Електронне наукове фахове видання **"Ефективна економіка"** включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України від 11.07.2019 № 975)
www. economy.nayka.com.ua | № 4, 2020 | 30.04.2020 р.

DOI: 10.32702/2307-2105-2020.4.6

УДК 336.368

*Н. В. Приказюк,*
*д. е. н., доцент, зав. кафедри страхування, банківської справи та ризик-менеджменту,*
*Київський національний університет імені Тараса Шевченка*
*ORCID ID: 0000-0002-7813-8590*
*Л. С. Гуменюк,*
*студентка 2 курсу магістратури,*
*спеціальність «Фінанси, банківська справа та страхування»,*
*Київський національний університет імені Тараса Шевченка*
*ORCID ID: 0000-0002-2803-913X*

# КІБЕР-СТРАХУВАННЯ ЯК ВАЖЛИВИЙ ІНСТРУМЕНТ ЗАХИСТУ ПІДПРИЄМСТВ В УМОВАХ ЦИФРОВІЗАЦІЇ ЕКОНОМІКИ

*N. Prykaziuk*
*Doctor of Economic Sciences, associate Professor,*
*Head of Department of Insurance, Banking and Risk Management*
*Taras Shevchenko National University of Kyiv*
*L. Gumenyuk*
*Master student of the Departament of Finance, banking and risk management,*
*Taras Shevchenko National University of Kyiv*

## CYBER-INSURANCE AS AN IMPORTANT TOOL OF ENTERPRISE PROTECTION IN THE DIGITIZATION ECONOMY

*У статті виявлено тенденції та перспективи розвитку кібер-страхування як важливого механізму захисту підприємств в умовах цифровізації економіки. З'ясовано, що розвиток технологій тягне за собою розвиток злочинності з використанням IT-інструментів, що негативно впливає на діяльність підприємств, оскільки для будь-якого підприємства кібер-загроза небезпечна двома видами наслідків. Встановлено, що кібер-страхування виступає ефективним інструментом, який мінімізує наслідки від настання страхових подій, пов'язаних з кібер-ризиками. Виявлено основні тенденції кібер-страхування у світі та визначено особливості кібер-страхування в Україні. Визначено, що сьогодні на шляху розвитку кібер-страхування багатьох країн стоїть низка перешкод, які проявляються як зі сторони підприємств-страхувальників, так і зі сторони страхових компаній. Окреслено основні перешкоди та відповідні перспективи розвитку кібер-страхування як важливого інструменту захисту підприємств в умовах цифровізації економіки.*

*The article examines the impact of cyber risks on business activity in the world, identifies the main trends of cyber insurance in the world, identifies the features of cyber insurance in Ukraine, outlines obstacles and prospects for the development of cyber insurance as an important tool for protecting businesses in the digital economy.*

*The accelerated transition of businesses to digital technologies, as well as the increasing links between the IT systems they use, make cyber threats one of the major global challenges for commercial companies. The risks of financial losses become more significant, which helps drive business demand for cyber insurance.*
*In progressive countries, cyber insurance is spreading due to the awareness of business owners and IT managers in the cybersecurity sector, namely through the inability to fully control information systems and the possibility of compromising them. That is why cyber insurance provides a number of coverages that protect companies in the case of targeted hacking, phishing, cyber extortion and breach of personal data, and in some insurance companies can compensate for such additional costs: cyber crime investigation, anti-crisis PR, costs court protection and IT systems resumption.*
*Today, there are a number of barriers to cyber insurance in many countries, both from insurers and from insurance companies. In particular, insurers are reluctant to disclose their information to insurers and to give proper access to their information systems, are not ready to allocate funds for cyber insurance, do not understand the possible amount of losses / losses and what exactly to insure, are not interested in disclosing the fact of cyber-attack.*
*From the standpoint of insurance companies, the obstacles hindering the development of cyber insurance are such as: uncertainty in the regulation of relationships in cyber insurance, lack of information for actuarial calculations, concentration of risks in the event of an insured event.*
*In addition, for insurers and insurers, the issue of risk sharing between the insurance company and the company, as well as the allocation of costs / losses to direct and indirect, are relevant.*
*The elimination of these problems will serve as a basis for the active development of cyber insurance as an important tool for protecting businesses in the digital economy.*

