DOI: 10.33663/0869-2491-2021-32-268-276
УДК 349

Н. Д. КРАСІЛІЧ,
кандидат юридичних наук, доцент[*]
ORCID: 0000-0002-8116-9515

ПРАВОВІ ПРОБЛЕМИ СТРАХОВОГО ЗАХИСТУ ВІД КІБЕРРИЗИКІВ У КОСМІЧНІЙ ДІЯЛЬНОСТІ

У статті досліджуються проблеми забезпечення захисту космічних інформаційних технологій від можливих кіберзагроз. Обґрунтовується необхідність подальшого розвитку особливого виду страхування – страхування кіберризиків як ефективного фінансово-правового механізму відшкодування збитків, зниження втрат, що виникли внаслідок кіберінцидентів у сфері космічної діяльності.

Ключові слова: *космічна діяльність, кібербезпека, кіберзагроза, страхування кіберризиків, кіберінцидент.*

Красилич Н. Д. **Правовые проблемы страховой защиты от киберрисков в космической деятельности**

В статье исследуются проблемы обеспечения защиты космических информационных технологий от возможных киберугроз. Обосновывается необходимость дальнейшего развития такого вида страхования – страхование киберрисков как эффективного финансово-правового механизма снижения убытков, возникающих вследствие киберинцидентов в сфере космической деятельности.

Ключевые слова: *космическая деятельность, кибербезопасность, киберугроза, страхование киберрисков, киберинцидент.*

Krasilich Nataliia. **Legal problems of insurance protection against cyber risks in space activities**

The article investigates the problems of ensuring the protection of space information technologies from possible cyber threats. The necessity of further development of a special type of insurance – cyber risk insurance, as an effective financial and legal mechanism for compensation of losses, reduction of losses caused by cyber incidents in the field of space activities is substantiated.

Key words: *space activity, cyber security, cyber threat, cyber risk insurance, cyber incident.*

Вступ (актуальність теми). Створення нових систем зв'язку, навігації та моніторингу як напрям розвитку космічних технологій завжди сприяв якісним змінам у житті людства. Значний сегмент сучасної космічної інфраструктури займають супутникові телекомунікації. Інформація з супутників активно використовується в різних сферах людської діяльності: науковій, економічній, військовій та ін. Зростають і інвестиції в космічні проекти та науково-дослідницькі програми. Поряд з тим космічна діяльність майже на будь-якому етапі її реалізації завжди характеризувалась підвищеним ризиком, наслідком якого можуть стати життя і здоров'я людей, а також значні збитки майнового характери, що виникають у разі аварій та катастроф. З появою і застосуванням новітніх інформаційних космічних технологій з'являються і нові ризики, які пов'язані із забезпеченням кібербезпеки в даній сфері.

[*] ***Krasilich Nataliia****, Candidate of Juridical Sciences (Ph. D.), Docent*

Отже, розвиток інформаційних технологій зумовив виникнення нових загроз, кіберзлочинність стала однією з головних проблем сучасного світу інформаційних технологій, які також безпосередньо стосуються і сфери космічної діяльності. За даними Allianz Global Corporate & Specialty інформаційні загрози (кіберзагрози) у 2019 р. уперше названі серед найбільш ризикових чинників, що спричиняють збої у діяльності бізнесу. У 2020 р. у зв'язку з пандемією COVID-19 та переривання бізнесу кіберзагрози перемістились на третю позицію, однак експерти вважають, що надалі кіберзагрози стануть більшою небезпекою, ніж у 2020 р. Експертна оцінка свідчить, що світова економіка втрачає більше одного відсотка світового ВВП, що на 50% більше, ніж два роки тому[1]. Тому загальні світові тенденції розвитку космічної діяльності значною мірою пов'язані з необхідністю забезпечення страхового захисту космічних інформаційних технологій від можливих кіберзагроз у даній сфері.

