

DOI <https://doi.org/10.18524/2411-2054.2025.60.349160>

УДК 347.764

В. В. Борщенко, кандидат юридичних наук, доцент
Одеський національний університет імені І. І. Мечникова
Кафедра конституційного права та правосуддя
Французький бульвар, 24/26, Одеса, 65058, Україна
e-mail: vladlena.1128@inbox.lv
ORCID iD: <https://orcid.org/0000-0001-9819-092X>

ПРАВО НА КІБЕРБЕЗПЕКУ СТРАХУВАЛЬНИКА: НОВІ СТАНДАРТИ ТА ЇХ ВПЛИВ НА СТРАХОВІ ПОСЛУГИ

У статті досліджується право страхувальника на кібербезпеку як ключовий елемент страхового права в умовах стрімкої цифрової трансформації економіки та зростання масштабів кіберзагроз. Показано, що розвиток інформаційно-комунікаційних технологій, зокрема Big Data, штучного інтелекту, блокчейну та хмарних обчислень, забезпечує підвищення ефективності управління й оптимізацію бізнес-процесів, водночас створюючи нові вразливості та економічні ризики. У таких умовах право страхувальника на кібербезпеку виступає важливим правовим механізмом захисту від цифрових загроз і стимулює запровадження нових стандартів оцінки й управління кіберризиками.

Проаналізовано розвиток ринку кіберстрахування, зокрема його зародження у США на початку 2010-х років, коли страхові компанії почали реагувати на зростання випадків витоку даних та кібератак, формуючи продукти для фінансової компенсації збитків. Запроваджені практики стали основою для міжнародного розвитку кіберстрахування та визначили стандарти організації страхових продуктів. Особливу увагу приділено морській галузі, де цифровізація, автоматизація суднового управління та впровадження електронних логістичних платформ трансформують традиційні страхові ризики в гібридні, поєднуючи майнові, операційні та інформаційно-технологічні загрози. Це потребує перегляду підходів до оцінки ризиків і формування страхового покриття в умовах цифрових реалій.

Висвітлено проблеми українського ринку кіберстрахування, зокрема відсутність належного нормативного регулювання, недостатню стандартизацію кіберризиків та низький рівень страхової активності потенційних страхувальників. Показано, що реалізація права на кібербезпеку сприяє посиленню превентивної функції страхування, захисту цифрових активів, інформаційних ресурсів і безперервності бізнес-процесів, а також формуванню партнерської моделі співпраці між страховиком і страхувальником.

Зроблено висновок, що право страхувальника на кібербезпеку є системоутворюючим у страхових правовідносинах, визначає зміст страхових послуг, умови договорів та характер взаємодії сторін. Його розвиток потребує вдосконалення нормативно-правового регулювання, гармонізації з міжнародними стандартами кібербезпеки та розвитку доктринальних основ страхового права для забезпечення балансу між інноваційним розвитком страхових послуг і захистом прав страхувальників у цифровій економіці.

Ключові слова: страхове право, кіберстрахування, кіберінциденти, цифрові права, новітні права, торговельне мореплавство, безпека мореплавства, кіберзагроза, кіберризик, управління кіберризиком, кібербезпека, страховий ризик.

Постановка проблеми. Стрімкий розвиток інформаційно-комунікаційних технологій та цифрова трансформація ключових сфер економічної діяльності зумовлюють формування нових можливостей для інноваційного зростання, оптимізації бізнес-процесів і підвищення конкурентоспроможності суб'єктів господарювання. Водночас широке впровадження цифрових рішень супроводжується зростанням масштабів і складності кіберзагроз, які створюють істотні ризики для стабільності функціонування інформаційної інфраструктури держави та приватного сектору. Використання технологій Big Data, штучного інтелекту, блокчейну та хмарних обчислень, крім безумовних переваг, породжує і нові форми вразливостей, що можуть призводити до значних економічних збитків та порушення конфіденційності даних.

У цьому контексті особливого значення набуває право страхувальника на кібербезпеку, яке трансформується у важливий правовий інструмент забезпечення захищеності в умовах цифрової економіки. Реалізація цього права безпосередньо впливає на зміст, якість та інноваційність страхових послуг, стимулюючи запровадження нових стандартів оцінювання й управління кіберризиками.

