ISSN 2786-5827

Електронне наукове видання
НАУКОВИЙ ВІСНИК МІЖНАРОДНОЇ АСОЦІАЦІЇ НАУКОВЦІВ.
Серія: економіка, управління, безпека, технології
SCIENTIFIC BULLETIN OF THE INTERNATIONAL ASSOCIATION OF SCIENTISTS.
Series: Economy, Management, Security, Technology
Том 2, № 2, 2023 **Volume 2, Issue 2, 2023** www.man.org.ua

Наказом МОН України від 10.10.2022 р. №894 видання включено до **категорії «Б»** за спеціальностями:
051 – економіка; 072 – фінанси, банківська справа та страхування; 073 – менеджмент;
076 – підприємництво, торгівля та біржова діяльність; 292 – міжнародні економічні відносини

DOI c
УДК 336.7:368

Рамський Андрій Юрійович,
доктор економічних наук, професор,
завідувач кафедри фінансів,
Київський університет імені Бориса Грінченка,
вул. Бульварно-Кудрявська, 18/2 м. Київ, 04053, Україна
email: a.ramskyi@kubg.edu.ua
ORCID ID: 0000-0001-7368-697X

Арабаджи Кирило Вадимович,
магістрант,
Київський університет імені Бориса Грінченка,
вул. Бульварно-Кудрявська, 18/2 м. Київ, 04053, Україна
email: kvarabadzhy.feu22@kubg.edu.ua
ORCID ID: 0000-0002-7535-6824

Ramskyi Andrii,
Doctor of economic sciences, professor,
Head of the Department of Finance,
Borys Grinchenko Kyiv University,
Bulvarno-Kudriavska str.,18/2, Kyiv, Ukraine, 04053
email: a.ramskyi@kubg.edu.ua
ORCID ID: 0000-0001-7368-697X

Arabadzhy Kyrylo,
master's student,
Borys Grinchenko Kyiv University,
Bulvarno-Kudriavska str.,18/2, Kyiv, Ukraine, 04053
email: kvarabadzhy.feu22@kubg.edu.ua
ORCID ID: 0000-0002-7535-6824

КІБЕРСТРАХУВАННЯ В БАНКІВСЬКОМУ СЕКТОРІ: ІДЕНТИФІКАЦІЯ РИЗИКІВ ТА ІНСТРУМЕНТИ ПІДТРИМКИ БЕЗПЕКИ

CYBER INSURANCE IN THE BANKING SECTOR: IDENTIFICATION OF RISKS AND SECURITY SUPPORT TOOLS

Вступ. Ця стаття містить огляд прогалин у знаннях, пов’язаних із кіберстрахуванням як стратегією управління ризиками саме для банківських установ, які є сучасними місцями алокацій для збору грошей населення, а також важливої персональної інформації. Найчастіше банки можуть бути цілями для кібератак, адже у сучасному світі, в умовах діджиталізації та технологічного розвитку вся банківська система тримається на системах та програмах, які мають уразливі місця саме від кіберзагроз. Загроза втрати важливих персональних даних клієнтів, коштів на індивідуальних рахунках фізичних та юридичних осіб, може призвести не тільки до особистих збитків банку, але й завдати втрат самим клієнтам банку, що прямо впливає на економіку цілої країни, саме тому питання кіберстрахування для банківських установ повинно підніматися на рівні держави. Кібер-ризик, як один з операційних ризиків, повинен включатися у систему ризик-менеджменту банківської діяльності, а найголовнішим інструментом хеджування від потенційних втрат за цим видом ризику, повинно стати кіберстрахування. Відповідно до цього, на тлі актуальності розгляду проблематики кібер-ризику, доцільно вивчити досвід інших країн та спробувати акліматизувати його із певними змінами в Україні, адже повне копіювання закордонної практики може не прижитися у нашій державі, через особливості та специфікації ведення банківського та страхового бізнесу України. На тлі підвищення кібератак на банківський сектор України, актуальність розгляду потенційних факторів хеджування підвищується, а кіберстрахування стає одним із основних напрямків перенесення кібер-ризику на третю сторону. Для зменшення ймовірності настання кіберінциденту та мінімізації втрат від такого ризику, кіберстрахування повинно діяти у поєднанні із модернізацією та постійним оновленням систем ІКТ, на яких працює банківська система, проведення тренінгів та навчань для співробітників на тему кіберзахисту, а також ряд інших чинників, які описані у цій статті.