Огляд літератури. В юридичній літературі правові питання захисту інформаційних технологій саме в космічній діяльності практично не досліджувались. Окремі питання правового забезпечення захисту космічної інфраструктури досліджувались у роботах Н.Р. Малишевої, Л.В. Сороки, В.В. Семеняки, Г.Ю. Зубка, А.М. Гурової, О.С. Стельмах. Поряд з тим проблеми захисту інформації та інформаційних ресурсів у кіберпросторі набули відображення в роботах фахівців різних галузей права (адміністративного, кримінального інформаційного, цивільного та ін.) І.В. Арістової, П.Д. Біленчука, К.І. Бєлякова, М.С. Вертузаєва, О.М. Джужи, В.П. Ємельянова, Р.А. Калюжного, Б.А. Кормич, В.А. Ліпкана, А.І. Марущака, Г.В. Форос, В.С. Цимбалюка, О.О. Чернонога, В.І. Шакуна та ін. Однак організаційно-правові питання страхування кіберризиків як способу мінімізації збитків, завданих кібератаками, у сфері космічної діяльності, практично не розглядались. Переважно окремі питання розвитку страхування кіберризиків досліджували науковці економічного профілю В.П. Братюк, Е.Д. Семенова, С. Волосович, Ю. Кожедуб, Н.В. Приказюк, Т.П. Моташко та ін.

Постановка проблеми дослідження. Порушення процесу отримання та обміну інформацією за допомогою космічних систем може призвести до значних негативних наслідків. У зв'язку з цим питання забезпечення страхового захисту інформаційних технологій у сфері космічної діяльності потребує ґрунтовного опрацювання та розв'язання, оскільки існуючі механізми правового і державного регулювання на сьогодні не врегульовані в достатньому обсязі та потребують вирішення. Зрозуміло, що страхування кіберризиків не зможе забезпечити повний захист від кіберзлочинності, проте залучення страхових інструментів захисту майнових інтересів суб'єктів космічної діяльності є об'єктивною необхідністю і дасть змогу мінімізувати можливі збитки, завдані внаслідок кіберінциденту.

Прикладом системного підходу розв'язання проблем кібербезпеки у сфері космічної діяльності вважають досвід США. Так, відповідно до Директиви з космічної політики № 5 від 4 вересня 2020 р.[2] до власників та операторів космічних систем ставиться вимога розробляти та реалізовувати плани кібербезпеки, які, серед іншого, мають містити: а) захист від несанкціонованого доступу до критичних функцій, б) заходи фізичного захисту систем управління та телеметричного приймача; в) захист зв'язку за допомогою захищених передавачів приймання, шифрування, моніторингу потужності сигналу, г) захист наземних систем з метою зменшення ризику зараження шкідливим

програмним забезпеченням та зловмисного доступу до систем, у тому числі від інсайдерських загроз; д) прийняття практик гігієни кібербезпеки, фізичної безпеки автоматизованих інформаційних систем і методологій виявлення вторгнень до елементів системи, таких як інформаційні системи, антени, термінали, приймачі, маршрутизатори, пов'язані локальні та глобальні мережі і джерела живлення; е) управління ризиками всього ланцюга поставок; оцінка інших доступних заходів зменшення ризику[3]. Водночас вимоги щодо необхідності страхування кіберризиків даний документ не містить, отже, вирішення цього питання віддається на розсуд власників космічних систем.

Виклад основного матеріалу. Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція) 2001 р. стала найбільш визнаним міжнародно-правовим документом у сфері боротьби з міжнародною і національною кіберзлочинністю (ратифікована Україною 07.09.2006 р.). У преамбулі Конвенції встановлено, що вона є «необхідною для зупинення дій, спрямованих проти конфіденційності, цілісності та доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, як це описано в Конвенції, надання повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню, як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого і надійного міжнародного співробітництва»[4]. Починаючи з 2011 р., Україна бере участь у реалізації проекту Ради Європи та Європейського Союзу «Кіберзлочинність@Східне партнерство», метою якого якраз і є ефективна імплементація Будапештської конвенції, удосконалення національного законодавства в сфері боротьби з кіберзлочинністю, налагодження державно-приватного партнерства в цій сфері. Але, як зазначають фахівці, ця робота ведеться за зачиненими дверима, за дуже обмеженої кількості учасників, і тому дуже легко нівелюється законопроектами, які вносяться тими, хто не є долученим до цієї роботи[5].

