

Електронний журнал «Ефективна економіка» включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України № 975 від 11.07.2019). Спеціальності – 051, 071, 072, 073, 075, 076, 292.
Ефективна економіка. 2024. № 5.

DOI: <http://doi.org/10.32702/2307-2105.2024.5.87>

УДК 336.368

О. В. Прокоф'єва,

к. е. н., доцент кафедри страхування, банківської справи та ризик-менеджменту, Київський національний університет ім. Т.Г. Шевченка

ORCID ID: <https://orcid.org/0009-0005-3715-3558>

Ю. Ю. Беспалова,

магістр, Київський національний університет ім. Т.Г. Шевченка

ORCID ID: <https://orcid.org/0009-0005-7086-7165>

КІБЕР-РИЗИКИ ТА УПРАВЛІННЯ НИМИ В УМОВАХ ГЛОБАЛІЗАЦІЇ ТА ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

O. Prokofjeva,

*PhD in Economics, Associate Professor of the Department of
Insurance, Banking and Risk Management,
Taras Shevchenko National University of Kyiv*

Y. Bepalova,

Master's degree, Taras Shevchenko National University of Kyiv

CYBER RISKS AND THEIR MANAGEMENT IN THE CONTEXT OF GLOBALIZATION AND DIGITAL TRANSFORMATION

У статті досліджуються кіберризики та роль страхування у пом'якшенні їх наслідків у контексті глобалізації та цифрової

трансформації. Визначено, що поширення інформаційних технологій породжує серйозні кіберризики, що загрожують значною фінансовою та репутаційною шкодою для організацій по всьому світу. Здійснено класифікацію основних типів збитків, що виникають в наслідок настання кіберризиків. Встановлено, що страхування є ключовим ринковим інструментом для ефективного управління кіберризиками та забезпечення фінансової стабільності підприємств та державних установ. Встановлено основні перешкоди на шляху розвитку страхування як інструменту управління ризиками в умовах глобалізації та цифрової трансформації. Визначено, що подолання цих перешкод вимагає узгоджених зусиль від зацікавлених сторін.

The relevance of this article stems from the fact that the development of information technology opens up limitless opportunities and at the same time gives rise to serious cyber threats, creating significant financial and reputational risks for organizations around the world. The purpose of this article is to study the role of cyber risk insurance in alleviating the financial and reputational fallout of cyber threats within the globalized digital landscape. It seeks to categorize the predominant forms of losses incurred, and expound upon the efficacy of insurance as a risk management tool.

The theoretical and methodological framework of the study was built on fundamental scientific concepts of Ukrainian and foreign scholars in the field of insurance. Additionally, the research employed methods of scientific investigation, including analysis and synthesis, observation and generalization, critical analysis of scientific sources, and synthesis.

The article explores the escalating cyber risks and the pivotal role of insurance in mitigating their repercussions amidst the backdrop of globalization and digital transformation. The study delineates the ramifications of cyber risks for both businesses and governmental bodies and classifies the principal types of losses stemming from these risks. It elucidates insurance as a paramount market

instrument for efficacious cyber risk management, crucial for ensuring the financial stability and reputation preservation of entities. Moreover, it identifies the primary impediments to insurance development within the context of globalization and digital transformation, underscoring the necessity for concerted stakeholder efforts to surmount these challenges.

The practical value of this article is that it offers valuable insights for policymakers, insurance professionals, cybersecurity experts, and businesses seeking to navigate the complexities of cyber risk management in an increasingly digital world. It may serve as a foundation for further research into the specific dynamics of cyber risks in Ukraine, regulatory changes, market trends, and effective strategies for enhancing cyber resilience through insurance mechanisms.

Ключові слова: кіберризик; кіберзагроза; кіберстрахування; кібербезпека; управління кіберризиками.

Keywords: cyber risk; cyber threat; cyber insurance; cybersecurity; cyber risk management.