***Ключові слова:*** *Кібер-страхування; кібер-ризик; кібер-атака; кібер-захист; підприємство; цифровізація економіки.*

***Key words:*** *Cyber insurance; cyber risk; cyber attack; cyber protection; enterprise; economy digitization.*

**Постановка проблеми.** В еру цифрових технологій ІТ-системи відіграють одну із ключових ролей у діяльності підприємств, оскільки більшість бізнес-процесів функціонують за їх допомогою. Виходячи з цього, важливість безпеки даних систем є пріоритетним питанням для менеджменту будь-якої компанії, задля попередження можливих втрат, що все частіше виникають через збільшення кількості кібер-атак.

Кібер-страхування є в першу чергу ефективним інструментом для «згладжування» наслідків кібер-атак. Світовий досвід доводить, що при своєчасному огляді інформаційного та технологічного забезпечення підприємства, у менеджменту є час на усунення проблем, а тому і зниження рівня вразливості систем.

Поширенню даного виду страхування в Україні перешкоджає недостатній рівень довіри страхувальників до страховиків, а також відсутність розуміння розміру можливих фінансових та репутаційних втрат від дій кібер-злочинців.

**Аналіз останніх досліджень та публікацій.** Питанням кібер-страхування та його розвитку на сучасному етапі займались такі вітчизняні вчені, як В.Д. Базилевич, Н.М.Внукова, О.О. Гаманкова, Ю.П. Гришан, О.М. Залєтов, А.Д. Заруба, Р.В. Пікус, а також зарубіжні науковці: Дж. Арчі, К. Сарда, Дж. Фінкл. У той самий час, проблематика розвитку кібер-страхування залишається недостатньо розкритою, оскільки існує потреба у виявленні сучасних світових тенденцій у сфері кібер-страхування та позиції вітчизняних страховиків щодо готовності представити продукти кібер-страхування на страховому ринку України.

**Формування цілей дослідження.** Метою роботи є виявлення тенденцій та перспектив розвитку кібер-страхування як важливого механізму захисту підприємств в умовах цифровізації економіки.

Для досягнення поставленої мети в роботі окреслено і вирішено такі завдання:

– з'ясувати вплив кібер-ризиків на діяльність підприємств у світі;

– виявити основні тенденції кібер-страхування у світі;

– визначити особливості кібер-страхування в Україні;

– окреслити перешкоди та перспективи розвитку кібер-страхування як важливого інструменту захисту підприємств в умовах цифровізації економіки.

**Виклад основного матеріалу дослідження.** Останні 5 років відзначились значним стрибком у розвитку цифрових технологій та вдосконаленні ІТ-інфраструктури. В основі вказаного масштабування і швидкої цифровізації всіх сфер життєдіяльності і бізнесу лежить використання ряду інформаційних засобів (не тільки уже імплементованих і перевірених, а й нових). Але навіть в уже існуючих цифрових інструментах

питання безпеки не є вирішеним. Тому розвиток технологій тягне за собою розвиток злочинності з використанням IT-інструментів, від якого потерпають не лише індивідуальні суб'єкти, а й підприємства та держави.

Протягом 2015-2019 рр. у світі було зареєстровано більше 1600 кібер-атак на суб'єкти підприємницької діяльності. Так у 2019 році їх кількість збільшилась на 40% у порівнянні з 2015, що пояснюється поширенням хмарних сервісів загального доступу та поширенням криптовалюти. Також за вказаний період спостерігався позитивний тренд росту кібер-інцидентів і був у середньому на рівні 9%.

Важливим індикатором стану кібер-захищеності підприємств є рівень успішності здійснених кібер-атак. Даний показник становив понад 70% протягом усього проаналізованого періоду та досягнув пікового значення 79% у 2017 році через популяризацію хмарних продуктів спільного доступу для малих та середніх підприємств (Рис1). Це свідчить про критично низький рівень розвитку кібер-захисту підприємств в усьому світі.