У 2013 р. Європейським Союзом була ухвалена Стратегія кібербезпеки, в якій були передбачені заходи з таких напрямів: досягнення кіберстійкості; суттєве скорочення кіберзлочинності; розробка політики кібероборони, пов'язаної зі Спільною політикою безпеки і оборони; розвиток виробничих і технологічних ресурсів для кібербезпеки; створення узгодженої міжнародної політики кіберпростору для ЄС і просування основних цінностей ЄС[6]. А вже у 2016 р. на розвиток даної Стратегії Європейським Парламентом була прийнята Директива ЄС щодо заходів із забезпечення високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі, згідно з якою кожна держава–член ЄС зобов'язана розробити власну стратегію кібербезпеки та співпрацювати з ЄС та урядами країн–членів ЄС через спеціально створену директивою Групу співробітництва, офіційну підтримку якій зобов'язано надавати Європейське агентство із мережевої та інформаційної безпеки (ENISA), яке делегує до складу групи своїх представників разом із членами ЄС та представниками Єврокомісії[7].

В Україні основу національного законодавства про кібербезпеку складають закони України «Про інформацію»[8], «Про захист інформації в інформаційно-телекомунікаційних системах»[9], «Про національну безпеку України»[10], «Про основні засади забезпечення кібербезпеки України»[11], а також низка нор-

мативних актів, зокрема Стратегія національної безпеки України[12] (яка містить питання і стратегії кібербезпеки України[13]), Доктрина інформаційної безпеки України[14], Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури[15] та ін. Водночас спеціальні нормативні положення, що безпосередньо стосуються забезпечення кібербезпеки в космічній сфері відсутні. Так, у Законі України «Про космічну діяльність»[16] навіть не згадується про необхідність забезпечення кібербезпеки в даній сфері. Отже, в Україні хоча й існує відповідна законодавча база, яка передбачає посилення заходів з кібербезпеки, однак її реалізація через правові механізми недостатньо ефективна.

За статистичними підрахунками, кількість кібератак зростає з кожним роком. Кіберінциденти здатні завдавати значних фінансових і репутаційних збитків як окремим компаніям, так і економіці країн. Наприклад, в Україні лише за останні кілька років державні установи неодноразово були атаковані з кіберпростору. Так, за даними Державної служби спеціального зв'язку та захисту інформації України, тільки за період з 30 грудня 2020 р. по 05 січня 2021 р. система захищеного доступу державних органів до мережі Інтернет заблокувала 76 328 атак різних видів, що на 32% більше, ніж попереднього тижня. Переважна більшість – це мережеві атаки прикладного рівня (99%). Переважна більшість зафіксованих підозрілих подій стосується спроб викрадення інформації (38%), мережевого сканування (27%), спроб отримання прав користувача (13%) та спроб отримання прав адміністратора (12%)[17].

На сьогодні одним з правових способів захисту від негативних наслідків кіберзагроз, зокрема і сфері космічної діяльності, може бути страхування кіберризиків як фінансово-правовий механізм відшкодування збитків, зниження витрат, завданих кібератаками. Страхування кіберризиків – доволі новий вид страхування. Перші договори страхування кіберризиків були укладені ще у 2010–2011 рр. у США. Ця тема активно обговорювалась на щорічному форумі в Давосі у 2012 р. Однак активне зростання цього виду страхування почалося дещо пізніше, після масових зламів корпоративних і урядових ресурсів у США. Тому 90% ринку страхування кіберризиків припадає на саме на цю державу[18].

В Україні кіберстрахування перебуває на початковому етапі становлення та потребує розробки інноваційних підходів до подальшого розвитку, враховуючи накопичений позитивний досвід зарубіжних країн у цьому напрямі. Наразі момент страхові компанії тільки напрацьовують практику страхування кіберризиків, і такі договори страхування поодинокі, оскільки подібних стандартизованих продуктів не існує. Загалом договір страхування кіберризиків спрямований на відшкодування збитків, які можуть виникнути у страхувальника внаслідок витоку даних, виходу з ладу різного обладнання, а також інших кіберзагрозагроз.