Постановка проблеми. У сучасну епоху, що характеризується глобалізацією та цифровою трансформацією, широке впровадження інформаційних технологій відкриває необмежені можливості в глобальних сферах. Однак така швидка цифровізація породжує серйозні кіберризики, що здатні завдати значних фінансових збитків та репутаційних втрат, які часто перевищують можливості окремих суб'єктів економіки. Державні та комерційні структури стають особливо чутливими до цих ризиків, оскільки все більше покладаються на цифрову інфраструктуру для своїх операцій, тим самим підвищуючи свою вразливість до потенційних кіберзагроз, таких як витоки даних або атаки зловмисного програмного забезпечення. Зростаюча поширеність кіберризиків як критичної комерційної проблеми підкреслює необхідність застосування надійних механізмів управління ними. Страхування кіберризиків стає єдиним ринковим інструментом, здатним

забезпечити фінансову стабільність цих суб'єктів та захистити їхню репутацію. Воно сприяє створенню стійких цифрових екосистем, захищаючи від майбутніх загроз і просуваючи культуру проактивного пом'якшення ризиків. Таким чином, розуміння та розвиток страхування кібер-ризиків є необхідною умовою для навігації в складному ландшафті сучасної цифрової економіки та захисту від потенційних загроз.

Аналіз останніх досліджень і публікацій. Вагомий внесок у дослідження кіберризиків та розвитку кіберстрахування зробили такі вітчизняні вчені, як: Н.М. Внукова, О.О. Гаманкова, Ю.П. Гришан, С. Гуменюк, О.М. Залєтов, А.Д. Заруба, Р.В. Пікус, Л. Н. В. Приказюк. Зарубіжними вченими, що досліджували проблематику кіберризиків та їх страхування є Д. Арчі, К. Сарда та Д. Фінк та інші.

Виділення невирішених раніше частин загальної проблеми. Невирішеною частиною загальної проблеми залишається відсутність всебічного розуміння ролі страхування кіберризиків у пом'якшенні фінансових та репутаційних наслідків кіберризиків.

Формулювання цілей статті (постановка завдання). Метою даної статті є дослідження кіберризиків та ролі страхування у пом'якшенні фінансових та репутаційних наслідків кіберзагроз у рамках глобалізації та цифрової трансформації.

Завдання роботи, виконання яких покликані досягти мету дослідження, полягають у наступному:

- Визначити роль страхування кіберризиків у пом'якшенні фінансових та репутаційних наслідків кіберзагроз у контексті глобалізації та цифрової трансформації;
- Класифікувати основні типи втрат від кіберризиків, з якими стикаються організації;
- Охарактеризувати ефективність страхування як інструменту управління кіберризиками;

- Визначити основні перешкоди для розвитку страхування кіберризиків в Україні.

Виклад основного матеріалу дослідження. Сучасне суспільство стає все більш залежним від цифрових технологій та ІТ-інфраструктури. Працюючі ІТ-інструменти тепер лежать в основі всіх аспектів людської діяльності, включаючи приватний та державний сектори. Однак в роботі цих служб можуть траплятись збої через ненавмисні помилки чи цільові кібератаки, наслідки яких відчуваються миттєво та можуть бути значними і поширюватись на взаємопов'язані бізнес-процеси по всьому світу. У цьому сенсі ІТ-системи стають критично важливою інфраструктурою, подібно до доріг, електропостачання, водопровідної системи та фінансових послуг. Розвиток ІТ-технологій породжує відповідне зростання кіберризиків.

Кіберризик – це ризик, пов'язаний з використанням комп'ютерного обладнання та програмного забезпечення як в місцевих (локальних) мережах, так і в глобальній інтернет-мережі; в розрахунково-платіжних системах, в системах інтернет-торгівлі і в промислових системах управління. Також це ризик, пов'язаний з накопиченням, зберіганням і використанням особистих персональних даних [2; 1, с. 422].

Кіберризик стосується потенційної шкоди або втрат внаслідок порушення безпеки цифрових систем, мереж або даних. Він охоплює широкий спектр загроз, включаючи кібератаки, витоки даних, зараження зловмисним програмним забезпеченням, внутрішні загрози та системні збої. По суті, кіберризик представляє ймовірність і вплив несприятливих подій, що відбуваються в цифровій сфері.

Кібератаки є одними з найпоширеніших кіберризиків на сьогодні. Аналіз динаміки кібератак, спрямованих на бізнес у всьому світі за останні п'ять років свідчить про значне збільшення як їх частоти, так і показників успішності. Згідно з даними Центру скарг на злочини в Інтернеті за період з 2015 по 2022 рік, спостерігався помітний сплеск скарг на кібератаки, загальна

кількість яких склала понад 4 мільйони в усьому світі. Варто відзначити, що кількість скарг у 2022 році зросла в 2,8 рази порівняно з 2015 роком (рис. 1).

