DOI: https://doi.org/10.32782/2524-0072/2021-34-90

УДК 336:368.330

СТРАХУВАННЯ РИЗИКІВ КІБЕРБЕЗПЕКИ ДІЯЛЬНОСТІ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ В СУЧАСНОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРІ

INSURANCE AGAINST CYBER SECURITY RISKS OF BUSINESS ENTITIES IN THE MODERN INFORMATION SPACE

Ксьонжик Ірина Володимирівна
доктор економічних наук, професор,
Миколаївський національний аграрний університет
ORCID: https://orcid.org/0000-0001-5172-3821

Жовта Наталія Анатоліївна
здобувач вищої освіти,
Миколаївський національний аграрний університет
ORCID: https://orcid.org/0000-0003-0237-2820

Павліна Анастасія Ігорівна
здобувач вищої освіти,
Одеська національна академія харчових технологій
ORCID: https://orcid.org/0000-0001-5070-4872

Ksonzhyk Iryna, Zhovta Nataliia
Mykolayiv National Agrarian University

Pavlina Anastasiia
Odessa National Academy of Food Technologies

У статті досліджуються чинники формування та розвитку ринку страхування ризиків діяльності суб'єктів господарювання, пов'язаних з всеохоплюючим застосуванням технологій штучного інтелекту в умовах єдиного інформаційного простору. Встановлено, що значний вплив на стрімке зростання кіберзлочинності мала епідемія COVID-19 та масштабне впровадження технологічних трендів штучного інтелекту. Здійснено аналіз наслідків кібератак як для економіки України, так і для світової економіки. Встановлено найбільш типові кіберризики, що зустрічаються в операційній діяльності суб'єктів господарювання. Визначено можливості убезпечення діяльності суб'єктів господарювання в інформаційному просторі засобами кіберстрахування. Охарактеризовано проблеми розвитку ринку страхування кіберризиків та виявлено інструменти активізації діяльності страхових компаній у страхуванні кіберризиків.

Ключові слова: кібербезпека, суб'єкт господарювання, страхування кіберризиків, інформаційне суспільство, штучний інтелект, кібератаки, ринок кіберстрахування, інструменти.

В статье исследуются факторы формирования и развития рынка страхования рисков деятельности субъектов хозяйствования, связанных со всеобъемлющим применением технологий искусственного интеллекта в условиях единого информационного пространства. Установлено, что значительное влияние на стремительный рост киберпреступности оказала эпидемия COVID-19 и масштабное внедрение технологических трендов искусственного интеллекта. Проведен анализ последствий кибератак как для экономики Украины, так и для мировой экономики. Установлены наиболее типичные киберриски, встречающиеся в операционной деятельности субъектов хозяйствования. Определены возможности обеспечения деятельности субъектов хозяйствования в информационном пространстве средствами киберстрахования. Охарактеризованы проблемы развития рынка страхования киберрисков и выявлены инструменты активизации деятельности страховых компаний в страховании киберрисков.

Ключевые слова: кибербезопасность, предприятие, страхование киберрисков, информационное общество, искусственный интеллект, кибератаки, рынок киберстрахования, инструменты.

The rapid digitalization of all spheres and areas of life across the globe, the transition of companies to remote work, the further rapid increase in the number of Internet users have made cyber risk a serious threat to information security of businesses entities around the world. The impact of these general trends has been exacerbated by the coronavirus pandemic. At the same time, there is an evolution in the environment of cyber risks, new types are emerging due to the improvement of criminal technology by hackers. The threat of financial losses from these new types of cyber risks puts insurance of cyber security risks of business entities at the forefront of the global insurance market. The purpose of this article is to study the preconditions for the formation of the cyber risk insurance market, to identify the most typical cyber risks, to systematize the sources of losses due to cyber-attacks; to identify problems in the development of the cyber risk insurance market and tools to intensify the activities of insurance companies in insuring cyber security risks of business entities. The methodological basis of the study is formed by the fundamental principles of information economy, insurance theory, cyber security, theoretical and applied studies of domestic and foreign scientists, which study the development of the world economy in the conditions of global spread of information technology and artificial intelligence. The research has been conducted using general scientific and special methods of scientific knowledge: scientific abstraction, analysis, synthesis of induction, deduction – to formulate the theoretical and methodological basis of the study; historical method – for periodization of stages of emergence and development of cyber risks; graphic – to display visually individual provisions of the study; abstract-logical – for theoretical generalization and formation of conclusions. It has been established that the risks insurance while the use of artificial intelligence in the activities of economic entities is an effective tool that allows both to stimulate the implementation of measures that enhance the cyber security of an enterprise and to compensate for losses from a cyber-threat that has already been implemented and which could not be prevented. Thus, cyber insurance is a specific, fast-growing segment of the general market of insurance services, which, based on the basic principles of insurance, develops completely new innovative approaches and solutions.