Попри зростаючий попит на страхування від кіберзагроз, український ринок кіберстрахування перебуває на початковому етапі розвитку та характеризується відсутністю належного нормативного регулювання. Невизначеність правової природи кіберризиків, нестача єдиних стандартів його ідентифікації, а також недостатній рівень страхової активності потенційних споживачів істотно стримують становлення цього виду страхування.

Таким чином, актуальність дослідження обумовлюється потребою у всебічному та системному аналізі права страхувальника на кібербезпеку, а також визначенні його ролі та значення у трансформації і розвитку сучасного страхового ринку.

Аналіз останніх досліджень і публікацій. Значний науковий внесок у дослідження різних аспектів страхування кіберризиків здійснили В. П. Братюк, Е. Д. Семенова, С. Волосович, Ю. Кожедуб, Н. В. Приказюк та інші вчені, однак актуальність теми залишається високою з огляду на низький рівень страхової активності потенційних постраждалих від кіберінцидентів і недостатній розвиток відповідних страхових продуктів.

Метою цієї наукової праці є дослідження права на кібербезпеку страхувальника.

Виклад основного матеріалу. Перші спроби запровадження спеціалізованих страхових продуктів, спрямованих на покриття кіберризиків, були здійснені у Сполучених Штатах Америки ще на початку 2010-х років [1]. Саме на цьому етапі американські страхові компанії почали усвідомлювати зростання загроз, пов'язаних із масовою цифровізацією бізнес-процесів, і необхідність створення інструментів фінансового компенсування витрат, спричинених кіберінцидентами. Розвиток перших страхових програм відбувався у відповідь на збільшення кількості випадків витоку даних, кібератак на корпоративні мережі та підвищення регуляторних вимог щодо захисту персональної інформації.

Запроваджені у США продукти кіберстрахування стали основою для формування ринку, який згодом почав активно розширюватися, охоплюючи нові види ризиків від атак типу ransomware до порушень у функціонуванні хмарних

сервісів та критичних інформаційних систем. Цей досвід заклав підґрунтя для подальшого міжнародного розвитку сегмента кіберстрахування та визначив базові стандарти його практичної організації. У сучасних умовах цифрової трансформації економіки дедалі більша кількість сфер господарської діяльності зазнає глибокої цифровізації, що, з одного боку, підвищує ефективність управління, швидкість обміну інформацією та рівень автоматизації виробничих і логістичних процесів, а з іншого – істотно підвищує вразливість таких сфер до кіберризиків. Так, «завдані у 2020 році збитки від кіберзагроз і кіберінцидентів є на 50 відсотків вищими, ніж у 2018 році» [2]. Практично всі сегменти економіки, інтегровані в цифрові інформаційні системи, опиняються під впливом загроз, пов'язаних із несанкціонованим доступом до даних, порушенням функціонування інформаційних ресурсів, втручанням у роботу автоматизованих систем і втратою цифрових активів.

Цікаво звернути увагу, наприклад, на галузь торговельного мореплавства. Вона тривалий час залишалася відносно консервативною галуззю, у якій процеси цифровізації впроваджувалися повільно та фрагментарно. Водночас сучасний етап розвитку міжнародної торгівлі та морського транспорту характеризується активним упровадженням цифрових технологій, автоматизованих систем управління суднами, електронних навігаційних комплексів і цифрових логістичних платформ.

У таких умовах цифровізація торговельного мореплавства зумовлює суттєву трансформацію традиційного страхового ризику. Класичні ризики, притаманні морському страхуванню, доповнюються новими загрозами інформаційно-технологічного характеру, пов'язаними з функціонуванням інформаційно-комунікаційних систем, обробкою та передачею даних, а також із можливістю втручання в цифрові процеси управління судноплавством. Це об'єктивно потребує переосмислення усталених підходів до оцінки страхових ризиків і формування страхового захисту в умовах цифрової трансформації мореплавної галузі.