Слід зазначити, що чинне законодавство України, зокрема Закон України «Про страхування»[19], не передбачають випадків страхування кіберризиків. У сфері космічної діяльності цим Законом передбачено лише обов'язкове страхування цивільної відповідальності суб'єктів космічної діяльності (п. 23 ст. 7) та страхування відповідальності щодо ризиків, пов'язаних з підготовкою до запуску космічної техніки на космодромі, запуском та експлуатацією її у космічному просторі (п. 25 ст. 7 Закону «Про страхування»). Певним чином страхування кіберризиків частково може бути віднесено на рахунок окремих видів добровільного страхування, якто страхування фінансових ризиків та інших видів (п. 18, п. 23 ст. 6 Закону «Про

страхування»). Однак слід зазначити, що характеристика та кваліфікаційні ознаки видів добровільного страхування, розроблена відповідно до ч. 5 ст. 6 Закону «Про страхування» (із подальшими змінами), також не містить положень щодо особливостей страхування кіберризиків[20].

Як зазначають фахівці, неготовність українського страхового ринку активно розвивати страхування кіберризиків зумовлена низкою причин: в Україні ще не сформований страховий ринок із страхування ризиків у цілому; обмежена кількість фахівців-страховиків у цій сфері; неготовність, недовіра потенційних страхувальників у саму можливість покриття кіберризиків страховиком; проблеми з отриманням необхідної інформації від потенційних страхувальників для складання програм страхування; фінансові причини, оскільки вартість страхового полісу може доходити до декількох десятків тисяч доларів[21]. В українських реаліях, а особливо це стосується сфери космічної діяльності, де більшість інформації засекречена і для цього є причини, далеко не завжди можна провести перевірку перед аудитом відповідної системи клієнта і, як результат, страховики не готові надавати повноцінні програми страхування кіберризиків. Крім того, значною перешкодою до укладення таких договорів страхування є висока вартість страхових програм, оскільки страховики працюють із недостатньою страховою статистикою.

В нинішніх умовах, як правило, питання страхування кіберризиків включається до комплексних договорів страхування майна, відповідальності, фінансових ризиків, що значно обмежує відшкодування завданих збитків, і основним страховим випадком вважаються збитки, які виникли внаслідок порушення роботи комп'ютерної мережі страхувальника або її систем безпеки, через втручання третіх осіб. В ідеалі договір страхування від кіберризиків максимально повинен покривати збитки страхувальника, завдані внаслідок кібератак, хоча на практиці всі ризики передбачити неможливою. Особливістю укладення договорів страхування кіберризиків – це визначення видів ризиків, які будуть покриватися таким договором. Так, на думку страхових експертів, виділяють такі групи ризиків: ризик втрати інформації страхувальником при порушенні роботи комп'ютерних систем; ризик фінансових втрат самого страхувальника при порушенні роботи комп'ютерних систем (наприклад, втрачена вигода); ризик фінансових втрат за регресними позовами (відповідальність перед третіми особами); ризик фінансових втрат на відновлення програмного забезпечення та інформації; ризик фінансових втрат за здирництвом при вірусному блокуванні комп'ютерних систем[22]. Крім того, у випадках кіберінцидентів можуть виникнути не тільки вищезгадані фінансові збитки, а й матеріальні збитки, пов'язані з пошкодженням техніки або взагалі знищенням.

Загалом збитки від кіберризиків, у більшості випадків, поділяють на три групи[2]. До першої групи входять прямі збитки, тобто витрати страхувальника на відновлення пошкодженої інфраструктури (наприклад, придбання нового обладнання, відновлення пошкодженого), усунення прогалин у системі кібербезпеки страхувальника, що стали причиною виникнення кіберінциденту, витрати на відновлення втраченої інформації, витрати на послуги спеціалістів, залучених для оперативного реагування на кіберінцидент.

