ФІНАНСИ, БАНКІВСЬКА СПРАВА, СТРАХУВАННЯ ТА ФОНДОВИЙ РИНОК

DOI: https://doi.org/10.32689/2523-4536/73-5
УДК 368

Брюховецька І. О.
кандидат економічних наук,
доцент кафедри фінансів, банківської справи та страхування,
Навчально-науковий інститут управління, економіки та бізнесу
Приватного акціонерного товариства «Вищий навчальний заклад
«Міжрегіональна Академія управління персоналом»
ORCID: https://orcid.org/0000-0002-1469-1485
Кришталь Г. О.
доктор економічних наук, професор,
завідувач кафедри фінансів, банківської та страхової справи,
Навчально-науковий інститут управління, економіки та бізнесу
Приватного акціонерного товариства «Вищий навчальний заклад
«Міжрегіональна Академія управління персоналом»
ORCID: https://orcid.org/0000-0003-3420-6253

Briukhovetska Iryna
PhD in Economics, Associate Professor
of the Department of Finance, Banking and Insurance,
Educational and Scientific Institute of Management, Economics and Business
Private Joint Stock Company "Higher Educational Institution
"Interregional Academy of Personnel Management"
Kryshtal Halyna
DCs in Economic, Professor,
Head of the Department of Finance, Banking and Insurance,
Educational and Scientific Institute of Management, Economics and Business
Private Joint Stock Company "Higher Educational Institution
"Interregional Academy of Personnel Management"

АНАЛІЗ ВПЛИВУ ДЕРЖАВНОЇ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ НА СТРАХОВИЙ РИНОК УКРАЇНИ: НОВІ МОЖЛИВОСТІ ТА РИЗИКИ

ANALYSIS OF THE IMPACT OF STATE DIGITAL TRANSFORMATION ON THE INSURANCE MARKET OF UKRAINE: NEW OPPORTUNITIES AND RISKS

В умовах інформаційного ландшафту, що швидко змінюється, і технологічних інновацій, цифрова трансформація стала ключовим фактором у розвитку фінансової та страхової галузей. Ця стаття досліджує вплив державної цифрової трансформації на страховий ринок України, аналізуючи нові можливості, які вона надає страховикам та клієнтам, а також ризики, пов'язані із цими змінами. У статті розглядаються такі аспекти, як використання великих даних, штучного інтелекту та цифрових платформ у страхуванні, а також питання кібербезпеки та конфіденційності даних. Основна увага зосереджена на дослідженнях різних стратегій зниження кіберризиків, надаючи читачеві огляд найефективніших методів та підходів, таких як прийняття відповідного законодавства, розробка державної стратегії безпеки, створення координаційного центру. Однак, навіть за найкращих зусиль щодо запобігання інцидентам, існує ймовірність виникнення кібератак. У зв'язку з цим страхування кіберризиків стає дедалі актуальнішим. Стаття також висвітлює переваги та нюанси страхування в даній галузі, надаючи читачеві інформацію про те, як вибрати відповідний страховий план, які ризики можуть бути покриті та як страхування може допо-

