Міністерство освіти і науки України
Сумський державний університет
Навчально-науковий інститут бізнесу, економіки та менеджменту
Кафедра економічної кібернетики

ВИКЛИКИ КІБЕРБЕЗПЕКИ ІНДУСТРІЇ ФІНАНСОВИХ ПОСЛУГ

Матеріали
II наукової онлайн-конференції

(Суми, 02 липня 2024)

Суми
Сумський державний університет
2024

004.056.5:336(082)
В43

Головний редактор
доц., к.е.н., ***Койбічук Віталія***, завідувачка кафедри економічної кібернетики, Сумський державний університет
.

Затверджено Вченою Радою Сумського державного університету (протокол № 1, 29.08.2024)

S62 Виклики кібербезпеки індустрії фінансових послуг: Матеріали наукової онлайн-конференції, Суми, 02 липня 2024. Збірник матеріалів тез наукової онлайн-конференції / за загальною редакцією доц. Койбічук В.В. – Суми : Сумський державний університет, 2024. – 72 с.

Матеріали наукової онлайн-конференції "Виклики кібербезпеки індустрії фінансових послуг" присвячені пошуку системного вирішення проблем у сфері протидії кібеззагрозам у сфері фінансових послуг, підвищенню рівня кіберзахисту об'єктів критичної інфраструктури.

Видання розраховане на науковців, викладачів, студентів вищих навчальних закладів, аспірантів, докторантів та інших зацікавлених осіб.

004.056.5:336(082)

ЗМІСТ

СЕКЦІЯ 1	***ЦИФРОВІ ТРАНСФОРМАЦІЇ В ЕКОНОМІЦІ***	**5**
Іван Нестеренко	ДОСЛІДЖЕННЯ ЦИФРОВИХ ТРАНСФОРМАЦІЙ В ЕКОНОМІЦІ	5
Катерина Дідоренко	ЦИФРОВІЗАЦІЯ ЯК ФАКТОР ПОСИЛЕННЯ КОНКУРЕНТОСПРОМОЖНОСТІ КРАЇНИ	9
Володимир Науменко	МОДЕЛЮВАННЯ ТА ПРОГНОЗУВАННЯ ВПЛИВУ РІВНЯ ЦИФРОВІЗАЦІЇ НА ЕКОНОМІЧНИЙ РОЗВИТОК	12
Дмитро Харченко	РОЛЬ ЦИФРОВІЗАЦІЇ В ПРОТИДІЇ КОРУПЦІЇ	16
Захарченко Андрій	ЦИФРОВІ НАВИЧКИ: ВИКЛИКИ ТА МОЖЛИВОСТІ	19
Даніїл Савченко, Тетяна Доценк	ТЕОРЕТИЧНІ АСПЕКТИ ВЗАЄМОЗВ'ЯЗКІВ КІБЕРБЕЗПЕКИ ТА БЕЗПЕКИ ОХОРОНИ ЗДОРОВ'Я	24
СЕКЦІЯ 2	***КІБЕРЗАГРОЗИ У СФЕРІ ФІНАНСОВИХ ПОСЛУГ***	***27***
Віталія Койбічук	ІДЕНТИФІКАЦІЯ ТА УПЕРЕДЖЕННЯ КІБЕРШАХРАЙСТВ В ЕЛЕКТРОННОМУ БАНКІНГУ: ДОСВІД ЄС	27
Роєнко Олександр	КОНВЕРГЕНЦІЙНІ ПРОЦЕСИ МІЖ КІБЕРЗЛОЧИННІСТЮ ТА ТІНЬОВОЮ ЕКОНОМІКОЮ	31
Ксенія Могильна	АНАЛІЗ ОСНОВНИХ ТРЕНДІВ НА СВІТОВОМУ РИНКУ КІБЕРСТРАХУВАННЯ	34
Ольга Горбачова	ТЕНДЕНЦІЇ РОЗВИТКУ РИНКУ КІБЕРСТРАХУВАННЯ У СВІТІ	39
Валерія Кочнєва	РОЛЬ КІБЕРСТРАХУВАННЯ У ПІДВИЩЕННІ РІВНЯ КІБЕРСТІЙКОСТІ КОМПАНІЙ	41
Іван Гончарук	КОРУПЦІЯ ЯК ІНСТРУМЕНТ ПРОНИКНЕННЯ ТА ВИКРАДАННЯ ІНСАЙДЕРСЬКИХ ДАНИХ	45
СЕКЦІЯ 3	***ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В ПРОТИДІЇ КІБЕРЗАГРОЗАМ***	92

