихідного програмного коду шляхом хакерських атак, використання шкідливого програмного забезпечення, патентного тролінгу тощо, що спричиняють негативні наслідки для суб'єктів господарювання чи органів, наділених господарською компетенцією.

3. Кіберстрахування як вид страхової діяльності характеризується спеціальним суб'єктним складом (страховиками та страхувальниками), об'єктом (інтересами власників інформаційно-телекомунікаційних систем, реєстрів і баз даних, а також володільців інформації) та предметом (власне самими інформаційно-телекомунікаційними системами, реєстрами, базами даних, інформацією, на яку спрямовані кіберризики), що вказує на необхідність визнання на законодавчому рівні за цим видом страхування значення окремого виду діяльності на ринку страхових послуг.

4. Враховуючи немайнову сутність предмета кіберстрахування та зважаючи на зміст інтересів страхувальників за цим видом страхування, страхове відшкодування повинно охоплювати не лише реальні втрати від кіберризиків, а й неодержані доходи, за умови, якщо, за загальним правилом, страхувальник мав право на їхнє одержання. При цьому важливо, щоб при формуванні страхових програм (продуктів) із кіберстрахування, страхове відшкодування покривало, поряд із майновими, і немайнові втрати.

5. З огляду на обґрунтовані у цій статті особливості кіберстрахування, актуальним вбачається внесення окремих змін та доповнень до Закону України "Про страхування", зокрема, в частині визначення нормативних вимог до страховиків і страхувальників, об'єкта та предмета кіберстрахування, умов страхового відшкодування, процедур проведення експертизи кіберризиків за дорученням страховиків тощо.

6. Оскільки значна група інформаційно-телекомунікаційних систем і публічних реєстрів безпосередньо використовуються для потреб національної економіки, важливою умовою забезпечення їхньої кібербезпеки є покладення на учасників відносин у сфері господарювання, які виконують від імені держави функції власника щодо цих інформаційних об'єктів, обов'язків щодо страхування ризиків, пов'язаних із їхнім створенням та експлуатацією.

7. З метою мінімізації наслідків кіберризиків на етапі проєктування та введення у промислову експлуатацію інформаційно-телекомунікаційних систем, реєстрів і баз даних актуальним вбачається поширення у межах національної інформаційної сфери практики встановлення

обов'язків для розробників інформаційних об'єктів, а після прийняття у експлуатацію для замовників таких об'єктів – страхування від майбутніх кіберризиків.

REFERENCES

Bibliography

Journal articles

1. Bratiuk V, 'Sutnist kiber-zlochyniv ta strakhovyi zakhyst vid kiber-ryzykiv v Ukraini' (2015) 9 Aktualni problemy ekonomiky 421–7 (in Ukrainian).
2. Nahaichuk N, Tretiak N, Tkalenko O, 'Strakhuvannia v systemi upravlinnia kiber-ryzykamy pidpryiemstva v umovakh tsyfrovoi ekonomiky' (2019) 1 Finansovyi prostir 98–9 (in Ukrainian).
3. Patsuriia N, 'Strakhovyi interes: teoretychne obgruntuvannia ta problemy pravovoho zakriplennia' (2011) 88 Visnyk Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. Yurydychni nauky 33 (in Ukrainian).
4. Prykaziuk N, Humeniuk L, 'Kiber-strakhuvannia yak vazhlyvyi instrument zakhystu pidpryiemstv v umovakh tsyfrovizatsii ekonomiky' (2020) 4 Efektyvna ekonomika (in Ukrainian).
5. Seliverstova L, Trukhan D, 'Pidkhody do rozvytku kiberstrakhuvannia yak sehmentu hlobalnoho strakhovoho rynku' (2020) 1 Ekonomika ta derzhava 25 (in Ukrainian).
6. Zaiarnyi O, 'Informatsiina sfera yak ob'iekt administratyvno-pravovoi okhorony: deiaki doktrynalni ta normatyvni aspekty' (2016) 22 Zhurnal skhidnoievropeiskoho prava (in Ukrainian).
7. Zaiarnyi O, 'Klasyfikatsiia administratyvnykh informatsiinykh pravoporushen, yak metod naukovoho doslidzhennia administratyvnoi deliktnosti ta instrument udoskonalennia administratyvno-deliktnoho zakonodavstva' [2014] 4 (10) Administratyvne pravo i protses 93 (in Ukrainian).

Conference papers

8. Mamonova H, 'Osoblyvosti strakhuvannia kiber-ryzykiv' v *Materialy konferentsii MTsND* (2020) 91–3 (in Ukrainian).
9. Perceva S, 'Kiberstrahovanie v cifrovoj jekonomike' *Sovremennoe sostojanie i perspektivy razvitija rynka strahovanija: Materialy III Mezhdunarodnoj nauchno-prakticheskoj konferencii* (2018) 60–4 (in Russian).

