

**Копайгора О. О.,**  
*здобувач вищої освіти обліково-фінансового факультету,  
Миколаївський національний аграрний університет,  
м. Миколаїв, Україна*

## **ПІДХОДИ ДО РОЗВИТКУ КІБЕРСТРАХУВАННЯ В УКРАЇНІ**

Розвиток процесів глобалізації та інтеграції в умовах інформаційної економіки приводить до появи нових видів ризиків, пов'язаних з кіберзагрозами й кібератаками, негативний вплив яких має транснаціональний і транскордонний характер та поширюється на декілька країн одночасно. За даними компанії Netjaves Group, яка спеціалізується на консалтингу у сфері кібер-безпеки, зараз у світі понад 4 млрд користувачів інтернету, у 2022 р. році їхня кількість зросте до 6 млрд, а в 2030 р. – до 7,5 млрд. А за прогнозами Ericsson, до 2023 року кількість підключених до глобальної мережі пристроїв досягне 30 млрд. Це майже вдвічі більше, ніж у 2017 році. У зв'язку з цим потребують негайного вирішення проблеми, пов'язані з удосконаленням системи кіберзахисту та розвитком інноваційних інструментів ризик-менеджменту, одним з яких є кіберстрахування. В Україні ринок кіберстрахування перебуває на етапі становлення та потребує розробки інноваційних підходів до подальшого розвитку [2].

В умовах розвитку штучного інтелекту, мережевих підприємницьких структур, хмарних технологій, ринку аутсорсингу вдосконалюються методи і прийоми хакерських атак, що призводить до зростання обсягів кіберзлочинів. У результаті цього зростає ймовірність настання кіберризиків, покриття яких потребує впровадження інноваційних підходів до продуктів страхування, чим і зумовлюється актуальність обраної теми дослідження.

Кібер-ризик – це ризик, пов'язаний з використанням комп'ютерного обладнання та програмного забезпечення як в місцевих (локальних) мережах, так і в глобальній інтернет-мережі; у розрахунково-платіжних системах, у системах інтернет-торгівлі та в промислових системах управління. Також це ризик, пов'язаний з накопиченням, зберіганням і використанням особистих персональних даних [2].

Відмітимо, що світовий ринок кіберстрахування розвивається швидкими темпами. За експертними оцінками обсяг операцій на такому ринку до 2020 р. може становити від 7,5 до 10 млрд дол. США., а загальна сума збитків від кібератак зросте до 2,1 трлн дол. США. Лідером за обсягами операцій на такому ринку є США [1]. Переконані, що темпи розвитку кіберстрахування в кожній країні світу зумовлюються їхнім соціально-економічним та техніко-технологічним становищем, впровадженням ІТ-технологій, рівнем інформатизації суспільства. Діапазон кіберзлочинів достатньо широкий і коливається від отримання доступу до інформаційних баз даних, об'єктів інтелектуальної власності, втручання в діяльність комп'ютерних систем до отримання фінансової вигоди. З одного боку, необхідність кіберстрахування виникає у зв'язку з розвитком інформаційних технологій та інноваційних

продуктів у різних сферах економічної діяльності, що викликає появу різноманітних кіберризиків, з іншого – кіберзлочини переважно відбуваються шляхом крадіжки інновацій або новітніх технологій [4].

В той же час, для ефективного та швидкого розвитку кіберстрахування в Україні необхідно впроваджувати певні заходи державної підтримки. Зокрема, важливим є доступність страховим компаніям достовірної інформації про ефективність заходів щодо зниження ризику, щоб встановлювати надбавки до цін, які спонукають компанії бути відповідальними за кібердії та можливість впроваджувати кращі світові практики у свою діяльність. Також, поштовхом для розвитку кіберстрахування в Україні стане прийняття відповідних законодавчих актів у сфері забезпечення кібербезпеки на рівні держави та окремих суб'єктів господарювання, чітке визначення в Законі України «Про страхування» сутності кіберстрахування, з віднесенням його до добровільного або обов'язкового виду страхування [3].

Інформаційні технології, що стрімко проникають в економічні й соціальні процеси, зумовлюють необхідність інноваційних змін на ринку страхування України і розвитку такого сегмента, як кіберстрахування, який забезпечує необхідний страховий захист і відшкодування суми збитку в розмірі, необхідному для компенсації витрат, пов'язаних із втратою баз даних страхувальників та їх подальшим відновленням у разі виникнення масштабних кібератак. Оскільки ринок кіберстрахування України перебуває на початковому етапі свого становлення, під час розроблення інноваційних підходів щодо його подальшого розвитку треба широко використовувати накопичений позитивний досвід багатьох країн світу, який свідчить про диверсифікацію спектра послуг кіберстрахування і застосування окремих полісів страхування від комп'ютерних злочинів, хакерських атак та покритті збитків у процесі їх настання.

#### Список використаних джерел:

1. Forbes (2016), “Cyber Crime Costs Projected To Reach \$2 Trillion by 2019”. <https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by2019/#7885d6313a91>.
2. Братюк В. П. Сутність кібер-злочинів та страховий захист від кібер-ризиків в Україні / В. П. Братюк // Актуальні проблеми економіки. – 2015. – № 9. – С. 421-427.
3. Shaun S. Wang. Integrated Framework for Information Security Investment and Cyber Insurance [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2918674](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2918674).
4. Jay P. Kesan & Carol M. Hayes Strengthening Cybersecurity with Cyber Insurance Markets and Better Risk Assessment 102 Minn. L. Rev. 191 (2017), University of Illinois College of Law Legal Studies Research Paper No. 17- 18.

Науковий керівник: **Шишпанова Н.О.**, канд. екон. наук, доцент,  
доцент кафедри фінансів, банківської справи та страхування,  
Миколаївський національний аграрний університет,  
м. Миколаїв, Україна