До другої групи слід віднести збитки внаслідок відповідальності страхувальника перед третіми особами. В даному випадку відшкодуванню можуть підлягати матеріальні збитки, моральна шкода, а також збитки за порушення прав інтелектуальної власності тощо. Слід зазначити, що факт настання страхового випадку

відповідальності перед третіми особами підтверджується рішенням суду, при цьому страховик не несе відповідальності за грубі порушення співробітниками компанії страхувальника вимог з кібербезпеки, за шахрайські дії страхувальника і дії його співробітників, які викликані їх недостатньою кваліфікацією.

До третьої групи віднесено витрати на так званий кризовий менеджмент, тобто витрати на розслідування кіберінциденту (залучення експертів з кібербезпеки, консультантів, юристів для мінімізації витрат на усунення негативних наслідків та ін.). До речі, останні страхові ризики не завжди включаються до страхових програм договорів.

Основною складністю в процесі відшкодування збитків за договором страхування кіберризиків є фіксація факту страхового випадку, розмір завданих збитків і доведення причинно-наслідкового зв'язку між страховим випадком і заявленими збитками, оскільки суму збитків необхідно не тільки підрахувати, а й документально підтвердити. У цих випадках проводиться відповідна експертиза, яка має довести або спростувати факт настання страхового випадку.

Зрозуміло, що сам факт укладення договору страхування кіберризиків не може забезпечити захист від можливих кіберзагроз, але може гарантувати страхувальникам відшкодування завданих йому збитків. І хоча на сьогодні в Україні не існує належної нормативно-правової бази страхування кібіррізиків, а також алгоритмів їх оцінювання, але Закон України «Про основні засади забезпечення кібербезпеки України» містить визначення основних термінів, на основі яких може визначатись ідентифікація майбутніх загроз у конкретному договорі та в майбутньому при настанні страхового випадку страхувальник отримає відповідне страхове відшкодування.

Висновки. Таким чином, розвиток інституту страхування кіберризиків є перспективним напрямом розвитку страхового ринку в Україні, а також складовою забезпечення кібербезпеки. На жаль, в Україні практично нерозвинений такий вид страхування, він перебуває на початковому етапі свого становлення. Його розвиток потребує відповідного правового врегулювання, державного стимулювання, інноваційного підходу з урахуванням досвіду розвинутих країн світу. Зокрема, цьому процесу може сприяти державно-приватна взаємодія у сфері кібербезпеки. Так, Законом України «Про правові засади забезпечення кібербезпеки України» передбачено періодичне проведення національного саміту з професійними постачальниками бізнес-послуг, включаючи страховиків, аудиторів, юристів, визначення їхньої ролі у сприянні кращому управлінню ризиками у сфері кібербезпеки. Це може стати важливим кроком у напрямі створення відповідних умов у країні для розвитку індустрії кібербезпеки, складовою якої має страховий захист інформаційних технологій у сфері космічної діяльності.

Космічні інформаційні технології, які все більше проникають в економічні і соціальні процеси, зумовлюють необхідність розвитку сегмента кіберстрахування також у сфері космічної діяльності, який забезпечуватиме відповідний страховий захист і відшкодування збитків для компенсації витрат страхувальнику внаслідок виникнення кіберінцидентів та кібератак. Питання страхування кіберризиків повинні знайти своє адекватне відображення в національному законодавстві. Наприклад, у Законі України «Про страхування» необхідно чітко визначити сутність та особливості страхування кіберризиків, місце цього виду в системі страхування, механізми його застосування та ін.