Матеріали та методи. Основу інформаційної бази для написання статті та проведення супутніх досліджень склала статистична інформація, наукові напрацювання закордонних та вітчизняних вчених, економістів, фінансистів та експертів у фінансовому секторі, а також джерела для інформаційних термінів кіберінцидентів.

Результати і обговорення. За результатами дослідження можна зробити висновки, що кіберстрахування, як вид страхування в Україні знаходиться на етапі становлення. При зростанні кількості кібератак на банківський сектор України актуальність кіберстрахування, як інструменту хеджування зростає з кожним роком. В умовах діджиталізації уся операційна діяльність банку працює на електронних системах ІКТ, які повинні бути захищені від потенційних кіберзагроз, адже несправна робота банку, потенційно призводить до збитків не лише для самого суб’єкту банківської діяльності, але й для клієнтів банку, що є загрозою для усієї економіки країни.

Висновки. На основі дослідження питання кіберстрахування, як головного інструменту хеджування кібер-ризиків для банківського сектору та проблем при складанні договорів кіберстрахування, були надані пропозиції, щодо визначення стратегічних напрямків розвитку кіберстрахування в Україні, що з’явилося на тлі нових викликів та загроз.

Ключові слова: кіберстрахування, банки, банківська система, кібер-ризик, ризик-менеджмент.

Introduction. This article provides an overview of the knowledge gaps related to cyber insurance as a risk management strategy specifically for banking institutions, which are today's allotment sites for collecting the public's money as well as sensitive personal information. Most often, banks can be targets for cyberattacks, because in today's world, in the conditions of digitalization and technological development, the entire banking system rests on systems and programs that have vulnerabilities precisely from cyber threats. The threat of loss of important personal data of customers, funds in individual accounts of individuals and legal entities, can lead not only to personal losses of the bank, but also cause losses to the bank's customers themselves, which directly affects

the economy of the entire country, which is why the question of cyber insurance for banking institutions should be raised at the state level. Cyber risk, as one of the operational risks, should be included in the risk management system of banking activity, and cyber insurance should be the most important tool for hedging against potential losses from this type of risk. Accordingly, against the background of the relevance of consideration of the issue of cyber risk, it is advisable to study the experience of other countries and try to acclimatize it with certain changes in Ukraine, because the complete copying of foreign practice may not take root in our country, due to the peculiarities and specifications of conducting banking and insurance business in Ukraine . Against the background of increasing cyber attacks on the banking sector of Ukraine, the urgency of considering potential hedging factors increases, and cyber insurance becomes one of the main directions of transferring cyber risk to a third party. To reduce the probability of a cyber incident and minimize losses from such a risk, cyber insurance should act in conjunction with the modernization and constant updating of ICT systems on which the banking system operates, conducting training and education for employees on the topic of cyber protection, as well as a number of other factors, which are described in this article.

Materials and methods. Statistical information, scientific works of foreign and domestic scientists, economists, financiers and experts in the financial sector, as well as sources for information terms of cyber incidents formed the basis of the information base for writing the article and conducting related research.

Results and discussion. Based on the results of the research, it can be concluded that cyber insurance as a type of insurance in Ukraine is at the stage of formation. With the growing number of cyber attacks on the banking sector of Ukraine, the relevance of cyber insurance as a hedging tool is growing every year. In the conditions of digitization, the entire operational activity of the bank works on electronic ICT systems, which must be protected from potential cyber threats, because the faulty operation of the bank potentially leads to losses not only for the subject of banking activity itself, but also for the bank's clients, which is a threat to of the entire economy of the country.