могти у відновленні після кіберінцидентів. У статті розкрито сутність поняття «кіберризик». Зокрема, розкрито різні наукові підходи щодо його тлумачення. А саме юридичний, статистичний, стратегічний, економічний. З урахуванням різних точок зору надано авторське визначення. Тема, якій присвячена стаття, надає можливість досліджувати актуальні виклики та можливості, з якими страхова галузь стикається в епоху державної цифрової трансформації, та може призвести до розуміння того, як страхові компанії можуть адаптуватися та використовувати сучасні технології для покращення своєї ефективності та обслуговування клієнтів. ***Мета роботи.*** *Метою статті є аналіз впливу державної цифрової трансформації на страховий ринок України для виявлення можливостей зниження ймовірних кіберзагроз та забезпечення максимального захисту у разі їх настання за допомогою страхування.* ***Методологія.*** *У запропонованій статті особливу увагу приділено аналізу аспектам державної цифрової політики, направленої на формування страхового ринку України для виявлення нових можливостей та ризиків.* ***Наукова новизна.*** *Доведено, що актуальною проблемою розвитку страхового ринку України є ефективне впровадження цифрових інновацій. Забезпечення цифрових інновацій не можливе без реалізації державної політики щодо цифрових перетворень у страховій галузі.* ***Висновки.*** *Державна політика, спрямована на цифровізацію страхових процесів створює нові можливості для страхового ринку України. Проте виникають і ризики. З'ясовано, що головними результатами впливу цифровізації є поліпшення клієнтського досвіду; машинне навчання дозволяє страховим компаніям більш точно визначати ризики, розробляти більш точні моделі ціноутворення та керувати страховими портфелями; цифрові роботи та боти забезпечують більш швидке та точне обслуговування клієнтів; технологія блокчейн спрощує процеси верифікації та аутентифікації даних; цифрова трансформація залучає нових учасників до страхового ринку, таких як стартапи та технологічні компанії, які пропонують інноваційні страхові продукти та послуги. Визначено, що державна цифрова трансформація впливає на появу нових страхових ризиків як, наприклад, DDoS-атаки, фішинг, кібератаки. Констатовано, що державні ініціативи щодо боротьби з кібрризиками є дієвими. Разом з тим констатовано, що найбільш надійним та ефективним способом захисту від зазначених ризиків є страхування.*

Ключові слова: *кіберризик, кібератака, цифрова трансформація, моделі страхування кіберризиків, соціальна інженерія, DDoS-атаки, фішинг.*

In the rapidly changing information landscape and technological innovations, digital transformation has become a key factor in the development of the financial and insurance sectors. This article explores the impact of state digital transformation on the insurance market in Ukraine, analyzing the new opportunities it provides for insurers and clients, as well as the risks associated with these changes. The article examines aspects such as the use of big data, artificial intelligence, and digital platforms in insurance, along with issues of cybersecurity and data confidentiality. The main focus is on researching various strategies to reduce cyber risks, providing the reader with an overview of the most effective methods and approaches, such as implementing appropriate legislation, developing a state security strategy, and establishing a coordination center. However, despite the best efforts to prevent incidents, there remains a probability of cyberattacks. Consequently, cyber risk insurance becomes increasingly relevant. The article also highlights the benefits and nuances of insurance in this field, offering readers information on how to choose the right insurance plan, what risks can be covered, and how insurance can aid in recovery after cyber incidents. The article elucidates the essence of the concept of "cyber risk." Specifically, it reveals various scientific approaches to its interpretation, namely legal, statistical, strategic, and economic. Taking various perspectives into account, the article provides an author's definition. The subject of the article provides an opportunity to explore the current challenges and opportunities that the insurance industry faces in the era of state digital transformation. It may lead to an understanding of how insurance companies can adapt and utilize modern technologies to improve their efficiency and customer service. ***Objective:*** *the aim of the article is to analyze the impact of state digital transformation on the insurance market in Ukraine to identify possibilities for reducing potential cyber threats and ensuring maximum protection in case of their occurrence through insurance.* ***Methodology:*** *the proposed article particularly focuses on analyzing aspects of state digital policy aimed at shaping Ukraine's insurance market to identify new opportunities and risks.* ***Scientific novelty:*** *it is proven that an essential problem in the development of Ukraine's insurance market is the effective implementation of digital innovations. Ensuring digital innovations is impossible without the implementation of state policy regarding digital transformations in the insurance sector.* ***Conclusions:*** *state policies aimed at digitizing insurance processes create new opportunities for Ukraine's insurance market. However, risks arise. It is established that the main results of digitization's influence are the improvement of customer experience; machine learning enables insurance companies to more accurately determine risks, develop more precise pricing models, and manage insurance portfolios; digital robots and bots provide faster and more precise customer service; blockchain technology simplifies data verification and authentication processes; digital transformation attracts new participants to the insurance market, such as startups and technological companies offering innovative insurance products and services. It is determined that state digital transformation leads to the emergence of new insurance risks, such as DDoS attacks, phishing, and cyberattacks. It is stated that state initiatives to combat cyber risks are effective. However, it is also noted that the most reliable and effective way to protect against these risks is insurance.*

Keywords: *cyber risk, cyberattack, digital transformation, models for insuring cyber risks, social engineering, DDoS attacks, phishing.*

Постановка проблеми. У період бурхливого технологічного розвитку та інновацій цифрова державна трансформація стала невід'ємною частиною багатьох галузей, включаючи страхування. З одного боку, це надає страховому сектору можливості для оптимізації бізнес-процесів, покращення клієнтського обслуговування та розробки нових товарів. З іншого боку, з трансформацією приходять і нові небезпеки, які можуть спричинити значні потрясіння у промисловості.