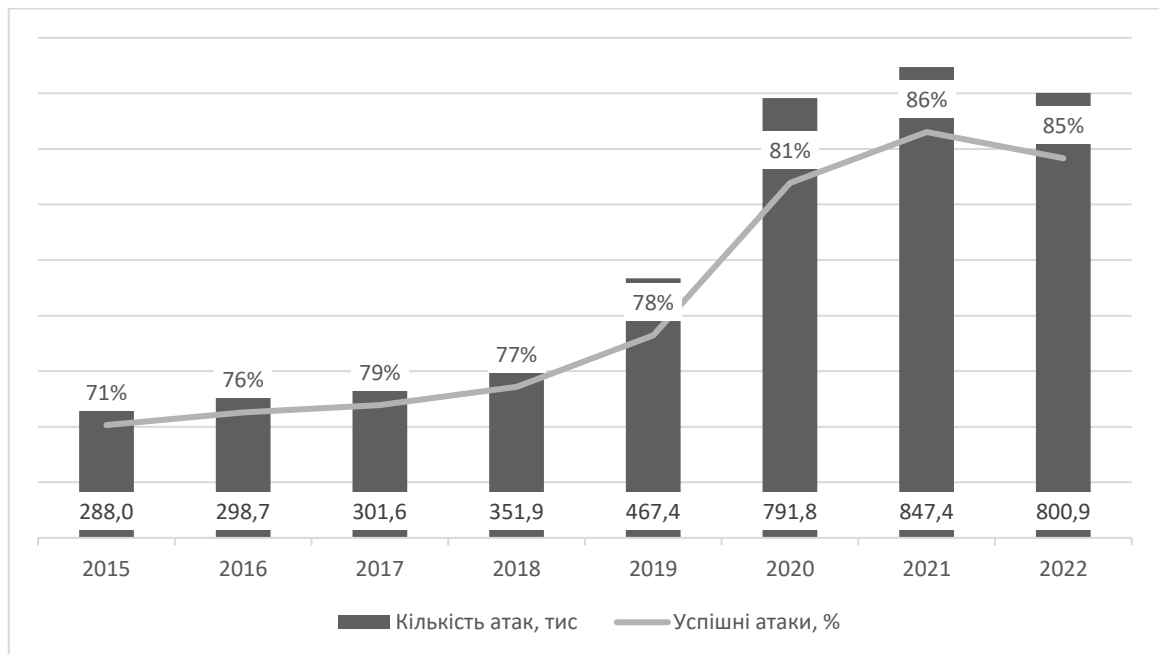


Рис. 1. Зареєстровані кібер-атаки у світі 2015-2022рр.

Джерело: складено автором на основі даних [7;8].

Одним із значних каталізаторів поширення кібератак стало широке впровадження хмарних сервісів і криптовалют. Ці технології, пропонуючи численні переваги з точки зору масштабованості, гнучкості та ефективності, також відкрили нові шляхи для кіберзлочинців. Децентралізована і часто анонімна природа криптовалют полегшила незаконну діяльність, таку як атаки з вимогами викупу, а зростаюча залежність від хмарної інфраструктури розширила поле для кібератак.

Крім того, глобальна пандемія COVID-19, яка розгорнулася протягом аналізованого періоду, стала каталізатором росту кіберзлочинності. Швидкий перехід до віддаленої роботи та цифрових платформ, спричинений заходами соціального дистанціювання та карантином, створив сприятливий ґрунт для кіберзловмисників. Раптовий перехід до віддаленого робочого середовища зробив організації досить вразливими, оскільки співробітники отримували доступ до конфіденційних даних і корпоративних мереж із потенційно

незахищених домашніх мереж і персональних пристроїв. Кіберзлочинці скористалися цією вразливістю, запустивши цілеспрямовані атаки на використання слабких місць інфраструктури віддаленої роботи та компрометацію конфіденційної інформації.

Важливим показником стану кібербезпеки на підприємствах, є рівень успішності кібератак, що становив вище 70% протягом аналізованого періоду, досягнувши піку в 86% у 2021 році. Зростання кількості успішних кібератак можна пояснити збільшення площі атак внаслідок поширення віддалених працівників. Зі зростанням кількості співробітників, які мають доступ до корпоративних мереж і даних із віддалених місць, захист кінцевих точок і забезпечення захисту даних стає все більш складним для організацій у всьому світі.