Conclusions. Based on the study of the issue of cyber insurance as the main tool for hedging cyber risks for the banking sector and problems in drawing up cyber insurance contracts, proposals were made to determine the strategic directions of the development of cyber insurance in Ukraine, which appeared against the background of new challenges and threats.

Keywords: cyber insurance, banks, banking system, cyber risk, risk management.

JEL Classification: E44, G22, G21

Вступ. Події кібер-ризику можуть спричинити значні та різноманітні наслідки для постраждалих бізнесів, насамперед йдеться про банківські установи. Банки є центральною точкою для будь-якого бізнесу, де відбувається їх операційна, інвестиційна або фінансова діяльність. Проведення бізнесом операцій з купівлею, продажем, як головними діями в операційній діяльності, безпосередньо пов’язані із банківськими установами, які є головними виконавцями таких дій. З точки зору того, що все платіжні операції банку виконуються різними системами інформаційно-комунікаційних технологій (ІКТ), які піддаються кібер-ризикам, можна зробити висновок, що порушення діяльності банку, через виведення зі строю таких систем, в результаті кібератаки, спричиняє збитки не тільки для банку, але й для усього бізнесу, який цей банк обслуговує, а отже й для економіки країни в цілому. Банки, які піклуються про безпеку, знають про кібер-ризики та вживають заходів для зменшення цього ризику. Однак захистити від усіх непередбачуваних випадків неможливо чи економічно доцільно. Таким чином, банки можуть отримати вигоду від змішаного підходу до управління кібер-ризиками, беручи до уваги широкий спектр заходів щодо зменшення ризиків, включаючи передачу ризиків у формі кіберстрахування.

Питаннями важливості кіберстрахування у банківській сфері займалися ряд експертів та науковців, як вітчизняного, так і закордонного походження, одними з яких є: Дубіна М., Середюк І., Білоус Н. (Дубіна, 2020), Кльоба Т., Кльоба Л. (Kloba, 2022), Doerr S., Gambacorta L., Leach T., Legros B. and Whyte D. (Doerr, 2022), Gatzert N., Schubert M. (Gatzert, 2022), Shinichi K., Kang Jun-Koo, Kim J., Andreas M., René M. Stulz (Shinichi, 2020). Попри те, що вже наявні роботи вчених та експертів у фінансовій і економічній сферах на тематику кібер-ризику, тема кіберстрахування вважається новою, що потребує більшої уваги до цього сегменту страхування, особливо у розрізі банківського сектору, який є найбільш уразливим до кібер-загроз.

Метою статті є дослідження та аналіз зарубіжного досвіду кіберстрахування у банківській сфері та огляд можливостей акліматизації практик інших країн в Україні, з метою формування стійкої системи банківського ризик-менеджменту у сфері кібер-ризиків, за допомогою кіберстрахування.

Матеріали та методи. Основу інформаційної бази для написання статті та проведення супутніх досліджень склала статистична інформація, наукові напрацювання закордонних та вітчизняних вчених, економістів, фінансистів та експертів у фінансовому секторі, а також джерела для інформаційних термінів кіберінцидентів.

Результати і обговорення. Сучасні умови розвитку бізнесу, як найголовнішої складової формування економіки у державі, зумовлює його перехід до повної співпраці із банківськими установами. На сьогодні, банки виконують великий об’єм транзакцій для суб’єктів господарювання, які пов’язані з операційною, інвестиційною та фінансовими діяльностями бізнесу (Рекуненко, 2021, С. 7-8). Уся банківська система побудована на системах ІКТ (Швачич, 2017), які піддаються загрозам з боку кібер-ризиків. Виведення зі строю таких систем, спричиняє збитки не тільки для банка, але й для усіх суб’єктів господарювання, які є клієнтами цього банку, що, вже на макрорівні впливає на економіку країни. З моменту відкриття технологічних банків та повного переходу до безготівкових розрахунків, актуальність захисту від кібер-ризиків стає ще більш актуальною. Розв’язання питання кіберзагроз для банківських установ полягає у кіберстрахуванні.