Цифрові технології змінюють вигляд страхового ринку, модифікують традиційні бізнес-моделі та вимагають від компаній гнучкості в адаптації до нового цифрового світу. Таким чином, аналіз цих змін та розуміння їх наслідків стають ключовими для успішного розвитку та виживання страхових компаній у майбутньому. У цій статті ми розглянемо основні напрямки цифрової трансформації у сфері страхування, а також запропонуємо рекомендації для страховиків щодо адаптації до ринку, що змінюється.

Виклад основного матеріалу дослідження. Вплив державної цифрової трансформації на страховий ринок є значним та охоплює безліч аспектів. Основними серед них є: поліпшення клієнтського досвіду, використання великих даних та аналітики, автоматизація процесів, використання блокчейну, зміна конкурентного середовища, кібербезпека, регулювання (табл. 1).

Отже, державна цифрова трансформація надає страховій галузі нові можливості для зростання та покращення обслуговування клієнтів, але вона також вносить нові виклики та ризики, якими необхідно ефективно керувати. Основними ризиками, з якими стикається страховий ринок, внаслідок цифровізації є кіберризики, зміна моделей ризиків, підробка запитів і шахрайство, залежність від технології, конкуренція і дефляція тарифів, проблеми з конфіденційністю, технічні і кадрові ризики.

Законодавство України визначає кіберризик як ризик виникнення збитків та/або додаткових втрат унаслідок реалізації кіберзагроз. Підходи вчених до розкриття сутності кіберризику відрізняються. На приклад, з технічної точки зору фокус зосереджено на технічних аспектах кіберризику і включає оцінку вразливостей в інформаційних системах, аналіз можливих атак і методів їх запобігання. Кіберризик визначається як ймовірність виникнення кібератаки та її потенційні наслідки.

Відповідно до фінансового підходу кіберризик розглядається з погляду потенційних фінансових збитків, які можуть виникнути в результаті кібератаки або інциденту в галузі кібербезпеки. Оцінка кіберризику включає розрахунки за вартістю відновлення після інциденту.

Таблиця 1

Результат впливу державної цифрової трансформації на страховий сектор

Вплив	Зміст
Поліпшення клієнтського досвіду	Цифрові технології дозволяють страховим компаніям краще розуміти потреби клієнтів та пропонувати персоналізовані страхові продукти та послуги. Цифрові канали обслуговування клієнтів, такі як мобільні програми та онлайн-портали, покращують доступність та зручність для клієнтів
Використання великих даних та аналітики	Аналіз великих даних та машинне навчання дозволяють страховим компаніям більш точно визначати ризики, розробляти більш точні моделі ціноутворення та керувати страховими портфелями. Ефективне використання даних дозволяє запобігати шахрайству та знижувати рівень збитків
Автоматизація процесів	Роботизовані процеси та автоматизовані системи обробки покращують ефективність та швидкість подання заявок, розгляду страхових випадків та виплат клієнтам. Цифрові роботи та боти можуть забезпечити більш швидке та точне обслуговування клієнтів.
Використання блокчейну	Технологія блокчейн може спростити процеси верифікації та аутентифікації даних, що особливо важливо у сфері страхування. Блокчейн також може допомогти у покращенні процесів врегулювання збитків та встановленні історії страхових випадків
Кіберстрахування	Цифрова трансформація супроводжується зростанням кіберзагроз та кіберзлочинності. У відповідь на це страхові компанії пропонують страхування від кіберрисків, що стає затребуваним продуктом
Зміна конкурентного середовища	Цифрова трансформація залучає нових учасників до страхового ринку, таких як стартапи та технологічні компанії, які пропонують інноваційні страхові продукти та послуги. Традиційні страхові компанії повинні адаптуватися та співпрацювати з такими компаніями, щоб залишатися конкурентоспроможними
Кібербезпека	Із цифровою трансформацією страхових компаній зростають загрози кібербезпеці. Ці компанії повинні уважно стежити за захистом конфіденційних даних клієнтів та інформації про страхові поліси.
Регулювання	Регулятори та законодавці також реагують на зміни, пов'язані з цифровою трансформацією, та вносять зміни до страхового законодавства та нормативних актів