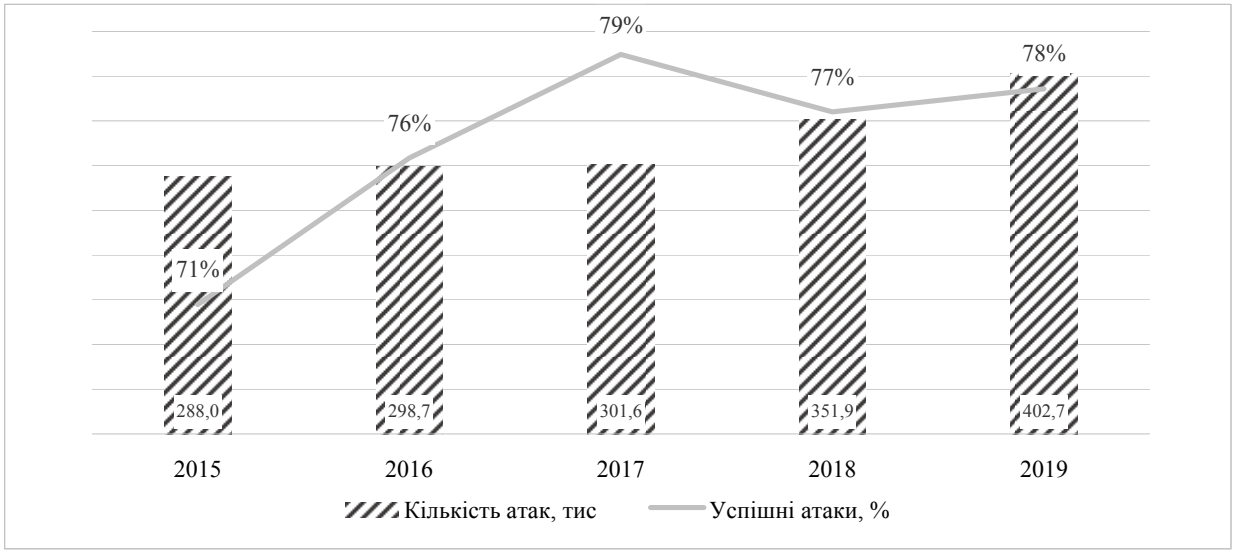


**Рис. 1. Зареєстровані кібер-атаки у світі 2015-2019рр.**
*Джерело: Складено авторами на основі [9]*

Зовнішнє несанкціоноване втручання в діяльність організацій порушує звичний порядок функціонування бізнес-процесів, що в свою чергу може мати такі негативні наслідки:

– економічні (викрадення корпоративної інформації, фінансової інформації, реквізитів клієнтів; втрата інформації про контракти та договори; ремонт пошкоджених систем та відновлення інформації);

– репутаційні (втрата клієнтів, інвесторів; зниження рівня продажів; розвив відносин з партнерами, постачальниками);

– юридичні (порушення законодавства щодо безпеки персональних даних).

У США існує ефективна система захисту приватної інформації для малого і середнього бізнесу, а також широкий набір інструментів, що забезпечують покарання за порушення її конфіденційності. За підсумками 2019 року у США середня сума втрат організацій була на рівні $8,1 млн, що на 39% більше, ніж у 2015 році (Рис. 2). В першу чергу це пояснюється таргетованими атаками, які включають в себе комплекс інструментів, які вражають одночасно кілька систем і пошкоджують кілька рівнів безпеки.


**Рис. 2. Середня сума втрат організації у США внаслідок кібер-атак 2015-2019 рр.**
*Джерело: Складено авторами на основі [10]*

Наслідками кібер-атак є не лише прямі грошові втрати, а й зменшення рівня довіри до організації, тому питання безпеки має бути одним із головних в сучасних умовах цифровізації. Задля повноцінного кіберзахисту процедури мають носити комплексний характер і включати в себе:

– навчання та тестування працівників організації щодо основних правил кібер-безпеки;

– імплементація та підтримка захищеності пристроїв та програмного забезпечення;

– налаштування захищених мереж та каналів передачі даних, шифрування даних, правильна конфігурація хмарних сервісів;

– впровадження системи обмеженого доступу до внутрішньої інформації;

– створення групи кібер-безпеки та найм відповідного персоналу [6].

