Список використаних джерел:

1. Pulse of Fintech. H2`2022. Global analysis of fintech investment. KPMG. 2023.
2. Stephanie Colestock. The 6 Best Digital Insurance Providers of 2023. URL: https://www.investopedia.com/best-digital-insurance-5069849 .
3. Самошкіна І.Д. Розвиток діджиталізації страхового ринку України. Економіка та суспільство. 2022. №41.
4. Шишпанова Н. О., Боднар О. А. Розвиток страхового ринку України в умовах трансформаційних змін. / Електронне наукове фахове видання з економічних наук Modern Economics. №26. 2021. С.185-189.

Нестерчук Т.В.,
здобувач вищої освіти обліково-фінансового факультету
Науковий керівник – **Мельник О. І**., канд. екон. наук, доцент,
доцент кафедри фінансів, банківської справи та страхування,
Миколаївський національний аграрний університет

КІБЕРАТАКИ ЯК ПРИЧИНИ АКТИВНОГО РОЗВИТКУ КІБЕРСТРАХУВАННЯ

Поняття кіберстрахування є досить новим і мало дослідженим для світу, але на сьогодні воно стає все більш актуальним, оскільки багато підприємств та організацій потребують захисту від кібератак. Статистичні дані свідчать, що втрати світової економіки в результаті кібератак зростають з кожним роком.

За даними дослідження IBM та Ponemon Institute, у 2022 році витік даних у всьому світі коштував 4,4 мільйона доларів проти 4,2 мільйона у 2021 році та 3,9 мільйона доларів у 2020 році [1].

Кібератаки спрямовані на завдання шкоди важливим документам та системам у комп'ютерній мережі, які можуть належати як корпоративному, так і персональному сектору, а також на отримання незаконного доступу до них. Ці атаки можуть бути здійснені окремими особами або цілими організаціями з політичних, кримінальних або особистих мотивів з метою вилучення секретної інформації або отримання доступу до неї [2].

Кілька прикладів кібератак, які частіше виникають в умовах сьогодення: використання шкідливого програмного забезпечення; розподілені атаки на відмову в обслуговуванні (DDoS); фітинг; SQL-ін'єкції; міжсайтові сценарії (XSS); бот-мережі та зловмисні програми з вимогою викупу [2].

Нещодавно компанія Munich Re провела дослідження Global Cyber Risk and Insurance Survey 2022, результати якого були оприлюднені на офіційному сайті компанії [3]. Більш ніж 7000 учасників із 14 країн були залучені до проведення цього опитування (рис. 1).

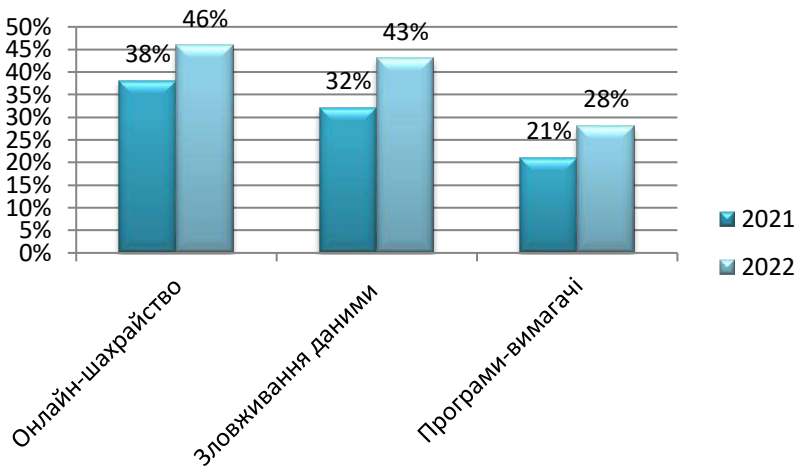

Рисунок 1 – **Найпоширеніші види кібератак у світі, 2021-2022 рр.**
Джерело: побудовано автором за даними [3]

На глобальному рівні результати опитувань свідчать про зростання кількості атак з використанням програмного забезпечення-вимагача, крадіжки даних та шахрайства в Інтернеті з кожним роком. Доля програм-вимагачів зросла з 21% до 28%, використання даних зросло з 32% до 43%, а шахрайства в Інтернеті зросли з 38% до 46 відсотків.

Оскільки зростає кількість кібератак на підприємства та організації, кіберстрахування стає все більш популярним. Кіберстрахування – це вид страхування, який надає захист від ризиків, пов'язаних з кібербезпекою, таких як кібератаки, крадіжки даних, порушення конфіденційності даних, вимагання викупу, втрата даних та інші. Кіберстрахування може включати різні види покриття, такі як страхування втрати даних, страхування відповідальності за порушення конфіденційності даних, страхування втрати прибутку внаслідок кібератаки та інші.

Поліси кіберстрахування це продукти страхування, які застосовуються для захисту бізнесу та фізичних осіб від кіберзагроз. Однак, наразі не існує стандартних характеристик для цих полісів. В різних страхових компаніях умови та ліміти відповідальності (покриття) суттєво відрізняються одне від одного [4].

Виплати за кіберстрахові договори зростають як в нашій країні, так і у світі, що підвищує рівень довіри страхувальників до цієї послуги. Зокрема, у 2021 році обсяг страхових виплат за ризиками, пов'язаними з вірусами-вимагачами, збільшився у 4 рази у всьому світі [4].

Для отримання адекватної страхової виплати у разі страхового випадку необхідно звернути достатню увагу на договір зі страховою компанією. Іноді страхові компанії пропонують розширення договорів страхування майна та відповідальності для відповіді на запити компаній щодо певного покриття, але покриття за кіберризиками в таких договорах зазвичай обмежене через специфіку страхування. Тому, рекомендується укладати окремий договір щодо страхування кіберризиків, щоб закріпити правовідносини [4].

У сучасних умовах страхові компанії дуже швидко змінюються. Особливо стрімко розвивається InsurTech, який використовує передові технології машинного навчання, розробки в галузі кібербезпеки, блокчейн та аналіз великих даних. Ці технології дозволяють страховим компаніям формувати дійсно актуальні продукти для споживачів зі страхування кіберризиків [4].

Отже, можна зробити висновок, що кіберстрахування є дуже важливою сферою страхового ринку, особливо в контексті зростаючих загроз від кібератак. За останні кілька років обсяги страхових виплат за кіберризиками значно збільшилися, що свідчить про зростання популярності цього виду страхування. Використання кіберстрахування може зменшити ризик фінансових втрат і репутаційних шкод для підприємства чи організації у разі кібератаки.

Список використаних джерел:

1. Global average total cost of a data breach in 2022 growth up to $4.4 mn. URL: https://beinsure.com/news/global-average-data-breach-2022/ (дата звернення 13.04.2023).
2. Що таке кібератака? URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-cyberattack (дата звернення 13.04.2023).
3. Munich Re Global Cyber Risk and Insurance Survey 2022. URL: https://www.munichre.com/landingpage/en/global-cyber-risk-and-insurance-survey-2022.html (дата звернення 14.04.2023).
4. Кіберстрахування: характеристика та особливості. URL: https://www.lawfirm-pryadko.com/articles/kiberstrahovanie_harakteristika_i_osobennosti (дата звернення 14.04.2023).
5. Полторак А. С., Мельник О. І., Баришевська І. В. Фінансова безпека страхового ринку України. *Modern Economics*. 2021. № 28. С 110-117.