1. ALLIANZ RISK BAROMETER: Identifying the major business risk for 2021. URL: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2021.pdf **2.** Memorandum on Space Policy Directive-5–Cybersecurity Principles for Space Systems. Issued on: September 4, 2020. URL: https://www.whitehouse.gov/wp-content/uploads/2020/09/2020SPD5.mem.pdf **3.** Малишева Н.Р., Гурова А.М. Правові засади кібербезпеки космічної діяльності в США: досвід для України. *Часопис Київського університету права*. 2020. № 3. С. 327–328. **4.** Конвенція про кіберзлочинність від 23.11.2001 р., ратифікована Україною 1-.03.2000 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text. **5.** Кольцов М., Приходько О., Аушев Є. Пропозиції щодо реформування сфери кібербезпеки в Україні. 2017. URL: http://eump.org/media/2019/Policy-Paper_Kiberbezpeka-1-1.pdf **6.** Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, 7.2.2013. URL: http://eur-lex.europa.eu/legalcontent/EN/TXT/?qid=1493795785820&uri=CELEX:52013JC0001 **7.** 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. URL: http://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01. **8.** Про інформацію: Закон України від 2.10.2002 р. № 2657-XII. Дата оновлення: 16.07.2020. URL: https://zakon.rada.gov.ua/laws/main/2657-12#Text **9.** Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5.08.1994 р.№ 80/94-ВР. Дата оновлення: 4.07.2020. URL: https://zakon.rada.gov.ua/laws/main/80/94-%D0%B2%D1%80#Text **10.** Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII. Дата оновлення: 24.10.2020 р. URL: https://zakon.rada.gov.ua/laws/main/2469-19#Text **11.** Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. Дата оновлення: 24.10.2020 р. URL: https://zakon.rada.gov.ua/laws/ show/2163-19 **12.** Стратегія національної безпеки України: затверджена Указом Президента України від 14.09.2020 р. № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037 **13**. Фахівці Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України розпочали розробку Стратегії кібербезпеки України. URL: https://www.unn.com.ua/uk/news/1893395-rnbo-rozpochala-rozrobku-strategiyi-kiberbezpeki-ukrayini-danilov **14.** Доктрина інформаційної безпеки України: затверджена Указом Президента України від 25.02.2017 р. № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text **15.** Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури. Затверджено постановою Кабінету Міністрів 19.06.2019 № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text **16.** Про космічну діяльність: Закон України від 15.10.1996 р. № 502/96-ВР. Дата оновлення: 24.10.2020 р. URL: https://zakon.rada.gov.ua/laws/main/502/96-%D0%B2%D1%80#Text **17**. В Україні зростає кількість кібератак. URL: https://www.epravda.com.ua/news/2021/01/6/669777/ **18.** Селіверстова Л.С., Трухан Д.А. Підходи до розвитку кіберстрахування як сегменту глобального страхового ринку. *Економіка і держава*. 2020. № 1. С. 23–27. URL: http://www.economy.in.ua/pdf/1_2020.pdf **19.** Про страхування: Закон України від 7.03.1996 № 85/96-ВР. Дата оновлення:10.12.2020. URL: https://zakon.rada.gov.ua/laws/main/85/96-%D0%B2%D1%80#Text **20.** Характеристика та кваліфікаційні ознаки видів добровільного страхування, затверджена розпорядженням Державної комісії з регулювання ринків фінансових послуг України від 09.07.2010 № 1119/18414. Дата оновлення: 7.04.2020 р. URL: https://zakon.rada.gov.ua/laws/show/z1119-10#n17 **21.** Єрмакова О.О. Страхування інформаційних ризиків. *Ризики нестабільності: безпека і управління*: зб. матеріалів міждисциплінар. наук.-практ. конф., Київ, 16 березня 2018 р. URL: http://futurolog.com.ua/publish/8/Zbirnyk.pdf **22**. Розвиток кіберстрахування як сегменту глобального страхового ринку. URL: https://kon-insurance.mnau.edu.ua/files/work_2020/6.pdf **23**. Пігулка від хакерів: як бізнес захищає себе від кібератак. URL: https://mind.ua/publications/20192978-pigulka-vid-hakeriv-yak-biznes-zahishchae-sebe-vid-kiberatak