Ми дотримуємося вже наявного визначення кібер-ризику у літературі, а також страхових регуляторів, і визначаємо кібер-ризики як підкатегорію операційного ризику. Вже наявна література визначає кібер-ризик, як операційні ризики для інформаційних і технологічних активів, які мають наслідки, що впливають на конфіденційність, доступність або цілісність інформації або інформаційних систем (Gatzert, 2022, С. 749). Також потрібно зазначити, що для банківських установ, як і для будь-якого бізнесу, кіберстрахування набуває актуальності у той момент, коли збитки від наслідків кібератак є дорожчими ніж сам захист від кіберзагроз (Shinichi, 2020). В розрізі банківського сектору, можна точно сказати, що збитки від кіберінцидентів в багатьох випадків є більшими ніж сама плата за страхування. Така тенденція пояснюється тим, що банку акумулюють грошові кошти своїх клієнтів більшою мірою саме в безготівковій формі, тобто електронно, тому захист електронних систем банк повинен бути однією з найголовніших тем, у питанні управління ризик-менеджментом банку.

Для розуміння розмірів банківського сектору України та доцільності прийняття кіберстрахування, було досліджено деякі показники банків за період 2020-2022 років. Насамперед, пропонується розглянути доходи банків за досліджуваний період часу, адже дана статистика повинна показувати діяльність банківських установ, що відбувається переважно на основі та за допомогою систем ІКТ, які є уразливими для кіберзагроз (табл. 1). Позитивна динаміка показників доходів в банківській сфері України свідчить про високий попит населення на банківські послуги, що більшою мірою підкреслює важливість страхування своєї електронної системи від кіберзагроз, адже в результаті реальної загрози збитки будуть не тільки у банка, але й у багатьох клієнтів, які є важливими бізнесами для економіки країни.

Таблиця 1

Доходи банківського сектору України, за 2020-2022 рр., у млн. грн.

Найменування доходу	2020 р.	2021 р.	2022 р.
Процентні доходи	147 743	168 746	216 992
Комісійні доходи	70 640	93 162	85 568
Результат від переоцінки та від операцій купівлі-продажу	21 507	–77	43 525
Інші операційні доходи	6 813	7 488	8 097
Інші доходи	2 705	3 175	2 353
Повернення списаних активів	763	1 370	853
Всього	250 171	273 864	357 388

Джерело: складено за даними Національного банку України.

Національний банк України. Наглядова статистика.
URL: https://bank.gov.ua/ua/statistic/supervision-statist#1 (дата звернення: 07.05.2023)

Як можна побачити із таблиці 1, доходи банків за період 2020-2022 років стрімко росли угору, це є підтвердженням того, що банківський сектор України має попит і велику частину від цього попиту забирає на себе бізнес, який є клієнтом для банків. Проведення усіх платежів та грошей, через електронні системи збільшує ризик кібератак з метою перебою у таких системах, або викраденням коштів з рахунків банку. Саме тому система ризик-менеджменту банків повинна бути побудована таким чином, аби усі методи, інструменти, організаційні центри, що є точками взаємозв'язку, для ідентифікації та усунення ризику, працювали на забезпечення захисту на контролю за кібер-ризиком, як за допомогою внутрішніх систем захисту, так і зовнішніх – кіберстрахування (Дубіна, 2020).

Банки, як правило, відповідають за управління та нагляд за критично важливою інфраструктурою (наприклад, платіжні системи) (Содома, 2020). Отже, успішна кібератака на систему ІКТ банку, як критичну інфраструктуру може призвести не лише до значних грошових та репутаційних витрат самому банку, а також призвести до широкомасштабних збоїв у фінансовій системі багатьох суб'єктів господарювання, через, що безперервна діяльність банку та бізнесу стає від питання, що призводить до ще більших збитків (Чкан, 2020).

Крім того, банки захищають дуже чутливі дані та інформацію, яку часто шукають злочинці. Наприклад, конфіденційний матеріал щодо майбутньої політики або інсайдерську інформацію (рівень збитків/доходів за фінансовий рік, юридичні та судові справи, надзвичайні випадки, шахрайство у середині банка, корупційні випадки), яка може стати мішенню для злочинців, особливо з точки зору того, якщо цей банк має акцій та котирує їх на біржі (S. Doerr, 2022). На цьому тлі встановлюється розуміння того, який тип кібератак є найпоширенішими, що може допомогти банкам визначити потенційні наслідки кіберзагроз та можливості, щодо захисту від цих ризиків.