Keywords: cyber security, business entity, cyber risk insurance, information society, artificial intelligence, cyber-attacks, cyber insurance market, tools.

Постановка проблеми. Глобалізаційні процеси, запущені всеохоплюючим впровадженням інформаційних технологій, надають необмежені можливості здійснення впливу на всі сфери життєдіяльності світової спільноти. В умовах зростаючого впливу діджиталізації на повсякденне життя, проникнення цифрових технологій у нові сфери суспільної взаємодії, особливого значення набуває створення як з боку держав, так і з боку суб'єктів господарювання, громадян, таких механізмів, які дозволять гарантувати інформаційний суверенітет та нейтралізувати ризики, пов'язані з кібербезпекою юридичних та фізичних осіб.

Актуальність проблем захисту простору дії штучного інтелекту зумовлена тим, що за останній час значно зросла кількість суспільно небезпечних дій, спрямованих на нанесення шкоди суб'єктам різного роду діяльності, не тільки в світовому, а й в українському кіберпросторі. Створення провокацій, втручання у процеси роботи для дестабілізації кібернетичного простору, виведення з ладу органів управління суб'єктів господарювання є кібернетичними загрозами, які розвиваються і модифікуються кожного дня [1, с. 294–296].

Аналіз останніх досліджень і публікацій. Питанням захисту інформаційного простору присвятили свої дослідження такі вітчизняні вчені, як В. Бурячок, Ю. Грицюк, О. Корченко, В. Мартинюк, В. Шлемко. Напрями розвитку кібербезпеки, запобігання кіберризикам та їх оцінка були розкриті у наукових працях О. Ілляшенка, С. Євсеєва, А. Коваленка, В. Лєбєдєва, І. Олійника, Д. Прозорова. Перспективи розвитку ринку кіберстрахування досліджені в наукових працях вітчизняних та зарубіжних дослідників та практиків, зокрема: Дж. Арчі, В. Братюка, В. Ільчука, Дж. Кесена, О. Кондратьєва, М. Керола, Й. Малкотра, Л. Мамаевої, Т. Моташко, О. Парубець, Н. Приказюка, Т. Ротової, Д. Сугоняко, Дж. Фінкла, К. Хейєса. Актуальність проблематики формування ринку страхування кіберризиків є надзвичайною в умовах тотальної діджиталізації і потребує подальшого дослідження.

Виділення невирішених раніше частин загальної проблеми. Враховуючи значні науково-практичні результати досліджень в площині страхування ризиків кібербезпеки діяльності суб'єктів господарювання, вважаємо, що недостатньо висвітленими у науковій літературі залишаються причини прискореного зростання рівня кіберзлочинності; визначення проблем та інструментів активізації діяльності страхових компаній у страхуванні кіберризиків.

Формулювання цілей статті (постановка завдання). Метою даної статті є дослідження передумов формування ринку страхування кіберризиків, виокремлення найбільш типових кіберризиків, систематизація джерел втрат у наслідок кібератак; визначення проблем розвитку ринку страхування кіберризиків та інструментів активізації діяльності страхових компаній у страхуванні ризиків кібербезпеки.

Виклад основного матеріалу дослідження. Застосування інформаційних систем і технологій у всіх сферах і галузях життєдіяльності зробило тему безпеки у кіберпросторі, запобігання кібератакам та подолання їх наслідків найпоширенішою і найбільш затребуваною суспільством, оскільки, стосується кожного [2].