Очевидно, що даний комплекс є дороговартісним і потребує значного часу на впровадження у організації. За підрахунками Gartner, для середньої за розмірами компанії (до 100 працівників) створення підрозділу, який буде відповідальний за кібер-безпеку, займе більше 6 місяців [4]. У зв'язку з цим необхідним і ефективним варіантом захисту підприємств є кібер-страхування.

Кібер-страхування є доволі новим явищем і втілюється через комплекс страхових продуктів, що мінімізують ризик настання страхової події, а також відшкодовують значну частину збитків після її настання. Перші договори кібер-страхування були підписані приватними підприємствами у США ще у 2010 році, в якості зменшення відповідальності власників за збереження наявної у них інформації про клієнтів. Починаючи з 2013 року відбувся активний ріст вказаного виду страхування в зв'язку з масовим зломом корпоративних і державних ресурсів США. Після чого у процесі розвитку кібер-страхування були виділені основні групи ризиків та витрати, які воно покриває (Табл. 1).

**Таблиця 1.**
**Покриття страховими компаніями витрат від кібер-ризиків**

| Вид ризику | Витрати, які покриваються |
|---|---|
| Збитки, пов'язані з порушенням бази даних (цільова атака) | - збитки в результаті порушення корпоративної інформації (комерційні таємниці, професійна інформація, бюджети, клієнтська база даних);<br>- збитки в результаті порушення безпеки комп'ютерної системи (Dos- і DDos-атаки, ураження вірусами, знищення, модифікація або видалення інформації, фізична крадіжка або втрата обладнання);<br>- пошкодження програмного забезпечення або комп'ютерів;<br>- збитки в результаті внутрішньої кібер-атаки (крадіжка співробітниками, знищення інформації, сприяння цільовій атаці). |
| Адміністративне розслідування відносно втрати даних | - збитки страхувальника спричинені розслідуванням в результаті порушення законодавства чи інших нормативно-правових актів у зв'язку з обробкою даних або корпоративної інформації, за які страхувальник несе відповідальність. |
| Витрати на реагування при порушенні даних (кібер-інцидент) | - витрати на реагування та проведення програмно-технічної експертизи, розслідування і встановлення причини інциденту;<br>- витрати на відновлення репутації страхувальника і фізичних осіб, через витік даних;<br>- витрати на відновлення електронних програм і даних. |
| Відповідальність за контент інформації | - збитки страхувальника спричинені публічним розкриттям інформації в результаті недостовірної заяви, викликаної помилкою або заявою, що вводить в оману. |
| Віртуальне вимагання | - збитки від віртуального вимагання: гроші, сплачені страхувальником з письмової згоди страховика з метою обмеження або припинення загрози небезпеки, в іншому випадку може привести до збитку (загрози про знищення даних); а також вартість проведення кримінального кібер розслідування з метою визначення причини загрози небезпеки. |
| Перерва в процесі виробництва | - збитки в результаті збою у роботі (припинення роботи) в мережі в сумі не отриманого прибутку (доходи, які повинні бути отримані, зменшені на суму витрат, які повинні бути зроблені);<br>- збитки і відшкодування втрачених доходів внаслідок порушення в роботі IT-системи, мережі та веб-сайтів через кібер-атаки (припинення роботи). Обсяг таких доходів розраховується на основі даних за попередні періоди діяльності компанії, а також планів на поточний період. |
| Соціальна інженерія (нецільова атака) | - збитки від втрати грошових коштів і активів страхувальника, які відбулися в результаті застосування технологій фішингу, картингу (нецільові атаки) |

*Джерело: Складено авторами на основі [2, 5, 7, 12]*

Таким чином кібер-страхування надає ряд покриттів, що захищають компанії в разі цілеспрямованих хакерських атак, фішингу, кібер-вимагань та порушення конфіденційності персональних даних. Додатково,

страхові компанії можуть компенсувати такі додаткові витрати: розслідування кібер-злочину, антикризовий піар, витрати на захист в суді і відновлення роботи IT-систем.