Websites

10. Leslie Scism, 'Insurers Creating a Consumer Ratings Service for Cybersecurity Industry' (*The Wall Street Journal,* 26.03.2019) <https://www.wsj.com/articles/insurers-creating-a-consumer-ratings-service-for-cybersecurity-industry-11553592600> (accessed: 15.06.2021) (in English).
11. 'Kiberzlochyntsi u 2020 rotsi zavdaly u sviti zbytkiv na trylion dolariv: doslidzhennia' <https://www.dw.com/uk/kiberzlochyny-u-2020-rotsi-zavdaly-svitu-zbytkiv-na-trylion-dolariv-doslidzhennia/a-55857766> (accessed: 15.06.2021) (in Ukrainian).
12. 'Kolychestvennaia otsenka kyberryskov' *(Deloitte Touche Tohmatsu Limited)* <https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/risk/russian/cyber-risk-quantification.pdf> (accessed: 15.06.2021) (in Ukrainian).
13. 'Posylennia tsyfrovoho seredovyshcha proty kiber-zahroz. Doslidzhennia hlobalnykh tendentsii informatsiinoi bezpeky za 2018 rik: osnovni vysnovky' <https://www.pwc.com/ua/uk/survey/2018/pwc-2018-gsiss-strengthening-digital-society-against-cyber-shocks-ukr.pdf> (accessed: 15.06.2021) (in Ukrainian).

14. 'Rozvytok kiberstrakhuvannia yak sehmentu hlobalnoho strakhovoho rynku' <https://kon-insurance.mnau.edu.ua/files/work_2020/6.pdf> (accessed: 15.06.2021) (in Ukrainian).
15. 'Strakhuvannia kiberryzykiv pidpryiemstv v umovakh internetu rechei' <https://kon-insurance.mnau.edu.ua/files/work_2019/20.pdf> (accessed:15.06.2021) (in Ukrainian).
16. Tykhonka U, 'Osoblyvosti strakhuvannia kiber-ryzykiv' (*Stratehichni oriientyry*, 13.04.2021) <http://libfor.com/index.php?newsid=3898> (accessed: 15.06.2021) (in Ukrainian).

Nino Patsuriia
Oleh Zaiarnyi

CYBER INSURANCE AS A MEANS OF ENFORCEMENT OF ECONOMIC LAW ENFORCEMENT IN THE INFORMATION SPHERE: CONCEPTS, MECHANISM AND CONDITIONS OF IMPLEMENTATION

Abstract. The relevance of the study is due to the current level of manifestation of the negative consequences of cyber threats in the field of management, insufficient functional potential of traditional means of ensuring economic order in overcoming cyber risks.

In recent years, in Ukraine, similarly to most countries with developed economies, cyber insurance has been actively used to solve these problems.

The lack of proper legal regulation of cyber insurance activities in Ukraine, along with repeated attempts by insurers to introduce cyber risk insurance offers on the insurance services market within other, often incompatible types of insurance, also increase the relevance of the selected issues.

The purpose of this article is to study the concept, mechanism and conditions of cyber insurance as a means of ensuring economic order in the information sphere, formulating some proposals to improve Ukrainian legislation on relevant issues, as well as identifying areas for further research on this type of insurance.

Within the article, the authors formulate the definition of "cyber insurance", provide a detailed description of the tasks of the remedy, which it denotes. On this basis, cyber insurance is analyzed as a means of legal and economic protection of participants in economic relations from cyber risks and their consequences, as well as in terms of the type of economic activity.

Based on such scientific and legal positions, the authors analyzed in detail the elements of the mechanism of cyber insurance, identified elements of insurance relations in this area, including the insurer, the insured, the object and content of cyber insurance. Considerable attention is paid to cyber threats in the meaning of insured events, the main approaches to their scientific classification are considered, the main types of illegal acts that cause cyber risks are identified. Along with this, the authors of the article analyzed the content and essence of the property interests of insurers against cyber risks, described the main types of losses that are subject to compensation under cyber insurance contracts. In addition, the subject of special attention within the article were cyber insurance contracts, insurance programs as a means of implementing the mechanism of cyber insurance, identified their essential conditions and requirements for the parties.

The conclusions of the study identified areas for further improvement of Ukrainian legislation in the field of cyber insurance, characterized the legal requirements that insurers must meet for these activities. Along with this, the authors offer specific recommendations for determining the amount of insurance indemnity under cyber insurance contracts, suggested ways to strengthen the legal significance of cyber insurance in the system of economic law enforcement.

Keywords: economic law and order; information sphere; cyber threat; cyber risk; cyber insurance; insurer; insured.