Наслідки атаки вірусу Petya.A влітку 2017 року для економіки України наочно показали: будь-яка компанія вразлива перед кібертероризмом, незалежно від її розмірів, специфіки та технічної оснащеності. Значний вплив на зростання такої злочинності мала епідемія COVID-19, через яку частина суб'єктів господарювання перейшла працювати в онлайн-простір. До 2022 року, за попереднім прогнозом Всесвітнього економічного форуму, сума планетарних збитків від кібератак виросте до 8 трлн доларів. Згідно з дослідженням, опублікованим IT-компанією Sophos, наприкінці квітня 2021 року, середні витрати бізнесу на відновлення після атаки вірусів-здирників у світі у річному обчисленні зросли більш, ніж удвічі. До початку 2020 року вони становили 761 106 тис. доларів США, а через рік – 1,85 млн. доларів США. Середній розмір викупу організаторам таких атак, що блокують роботу комп'ютерів, перевищив 170 тис. доларів США [3]. Ще однією причиною прискореного зростання рівня кіберзлочинності, на думку фахівців, є технологічні тренди. До 2022 року до Інтернету буде підключено один трильйон пристроїв.

Виклики та загрози національній безпеці України в кіберпросторі призвели до створення Стратегії кібербезпеки України, що була впроваджена указом Президента України від 15 березня 2016 року [4], а реалізація її положень призвела до прийняття Закону України «Про основні засади забезпечення кібербезпеки України» [5, с. 270] і визначила основні принципи забезпечення кібербезпеки в Україні (рис. 1).

Кібератаки на суб'єктів господарювання та їх діяльність можуть набувати абсолютно різних форм. Джерелами втрат можуть стати: DDoS атаки, фішинг, кібервимагання, крадіжка даних, знищення даних, отримання контролю над IT-системою, атаки на POS-термінали, комп'ютерні віруси.

Хакери все частіше використовують уразливість систем безпеки для крадіжки цінних даних клієнтів, включаючи фінансові відомості та конфіденційні персональні дані. Для великих компаній такі атаки означають не тільки втрату даних. Суспільний резонанс, втрата довіри клієнтів та серйозні штрафи з боку регулюючих органів – такі наслідки лише однієї успішної кібератаки, яка може паралізувати роботу всього суб'єкта господарювання, завдати шкоди репутації та доходам на багато наступних років [6, с. 130–144].

Важливим елементом безпеки господарської діяльності суб'єкта господарювання є політика інформаційної безпеки, заходи корпоративного або інформаційного комплаєнса, та, безперечно, страхування ризиків втручання штучного інтелекту у бізнесові системи та процеси [7].

Всі організації, установи, підприємства, що керуються сучасними технологіями, зобов'язані вживати заходи захисту інформаційної безпеки, якщо вони зацікавлені в успішному, а головне безпечному майбутньому своєї компанії. Сучасні технології здатні протидіяти кібернетичним атакам, але цього не достатньо, організації повинні подбати, щоб виробничі процеси, політика та поведінка працівників сприяла мінімізації і протидії ризикам. Для забезпечення захисту інформаційних баз потрібно діяти системно [8, с. 235].

Незважаючи на те, що ризики кібератак цілком реальні, багато суб'єктів господарювання ще не знайшли оптимального засобу боротьби з ними. Результати Глобального опитування керівників великих корпорацій, проведеного KPMG у 2018 році [9], показували, що багато респондентів ставляться до кібератак на свій бізнес як до неминучості, а 68% керівників американських компаній назвали це лише питанням часу. При цьому лише 51% керівників компаній із різних країн зазначили, що вони добре підготовлені до кібератак.

Сьогодні суб'єкти господарювання всіх розмірів та форм власності намагаються визначити і оцінити рівень вразливості своїх інформаційних систем і застосовувати заходи реагування на цифрові загрози, що постійно зростають, і цілеспрямовані кібератаки. Оскільки профілактика кіберінцидентів не гарантує 100% успіху, політика ризик-менеджменту багатьох компаній Європи та США обов'язково включає інструменти «пізнього реагування» – страхування від кіберризиків. На відміну від превентивних заходів, таке страхування дозволяє компенсувати втрати від кіберзагрози, якщо її так і не вдалося нейтралізувати.