ВИКЛИКИ КІБЕРБЕЗПЕКИ ІНДУСТРІЇ ФІНАНСОВИХ ПОСЛУГ

Avhusta Hrytsenko	*THE ROLE OF ARTIFICIAL INTELLIGENCE IN COUNTERING CYBER THREATS*	*48*
Вікторія Біловодська	*РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В ПРОТИДІЇ КІБЕРЗАГРОЗАМ*	*53*
Оголь Дмитро	*МЕТОДИ ПІДВИЩЕННЯ ЦИФРОВОЇ ОБІЗНАНОСТІ СПОЖИВАЧІВ ФІНАНСОВИХ ПОСЛУГ: УСПІШНІ ВІТЧИЗНЯНІ ТА ЗАКОРДОННІ КЕЙСИ*	*57*
Анна Шаповалова	*ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ ПІДВИЩЕННЯ КІБЕРБЕЗПЕКИ*	*61*
Еліна Шрамко	*ШТУЧНИЙ ІНТЕЛЕКТ У БОРОТЬБІ З КІБЕРЗЛОЧИННІСТЮ: ЕФЕКТИВНІ СТРАТЕГІЇ ТА ІНСТРУМЕНТИ*	*64*
Єлизавета Литюга	*ШТУЧНИЙ ІНТЕЛЕКТ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ*	*69*

АНАЛІЗ ОСНОВНИХ ТРЕНДІВ НА СВІТОВОМУ РИНКУ КІБЕРСТРАХУВАННЯ

ANALYSIS OF THE MAIN TRENDS IN THE GLOBAL CYBER INSURANCE MARKET

Ксенія Могильна, *студентка*
Сумський державний університет, Україна

Науковий керівник:
Сергій Миненко, доктор філософії
Сумський державний університет, Україна

У сучасному світі новітні технологічні досягнення переплітаються з повсякденним життям, а шкода від кібератак і кіберінцидентів стає надзвичайно вагомою. На тлі повномасштабного вторгнення Росії в Україну імператив захисту від кіберзагроз вийшов на новий рівень, про що свідчить хвиля кібератак, спрямованих на українські організації протягом 2022-2023 років. У цьому контексті розуміння й аналіз ринку кіберстрахування набуває першорядного значення, адже розвиток кіберстрахування дозволяє організаціям зменшити ризики пов'язані з кіберзагрозами. З огляду на актуальність цієї теми метою цього дослідження є вивчення останніх тенденцій ринку кіберстрахування у глобальному світовому ландшафті, контекстуалізуючи дискурс у горнилі ринкових тенденцій, сучасних геополітичних подій і розвитку технологій штучного інтелекту.

Нюансоване вивчення тенденцій ринку кіберстрахування вимагає розуміння основних теоретичних засад цієї сфери, з цією метою необхідно розтлумачити головну дефініцію. За визначенням Л. Албон та ін. «Кіберстрахування – це широкий термін для позначення страхових полісів, які стосуються збитків першої та третьої сторони в результаті комп'ютерної атаки або збою в роботі систем інформаційних технологій організації» (S. Romanosky et al., 2019). Таке визначення є достатньо повним, однак його можна дещо доповнити узагальнивши небезпеки «комп'ютерної атаки або збою в роботі систем інформаційних технологій фірми» (S. Romanosky et al., 2019) за допомогою терміну «кіберризик», оскільки саме він є основним об'єктом кіберстрахування.

За тлумаченням Р. Пікус і Ю. Бабенко «Кіберризик – це ймовірність настання подій, які вражають роботу IT-систем та кібербезпеку організації через стороннє втручання цифрових та інших електронних технологій, що призводить до отримання збитків, руйнування цифрових активів та можливої втрати репутації організації (Пікус & Бабенко, 2022). Таке

визначення наголошує на широкому спектрі інцидентів, які підпадають під сферу дії кіберстрахування.

