УДК 336.368

ПРИКАЗЮК Наталія Валентинівна
доктор економічних наук, професор,
завідувач кафедри страхування, банківської справи та ризик-менеджменту,
Київський національний університет імені Тараса Шевченка, Україна
ORCID ID: 0000-0002-7813-8590
e-mail: pnvuniv15@ukr.net

ГУМЕНЮК Людмила Сергіївна
аспірант,
Київський національний університет імені Тараса Шевченка, Україна
ORCID ID: 0000-0002-2803-913X
e-mail: mila20071997@gmail.com

ДОРОЖНЯ КАРТА ВПРОВАДЖЕННЯ КІБЕР-СТРАХУВАННЯ В УКРАЇНІ

У статті проаналізовано процес впровадження кібер-страхування у світі та запропонована Дорожня карта його впровадження в Україні. Розглянуто ключові цілі та завдання, які стоять перед страховим ринком України та регулятором задля досягнення вказаної мети. Окреслено орієнтовні терміни на проведення необхідних заходів по підготовці впровадження кібер-страхування в українській економіці. Виокремлено ключові особливості нормативно-правових актів у сфері кібер-безпеки у країнах ЄС та Австралії та запропоновано способи їх адаптації в Україні. Виділено перспективні засоби по підвищенню захищеності фізичних та юридичних осіб у цифровому просторі на прикладі механізму взаємодії страховиків і експертних організацій у Австралії. Окреслено основні вектори співпраці страхових компаній та експертних організацій у сфері кібер-безпеки на українському та світовому страхових ринках. Розроблено систему взаємодії суб'єктів кібер-страхових відносин із позиціонуванням страхувальника в центрі відносин, як ключового учасника страхування, що доводить високу клієнтоорієнтованість даного напрямку страхового бізнесу. Обґрунтовано актуальні проблеми українського страхового ринку та з'ясовано шляхи їх вирішення через механізм впровадження кібер-страхування: моделювання механізму оцінки втрат від кібер-атак, моніторинг поточного стану страхувальників, розробка шляхів мінімізації настання кібер-інцидентів. Проаналізовано динаміку настання кібер-інцидентів у 2020 році та виявлено кореляцію між настанням світових локдаунів, спричинених COVID-19, та ростом кількості кібер-атак. На основі проведеного аналізу доведено, що впровадження кібер-страхування в Україні є необхідним інструментом для убезпечення усіх учасників страхових відносин від кібер-ризиків та для розвитку страхового ринку в цілому.

***Ключові слова**: кібер-страхування; кібер-ризик; кібер-атака; кібер-захист; дорожня карта кібер-страхування; цифровізація; ризик-менеджмент.*

JEL classification: G22
DOI: https://doi.org/10.31649/ins.2021.1.64.72

1. ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Економіки всіх країн відчули на собі негативний вплив глобальної епідемії COVID-19. Окрім впливу локдаунів, з простоями виробництва, безробіттям та високим навантаженням на медичну систему, в цей період було виявлено ще одну критичну проблему – масові та нищівні кібер-атаки, суб'єктами яких стають як звичайні

громадяни, так і компанії, організації та навіть державні установи. Варіантом убезпечення та мінімізації насідків від кібер-інцидентів є кібер-страхування. Даний вид страхування уже поширений в США, ЄС, Китаї, Австралії та інших прогресивних країнах, але поки не популярний в Україні. Вважаємо, що необхідно дослідити необхідність та особливості впровадження кібер-страхування в Україні.

2. АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Теоретичні аспекти створення та розвитку кібер-страхування розглядаються як національними, так і зарубіжними вченими, праці яких були проаналізовані у попередніх дослідженнях [1]. Для створення Дорожньої карти впровадження кібер-страхування в Україні та окреслення її прикладних аспектів доцільно брати до уваги результати аналітичних звітів IT Governance [2] та Assets [5], Положення стратегій кібер-безпеки ЄС [6] та Австралії [8], а також позиції, окресленні в Цифровій стратегії України [4].

3. ВИДІЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ, КОТРИМ ПРИСВЯЧУЄТЬСЯ ОЗНАЧЕНА СТАТТЯ

Невирішеними залишаються проблеми по розробці механізму впровадження кібер-страхування на українському страховому ринку, опису системи співпраці учасників кібер-страхових відносин та окресленню його векторів розвитку в Україні.

4. ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є розробка Дорожньої карти впровадження кібер-страхування в Україні з окресленням завдань та механізму взаємодії учасників страхових відносин.

Під час написанні статті був використані наступні методи досліджень: методи аналізу та синтезу – при окресленні необхідних заходів для впровадження кібер-страхування в Україні та формуванні Дорожньої карти його впровадження; метод порівняння – під час співставлення Стратегій кібер-безпеки ЄС і Австралії та Цифрової стратегії України; методи наукової абстракції та дедукції – в процесі побудови системи взаємозв'язків між суб'єктами кібер-страхових відносин

5. ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ З ПОВНИМ ОБҐРУНТУВАННЯМ ОТРИМАНИХ НАУКОВИХ РЕЗУЛЬТАТІВ

Питання захищеності та конфіденційності даних є особливо важливим в період відновлення економіки після кризи, спричиненої COVID-19. Цифровізація економіки є сучасним світовим трендом, який дозволяє відновити стабільність та стати драйвером розвитку традиційних фінансових ринків та технологій. З іншого боку, масовий процес діджиталізації стає причиною розвитку зловмисниками IT-технологій, спрямованих на активізацію кібер-атак, задля отримання коштів або особистих даних від потенційних жертв, компаній та навіть державних установ.

У період пандемії COVID-19 більшість організацій перейшли на віддалений режим роботи та закрили фізичні відділення своїх компаній, що стало причиною збільшення навантажень на працівників через необхідність додаткового навчання та підвищення кваліфікації. Швидкий перехід на онлайн-співпрацю не забезпечив повний контроль над захищеністю каналів спілкування та передачі даних, про що свідчить значний ріст кібер-інцидентів у 2020 році (на 64% порівняно з 2019 роком [2]). Найбільша активізація кібер-атак відбулась в період жорсткого світового локдауну у лютому-квітні 2020 року, що змусило світові організації шукати варіанти захисту та мінімізації нападів (Рисунок 1).

Відповідно до активного росту успішності кібер-атак виникає необхідність розвитку спеціалізованого виду страхування від кібер-ризиків. На сьогоднішній день у світі даний сегмент страхування є одним з найбільш перспективних та ключових напрямків у стратегіях розвитку економік країн-лідерів страхової сфери, а також організацій, що займаються захистом персональних даних.

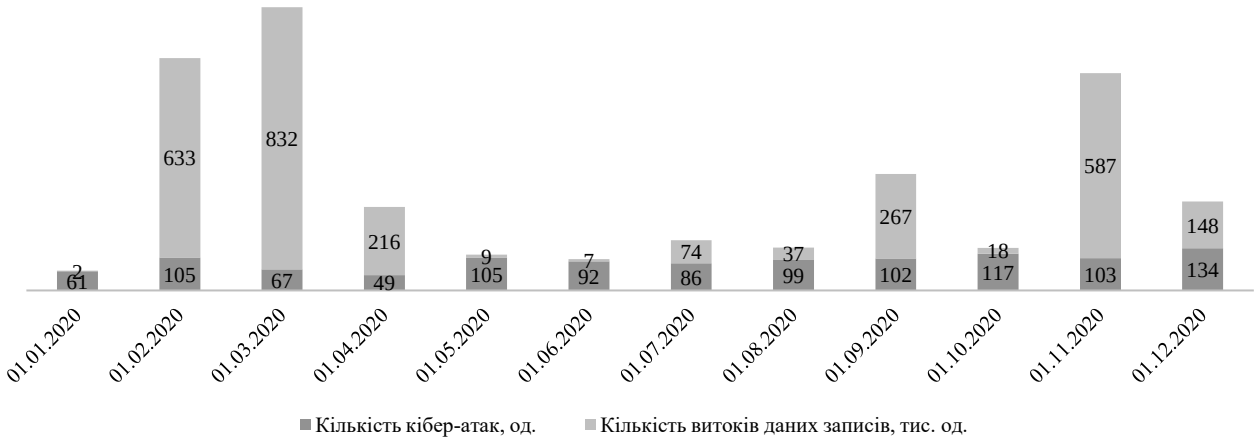

Рис. 1. **Динаміка підтверджених витоків даних у 2020 році, спричинених кібер-атаками**
Джерело: складено та розраховано авторами за матеріалами [2]