Згідно з даними, представленими у лютому 2020 року на конференції OECP з розкриття потенціалу ринку кіберстрахування, рівень

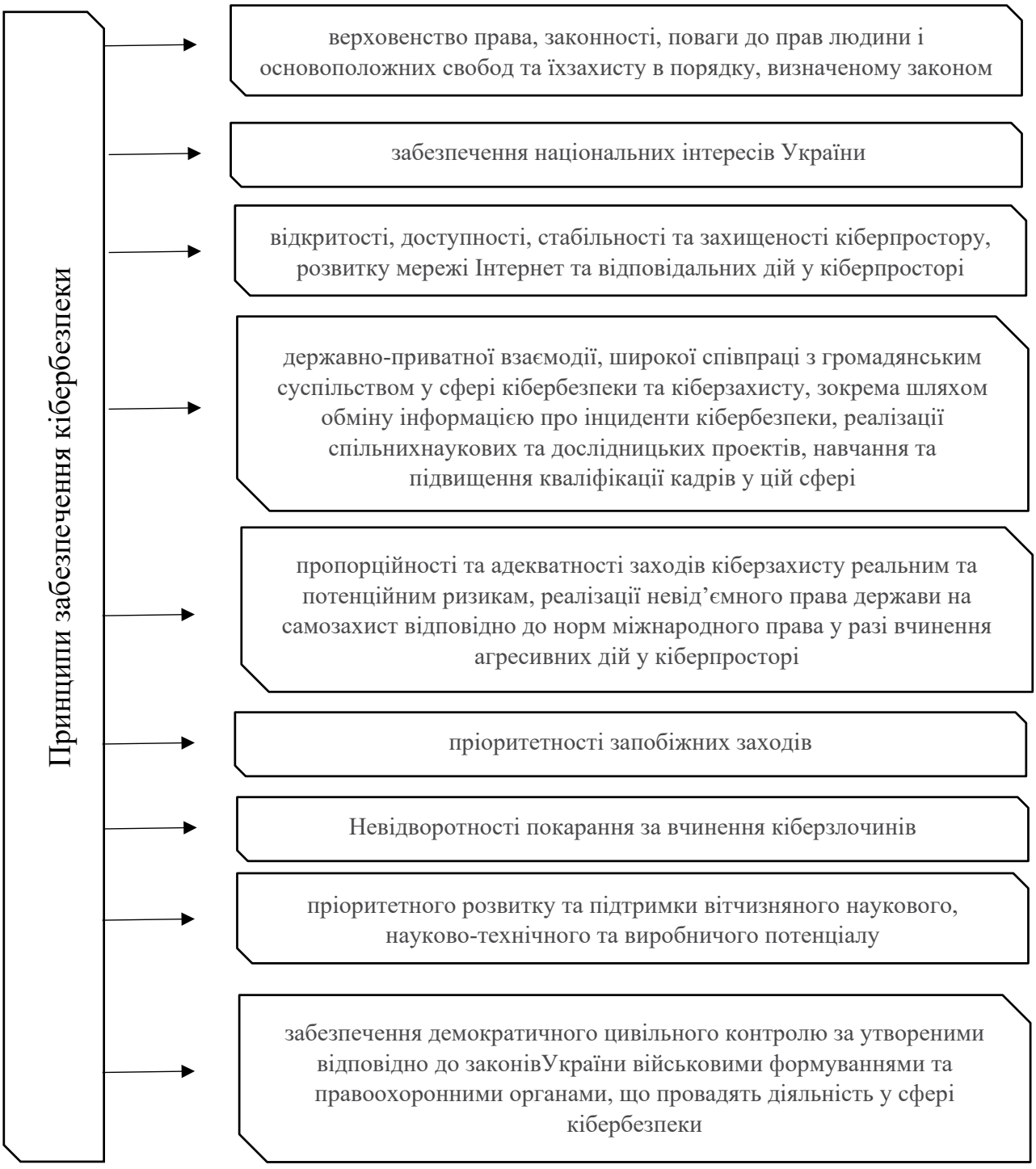

Рис 1. Основні принципи забезпечення кібербезпеки інформаційного простору в Україні

Джерело: сформовано на основі даних [5]

охоплення цими послугами в 37 країнах з розвиненою економікою досягає 60-70% серед компаній-представників великого бізнесу [10].

Кіберстрахування призначене для захисту суб'єкта господарювання від найрозповсюдженіших кіберризиків, а саме: ризиків конфіденційності, ризиків безпеки, операційних ризиків та ризиків обслуговування.