Ці результати підкреслюють критично низький рівень розвитку кібербезпеки серед компаній у всьому світі. Незважаючи на прогрес у технологіях кібербезпеки та зусилля з підвищення обізнаності, організації продовжують пошук ефективних засобів захисту від кіберзагроз.

Збитки від кіберризиків можна поділити на три окремі групи [6]:

1. Прямі збитки. Втрачені або недоотримані прибутки, тобто фінансові втрати, понесені через перерву в роботі внаслідок кіберінциденту – це дохід, який був би отриманий за період простою або збоїв, а також будь-які додаткові витрати, понесені для відновлення нормального ведення бізнесу; Витрати, пов'язані із затримками у відновленні пошкодженої інфраструктури – витрати на придбання нового комп'ютерного обладнання або ремонт скомпрометованих систем.

2. Збитки завдані третім особам. Матеріальні збитки завдані третім особам в результаті кіберінциденту – фізична шкода майну, обладнанню або активам, що належать третім особам, які постраждали від кібератаки; Моральна або репутаційна шкода завдана третім особам, таким як клієнти, партнери або зацікавлені сторони - суб'єкт може нести відповідальність за компенсацію третім особам збитків, спричинених шкодою їх діловій

репутації; Порухення прав інтелектуальної власності, несанкціонований доступ, крадіжка або неправомірне використання інтелектуальної власності, що належить третім особам – суб'єкти можуть нести відповідальність за покриття збитків, спричинених порушенням прав інтелектуальної власності, включаючи судові витрати та відшкодування збитків, присуджені за позовами про порушення прав інтелектуальної власності.

3. Витрати на антикризове управління. Витрати, пов'язані із залученням експертів, консультантів та юристів з ІТ-безпеки для пом'якшення наслідків кібератаки та мінімізації збитків – це можуть бути витрати на судові розслідування, реагування на інциденти, послуги юрисконсультів, зв'язки з громадськістю та кризові комунікації, спрямовані на управління наслідками кіберінциденту.

Ефективним інструментом для пом'якшення наслідків кібератак є страхування кіберризиків. Воно забезпечує фінансовий захист організацій, покриваючи витрати, пов'язані з кіберінцидентами.

На сьогодні лідером у сфері страхування кіберризиків можна вважати Сполучені Штати, де кіберзагрози для бізнесу є значними, а суворі закони про захист даних висувають високі вимоги до кібербезпеки, кіберстрахування стає важливим інструментом управління ризиками. Натомість в Україні сплеск інтересу до кіберстрахування можна було побачити після атаки вірусу Petya у 2017 році, що підкреслило його важливість для пом'якшення фінансових наслідків кіберзагроз. Триваючі кібератаки росії на українську ІТ-інфраструктуру ще більше підкреслюють критичну потребу в кіберстрахуванні, для компенсування витрат, пов'язаних з витоком даних, перебоями в комунікаціях та крадіжками інформації.

Поліси кіберстрахування дозволяють компаніям підтримувати стабільність бізнесу під час і після кіберінциденту, надаючи фінансову підтримку для відновлення. Компенсуючи витрати на профілактичні заходи та дії з реагування на інциденти, кіберстрахування допомагає організаціям мінімізувати збої в роботі та фінансові втрати. Ця стабільність є особливо

важливою в сучасних умовах для України, під час кібератак росії на українські підприємства та інфраструктуру, коли безперервність роботи є важливою для виживання бізнесу.

Залежно від страхової компанії та умов полісу покриття може відрізнятися, а також можуть бути доступні додаткові ризики або спеціальні варіанти покриття для вирішення конкретних кіберзагроз, з якими стикаються організації. У Таблиці 1 наведено опис основних ризиків, які можуть бути покриті полісом кіберстрахування.