Оскільки в Україні кібер-страхування поки знаходиться на етапі зародження, з одного боку, страхові компанії не готові гарантувати захист від кібер-ризиків, а з іншого боку, споживачі не розуміють повний перелік переваг, які вони отримають за умови страхування, та методику оцінки втрат від таких ризиків.

Впровадження кібер-страхування в Україні має підвищити рівень захищеності інформації в умовах масового переходу бізнес-процесів у дистанційний формат. Для цього варто окреслити положення, які будуть включені у Дорожню карту впровадження кібер-страхування в Україні. Основною метою впровадження є підвищення захищеності каналів передачі даних та мінімізації ймовірності настання кібер-інцидентів. Для досягнення вказаної мети перед страховим ринком України та регулятором стоять завдання по реалізації наступних цілей:

1. Розширити асортимент доступних страхових послуг, що відповідають глобальним страховим трендам та регламентуються міжнародним законодавством.

2. Розробити єдину методологію оцінки наслідків кібер-атак для фізичних та юридичних осіб.

3. Підвищити рівень освіченості населення через комплексний процес інформування про кібер-ризики та варіанти захисту від них.

На підставі вищезазначеної мети окреслимо перелік заходів та орієнтовні терміни, що відводяться для їх виконання, які допоможуть досягнути вказані завдання та відобразимо у табл. 1.

Для реалізації першої цілі по розширенню продуктового портфелю страховика, з тим, щоб він відповідав міжнародним стандартам, насамперед необхідно дослідити існуючі міжнародні нормативно-правові акти, які стосуються кібер-страхування.

В першу чергу до уваги варто взяти Європейський регламент по захисту персональних даних GDPR [3], який містить уніфіковані положення і вимоги для країн-членів ЄС. Даний регламент включає директиви, положення яких спонукають змінити існуючі бізнес-процеси в Україні по обробці і передачі особистих даних всередині компаній, які ведуть діяльність та/або планують співпрацю в міжнародному полі з метою підвищення інвестиційної привабливості. Зміни будуть передбачати ведення звітності компанією про те, як збирають конфіденційну інформацію з чітким пояснення які саме дані збираються, яка мета збору, наскільки довго вони зберігаються та чи передаються третім особам. Даний процес, окрім позитивного ефекту, має зворотній негативний бік для самої компанії: перехід стане доволі дорогим, оскільки цифрова трансформація вимагає повної або часткової перебудови IT-інфраструктури, а також додаткових витрат на навчання працівників.

Таблиця 1

Дорожня карта заходів для впровадження кібер-страхування в Україні

№ Цілі	Місяць / Завдання	1	2	3	4	5	6	7	8	9	10	11	12
1.	Опрацювання міжнародних нормативно-правових актів робочою групою (представники страхових асоціацій, регулятора, страхових компаній та консультантів) та їх адаптація під український ринок	■	■	■									
	Визначення місця кібер-страхування в системі українських видів страхування та опис змін, необхідних для внесення в актуальний ЗУ «Про Страхування»	■	■	■	■	■							
2.	Кооперація страховиків та спеціалізованих організацій в галузі кібер-захисту та розробка єдиної моделі оцінки втрат від кібер-атак				■	■	■	■					
	Створення механізму взаємодії страхових компаній та спеціалізованих організацій задля оцінки стану страхувальника до моменту укладання страхового договору					■	■	■	■				
	Розробка рекомендацій по мінімізації ризиків для страхувальників на основі оцінки їх IT-інфраструктури						■	■	■	■			
3.	Розробка маркетингової стратегії для інформування населення про кібер-ризики та можливі наслідки від їх настання							■	■	■	■		
	Створення єдиної платформи для реєстрації клієнтами інформації про можливий кібер-інцидент задля отримання експертної оцінки та подальшого вибору страховика, який надає послуги захисту за отриманим видом втрат										■	■	■