Розглянутий теоретичний підхід підкреслює важливість кіберстрахування для зменшення ризиків у цифровому середовищі. Однак, через молодий статус цієї сфери воно може бути недостатньо впровадженим у стратегії управління ризиками компаній. Результати аналізу статистичних даних звіту Hiscox про кібернетичну готовність 2023 року вказують на зростання використання кіберстрахування серед великих компаній з 72% у 2021 році до 75% у 2022-2023 роках (Lamb, 2023). Це свідчить про збільшення усвідомлення необхідності захисту від кіберризиків серед цих компаній. Однак серед малих підприємств з меншою кількістю працівників використання кіберстрахування менш поширене. Частка малих компаній, які користуються кіберстрахуванням, зросла з 50% у 2021 році до 57% у 2022 році, але незначно знизилася до 56% у 2023 році (Lamb, 2023), можемо приспустити, що причиною нижчого рівня використання кіберстрахування серед малого бізнесу можуть бути такі фактори, як висока вартість, недостатня обізнаність про ризики, складність полісів та недооцінка кіберзагроз.

Іншим важливим показником для аналізу ринку кіберстрахування є річні світові витрати на кіберстрахування. За статистичними даними можна стверджувати, що світові витрати на кіберстрахування показують стабільний ріст, з 2,5 мільярдів доларів у 2015 році до 16,4 мільярдів доларів у 2023 році (Cybersecurity Insurance Market: Forecast 2024 – 2032, 2023). Цей ріст є наслідком зростаючого усвідомлення кіберризиків і збільшення попиту на страховий захист. За результатами аналізу статистичних даних (Cybersecurity Insurance Market: Forecast 2024 – 2032, 2023), можемо побачити, що темпи зростання підсилилися під час початку пандемії COVID-19 у 2020 році (зростання на 60,0%) та під впливом повномасштабного вторгнення Росії в Україну в 2022 році (зростання на 51,1%). Такі події підвищили кіберризики, спонукаючи компанії збільшувати свої витрати на кібербезпеку, включаючи кіберстрахування.

У рамках дослідження було виявлено, що збільшення кіберризиків через пандемію COVID-19 та російсько-український конфлікт призвело не лише до зростання попиту на кіберстрахування, але й до перегляду умов полісів. Наприклад, премії кіберстрахування на ринку США зросли з 10 млрд. доларів США у 2021 році до близько 12 млрд. доларів США у 2022 році й очікувано продовжуватимуть зростати з середнім приростом у 20% на рік до 2025 року (Farley, 2023). Іншою поширеною зміною змісту страхових полісів пов’язаною з війною в Україні є виключення або значне зниження рівня покриття для кіберінцидентів, які можуть бути пов’язані кібервійнами.

Прикладом таких винятків для таких інцидентів є чотири виключення щодо кібервійни та кібероперацій Lloyd's Market Association (Farley, 2023).

Ще однією важливою характеристикою ринку кіберстрахування є асиметричність у поширеності кіберстрахування в різних галузях. Деякі, такі як освіта, готельний бізнес та ігрова індустрія, показують високий рівень використання кіберстрахування, перевищуючи 65% (Pendleton et al., 2021). З цього зрозуміло, що у цих галузях фахівці визнають ризики цифрових операцій, обробки конфіденційної інформації та потребу їх надійного страхового захисту. Однак у виробництві, професійних послугах та фінансових установах використання кіберстрахування нижче 45% (Pendleton et al., 2021). Ця різниця може бути зумовлена різним сприйняттям ризиків, обмеженістю ресурсів або регуляторними міркуваннями у кожному секторі. Втім, варто відмітити, зростання частки компаній, які використовують кіберстрахування у всіх галузях протягом 2016-2020 років (Pendleton et al., 2021), на основі якого можна стверджувати, що перегляд стратегій кібербезпеки ставав все важливішим для компаній різних галузей протягом досліджуваного періоду.