Таблиця 1. Кіберризики, що покриваються полісами страхування

Категорія ризику	Опис
Витік даних	Несанкціонований доступ, крадіжка або розголошення чутливих або конфіденційних даних, включаючи особисту, фінансову або медичну інформацію.
Атаки з вимогою викупу	Шкідливе програмне забезпечення, яке шифрує дані або системи, вимагаючи викуп за ключі дешифрування, а також витрати, пов'язані з перериванням роботи.
Переривання діяльності	Порушення нормальних бізнес-процесів через кіберінциденти, включно з простоєм, втраченим доходом і додатковими витратами на відновлення роботи.
Відповідальність за безпеку мережі	Юридична відповідальність, що виникає внаслідок несанкціонованого доступу, витоку даних або кібератак, які впливають на мережі, системи або дані третіх сторін.
Відповідальність за порушення конфіденційності	Юридичні зобов'язання, що виникають внаслідок порушення законів чи правил про конфіденційність, включно з несанкціонованим доступом до особистої інформації або її розголошенням.
Штрафи та санкції регуляторних органів	Фінансові санкції, накладені регуляторними органами за недотримання законів про захист даних, нормативних вимог про конфіденційність або галузевих стандартів.
Витрати на антикризове управління	Витрати, пов'язані з реагуванням на інциденти, судовою експертизою, зв'язками з громадськістю, юридичними консультантами, повідомленням постраждалих сторін та послугами кредитного моніторингу.
Шахрайство за допомогою соціальної інженерії	Обманна тактика, що використовується для маніпулювання людьми з метою розкриття конфіденційної інформації, переказу коштів або виконання несанкціонованих дій.
Репутаційна шкода	Шкода репутації бренду, діловій репутації або громадській думці, спричинена негативною рекламою, витоком даних або кіберінцидентами.
Ненавмисна втрата даних	Ненавмисна втрата, видалення, пошкодження або знищення даних через людську помилку, збій обладнання, програмні помилки або кібератаки.

Джерело: складено автором на основі [3;4;5].

Страхування кібер-ризиків часто включає стимули для впровадження надійних заходів кібербезпеки та дотримання нормативних вимог. Страховики можуть пропонувати знижки або вигідні умови для компаній, які демонструють проактивну практику управління ризиками, як-от впровадження найкращих практик кібербезпеки, проведення регулярних оцінок безпеки та дотримання правил захисту даних. Це не тільки знижує ймовірність кіберінцидентів, але й допомагає організаціям підтримувати відповідність стандартам і нормам кібербезпеки, що ще більше підвищує їх загальну кіберстійкість.

Сьогодні ринок страхування кіберризиків в Україні зіштовхується з певними перешкодами, такими як:

1. Недостатній рівень поінформованості. Багато українських підприємств не усвідомлюють серйозності кіберризиків та не розуміють переваг кіберстрахування. Відсутність належного поінформованості та доступних ресурсів, що пояснюють суть кіберстрахування та його потенційну користь, може стримувати розвиток ринку.
2. Недосконала нормативна база. Законодавство та регулювання кібербезпеки в Україні все ще перебувають у стадії розвитку. Відсутність чітких норм та правил, що стосуються кіберстрахування, може ускладнювати роботу страхових компаній та заважати розвитку ринку.
3. Нестача досвіду та експертизи. У страхових компаніях може бракувати кваліфікованих фахівців, які мають глибокі знання в сфері кібербезпеки та кіберризиків. Це може ускладнювати процес оцінки ризиків, розробку страхових продуктів та обслуговування клієнтів.
4. Низький рівень довіри до страхових компаній. Історично склалося так, що довіра до страхових компаній в Україні не є високою. Це може стримувати підприємства від придбання полісів кіберстрахування, навіть якщо вони усвідомлюють ризики.
5. Висока вартість страхових продуктів. Зважаючи на високий рівень кіберризиків, страхові компанії можуть встановлювати значні тарифи на

кіберстрахування. Це може зробити кіберстрахування недоступним для малого та середнього бізнесу.

6. Недостатня кількість статистичних даних. Відсутність надійних даних про кібератаки та їх наслідки в Україні може ускладнювати процес оцінки ризиків для страхових компаній. Це може призвести до неточної цінової політики та невідповідності страхових продуктів реальним потребам ринку.

7. Недосконала культура кібербезпеки. На багатьох українських підприємствах не приділяється належна увага питанням кібербезпеки. Це може призводити до частих кібератак та збільшувати ризики для страхових компаній.

Для подолання цих перешкод та стимулювання розвитку кіберстрахування в Україні необхідні спільні зусилля з боку уряду, страхових компаній, експертів з кібербезпеки та представників бізнесу.

Висновки. Залежність сучасного суспільства від цифрових технологій та ІТ-інфраструктури продовжує зростати, охоплюючи всі аспекти людської діяльності. Оскільки ІТ-системи стають критично важливою інфраструктурою відповідне зростання кіберризиків вимагає ефективних стратегій управління ними.