Використання електронних навігаційних систем, автоматизованих засобів управління суднами, цифрових платформ логістики й електронного документообігу зумовлює появу нових загроз, які не вкладаються у класичні моделі морських ризиків. Кіберінциденти у вигляді несанкціонованого доступу до навігаційних систем, втручання в роботу судового програмного забезпечення, маніпулювання даними про вантаж або маршрут, блокування інформаційних систем портової інфраструктури здатні призводити не лише до майнових втрат, а й до порушення безпеки судноплавства, зупинки торговельних операцій та міжнародних ланцюгів постачання.

У зв'язку із цим страховий ризик у сфері торговельного мореплавства набуває гібридного характеру, поєднуючи в собі елементи традиційного морського ризику й інформаційно-технологічного ризику. Цифровізація змінює саму природу страхового інтересу: об'єктом страхового захисту стають не лише судно, вантаж чи фрахт, а й цифрові активи, інформаційні системи, дані та безперервність бізнес-процесів. Отже, кіберстрахування у сфері морської торгівлі виконує не лише компенсаторну функцію, а й превентивну, стимулюючи суб'єктів господарювання до впровадження стандартів кібербезпеки, управління ризиками та внутрішнього контролю.

Таким чином, трансформація страхового ризику в умовах цифровізації торговельного мореплавства зумовлює потребу в переосмисленні традиційних підходів до страхового правового регулювання та формування нових моделей страхового захисту. Кіберстрахування постає як інструмент адаптації страхового права до цифрової економіки, спрямований на забезпечення стабільності господарського обороту, захист інтересів учасників морської торгівлі та підтримання належного рівня економічної безпеки в інформаційній сфері.

В умовах цифрової трансформації страхового ринку право страхувальника на кібербезпеку утверджується як самостійна складова системи новітніх, зокрема цифрових, прав людини та водночас виступає важливим механізмом забезпечення економічної та інформаційної безпеки учасників страхових правовідносин. Зростання залежності страхової діяльності від інформаційно-комунікаційних технологій обумовлює трансформацію традиційних підходів до страхового захисту й актуалізує необхідність нормативного закріплення нових стандартів кібербезпеки.

Установлення й імплементація нових стандартів кібербезпеки істотно впливають на зміст і структуру страхових послуг, зумовлюючи розширення кола страхових ризиків та об'єктів страхового захисту. Страхові послуги дедалі більше орієнтуються на захист цифрових активів, інформаційних ресурсів та безперервності бізнес-процесів страхувальника, що свідчить про еволюцію страхування від суто компенсаційного механізму до комплексного інструменту управління кіберризиками.

Право на кібербезпеку страхувальника також змінює договірні засади страхування, зумовлюючи появу нових істотних умов договору, пов'язаних із вимогами до рівня кіберзахисту, обміну інформацією про кіберінциденти та взаємодії сторін у процесі реагування на кіберзагрози. Це сприяє підвищенню ролі превентивної функції страхування та формуванню партнерської моделі взаємовідносин між страховиком і страхувальником. Крім того, договір страхування кіберризиків допомагає захиститися від загроз, унаслідок яких може статися витік даних, вихід з ладу різного обладнання та збитки, які через ці події несе страхувальник. Найчастіше попит компаній на таке покриття задовольняється через покупку додаткових розширень у договорах майна, відповідальності. Але покриття за кіберризиками в таких договорах з огляду на специфіку цих видів страхування досить обмежене [3].

Отже, реалізація права на кібербезпеку страхувальника є чинником удосконалення регуляторних підходів у страховій сфері, зокрема щодо захисту інформації, конфіденційності даних і стійкості інформаційних систем страховиків.

Таким чином, право на кібербезпеку страхувальника є ключовим чинником модернізації страхових послуг, що зумовлює потребу в подальшому розвитку доктринальних підходів та нормативно-правовому регулюванні в цій сфері з метою забезпечення належного балансу між інноваційним розвитком страхування та захистом прав і законних інтересів страхувальників.

Окремо треба зазначити, що сучасний ринок кіберстрахування формується в умовах стрімкої цифровізації економіки та зростання системних кіберзагроз, що зумовлює трансформацію підходів страховиків до оцінки, прийняття й розподілу страхових ризиків.