Джерело: складено авторами за матеріалами [3-5]

Ще одним важливим документом, створеним ЄС разом з групою хакерів, є Стратегія кібер-безпеки ЄС [6], яка включає в себе опис заходів та інструментів, які дозволять зберігати технологічну незалежність їх кінцевими споживачами, такими як фізичні та юридичні особи, уряди та регулятори країн, а також міжнародні асоціації та організації. Стратегія охоплює медичну, транспортну, енергетичну, та інші сфери, що дозволяє охарактеризувати найбільш поширені кібер-ризики у кожному окремому напряму. Також у документі підкреслюється необхідність створення наглядового органу, який займатиметься моніторингом кібер-загроз та консультаціями у цій сфері. Таким чином, створюється підґрунтя для об'єднання країн у єдиний глобальний кібер-простір з високим рівнем технологічної захищеності.

Однією із перших країн, які розробити всеохоплюючу кібер-стратегію є Австралія. Уже сьогодні в них функціонує центр по кібер-захисту, який був створений Австралійським урядом, який виконує консультаційну та наглядову функцію у кібер-просторі країни. Даний центр діє на основі положень, закріплених у Стратегії по кібер-безпеці населення та бізнесу (Таблиця 2).

Таблиця 2

Положення Стратегії по кібер-безпеці населення та бізнесу Австралії

№	Положення
1.	Активний захист та перевірка критичної інфраструктури, якою на щоденній основі користуються австралійці.
2.	Розробка нових способів ідентифікації та розслідування кібер-злочинів, в тому числі у даркнеті.
3.	Створення багатофакторної системи захисту урядових мереж та даних.
4.	Співпраця уряду та експертів у сфері кібер-безпеки для розвитку навичок захисту від кібер-атак у населення, а також підвищення їх обізнаності.
5.	Посилення партнерства уряду з бізнесом через програму співпраці на взаємовигідних умовах у Центрі кібер-безпеки.
6.	Надання консультацій для малого та середнього бізнесу по підвищенню рівня їх захисту.
7.	Організація цілодобової гарячої лінії для громадян з питань кібер-безпеки.

Джерело: складено авторами за матеріалами [7, 8]

Детальне ознайомлення з міжнародним нормативно-правовими актами дасть змогу окреслити місце кібер-страхування в системі кібер-безпеки. Законодавство України поки не описує поняття «кібер-страхування», тому перед отриманням позитивного рішення на користь його виокремлення в окремий вид страхування, робочій групі варто визначити дане поняття саме в українському правовому полі.

Після цього отримані результати варто використати у проекті внесення змін до поточного або нового ЗУ «Про страхування».

Розробка єдиної методології оцінки наслідків кібер-атак, яка є другою ціллю, має реалізовуватись на основі комплексу заходів співпраці страховиків та експертних організацій у сфері кібер-безпеки. У європейській практиці такі організації є міжнародними та створюють єдиний механізм захисту для всіх учасників ринку. На нашу думку, для українського ринку страхування варто залучати міжнародні компанії на початковому етапі розробки загальних рекомендацій, а прикладні механізми створювати з залученням українських компаній. Така синергія буде оптимальною, оскільки в розробників є розуміння особливостей ведення бізнесу в Україні, а витрачені на імплементацію кошти будуть повертатись в українську економіку.

Співпраця з експертними організаціями може будуватись за кількома векторами, які включають в себе різні аспекти розвитку страхових компаній і оцінки їх клієнтів (Рисунок 2).

Таким чином, ми виділяємо три ключових напрямки співпраці страхових компаній та експертних організацій, за якими варто будувати систему оцінки страхувальників та створення оптимальних умов для захисту їх IT-інфраструктури.