Організаційний підхід зосереджується на внутрішніх процесах та політиках організації. Кіберризик розглядається як частина стратегічного управління ризиками і включає аналіз того, як організація управляє своїми інформаційними активами і реагує на потенційні загрози.

Правовий підхід приділяє увагу юридичним аспектам кіберризику, включаючи дотримання законів та нормативних вимог щодо кібербезпеки. Кіберризик може бути визначений як порушення законодавства, пов'язане з інцидентами в галузі кібербезпеки.

Вчені, які дотримуються статистичного підходу, можуть використовувати статистичні методи для оцінки кіберризику на основі історичних даних про кібератаки та інциденти в галузі кібербезпеки. Цей підхід може включати аналіз частоти і серйозності інцидентів.

У межах стратегічного підходу кіберризик розглядається у контексті ширшої стратегії організації. Цей підхід приділяє увагу тому, як кіберризик співвідноситься з бізнес-цілями та які довгострокові стратегії можуть бути розроблені для управління ризиками [1, с. 110–115].

З огляду на існуючі підходи до визначення сутності кіберризику, на нашу думку, кіберризики у страхуванні – це ризики, пов'язані з потенційними загрозами та втратами, які можуть виникнути в результаті кібератак, кіберзлочинності та інших подій, пов'язаних з інформаційною безпекою та технологічними системами.

Рис. 1. Структура кіберризиків

Кіберризики можуть охоплювати широкий спектр подій, включаючи, але не обмежуючись:

1. Кібератаки: це включає спроби несанкціонованого доступу до комп'ютерних систем, зломи, поширення шкідливих програм та інші активності, спрямовані на крадіжку, руйнування або зміна даних.

2. Виток даних: коли конфіденційна інформація, така як дані клієнтів або фінансові записи, потрапляє в руки зловмисників через порушення безпеки.

3. Мережеві збої: це може включати збої в роботі інформаційних систем, що може призвести до зупинки бізнес-процесів, втрати даних і фінансових збитків.

4. Соціальна інженерія: зловмисники можуть використовувати обман та маніпуляцію, щоб отримати доступ до інформації або засобів організації, вводячи співробітників в оману або змушуючи їх надати конфіденційні дані.

5. Кіберзлодійство: крадіжка електронних активів, таких як криптовалюти, або маніпуляції з цифровими засобами.

6. Відмова в обслуговуванні (DDoS-атаки): зловмисники можуть перевантажити сервери або мережі, роблячи їх недоступними для легітимних користувачів.

7. Поширення хибної інформації: поширення дезінформації чи фейкових новин з метою дискредитації організації чи виклику паніки на ринку [2, с. 4–12].

За даними Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України фішингові атаки займають значну частку у структурі подій ризикового характеру [3, с. 97–111]. Не менш небезпечними є шкідливі програми (віруси, трояни, ransomware та ін.), частка яких складає 25% (рис. 1).

На забезпечення захисту від кіберризиків спрямована державна політика. Так, у 2021 році Указом Президента України № 447/2021 введено в дію Стратегію кібербезпеки України, яка встановлює ключові напрямки, цільові установки та місії у сфері кібербезпеки для гарантування безпечної взаємодії у кіберпросторі та його застосування на благо індивіда, громадськості та державних інтересів. При Раді національної безпеки і оборони України у 2016 році створено Національний координаційний центр кібербезпеки. Він є робочим органом Ради національної безпеки і оборони України, утвореним відповідно до рішення Ради національної безпеки

і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», уведеного в дію Указом Президента України від 15 березня 2016 року № 96. Національним банком України спільно з Національним координаційним центром кібербезпеки при Раді національної безпеки і оборони України у 2023 році запущено проєкт із протидії кібершахрайству у фінансовому секторі. Головна його мета – посилити захист населення від злочинців, які значно посилили свою кіберзлочинність в Україні у період воєнного стану.