Сучасний ринок страхування кіберризиків – це невелика частина сектора послуг страхування, яка поступово зростає, що дозволяє суб'єктам господарювання захиститися від цифрових загроз. За оцінками Allianz, наразі розмір страхових премій у секторі кіберстрахування становить 2 млрд. доларів США у світі, при цьому на частку ринку США припа-

дає близько 90%. Однак у міру зростання кількості кібератак та регулярного висвітлення у ЗМІ випадків крадіжки або втрати даних клієнтів великими корпораціями, необхідність отримання ефективних послуг зі страхування кіберризиків стає пріоритетним питанням для компаній. Очікується, що до 2025 року страхові премії в цьому секторі по всьому світу досягнуть 20 млрд. доларів [11]. До 2026 року страховики отримуватимуть $28 млрд у вигляді валових підписаних премій кіберстрахування. Страховики продовжать пропонувати страхування кібербезпеки, тому воно є прибутковим.

Зростаюча потреба у послугах, ситуація на ринку страхування кібербезпеки та поінформованість про існуючі ризики створюють сприятливі можливості для страхових компаній, які готові діяти вже зараз, щоб отримати власну частку на ринку та завоювати довіру клієнтів. Можливості та вигоди для страхування від кіберризиків не однакові для компаній із різних сфер та індустрій. Згідно зі світовою статистикою, близько 35% усіх платежів зі страхування від кіберризиків генерують клієнти з фінансового сектора – банки, інші фінансові установи та fintech-стартапи, на другому місці – представники енергетики [11].

Незважаючи на широкі можливості, надання послуг у сфері страхування кіберризиків супроводжується низкою складностей, вирішення яких потребує чіткої ідентифікації проблем та запровадження дієвих методів їх вирішення. Основна проблема полягає в тому, що більшість страхових продуктів були розроблені на підставі актуарно обґрунтованих, агрегованих загальних даних за кілька десятків років, тому послуги в галузі страхування кіберризиків вважаються пов'язаними з ще більшими ризиками: адже цей вид страхування з'явився зовсім недавно, а інформація про супутні ризики та вразливості також є більш фрагментованою.

Оцінка ризику та суми цифрових ризиків також утруднена: багато страхових компаній стикаються зі складністю формування цін на продукти у цій сфері. Крім того, на ринку існує певна невизначеність щодо того, чи надаються послуги зі страхування від кібератак у рамках поточного договору страхування та відповідного обсягу страхового покриття [12].

Ще один фактор, який необхідно враховувати, полягає в тому, що оскільки страхові компанії володіють значними обсягами суворо конфіденційних даних про клієнтів, то вони самі можуть стати кінцевою метою кібератак. Це означає, що питання кібербезпеки мають стати пріоритетом для всіх страхових компаній незалежно від клієнтської бази, якій надаються послуги, та типу страхового покриття.

Інструментами активізації діяльності страхових компаній при страхуванні кіберризиків є:

1. Проактивність. Проактивне визначення рівня зрілості систем забезпечення безпеки клієнтських даних допоможе страховим компаніям оцінити потенційні наслідки кібератак для бізнесу ще до атаки. Це дозволяє знизити окремі області ризику, а також сформувати структуру та визначити ціни на продукти у галузі кіберстрахування.

2. Навчання. Не всі клієнти у повній мірі усвідомлюють потенційні ризики кібератак та їх наслідки, а також те, які послуги їм доступні в кіберстрахуванні. Продумані спеціалізовані освітні програми навчання, присвячені питанням кіберризиків та стратегіям зниження наслідків у випадку їх реалізації, можуть допомогти клієнтам оцінити необхідність в послугах та зрозуміти, які існують типи страхування кібербезпеки.

3. Співпраця для збирання даних. Спільна робота страхових компаній, професійних асоціацій та регулюючих органів дозволить створити базу даних, необхідну для належного структурування, ціноутворення та продажу послуг у сфері страхування кіберризиків, як основної складової загального страхового профілю будь-якого суб'єкту господарювання.

4. Орієнтованість на мікроклієнтів. Кібератаки можуть бути направлені на суб'єктів господарювання будь-якого розміру, а також окремих фахівців, які мають доступ до конфіденційної інформації. Продукти в галузі страхування кіберризиків для таких невеликих учасників ринку – це величезний, мало опанований ринок [13].

Висновки. Початок XXI століття ознаменувався стрімким розвитком і глобальним поширенням інформаційних технологій та штучного інтелекту. Цей процес супроводжується посиленням кіберризиків, викликаних, переважно, діяльністю кіберзлочинців. Така тенденція до зростання кіберінцидентів та збитків, викликаних ними, не тільки збережеться у майбутньому, а й має стійкі перспективи до зростання [14, с. 65–73].