Моделювання механізму оцінки втрат від кібер-атак як правило здійснюється на основі результатів досліджень природи існуючих кібер-атак та можливих наслідків від їх настання, які проводяться відповідними експертами. Найчастіше виділяють такі фінансові та репутаційні втрати від кібер-інцидентів [10]. Під прямими фінансовими втратами розуміють припинення роботи обладнання, збій сервісів та виведення коштів. Репутаційні втрати, або непрямі, пов’язують з шкодою для бренду або для імені власників компаній, що можуть бути виражені у вигляді пропаганди, викритті конфіденційної інформації, викраденні даних клієнтів та кібер-шпигунством. Для страховиків, задля оцінки точної суми відшкодування, важливо розуміти об’єм втрат від кожного окремого ризику.

Моніторинг поточного стану страхувальників є виграшним інструментом для трьох суб’єктів страхування: 1) для страхувальників, оскільки вказуються існуючі проблеми і прогалини у IT-забезпеченні організації; 2) для страховиків, так як мінімізується ймовірність настання страхового випадку та проводиться перевірка доцільності прийняття ризиків даної організації на страхування; 3) для експертних організацій, через те, що компанії автоматично стають їх клієнтами, тобто збільшується обсяг покриття продуктами кібер-захисту.

Рис. 2. Вектори співпраці страховиків та експертних організацій у сфері кібер-безпеки
Джерело: складено авторами за матеріалами [7-9]

Розробка шляхів мінімізації настання кібер-інцидентів допомагає реалізувати платформу по швидкому реагуванню експертних організацій у разі настання страхового випадку, оскільки у них в їхній вже є профайл клієнта. Вказаний комплекс заходів допомагає страховим компаніям мінімізувати витрати на відшкодування, і тим самим дозволяє інвестувати в механізм співпраці та підвищення ефективності існуючих інструментів захисту.

Вважаємо за доцільне акцентувати увагу на соціальній місії впровадження кібер-страхування в Україні. Таке впровадження допоможе підвищити обізнаність населення про можливі ризики, що існують в кібер-просторі. На нашу думку, варто розпочати роботу в даному аспекті за двома напрямками:

– оцінити рівень знань населення окремо про страхування та кібер-безпеку. Після цього сегментувати потенційних споживачів на групи за рівнем обізнаності та розробити окремі програми інформування про кожен з вказаних аспектів;

– реалізувати єдину державну платформу для реєстрації заяв про кібер-інцидент з можливістю отримання консультації від спеціалістів у даній сфері. В залежності від потреб клієнта, на платформі будуть доступні списки страхових компаній, які забезпечують захист від обраних ризиків.

Виходячи з цього, в процесі впровадження кібер-страхування в Україні утвориться система взаємодії учасників страхових відносин, у центрі якої буде кінцевий споживач, тобто страхувальник (Рисунок 3).

Варто зауважити, що на стику інтересів учасників страхування формуються нові організації, які є специфічними для страхування від кібер-інцидентів, що в свою чергу допомагає забезпечити надання релевантної послуги клієнтам. Також відповідний механізм співпраці забезпечує комплексний підхід до окреслення місця кібер-страхування у страховій системі України.