В ідеальному стані, можна сказати, що поліс кібер-страхування – це комплексний продукт, який включає в себе страхування майна, відповідальності та фінансових ризиків. Основний страховий випадок – збитки, які виникли в результаті порушення роботи комп'ютерної мережі (або її систем безпеки) страхувальника через вторгнення третіх осіб. Якщо брати в цілому, то кібер-страхування можна поділити на два види: страхування першої особи та третьої особи, тобто організації і даних її клієнтів відповідно.

Світовий досвід свідчить, що кібер-атаки направлені на викрадення агрегованих конфіденційних даних, тобто таких, які зберігаються організаціями на цифрових носіях, тому питання розвитку кібер-страхування третьої особи набуває особливої важливості. Організації у США, після серії атак на домогосподарства у 2014 році, почали активно користуватись послугами страховиків у розрізі кібер-захисту. Починаючи з 2015 року сума страхових премій почала щорічно зростати в середньому на 20% і в 2019 році становила $6,2 млдр, що вдвічі більше від початкової суми (Рис. 3).

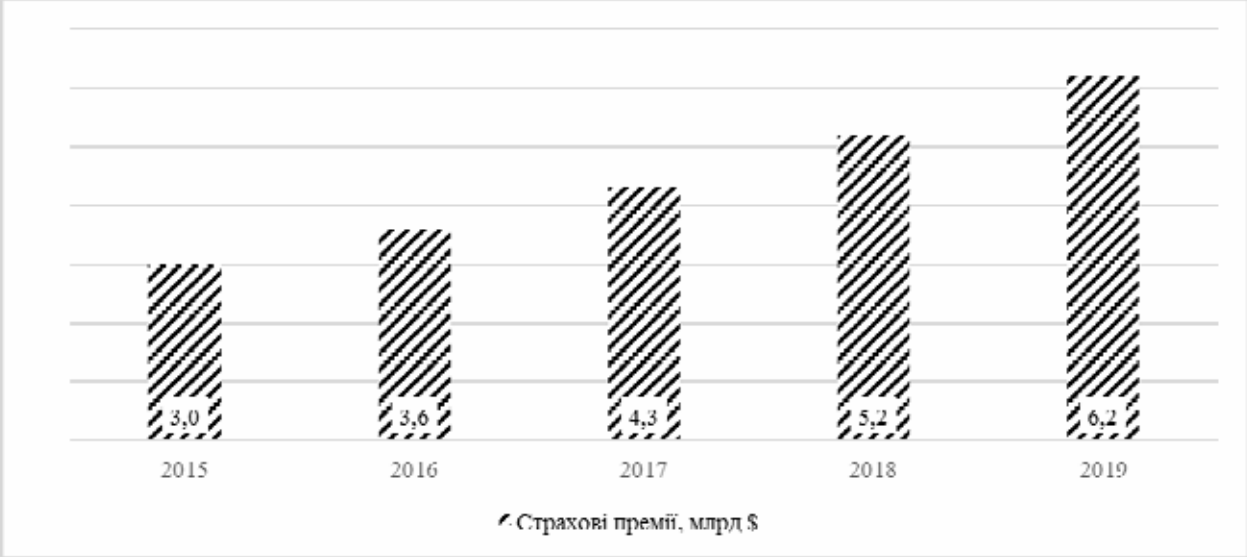


**Рис. 3. Страхові премії на кібер-страхування у світі в 2015-2019 рр.**
*Джерело: Складено авторами на основі [11]*

Щодо України, то кібер-страхування є новим і малопопулярним явищем, хоча менеджмент підприємств і розуміє необхідність його впровадження, але в середньостроковій перспективі ситуація не зміниться, оскільки у компаній відсутні достатні фінансові резерви для таких змін. Незважаючи на низький попит, в Україні дві страхові компанії пропонують страхові поліси, що покривають частину кібер-ризиків. Наприклад страхова компанія «UPSK» надає повний комплекс покриття ризиків, у той час коли страхова компанія «АСКА» пропонує індивідуальний підхід з можливістю вибору необхідних ризиків залежно від специфіки господарської діяльності (Табл. 2).