Характерною тенденцією розвитку ринку кіберстрахування є посилення умов страхування та розширення переліку винятків зі страхового покриття. Попри стале зростання попиту на кіберстрахові продукти, пропозиція на відповідних сегментах страхового ринку зазнає скорочення, оскільки страховики та перестраховики переглядають і вивчають більш детально власні ризикові стратегії, коригуючи очікування щодо прибутковості такого виду страхування.

Збільшення кількості кібератак і пов'язаних із ними страхових вимог та судових позовів знижує передбачуваність збитковості, що змушує страхові компанії зосереджуватися на більш глибокій експертизі ризиків і запроваджувати підвищені вимоги до потенційних страхувальників. У цьому контексті особливого значення набувають збір і аналіз детальної інформації про інциденти кібербезпеки, рівень цифрової зрілості компаній, наявність внутрішніх політик управління ризиками й ефективність технічних і організаційних засобів захисту. Посилення співпраці страховиків із працівниками правоохоронних органів у сфері кібербезпеки спрямоване на більш точне розуміння природи та динаміки кіберризиків конкретних організацій, а також чинників, що впливають на їх імовірність і масштаб можливих збитків.

Дані, зібрані виданням Insurance Journal, показують, що «на кінець 2017 року 51 % американських компаній не мають полісів кіберстрахування, а 27 % не планують купувати його в майбутньому. Заперечення в значній мірі пов'язані зі структурою витрат і передбачуваною недостатньою прозорістю в галузі кіберстрахування» [4].

Як наслідок, суб'єкти, які не здатні забезпечити належний рівень прозорості або не відповідають мінімальним стандартам кіберзахисту, можуть бути обмежені в доступі до страхового покриття, зазнавати підвищення страхових тарифів чи отримувати зменшені ліміти відповідальності, що дає змогу страховикам частково компенсувати додатковий прийнятий ризик. Слушно звернути увагу, що визначення суми завданих збитків потребує їх чіткого розрахунку, належного обґрунтування та документального підтвердження. Водночас однією з найбільш проблемних сфер сучасного страхування залишається оцінювання вартості масивів даних, які з огляду на їх нематеріальну природу не піддаються однозначному грошовому виміру. Особливої складності набуває встановлення економічних наслідків витоку інформації для малих підприємств або окремих фізичних осіб, а також розроблення уніфікованих підходів і методологій оцінювання відповідного виду шкоди.

У зв'язку із цим актуалізується потреба у формуванні та підготовці висококваліфікованих фахівців, здатних комплексно аналізувати кіберризики, здійснювати їх економіко-правову оцінку та визначати обґрунтований розмір страхових збитків. Підготовка таких кадрів має поєднувати знання у сфері страхового права, кібербезпеки, економічного аналізу й управління ризиками, що є необхідною передумовою для підвищення ефективності механізмів страхового захисту в умовах цифровізації та зростання кіберзагроз.

Разом із цим спостерігається тенденція до зростання ролі самострахування та збільшення обсягу ризику, що залишається на утриманні страхувальників. За умов скорочення лімітів страхового покриття та підвищення страхових премій страховики дедалі частіше очікують від клієнтів готовності нести більшу

частку потенційних збитків шляхом застосування механізмів утримання. Такі умови фактично перерозподіляють відповідальність між сторонами страхового договору, стимулюючи страхувальників до більш активного управління власними кіберризиками та інвестування у превентивні заходи. Помітною стає готовність окремих компаній погоджуватися на підвищений рівень утримання з метою зниження розміру страхових платежів, що відображає прагнення оптимізувати співвідношення між вартістю страхового захисту та прийнятним рівнем фінансового ризику.

На тлі зазначених процесів простежуються й інші важливі напрями еволюції страхових послуг. Однією з таких тенденцій є поступова індивідуалізація страхових продуктів, що проявляється у відході від універсальних полісів на користь гнучких договорів, адаптованих до специфіки галузі, масштабів діяльності та цифрової інфраструктури конкретного страхувальника. Це дає змогу точніше узгоджувати умови страхового покриття з реальним профілем ризиків і підвищувати ефективність страхового захисту. Іншою тенденцією є зростання значення превентивної функції страхування, коли страхові компанії дедалі активніше інтегрують у свої пропозиції консультаційні, моніторингові та сервісні елементи, спрямовані на запобігання кібератакам і мінімізацію їх наслідків. Таким чином, кіберстрахування поступово трансформується з інструменту компенсації збитків у комплексний механізм управління кіберризиками, що поєднує фінансовий захист із підвищенням загального рівня кіберстійкості суб'єктів господарювання.