References

1. ALLIANZ RISK BAROMETER: Identifying the major business risk for 2021. URL: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2021.pdf **2.** Memorandum on Space Policy Directive-5 – Cybersecurity Principles for Space Systems. Issued on: September 4, 2020. URL: https://www.whitehouse.gov/wp-content/uploads/2020/09/2020SPD5.mem.pdf **3.** Malysheva N.R., Ghurova A.M. Pravovi zasady kiberbezpeky kosmichnoji dijaljnosti v SShA: dosvid dlja Ukrajiny. *Chasopys Kyjivsjkogho universytetu prava*. 2020. №3, S. 327–328. [ukr]. **4.** Konvencija pro kiberzlochynnistj vid 23.11.2001 r., ratyfikovana Ukrajinoju 1-.03.2000 r. URL: http://zakon.rada.gov.ua/laws/show/994_575#Text. [ukr]. **5.** Koljcov M., Prykhodjko O., Aushev Je. Propozyciji shhodo reformuvannja sfery kiberbezpeky v Ukrajini. 2017. URL: http://eump.org/media/2019/Policy-Paper_Kiberbezpeka-1-1.pdf [ukr]. **6.** Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, 7.2.2013. URL: http://eur-lex.europa.eu/legalcontent/EN/TXT/?qid=1493795785820&uri=CELEX:52013JC0001 **7.** 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. URL: http://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01. **8.** Pro informaciju: Zakon Ukrajiny vid 2.10.2002 r. № 2657-XII. Data onovlennja: 16.07.2020. URL: https://zakon.rada.gov.ua/laws/main/2657-12#Text [ukr]. **9.** Pro zakhyst informaciji v informacijno-telekomunikacijnykh systemakh: Zakon Ukrajiny vid 5.08.1994 r. № 80/94-VR. Data onovlennja: 4.07.2020. URL: https://zakon.rada.gov.ua/laws/main/80/94-%D0%B2%D1%80#Text [ukr]. **10.** Pro nacionaljnu bezpeku Ukrajiny: Zakon Ukrajiny vid 21.06.2018 r. № 2469-VIII. Data onovlennja: 24.10.2020 r. URL: https://zakon.rada.gov.ua/laws/main/2469-19#Text [ukr]. **11.** Pro osnovni zasady zabezpechennja kiberbezpeky Ukrajiny: Zakon Ukrajiny vid 05.10.2017 № 2163-VIII. Data onovlennja: 24.10.2020 r. URL: https://zakon.rada.gov.ua/laws/ show/2163-19 [ukr]. **12.** Strateghija nacionaljnoji bezpeky Ukrajiny: zatverdzhena Ukazom Prezydenta Ukrajiny vid 14.09.2020 r. № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037 [ukr]. **13.** Fakhivci Nacionaljnogho koordynaciy̆nogho centru kiberbezpeky pry Radi nacionaljnoji bezpeky i oborony Ukraïny rozpochaly rozrobku Strateghiji kiberbezpeky Ukrajiny. URL: https://www.unn.com.ua/uk/news/1893395-rnbo-rozpochala-rozrobku-strategiyi-kiberbezpeki-ukrayini-danilov [ukr]. **14.** Doktryna informacijnoji bezpeky Ukrajiny: zatverdzhena Ukazom Prezydenta Ukrajiny vid 25.02.2017 r. № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text [ukr]. **15.** Zaghaljni vymoghy do kiberzakhystu ob'jektiv krytychnoji infrastruktury. Zatverdzheno postanovoju Kabinetu Ministriv 19.06.2019 № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text [ukr]. **16.** Pro kosmichnu dijaljnistj: Zakon Ukrajiny vid 15.10.1996 r. № 502/96-VR. Data onovlennja: 24.10.2020 r. URL: https://zakon.rada.gov.ua/laws/main/502/96-%D0%B2%D1%80#Text [ukr]. **17.** V Ukrajini zrostaje kiljkistj kiberatak. URL: https://www.epravda.com.ua/news/2021/01/6/669777/ [ukr]. **18.** Seliverstova L.S., Trukhan D.A. Pidkhody do rozvytku kiberstrakhuvannja jak seghmentu ghlobaljnogho strakhovogho rynku. *Ekonomika i derzhava,* 2020. № 1. S. 23–27. URL: http://www.economy.in.ua/pdf/1_2020.pdf [ukr]. **19.** Pro strakhuvannja: Zakon Ukrajiny vid 7.03.1996 № 85/96-VR. Data onovlennja: 10.12.2020. URL: https://zakon.rada.gov.ua/laws/main/85/96-%D0%B2%D1%80#Text [uk]. **20.** Kharakterystyka ta kvalifikacijni oznaky vydiv dobroviljnogho strakhuvannja, zatverdzhena rozporjadzhennjam Derzhavnoji komisiji z reghuljuvannja rynkiv finansovykh poslugh Ukrajiny vid 09.07.2010 № 1119/18414. Data onovlennja: 7.04.2020 r. URL: https://zakon.rada.gov.ua/laws/show/z1119-10#n17 [ukr]. **21.** Jermakova O.O. Strakhuvannja informacijnykh ryzykiv. *Ryzyky nestabiljnosti: bezpeka i upravlinnja*: zb. materialiv mizhdyscyplinar. nauk.-prakt. konf., Kyiv, 16 bereznja 2018 r. URL: http://futurolog.com.ua/publish/8/Zbirnyk.pdf [ukr]. **22.** Rozvytok kiberstrakhuvannja jak seghmentu ghlobaljnogho strakhovogho rynku. URL: https://kon-insurance.mnau.edu.ua/files/work_2020/6.pdf [ukr]. **23.** Pighulka vid khakeriv: jak biznes zakhyshhaje sebe vid kiberatak. URL: https://mind.ua/publications/20192978-pigulka-vid-hakeriv-yak-biznes-zahishchae-sebe-vid-kiberatak [ukr].