**Таблиця 2.**
**Види кібер-ризиків, які покривають страхові компанії «UPSK» та «АСКА»**

| Вид ризику | СК «UPSK» | СК «АСКА» |
|---|---|---|
| Збитки, пов'язані з порушенням бази даних (цільова атака) | + | + |
| Адміністративне розслідування відносно втрати даних | + | - |
| Витрати на реагування при порушенні даних (кібер-інцидент) | + | + |
| Відповідальність за контент інформації | + | - |
| Віртуальне вимагання | + | + |
| Перерва в процесі виробництва | + | + |
| Соціальна інженерія (нецільова атака) | + | - |

*Джерело: Складено авторами на основі [7,8]*

Таким чином для українських страховиків залишається поки незайнятою ніша кібер-страхування. Але тут важливим аспектом виступає правильне позиціонування страхових компаній, оскільки кібер-страхування не створить безпеку для бізнесу, а стане додатковим інструментом для відшкодування збитків.

У сучасних умовах спостерігається штучний попит на страхування кібер-ризиків, який створюється страховими компаніями, а не постраждалими суб'єктами. Це пояснюється тим, що більшість підприємств не готові виділити необхідну суму коштів на захист від кібер-інцидентів, оскільки не розуміють можливої суми

збитку, або не впевнені, що саме варто застрахувати. Якщо взяти для порівняння автострахування, з чітким розумінням об'єкту страхування і логікою розрахунку відшкодування збитку, в залежності від моделі та року випуску автомобіля, то в кібер-страхуванні точної кінцевої суми немає.

Крім того, найчастіше страхувальники не хочуть розголошувати факт кібер-нападу, оскільки це матиме вплив на їх репутацію і, якщо дивитись у довгостроковій перспективі, знизить ймовірність надходження нових клієнтів.

Ще однією перешкодою на шляху розвитку кібер-страхування з позиції підприємств-страхувальників є небажання останніх розкривати свою інформацію перед страховими компаніями та надавати належний доступ до своїх інформаційних систем.

З позиції страхових компаній, основними проблемами, що стримують розвиток кібер-страхування, є такі як невизначеність регулювання відносин у кібер-страхуванні (відсутність у багатьох країнах законодавства, яке регулює відносини у сфері захисту особистих даних, регламентації вимог щодо способу їх зберігання і визначення покарання за їх порушення), нестача інформації для проведення актуарних розрахунків, концентрація ризиків у разі настання страхового випадку [1].

Усунення окреслених вище перешкод (як з позиції підприємств-страхувальників, так і з позиції страхових компаній), слугуватиме підґрунтям для активного розвитку кібер-страхування як важливого інструменту захисту підприємств в умовах цифровізації економіки.

Також питання розподілу втрат/збитків на прямі і непрямі є критичним як для страхувальника, так і для страховика. Для якісного захисту необхідним є здійснення оцінки стану підприємства до підписання угод, щоб врахувати усі особливості ведення операційної діяльності, а також щоб виявити недоліки в існуючих системах. Цей процес є складним як для окремих менеджерів напрямків підприємства, так і для його власників, оскільки не існує конкретної методології підрахунку кількісних і якісних показників компанії з позиції визначення кібер-ризиків та покриття по ним.

Сьогодні, відповідно до міжнародних стандартів PCI DSS (Payment Card Industry Data Security Standard) та GDPR (General Data Protection Regulation), можливими стали розрахунки прямих збитків – штрафів за втрату або порушення умов зберігання персональних даних клієнтів міжнародних фінансових організацій, сервісних компаній та транснаціональних ритейлерів[3].