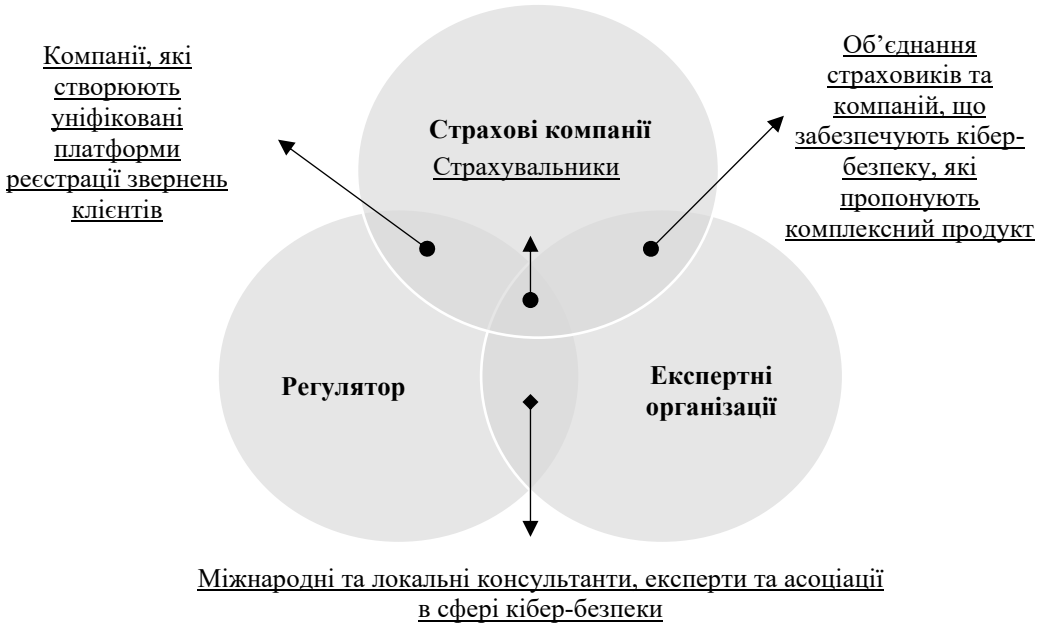

Рис. 3. Система взаємодії суб'єктів кібер-страхових відносин

Шляхом впровадження кібер-страхування в Україні, з використанням запропонованої Дорожньої карти, можуть стати вирішеними наступні проблеми:

1. Низький рівень захисту критичної інфраструктури. Завдячуючи захисту критичних елементів інфраструктури, буде мінімізована ймовірність їх зупинки, яка в свою чергу може негативно вплинути на економічну, соціальну, політичну сфери діяльності держави.

2. Неосвіченість громадян у страховій сфері. Підвищення рівня знань населення про страхування та кібер-ризики, а також донесення важливості кібер-безпеки в сучасному світі, де цифрова трансформація присутня у всіх сферах життя дозволить підвищити рівень проникнення страхування в Україні.

3. Високий рівень безробіття через вплив COVID-19. Створення додаткових робочих місць буде реалізовано через розширення асортименту послуг страхових компаній, а також шляхом залучення компаній, що займаються кібер-безпекою, до співпраці з локальними замовниками.

4. Низький рівень захищеності компаній. IT-системи будуть оцінені експертами, як нададуть рекомендації по їх вдосконаленню, що спричинить стрімкий ріст рівня захищеності систем, конфіденційних даних та каналів їх передачі.

6. ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМКУ

На основі проведеного дослідження міжнародного досвіду та глобальних тенденцій впровадження кібер-безпеки в систему національної економіки, очевидним стає необхідність створення кібер-страхування в Україні. Опираючись на аналіз нормативно-правових документів у сфері кібер-страхування країн ЄС та Австралії, були розроблені та обґрунтовані цілі по підвищенню захищеності каналів передачі даних та мінімізації ймовірності настання кібер-інцидентів в Україні та окреслені орієнтовні терміни на їх виконання у Дорожній карті.

Подальшими напрямками дослідження є аналіз готовності страхових компаній, регулятора та експертних організацій до співпраці та трансформації у напрямку впровадження кібер-страхування в Україні, а також розробка рекомендацій по підвищенню рівня довіри страхувальників до такого інноваційного напрямку.

ЛІТЕРАТУРА

1. Приказюк Н. В., Гуменюк Л. С. Передумови розвитку кібер-страхування. *Інвестиції: практика та досвід*. 2020. № 15-16. С. 28–34. URL: http://www.investplan.com.ua/pdf/15-16_2020/7.pdf.
2. List of data breaches in 2020, IT Governance. URL: https://www.itgovernance.co.uk/infographics/list-of-data-breaches-in-2020.
3. General Data Protection Regulation (GDPR). URL: https://gdpr-info.eu/.
4. Цифрова стратегія України. URL: https://hromada.gov.ua/template/digitalStrategy.
5. Reducing the Cyber Risk in 10 Critical Areas. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/395716/10_steps_ten_critical_areas.pdf.
6. Shaping Europe's digital future. URL: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.
7. The Australian Cyber Security Centre (ACSC). URL: https://www.cyber.gov.au/.
8. The Australian Cyber Security Strategy 2020. URL: https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf.
9. CISA. URL: https://www.cisa.gov/cybersecurity-insurance.
10. Кібер-безпека як важлива складова всієї системи захисту держави. URL: https://www.mil.gov.ua/ukbs/kiberbezpeka-yak-vazhliva-skladova-vsiei-sistemi-zahistu-derzhavi.html.