Не дивлячись на державні ініціативи із забезпечення кіберризиків, дієвим у цьому сенсі виступає страхування. Страхування кіберризиків стає все більш популярним, особливо з урахуванням зростаючого числа кібератак та їхнього потенційного впливу на бізнес. Однак, за різними джерелами, більшість компаній досі не страхують кіберризики або страхують їх не повністю. Деякі звіти стверджують, що менше ніж 50% компаній у світі мають страховку від кіберризиків, хоча цей відсоток поступово збільшується.

Проблема полягає в тому, що страхування кіберризиків є складною і відносно новою областю, і багато страхових компаній ще визначають свої підходи до оцінки та покриття цих ризиків. Крім того, багато потенційних страхувальників не усвідомлюють повний обсяг потенційних загроз або вважають, що їхні поточні заходи безпеки є достатньо надійними, щоб уникнути серйозних інцидентів. Наразі відомими є кілька моделей страхування кіберризиків (табл. 2).

Цифровізація страхового ринку зумовила ряд негативних ефектів. На нашу думку, основними серед них можна виділити:

– по-перше, цифровізація страхової галузі спричинила зміну моделей ризику. Тобто, цифровізація дозволяє збирати та аналізувати великі обсяги даних, які можуть змінити традиційні моделі оцінки ризиків. Нові дані та аналітичні методи призвели до перегляду тарифів та страхових полісів;

– онлайн-запити і документи підроблюють, клієнти вдаються до надання недостовірних відомостей для отримання нижчих страхових тарифів. Це створює ризик для страхових компаній, які можуть бути обдурені шахраями;

– з розвитком цифрових систем страхові компанії стають залежнішими від технології. Збої в IT-системах або атаки на інформаційну інфраструктуру можуть призвести до втрати доступу до даних і навіть призупинення діяльності;

– цифровізація посилила конкуренцію на страховому ринку. Порівняльні сайти та онлайн-платформи можуть знижувати вартість страхових полісів та стискати маржі страхових компаній, що може створити тиск на прибутковість;

– збирання та зберігання великих обсягів даних викликає питання про конфіденційність та відповідність законодавству про захист даних (наприклад, GDPR у Європі). Порушення нормативних вимог може призвести до юридичних наслідків та штрафів [6, с. 403];

– страховим компаніям необхідно мати достатньо кваліфікований персонал та сучасні технічні ресурси для ефективної цифрової трансформації. Недолік кадрових ресурсів чи неправильна реалізація технологій може створити додаткові ризики.

У першому півріччі 2023 р. кількість атак із використанням програм-вимагачів значно

Таблиця 2

Моделі страхування кіберризиків

Модель	Механізм дії страхування
Первинне покриття кіберризиків	Це основне страхування, яке покриває безпосередні збитки, що виникають через кібератаки, такі як витрати на відновлення даних, усунення наслідків злому і т.д.
Відповідальність за кіберризики	Ця модель покриває збитки, які компанія може зазнати через треті сторони, наприклад, через порушення конфіденційності даних клієнтів.
Страхування переривання бізнесу через кіберподії	Таке страхування призначене для компенсації збитків, пов'язаних із перериванням або простоєм бізнесу через кібератаки.
Страхування витрат на PR та комунікації	Покриває витрати на PR-кампанії та комунікації, пов'язані з реакцією на кіберінцидент.
Страхування штрафів та штрафних санкцій	Орієнтовано на покриття потенційних штрафів та санкцій, які можуть бути накладені регулюючими органами внаслідок порушення законодавства про захист даних [4–5].
Страхування витрат на викуп	Призначено для компенсації суми викупу, яку запитують зловмисники у разі атаки з використанням ransomware.
Розширене покриття	Включає додаткові послуги, такі як консультації з кібербезпеки, надання послуг з відновлення після інциденту та ін.