Проведене дослідження дозволило встановити, що до найбільш типових кіберризиків, які зустрічаються у діяльності суб'єктів господарювання, відносять: ризики конфіденційності, ризики безпеки, операційні ризики та ризики обслуговування. Встановлено, що основними джерелами втрат у наслідок кібе-

ратак є: DDoS атаки, фішинг, кібервимагання, крадіжка даних, знищення даних, отримання контролю над IT-системою, атаки на POS-термінали, комп'ютерні віруси.

Охарактеризовано спільні проблеми розвитку ринку страхування кіберризиків, до яких відносять фрагментованність інформації, складність формування цін на страховий продукт в цій сфері, кібернезахищеність страхових компаній. Авторами було визначено, що інструментами активізації діяльності страхових компаній у страхуванні ризиків кібербезпеки діяльності суб'єктів господарювання є: проактивність, навчання, орієнтування на мікроклієнтів та співробітництво у формуванні загальної інформаційної бази

Встановлено, що страхування ризиків застосування штучного інтелекту у діяльності суб'єктів господарювання є дієвим інструментом, який дозволяє як стимулювати впровадження заходів, що посилюють кібербезпеку підприємства, так і компенсувати втрати від кіберзагрози, що вже було реалізовано і якій не вдалося запобігти.

Таким чином, кіберстрахування є специфічним, швидко зростаючим сегментом загального ринку послуг страхування, який, базуючись на основних принципах страхової діяльності, розвиває абсолютно нові інноваційні підходи та рішення. Так, очікується, що вже в найближчі роки крім суто фінансової компенсації, страхові компанії зможуть забезпечити клієнтам повноцінний консалтинг, організаційну та технічну підтримку зі зниження кіберризиків та протистоянню кібератакам, ставши, таким чином, максимально затребуваним сервісом. Тому страхові компанії, які зроблять ключові кроки вже зараз, зможуть зайняти лідируючі позиції на цьому новому, дедалі актуальнішому ринку, і в майбутньому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Олійник І.О. Загальні проблеми захисту кібернетичного простору України. Актуальні проблеми управління інформаційною безпекою держави : зб. тез наук. доп. наук.-практ. конф. (Київ, 26 березня 2021 р.). [Електронне видання]. Київ : НА СБУ, 2021. С. 294–296.

2. Bolot J., Lelarge, M. Cyber Insurance as an Incentivefor Internet Security. In M. E. Johnson (Ed.), Managing Information Risk and the Economics of Security (pp. 269–290). Boston : Springer.

3. Потери организаций от киберпреступности. URL: https://tadviser.ru/index.php/Статья:Потери_организаций_от_киберпреступности#.D0.9C.D0.92.D0.94:_.D0.A3.D1.89.D0.B5.D1.80.D0.B1_.D0.BE.D1.82

4. Про кіберзлочинність : Конвенція Ради Європи від 21.11.2001 // Офіційний вісник України від 10.09.2007 р., № 65, с. 107, стаття 2535, код акту 40846/2007.

5. Про захист прав людини і основних свобод : Європейська конвенція від 04.11.1950. Офіційний вісник України від 16.04.1998 № 13 / № 32 від 23.08.2006 / с. 270.

6. Franke U. The cyber insurance market in Sweden. Computers & Security, 68, 130–144.

7. Бакалінська О.О., Бакалинський О.О. Правове забезпечення кіберзахисту в Україні. URL: https://coordynata.com.ua/pravove-zabezpecenna-kiberzahistu-v-ukraini

8. Шилов М.С., Жевелєва І.С. Удосконалення системи управління інформаційною безпекою в організаціях. Актуальні проблеми управління інформаційною безпекою держави : зб. тез наук. доп. наук.-практ. конф. (Київ, 26 березня 2021 р.). Київ : НА СБУ, 2021. С. 325.