Кіберризик охоплює різні загрози, пов'язані з комп'ютерним обладнанням та програмним забезпеченням, включаючи локальні та глобальні мережі, платіжні системи, платформи електронної комерції та системи управління промисловістю.

Аналіз глобальних кібератак за останні п'ять років свідчить про значний сплеск як їх частоти, так і успішності, зумовлений такими факторами, як широке використання хмарних сервісів і криптовалют та пандемією COVID-19, яка прискорила зростання кіберзлочинності, посиливши вразливість інфраструктури віддаленої роботи.

Кіберстрахування стає важливим інструментом пом'якшення наслідків кібератак, забезпечуючи фінансовий захист організацій та покриваючи пов'язані з ними витрати.

Незважаючи на свою важливість, ринок кіберстрахування в Україні стикається з такими перешкодами, як недостатня обізнаність, недосконала нормативно-правова база, обмежений досвід, низька довіра до страховиків, високі витрати, недостатня кількість даних та недосконала культура кібербезпеки.

Надалі необхідні подальші дослідження, щоб заглибитися в конкретну динаміку кіберризиків в Україні, включаючи еволюцію ландшафту загроз, регуляторні зміни, ринкові тенденції і т.д.

Література

1. Братюк В. П. Сутність кібер-злочинів та страховий захист від кіберризиків в Україні. Актуальні проблеми економіки. 2015. № 9. С. 421-427
2. Кібер-ризик. Вікідата. URL: <https://www.wikidata.uk-ua.nina.az/%D0%9A%D1%96%D0%B1%D0%B5%D1%80-%D1%80%D0%B8%D0%B7%D0%B8%D0%BA.html> (дата звернення: 27.03.2024).
3. Офіційний сайт страхової компанії Allianz URL: <https://www.upguard.com/> (дата звернення: 27.03.2024).
4. Офіційний сайт страхової компанії UpGuard URL: <https://www.upguard.com/> (дата звернення: 27.03.2024).
5. Приказюк Н. В., Гуменюк Л. С. Кібер-страхування як важливий інструмент захисту підприємств в умовах цифровізації економіки. *Ефективна економіка*. 2020. № 4. DOI: 10.32702/2307-2105-2020.4.6
6. Селіверстова Л. С., Трухан Д. А. Підходи до розвитку кіберстрахування як сегменту глобального страхового ринку. *Економіка та держава*. 2020. № 1. С. 23–26. DOI: 10.32702/2306-6806.2020.1.23
7. Internet Crime Report 2022 URL: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf (дата звернення: 27.03.2024).

8. 2023 Cyberthreat Defense Report URL:
https://www.humansecurity.com/hubfs/HUMAN_Report_2023-Cyberthreat-Defense-Report.pdf (дата звернення: 27.03.2024).

References

1. Bratuk, V.P. (2015), "The essence of cyber crimes and the insurance coverage against cyber risks in Ukraine", *Actual problems of economics*, vol. 9, pp. 421-427.
2. Wikidata (2024), "Cyber risk", Available at: <https://www.wikidata.uk-ua.nina.az/%D0%9A%D1%96%D0%B1%D0%B5%D1%80-%D1%80%D0%B8%D0%B7%D0%B8%D0%BA.html> (accessed March 27, 2024).
3. Official website of Allianz Insurance Company (2024), Available at: <https://www.allianz.com/en.html> (accessed March 27, 2024).
4. Official website of the UpGuard (2024), Available at: <https://www.upguard.com/> (accessed March 27, 2024).
5. Prykaziuk, N. and Gumenyuk, L. (2020), "Cyber-insurance as an important tool of enterprise protection in the digitization economy", *Efektivna ekonomika*, vol. 4. DOI: 10.32702/2307-2105-2020.4.6
6. Seliverstova, L. and Truhan, D. (2020), "Approaches to the development of cyber insurance as a segment of the global insurance market", *Ekonomika ta derzhava*, vol. 1, pp. 23–26. DOI: 10.32702/2306-6806.2020.1.23
7. Federal Bureau of Investigation (2022), "Internet Crime Report", Available at: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf (accessed March 27, 2024).
8. CyberEdge Group (2023), "2023 Cyberthreat Defense Report", Available at: https://www.humansecurity.com/hubfs/HUMAN_Report_2023-Cyberthreat-Defense-Report.pdf (accessed March 27, 2024).

Стаття надійшла до редакції 29.04.2024 р.