збільшилася. Проте статистика страхових та перестрахувальних компаній за 1 квартал 2023 р. показує, що страхові виплати не збільшились пропорційно. Ці дані підтверджують, що заходи контролю ризиків виявилися ефективними, сприяючи зміцненню стійкості підприємств і стабілізації ринку кіберстрахування. Нині вимоги стають менш суворими, і клієнти, які правильно управляють ризиками, отримують пільги у вигляді привабливіших ставок та умов страхування. Пройшовши початкові етапи, які часто пов'язані з появою нових сфер бізнесу, що динамічно розвиваються, ціноутворення в галузі кіберстрахування тепер більше відображає реальні збитки після нещодавніх коригувань вартості [7–9].

Незважаючи на зниження цін у першому півріччі 2023 року, майбутнє цієї тенденції залишається незрозумілим через постійну загрозу кібератак. Поточні страхові тарифи неспроможні стимулювати зростання страхового ринку, оскільки це відбувалося раніше, що передбачає необхідність розробки стратегій зростання у цій сфері. З цієї причини входження страхових компаній на нові ринки та облік демографічних даних стають ключовими у пошуку нових можливостей для кіберстрахування. Страхові компанії повинні інвестувати в кібербезпеку, навчання співробітників, розробку стійких бізнес-моделей та дотримання відповідних регулювань. Вони також повинні постійно моніторити зміни у технологічному середовищі та швидко адаптуватися до них, щоб залишатися конкурентоспроможними на ринку.

Висновки. Державна цифрова трансформація справила проникливий вплив на страховий ринок, змінюючи звичні бізнес-моделі та методи взаємодії зі страхувальниками. Використання нових технологій, таких як блокчейн, штучний інтелект та великі дані, дозволило страховим компаніям створювати більш персоналізовані продукти, оптимізувати процеси обліку та управління ризиками, а також удосконалювати методи врегулювання збитків. Цифрові канали спілкування та дистрибуції дозволили зміцнити зв'язок із страхувальниками, надаючи їм зручність та доступність послуг у режимі реального часу. Незважаючи на численні переваги, цифрова трансформація також привнесла нові ризики, включаючи загрози кібербезпеці, проблеми із захистом особистих даних та потенційне посилення конкуренції за рахунок появи нових гравців на ринку. Традиційні страхові компанії повинні активно адаптуватися до змінної цифрової реальності, інвестувати в інновації та підвищувати кваліфікацію свого персоналу для підтримки конкурентоспроможності. Хоча цифрова трансформація може бути викликом в короткостроковій перспективі, вона надає великі можливості для зростання та розвитку страхового ринку в довгостроковій перспективі. Цифрова трансформація страхового ринку є невід'ємною частиною сучасної економічної реальності. Правильне використання нових технологій і адаптація до ринку, що змінюється, дозволять страховим компаніям не тільки вижити, а й процвітати в нових умовах.

Список використаних джерел:

1. Волосович С., Клапків Л. Детермінанти виникнення та реалізації кіберризиків. *Зовнішня торгівля: економіка, фінанси, право*. 2018. № 3. С. 101–115. URL: http://nbuv.gov.ua/UJRN/uazt_2018_3_10

2. Гудзь О. Розвиток страхування: нові інструменти та методи управління ризиками в цифровій економіці. *Економіка. Менеджмент. Бізнес*. 2019. № 3 (29). С. 4–12. DOI: https://doi.org/10.31673/2415-8089.2019.030412

3. Нагайчук Н.Г., Третяк Н.М., Ткаленко О. Страхування в системі управління кіберризиками підприємства в умовах цифрової економіки. *Фінансовий простір*. 2019. № 1 (33). С. 97–111. DOI: https://doi.org/10.32702/2307-2105-2020.4.6

4. Правова база української кібербезпеки: загальний огляд і аналіз. Міжнародна фундація виборчих систем в Україні. 2019. URL: https://ifesukraine.org/wp-content/uploads/2019/10/IFES-Ukraine-Ukrainian-Cybersecurity-Legal-Framework-Overview-and-Analysis-2019-10-07-Ukr.pdf