Відповідно до закордонних практик банків у країнах, що розвиваються та країнах із розвиненою економікою, однаково вважають фішинг та інші форми ІТ-атак, як найбільш вірогідний тип атаки (рис. 1). Цей тип атак зазвичай передбачає надсилання багатьох електронних листів для підвищення ймовірності що особа стане жертвою такого нападу, якщо такий лист потрапить до недосвідченого працівника банку, то це може стати причиною витоку цінної інформації. Причому для таких нападів потрібно небагато інвестиції від імені зловмисників. Окрім цього, витрати на сам інцидент будуть відрізнятися від ймовірності кіберкейса, адже найбільші витрати від інциденту покладаються на вдосконалене шкідливе

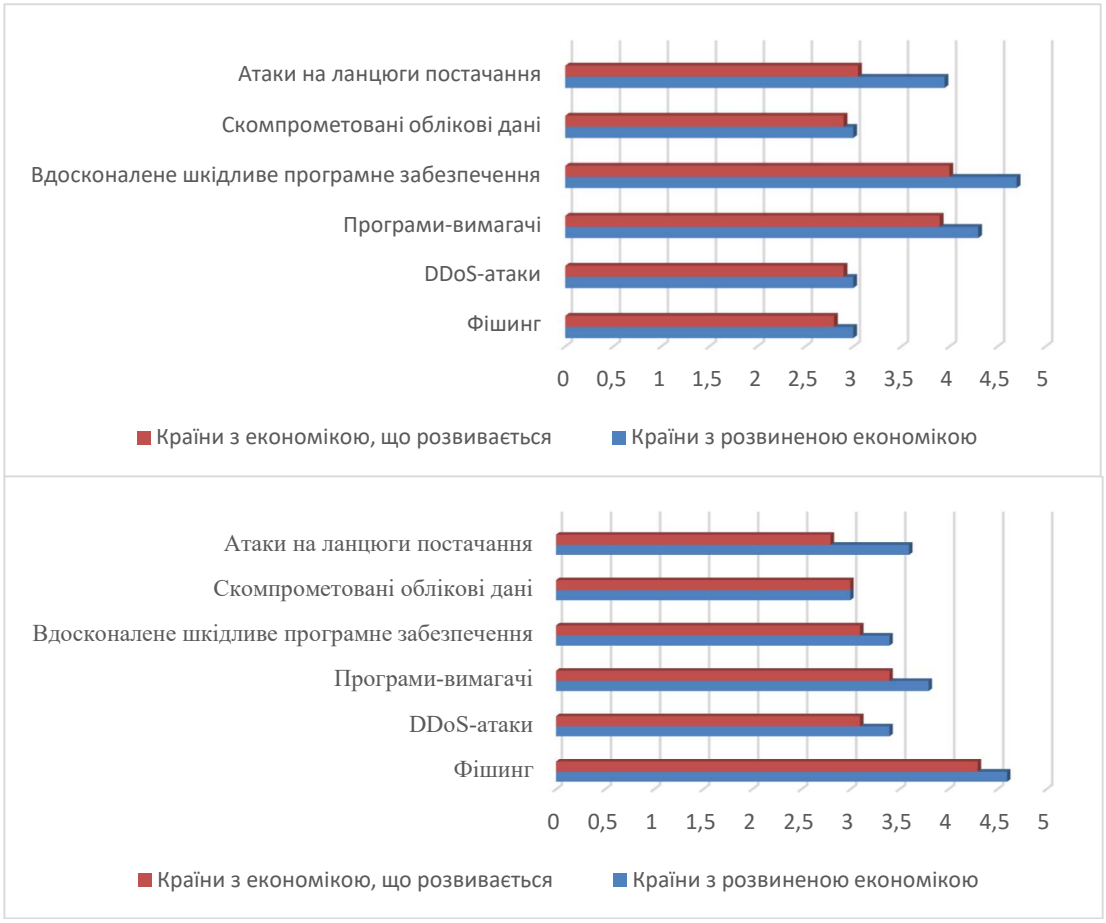

Рис.1. Витрати від кіберінциденти та їх ймовірність в країнах з розвиненою економікою та економікою, що розвивається, за шкалою оцінки 1-5