Для світового ринку кібер-страхування актуальним постає питання, що пов'язане з розподілом ризиків між страховиком та страхувальником, або ж частиною ризиків, що можуть покриватись страховою компанією. Для українських реалій ведення бізнесу приклади американської та європейської практики, у якій під час врегулювання питань щодо суми компенсації клієнтам за розповсюдження їх персональних даних, суди були на стороні страхової компанії, стануть відштовхуючими по відношенню до напрямку кібер-страхування в цілому.

Таким чином перед державами та страховими компаніями постає завдання в першу чергу підвищення рівня довіри до страхування, а згодом і вжиття заходів щодо поширення необхідного в сучасних умовах виду страхування, який покриває кібер-ризики.

**Висновки і перспективи подальших досліджень у даному напрямку.** Ефективне функціонування будь-якої організації залежить від узгодженості та неперервності усіх її внутрішніх бізнес процесів. Для будь-якого підприємства кібер-загроза небезпечна двома видами наслідків: по-перше, це можливий фізичний збиток устаткуванню або продукції і зупинка виробництва внаслідок збою; по-друге, це втрата інформації і, як наслідок, репутаційні і фінансові збитки.

Кібер-страхування виступає ефективним інструментом, який мінімізує наслідки від настання страхових подій, пов'язаних з кібер-ризиками. На міжнародному ринку даний вид страхування почав набувати поширення після ряду кібер-атак у 2010 році, і сьогодні у світі більше 60 компаній, які пропонують поліси кібер-страхування. Даний інструмент забезпечує фінансову процедуру відновлення компанії, її повернення до стабільного функціонування та зниження ймовірності перерви у виробництві.

У розвинених країнах кібер-страхування поширюється через обізнаність власників та IT-менеджерів підприємств у сфері кібер-безпеки, а саме через розуміння неспроможності повного контролю інформаційних систем і існування можливості їх компрометації. Саме тому кібер-страхування надає ряд покриттів, що захищають компанії в разі цілеспрямованих хакерських атак, фішингу, кібер-вимагань та порушення конфіденційності персональних даних, а в окремих страхові компанії можуть компенсувати такі додаткові витрати: розслідування кібер-злочину, антикризовий піар, витрати на захист в суді і відновлення роботи IT-систем.

На даному етапі український страховий ринок відстає від світового рівня розробки і впровадження напрямку кібер-страхування. Лише дві компанії пропонують комплексний поліс покриття кібер-ризиків, що свідчить про перспективність розвитку вказаної ніші страхування.

Сьогодні на шляху розвитку кібер-страхування багатьох країн стоїть низка перешкод, які проявляються як зі сторони підприємств-страхувальників, так і зі сторони страхових компаній. Зокрема, страхувальники не бажають розкривати свою інформацію перед страховиками та надавати належний доступ до своїх інформаційних систем, не готові виділяти кошти на кібер-страхування, не розуміють можливу суму втрат/збитків та що саме варто застрахувати, не зацікавлені розкривати факт кібер-атаки.

З позиції страхових компаній перешкодами, що стримують розвиток кібер-страхування, є такі як: невизначеність регулювання відносин у кібер-страхуванні, нестача інформації для проведення актуарних розрахунків, концентрація ризиків у разі настання страхового випадку.

Крім того, для страховиків і страхувальників актуальними є питання розподілу ризиків між страховою компанією і підприємством, а також розподілу витрат/збитків на прямі і непрямі.

Усунення даних проблем, слугуватиме підґрунтям для активного розвитку кібер-страхування як важливого інструменту захисту підприємств в умовах цифровізації економіки.