Висновки та пропозиції. Становлення кіберстрахування як окремого сегмента страхового ринку є безпосереднім наслідком цифрової трансформації економіки та зростання ролі інформаційно-комунікаційних технологій у господарській діяльності. Формування перших спеціалізованих страхових продуктів у Сполучених Штатах Америки на початку 2010-х років було зумовлене необхідністю забезпечення реалізації права страхувальників на кібербезпеку в умовах поширення кібератак, ускладнення цифрових бізнес-процесів і посилення вимог до захисту інформації.

Під час аналізу встановлено, що цифровізація охоплює практично всі галузі економіки, включно з традиційно консервативними сферами, що об'єктивно розширює зміст права страхувальника на кібербезпеку. На прикладі торговельного мореплавства доведено, що впровадження автоматизованих систем управління, електронних навігаційних комплексів і цифрових логістичних платформ трансформує класичні страхові ризики в гібридні, поєднуючи майнові, операційні та інформаційно-технологічні загрози. За таких умов забезпечення права на кібербезпеку потребує перегляду традиційних підходів до оцінки ризиків і формування страхового покриття, а також адаптації страхового правового регулювання до цифрових реалій.

Обґрунтовано, що право на кібербезпеку страхувальника набуває системоутворюючого значення у структурі страхових правовідносин, впливаючи на зміст страхових послуг, умови договорів страхування та характер взаємодії сторін. Його реалізація зумовлює посилення превентивної функції страхування, орієнтацію страхових продуктів на захист цифрових активів, інформаційних ресурсів і безперервності бізнес-процесів, а також формування партнерської моделі співпраці між страховиком і страхувальником у сфері управління кіберризиками.

Запровадження нових стандартів кібербезпеки істотно впливає на еволюцію страхових послуг, зумовлюючи посилення умов страхування, розширення переліку винятків зі страхового покриття, підвищення вимог до рівня кіберзахисту страхувальників і зростання ролі механізмів самострахування. Водночас простежується тенденція до індивідуалізації страхових продуктів та інтеграції превентивних і сервісних елементів, що свідчить про трансформацію кіберстрахування із суто компенсаційного інструменту в комплексний механізм забезпечення права страхувальника на кібербезпеку.

Узагальнюючи викладене, слід констатувати, що подальший розвиток права на кібербезпеку страхувальника та пов'язаних із ним стандартів потребує системного вдосконалення нормативно-правового регулювання страхових відносин, гармонізації національних підходів із міжнародними вимогами у сфері кібербезпеки та розвитку доктринальних засад страхового права. Реалізація цих завдань є необхідною умовою забезпечення балансу між інноваційним розвитком страхових послуг, стабільністю господарського обороту та належним захистом прав і законних інтересів страхувальників у цифровій економіці.

Список використаної літератури

1. Leslie Scism. Insurers Creating a Consumer Ratings Service for Cybersecurity Industry. *The Wall Street Journal*. 2019. <https://www.wsj.com/articles/insurers-creating-a-consumer-ratings-service-for-cybersecurity-industry-11553592600>.
2. Кіберзлочинці у 2020 році завдали у світі збитків на трильйон доларів: дослідження. URL: <https://www.dw.com/uk/kiberzlochyny-u-2020-rotsi-zavdaly-svitu-zbytkiv-na-trylion-dolariv-doslidzhennia/a-55857766>.
3. Ротова Т. А., Шевченко Ю. Страхування як фінансовий інструмент захисту від кіберризиків. Безпека соціально-економічних процесів в кіберпросторі : матеріали Всеукр. наук.-практ. конф. Київ : КНТЕУ, 2019. С. 177–178.
4. Jay P. Kesan & Carol M. Hayes Strengthening Cybersecurity with Cyber Insurance. Markets and Better Risk Assessment 102 Minn. L. Rev. 191. *University of Illinois College of Law Legal Studies Research*. 2017. P. 17–18.