5. Приказюк Н.В., Гуменюк Л.С. Кібер-страхування як важливий інструмент захисту підприємств в умовах цифровізації економіки. *Ефективна економіка*. 2020. № 4. DOI: https://doi.org/10.32702/2307-2105-2020.4.6

6. Про основні засади забезпечення кібербезпеки України : Закон України № 2469-VIII від 21.06.2018. *Відомості Верховної Ради України.* 2017. № 45. Ст. 403. Поточна редакція від 15.12.2021. URL: https://zakon.ra-da.gov.ua/laws/show/2163-19#Text

7. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України із змінами № 447/2021 від 26.08.2021. URL: https://zakon5.rada.-gov.ua/laws/show/96/2016

8. Bohme R., Schwartz G. Modeling Cyber-Insurance: Towards A Unifying Framework. Conference. 2010. URL: ttp://www.icsi.berkeley.edu/pubs/networking/mode-lingcyber10.pdf

9. Burke D. Cyber Insurance 101: What Cyber Insurance Covers. Woodruff Sawyer. 2021. URL: https://woodruffsawyer.com/cyber-liability/cyber-101-liability-insurance/

10. CRO Forum Concept Paper on a proposed categorisation methodology for cyber risk. CRO Forum. June 2016. URL: https://www.thecroforum.org/wp- content/uploads/2016/06/ZRH-16-09033-P1_CRO_-Forum_Cyber-Risk_web-2.pdf

References:

1. Volosovych, S. and Klapkiv, L. (2018) Determinants of the emergence and implementation of cyber risks. *Zovnishnia torhivlia: ekonomika, finansy, pravo*, no. 3, pp. 101–115. Available at: http://nbuv.gov.ua/UJRN/uazt_-2018_3_10

2. Hudz', O. (2019) Insurance development: new instruments and methods of risk management in the digital economy. *Ekonomika. Menedzhment. Biznes,* no. 3 (29), pp. 4–12. DOI: https://doi.org/10.31673/2415-8089.2019.030412

3. Nahajchuk, N.H. Tretiak, N.M. and Tkalenko, O. (2019) Insurance in the cyber risk management system of the enterprise in a digital economy. *Finansovyj prostir*, no. 1 (33), pp. 97–111.

4. Shypilova, Yu. (2019) The legal framework of Ukrainian cybersecurity: an overview and analysis. Available at: https://ifesukraine.org/wp-content/uploads/2019/10/IFES-Ukraine-Ukrainian-Cybersecurity-Legal-Framework-Overview-and-Analysis-2019-10-07-Ukr.pdf

5. Prykaziuk, N. and Gumenyuk, L. (2020) Cyberinsurance as an important tool of enterprise protection in the digitization economy. *Efektyvna ekonomika*, [Online]. DOI: https://doi.org/10.32702/2307-2105-2020.4.6

6. Verkhovna Rada of Ukraine (2018) The Law of Ukraine "On the Basic Principles of Cybersecurity in Ukraine. Available at: https://zakon.rada.gov.ua/laws/show/2163-19#Text

7. President of Ukraine (2016) Decree "On the decision of the National Security and Defense Council of Ukraine of January 27, 2016 "On the Cyber Security Strategy of Ukraine". Available at: https://zakon5.rada.gov.ua/laws/show/96/2016

8. Bohme, R. and Schwartz, G. (2010) Modeling Cyber-Insurance: Towards A Unifying Framework. Conference. Available at: http://www.icsi.berkeley.edu/pubs/networking/modelingcyber10.pdf

9. Burke, D. (2021) Cyber Insurance 101: What Cyber Insurance Covers. Woodruff Sawyer. Available at: https://woodruffsawyer.com/cyber-liability/cyber-101-liability-insurance/

10. CRO Forum (2016) CRO Forum Concept Paper on a proposed categorisation methodology for cyber risk. Available at: https://www.thecroforum.org/wp-content/uploads/2016/06/ZRH-16-09033-P1_CRO_Forum_-Cyber-Risk_web-2.pdf