Krasilich Nataliia. **Legal problems of insurance protection against cyber risks in space activities**

General global trends in space activities are largely related to the need to protect space information technology from possible cyber threats. The issue of cybersecurity in space activities needs to be thoroughly studied and resolved, as the current state of space activities and existing mechanisms of international and state regulation do not provide a sufficient solution.

Disruption of the process of receiving and exchanging information through space information systems can lead to significant consequences. The growing number of cyber threats is becoming more common and destructive. Therefore, the assessment of cyber vulnerabilities in space systems is an important task that must be addressed both at the stage of creation and development, and in the operation of such systems. This, in turn, requires the availability of tools to address the above tasks and qualified personnel.

One of the legal ways to protect against the negative effects of cyber threats, including in the field of space activities, may be cyber risk insurance, as a financial and legal mechanism for compensation, loss of losses caused by cyber attacks. In Ukraine, cyber insurance is in its infancy and needs to develop innovative approaches to further development, taking into account the accumulated positive experience of foreign countries in this area. At the moment, insurance companies are only developing the practice of cyber risk insurance and such insurance contracts are isolated.

In the current environment, as a rule, the issue of cyber risk insurance is included in comprehensive property insurance contracts, liability insurance, financial risks, which significantly limits the compensation of damages. The main difficulty in the process of indemnification under a cyber risk insurance contract is to record the fact of the insured event, the amount of damage and prove the causal link between the insured event and the claimed losses, as the amount of damage must not only be calculated but also documented.

Space information technologies, which are increasingly penetrating economic and social processes, necessitate the development of a segment of cyber insurance in the field of space activities, which will provide adequate insurance protection and compensation for damages to the insured due to cyber incidents. Cyber risk insurance issues should be reflected in national legislation.

Key words: *space activity, cyber security, cyber threat, cyber risk insurance, cyber incident.*

DOI: 10.33663/0869-2491-2021-32-276-287
УДК 349.41

О. А. ПОЛІВОДСЬКИЙ**,**
кандидат юридичних наук, доцент[*]
ORCID: 0000-0002-9900-8664

ЕЛЕКТРОННА ФОРМА ДОГОВОРУ: ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ У СФЕРІ ПЕРЕХОДУ ПРАВ НА ЗЕМЛЮ ТА ІНШУ НЕРУХОМІСТЬ

Стаття присвячена питанням застосування електронної форми договору у сфері обороту нерухомості. Автор аналізує ризики, що пов'язані з застосуванням електронної форми договору, літературу, яка стосується порушеного питання, законодавство та судову практику України, надає пропозиції щодо уникнення ризиків та вдосконалення законодавства у цій сфері. Автор обґрунтовує та пропонує: перелік вимог до електронних документів, яким вони мають відповідати; на рівні закону слід визнати, що ЕП, інші засоби ідентифікації, файли та паролі повинні бути предметом правової охорони у кримінальному законодавстві;

[*] ***Polivodskyi Oleksandr,*** *Candidate of Juridical Sciences (Ph. D.), Docent*