**Список використаної літератури.**


1. Приказюк Н. В. Необхідність та можливість впровадження нових страхових продуктів у страховій системі (на прикладі кіберстрахування) / Н. В. Приказюк // *Економіка і фінанси*. – 2016. – № 12. – С. 109–117.
2. Якушев В.О., Кібербезпека-2018: чого чекати бізнесу? [Електронний ресурс]. – Режим доступу: https://mind.ua/openmind/20180414-kiberbezpeka-2018-chogo-chekati-biznesu/ (Дата звернення: 06.04.2020).
3. Офіційний сайт DGPR [Електронний ресурс]. – Режим доступу: https://gdpr-info.eu/ (Дата звернення: 06.04.2020).
4. Офіційний сайт компанії Gartner [Електронний ресурс]. – Режим доступу: https://www.gartner.com/en/ (Дата звернення: 06.04.2020).
5. Офіційний сайт страхової компанії Allianz [Електронний ресурс]. – Режим доступу: https://www.agcs.allianz.com/ (Дата звернення: 06.04.2020).
6. Офіційний сайт страхової компанії UpGuard [Електронний ресурс]. – Режим доступу: https://www.upguard.com// (Дата звернення: 06.04.2020).
7. Офіційний сайт страхової компанії UPSK [Електронний ресурс]. – Режим доступу: https://upsk.com.ua/ (Дата звернення: 06.04.2020).
8. Офіційний сайт страхової компанії АСКА [Електронний ресурс]. – Режим доступу: https://aska.ua/ (Дата звернення: 06.04.2020).
9. 2019 Cyberthreat Defense Report [Електронний ресурс]. – Режим доступу: https://www.imperva.com/resources/reports/CyberEdge-2019-CDR-Report-v1.1.pdf (Дата звернення: 06.04.2020).
10. Average cost per data breach in the United States 2006-2019 [Електронний ресурс]. – Режим доступу: https://www.statista.com/statistics/273575/average-organizational-cost-incurred-by-a-data-breach/ (Дата звернення: 06.04.2020).
11. Estimated value of cyber insurance premiums written worldwide from 2014 to 2020 [Електронний ресурс]. – Режим доступу: https://www.statista.com/statistics/533314/estimated-cyber-insurance-premiums/ (Дата звернення: 06.04.2020).
12. The Global Risks Report 2017 [Електронний ресурс]. – Режим доступу: http://wef.ch/risks2017/ (Дата звернення: 06.04.2020).


**References.**


1.Prykaziuk, N. V. (2016), "Necessity and possibility of introduction of new insurance products in the insurance system (on the example of cyber insurance)", Ekonomika i finansy, vol. 12, pp. 109–117.

2.Yakushev, V.O. (2018), "Cybersecurity 2018: What to Expect for Business?", [Online], available at: https://mind.ua/openmind/20180414-kiberbezpeka-2018-chogo-chekati-biznesu/ (Accessed 06 Apr 2020).

3.DGPR Official Website (2020), [Online], available at: https://gdpr-info.eu/ (Accessed 06 Apr 2020).

4.Gartner Official Website (2020), [Online], available at: https://www.gartner.com/en/(Accessed 06 Apr 2020).

5.Official site of Allianz Insurance Company (2020), [Online], available at: https://www.agcs.allianz.com/ (Accessed 06 Apr 2020).

6.The official website of UpGuard Insurance Company (2020), [Online], available at: https://www.upguard.com/ (Accessed 06 Apr 2020).

7.Official Website of UPSK Insurance Company (2020), [Online], available at: https://upsk.com.ua/ (Accessed 06 Apr 2020).

8.Official site of ASKA Insurance Company (2020), [Online], available at: https://aska.ua/ (Accessed 06 Apr 2020).

9.CyberEdge Group (2019), “Cyberthreat Defense Report”, [Online], available at: https://www.imperva.com/resources/reports/CyberEdge-2019-CDR-Report-v1.1.pdf (Accessed 06 Apr 2020).

10. Statista (2020), “Average cost per data breach in the United States 2006-2019”, [Online], available at: https://www.statista.com/statistics/273575/average-organizational-cost-incurred-by-a-data-breach/ (Accessed 06 Apr 2020).

11. Statista (2020), “Estimated value of cyber insurance premiums written worldwide from 2014 to 2020”, [Online], available at: https://www.statista.com/statistics/533314/estimated-cyber-insurance-premiums/ (Accessed 06 Apr 2020).

12. World Economic Forum (2017), “The Global Risks Report”, [Online], available at: http://wef.ch/risks2017/ (Accessed 06 Apr 2020).



*Стаття надійшла до редакції 11.04.2020 р.*