Після виконаного аналізу ринку кіберстрахування стає очевидним, що ця галузь активно розвивається в умовах цифровізації, а декілька домінуючих тенденцій, виявлених у попередньому аналізі, змінюють ландшафт страхового покриття та стратегії управління ризиками у всьому світі. На основі проведеного аналізу можна виокремити основні тенденції притаманні ринку кіберстрахування, перелік яких наведено нижче.

1. Зростання обсягу ринку. Останні світові події, такі як пандемія COVID-19 та російсько-українська війна, підвищили кількість, масштаби та вартість кіберризиків, підкресливши потребу у надійному страховому захисті для зменшення фінансових втрат від кіберінцидентів.

2. Збільшення глобальних премій. Зростання потенційної вартості збитків від кіберінцидентів призвело до збільшення глобальних страхових премій, відображаючи зростаюче визнання фінансового впливу кібератак на підприємства та організації в усьому світі.

3. Зменшення покриття кіберризиків, пов'язаних з кібервійнами та кіберопераціями. Спостерігається тенденція до скорочення покриття ризиків, пов'язаних з кібервійнами та кіберопераціями, через зростання світової геополітичної напруженості. Шляхом оновлення умов покриття цих ризиків у страхових полісах, страховики намагаються впоратися зі складнощами та невизначеністю, притаманними цим новим загрозам.

4. Асиметрія у різних галузях. Рівень поширення кіберстрахування значно варіюється між галузями, з освітою, послугами та охороною здоров'я, які виявляють вищі темпи впровадження порівняно з виробництвом, професійними послугами та фінансовими установами.

5. Складність андеррайтингу. Відсутність стандартизованого покриття, обмежений досвід менших страхових організацій, труднощі у доступі до статистичної інформації значно ускладнюють процес андеррайтингу – виявлення, аналіз та оцінка ризиків.

6. Використання інструментів аналізу даних. Застосування сучасних інструментів аналізу даних, таких як штучний інтелект та машинне навчання, може полегшити проблеми з андеррайтингом. Ці інструменти дозволяють страховикам розробляти складніші моделі оцінки та прогнозування кіберризиків, що допомагає їм адаптувати страхові рішення до змінних потреб клієнтів у цифровому середовищі.

Підсумовуючи, у дослідженні було проаналізовано загальні тенденції сучасного світового ринку кіберстрахуваня, включаючи вплив соціальних та геополітичних процесів, зміну умов страхових полісів, ускладнення процесів андеррайтингу та інтеграцію передових інструментів аналізу даних, які сприяють глибшому розумінню управління ризиками у кіберстрахуванні. Отримані результати можуть будуть використані для подальших досліджень ринку кіберстрахування в Україні, включаючи розробку стандартизованого покриття та політик, спрямованих на спрощення процесу андеррайтингу та підвищення прозорості ринку.

Роботу виконано в рамках НДР № 0122U000783 «Моделювання механізмів детінізації та декорумпізації економіки для забезпечення національної безпеки: вплив трансформації фінансових поведінкових патернів»

Список використаних джерел

1. Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity*, 5(1). https://doi.org/10.1093/cybsec/tyz002

2. Пікус, Р. В., & Бабенко, Ю. Л. (2022). Кіберстрахування: нові можливості для страхового ринку України. *Економіка та держава*, (2), 134–140. https://doi.org/10.32702/2306-6806.2022.2.134

3. Lamb, E. (2023). *Hiscox cyber readiness report* 2023. Hiscox. https://www.hiscox.co.uk/sites/default/files/documents/2023-10/Cyber-Readiness-Report-2023-UK.pdf

4. *Cybersecurity Insurance Market: Forecast 2024 – 2032* (Report GMI6407). (2023). Global Market Insights. https://www.gminsights.com/industry-analysis/cybersecurity-insurance-market

5. Farley, J. (2023). 2023 U.S. cyber market conditions outlook report. Gallagher. https://www.ajg.com/us/-/media/files/gallagher/us/2023-us-cyber-market-conditions-outlook-report.pdf

6. Parashchak, O. (2023). *Cyber insurance 2023 global insurance ranking of cyber insurers by premiums*. Beinsure Digital Media. https://beinsure.com/global-ranking-cyber-insurers/#top-5-insurer-by-gross-direct-premiums-written-for-cyber-insurance