References

1. Scism, L. (2019, March 26). Insurers creating a consumer ratings service for cybersecurity industry. *The Wall Street Journal*. <https://www.wsj.com/articles/insurers-creating-a-consumer-ratings-service-for-cybersecurity-industry-11553592600>.
2. DW (2021). *Kiberzlochynsi u 2020 rotsi zavdaly u sviti zbytkiv na trylyon dolariv: doslidzhennia* [Cybercriminals caused one trillion dollars in global damage in 2020: research]. URL: <https://www.dw.com/uk/kiberzlochyny-u-2020-rotsi-zavdaly-svitu-zbytkiv-na-trylion-dolariv-doslidzhennia/a-55857766> [in Ukrainian].
3. Rotova T. A., & Shevchenko Yu. (2019). Strakhuvannia yak finansovyi instrument zakhystu vid kiber-ryzykiv [Insurance as a financial instrument for protection against cyber risks]. In *Bezpeka sotsialno-ekonomichnykh protsesiv v kiberprostorii: materialy Vseukr. nauk.-prakt. konf.* [Security of socio-economic processes in cyberspace: Materials of the All-Ukrainian scientific and practical conference] (pp. 177–178). Kyiv: KNTEU [in Ukrainian].
4. Kesan, J. P., & Hayes, C. M. (2017). Strengthening cybersecurity with cyber insurance: Markets and better risk assessment. *Minnesota Law Review*, 102 (191), 17–18.

Дата надходження статті: 26.11.2025

Дата прийняття статті: 18.12.2025

Опубліковано: 30.12.2025

V. V. Borshchenko, PhD, Associate Professor
Odesa I. I. Mechnikov National University
Department of Constitutional Law and Justice
24/26 Frantsuzkyi Blvd, Odesa, 65058, Ukraine
e-mail: vladlena.1128@inbox.lv
ORCID iD: <https://orcid.org/0000-0001-9819-092X>

THE POLICYHOLDER'S RIGHT TO CYBERSECURITY: NEW STANDARDS AND THEIR IMPACT ON INSURANCE SERVICES

Summary

The article examines the policyholder's right to cybersecurity as a key component of insurance law in the context of rapid digital transformation of the economy and the increasing scale of cyber threats. It is shown that the development of information and communication technologies, including Big Data, artificial intelligence, blockchain, and cloud computing, enhances management efficiency and optimizes business processes, while simultaneously creating new vulnerabilities and economic risks. In this context, the policyholder's right to cybersecurity serves as an important legal mechanism for protection against digital threats and promotes the introduction of new standards for assessing and managing cyber risks.

The development of the cyberinsurance market is analyzed, particularly its emergence in the United States in the early 2010s, when insurance companies began responding to the rise in data breaches and cyberattacks by creating products to financially compensate for damages. These practices laid the foundation for the international development of cyberinsurance and defined standards for organizing insurance products. Special attention is given to the maritime sector, where digitalization, automated ship management systems, and electronic logistics platforms are transforming traditional insurance risks into hybrid risks, combining property, operational, and information-technological threats. This necessitates revising approaches to risk assessment and the formation of insurance coverage in the context of digital realities.

The article highlights the challenges of the Ukrainian cyberinsurance market, including insufficient regulatory framework, lack of standardized approaches to cyber risks, and low insurance activity among potential policyholders. It is shown that the implementation of the policyholder's right to cybersecurity strengthens the preventive function of insurance, protects digital assets, information resources, and business continuity, and fosters a partnership model between insurers and policyholders.

It is concluded that the policyholder's right to cybersecurity is system-forming in insurance relations, shaping the content of insurance services, contract conditions, and the nature of interaction between parties. Its development requires improvement of legal regulation, harmonization with international cybersecurity standards, and the development of doctrinal foundations of insurance law to ensure a balance between the innovative development of insurance services and the protection of policyholders' rights in the digital economy.

Keywords: insurance law, cyber insurance, cyber incidents, digital rights, modern rights, commercial shipping, maritime safety, cyber threat, cyber risk, cyber risk management, cybersecurity, insurance risk.