REFERENCES

1. Prikazyuk N. V., Gumenyuk L. S. (2020) Peredumovi rozvitku kiber-strahuvannya [Prerequisites for the development of cyber insurance] *Investytsiyi: praktyka ta dosvid*, vol. 15-16, pp., available at: http://www.investplan.com.ua/pdf/15-16_2020/7.pdf.
2. List of data breaches in 2020, IT Governance. Available at: https://www.itgovernance.co.uk/infographics/list-of-data-breaches-in-2020.
3. General Data Protection Regulation (2021). Available at: https://gdpr-info.eu/.
4. Digital strategy of Ukraine. Available at : https://hromada.gov.ua/template/digitalStrategy.
5. Reducing the Cyber Risk in 10 Critical Areas. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/395716/10_steps_ten_critical_areas.pdf.
6. Shaping Europe's digital future. Available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.
7. The Australian Cyber Security Centre (2021). URL: https://www.cyber.gov.au/.
8. The Australian Cyber Security Strategy 2020. URL: https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf.
9. CISA (2021). Available at: https://www.cisa.gov/cybersecurity-insurance.
10. Cyber security as an important component of the entire state protection system. Available at: https://www.mil.gov.ua/ukbs/kiberbezpeka-yak-vazhliva-skladova-vsiei-sistemi-zahistu-derzhavi.html.

Abstract

PRYKAZIUK Nataliia, GUMENYUK Lyudmila. Roadmap for the introduction of cyber insurance in Ukraine

The article examines the process of implementing cyber insurance in the world and proposes a Roadmap for implementation in Ukraine. The key goals and objectives facing the insurance market of Ukraine and the regulator in order to achieve this goal are considered. Approximate deadlines for the necessary measures to prepare for the introduction of cyber insurance in the Ukrainian economy are outlined. The key features of regulations in the field of cyber security in the EU and Australia are highlighted and ways to adapt them in Ukraine are proposed. Promising means to increase the security of individuals and legal entities in the digital space on the example of the mechanism of interaction between insurers and expert organizations in Australia. The main vectors of cooperation between insurance companies and expert organizations in the field of cyber security in the Ukrainian and global insurance markets are listed. A system of interaction between the subjects

of cyber-insurance relations with the positioning of the insured in the center of relations as a key participant in insurance has been developed, which proves the high customer orientation of this area of insurance business. The current problems of the Ukrainian insurance market are substantiated and the ways of their solution through the mechanism of cyber insurance implementation are offered: modeling of the mechanism of estimation of losses from cyber attacks, monitoring of the current state of insurers, development of ways to minimize cyber incidents. The dynamics of cyber incidents in 2020 is analyzed and the correlation between the occurrence of global lockdowns caused by COVID-19 and the growth in the number of cyber attacks is revealed. Based on the analysis, it is proved that the introduction of cyber insurance in Ukraine is a necessary tool to protect all participants in insurance relations from cyber risks and for the development of the insurance market as a whole.

Keywords: *cyber insurance; cyber risk; cyber attack; cyber protection; cyber insurance roadmap; digital transition.*

Стаття надійшла до редакції 05.12.2021 р.

Бібліографічний опис статті:

Приказюк Н. В., Гуменюк Л. С. Дорожня карта впровадження кібер-страхування в Україні. *Innovation and Sustainability*. 2021. № 1. С. 64-72.

Prykaziuk N., Gumenyuk L. (2021) Roadmap for the introduction of cyber insurance in Ukraine. *Innovation and Sustainability*, № 1, pp. 64-72.