9. Businesses must prepare for new generation of cyber risks. Press Release. URL: https://www.agcs.allianz.com/news-and-insights/news/cyber-risk-guide.html

10. Как компании страхуют киберриски в Украине. URL: https://insart.com.ua/company/news/kak-strahuyt-kiberrisk-ua.html

11. Allianz Global Corporate & Specialty. URL: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/AGCS-Cyberrisk-report.pdf

12.Sullivan J., Nurse J. Cyber Security Incentives and the Role of Cyber Insurance. URL: https://static.rusi.org/246_ei_cyber_insurance_final_web_version.pdf

13. Marais V. L'assurance cyberrisque : une opportunité de devenir leader sur un marché émergent. URL: https://home.kpmg/kz/ru/home/insights/2018/11/cyber-insurance.html

14. Kurmaiev P., Seliverstova L., Bondarenko O., Husarevych N. Cyber insurance: the current situation and prospects of development. *Amazonia Investiga*, 9(28), 65–73. DOI: https://doi.org/10.34069/AI/2020.28.04.8

REFERENCES:

1. Oliinyk, I.O. (2021) Zahalni problemy zakhystu kibernetychnoho prostoru Ukrainy [General problems of protection of cyberspace of Ukraine]. Actual problems of information security management of the state: coll. thesis science. ext. scientific-practical conf. (Kyiv, March 26, 2021). [Electronic edition]. Kyiv: NA SBU, pp. 294–296. (in Ukrainian)

2. Bolot, J. & Lelarge, M. (2009) Cyber Insurance as an Incentivefor Internet Security. In M. E. Johnson (Ed.), Managing Information Risk and the Economics of Security (pp. 269–290). Boston: Springer.

3. Poteri organizatsiy ot kiberprestupnosti [Losses of organization from cybercrime]. Available at: https://tadviser.ru/index.php/Статья:Потери_организаций_от_киберпреступности#.D0.9C.D0.92.D0.94:_.D0.A3.D1.89.D0.B5.D1.80.D0.B1_.D0.BE.D1.82 (in Russian)

4. Pro kiberzlochynnist: Konventsiia Rady Yevropy vid 21.11.2001 [About cybercrime. Council of Europe Convention of 21 November 2001]. Official Gazette of Ukraine of September 10, 2007, № 65, p. 107, Article 2535, act code 40846/2007 (in Ukrainian)

5. Pro zakhyst prav liudyny i osnovnykh svobod: Yevropeiska konventsiia vid 04.11.1950 [On protection of human rights and fundamental freedoms. European Convention of 4 November 1950]. Official Gazette of Ukraine of April 16, 1998, № 13 / № 32 of August 23, 2006 / p. 270. (in Ukrainian)

6. Franke, U. (2017) The cyber insurance market in Sweden. Computers & Security, 68, 130–144.

7. Bakalinska, O.O., Bakalynskyi, O.O. (2020) Pravove zabezpechennia kiberzakhystu v Ukraini [Legal support of cyber defense in Ukraine]. Available at: https://coordynata.com.ua/pravove-zabezpecenna-kiberzahistu-v-ukraini (in Ukrainian)

8. Shylov, M.S., Zhevelieva, I.S. (2021) Udoskonalennia systemy upravlinnia informatsiinoiu bezpekoiu v orhanizatsiiakh [Improving the information security management system in organizations]. Actual problems of information security management of the state: coll. thesis science. ext. scientific-practical conf. (Kyiv, March 26, 2021). Kyiv: NA SBU, p. 325. (in Ukrainian)

9. Businesses must prepare for new generation of cyber risks. Press Release. Available at: https://www.agcs.allianz.com/news-and-insights/news/cyber-risk-guide.html

10. Kak kompanii strahuyut kiberriski v Ukraine [How companies insure cyber risks in Ukraine]. Available at: https://insart.com.ua/company/news/kak-strahuyt-kiberrisk-ua.html (in Russian)

11. Allianz Global Corporate & Specialty. Available at: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/AGCS-Cyberrisk-report.pdf

12. Sullivan, J., Nurse, J. (2020) Cyber Security Incentives and the Role of Cyber Insurance. Available at: https://static.rusi.org/246_ei_cyber_insurance_final_web_version.pdf

13. Marais, V. (2018) L'assurance cyberrisque: une opportunité de devenir leader sur un marché émergent. Available at: https://home.kpmg/kz/ru/home/insights/2018/11/cyber-insurance.html

14. Kurmaiev, P., Seliverstova, L., Bondarenko, O., & Husarevych, N. (2020) Cyber insurance: the current situation and prospects of development. *Amazonia Investiga*, 9(28), 65–73. DOI: https://doi.org/10.34069/AI/2020.28.04.8