Джерело: складено за S. Doerr et al (S. Doerr, 2022)

програмне забезпечення та програми атаки від програм-вимагачів (тип шкідливого програмного забезпечення, призначеного для блокування доступу до комп'ютерної системи, доки не буде сплачена певна сума грошей). Особливістю таких загроз є особи, які можуть стояти за кіберінцидентами, це можуть бути як зовнішні суб'єкти, такі як кіберзлочинці, організовані зловмисники, хакери так і внутрішні суб'єкти – інсайдери, звичайні працівники банку. Якщо, особа, яка здійснили кіберінцидент є внутрішньої, то це також може вказувати на неефективність HR-політик банку, антифрод політик й системи внутрішніх контролів, які повинні бути у банківської установи.

Перша діаграма на рисунку 1 відповідає за витрати на кіберінциденти, друга діаграма за їх ймовірність. Оцінка 1 відповідала за дуже низьку ймовірність інциденту та низьку ціну витрат від кіберінциденту, а оцінка 5 відповідала за високу ймовірність настання ризику та найвищий ступінь витрат від такої загрози. Тепер доцільно розглянути, що собою представлять ці види загроз.

Атаки на ланцюги постачання – це нові загрози, націлені на розробників і постачальників програмного забезпечення. Мета полягає в тому, щоб отримати доступ до вихідних кодів, створювати процеси або оновлювати механізми шляхом зараження легітимних програм для розповсюдження шкідливого ПЗ (програмного забезпечення)[1]. Скомпрометовані облікові дані — це випадки, коли неавторизований користувач отримує доступ до дійсних

[1] Microsoft Learn. URL:https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/supply-chain (Accessed 1 May, 2023).

облікових даних авторизованого користувача, щоб використовувати їх у нечесних цілях. Це ніколи не є найкращим сценарієм для здоров'я та безпеки мережі вашої організації[2].

Розширене зловмисне програмне забезпечення – це різновиди зловмисного програмного забезпечення, розроблені з розширеними можливостями для зараження, зв'язку та контролю, переміщення або вилучення даних/виконання корисного навантаження (Прищепа, 2020).

Розширене зловмисне програмне забезпечення часто створюється для скритності або стійкості та здатне уникнути виявлення традиційними антивірусними рішеннями. Останніми роками спостерігається зростання кількості атак із застосуванням передового зловмисного програмного забезпечення, що наражає бізнес на небезпеку через складні можливості зловмисного програмного забезпечення та швидкість, з якою воно розвивається, щоб випередити виявлення. DDoS-атаки – це кібератаки на комп'ютерні системи управління банком, головна мета яких, зробити обмеженість доступу до цих систем та припинити їх діяльність.

Кіберінциденти у банківській сфері це вже певна константа, тому для банків питання захисту від кібер-ризику є актуальним завжди. Кіберстрахування може стати розв'язком цього питання, в умовах, коли велика кількість хакерських атак та сторонніх програм-шкідників готові завдати збитків банківському сектору та бізнесу в цілому. За 2022 рік багато електронних систем та джерел піддалися впливу від кібератак (Бараненко, 2021). Починаючи із січня 2022 року, коли на деяких державних сайтах з'являлася інформація провокаційного змісту, одними із таких були сайти, де банки могли перевірити кредитні історії клієнтів (Kloba, 2022). Наприклад, згаданий на рис.1 кіберінцидент "атаки на ланцюги постачання" дав можливість порушникам вивести із ладу телекомунікаційні та автоматизовані системи банків. Під час лютневих подій 2022 року, відбулася велика кількість кібероперацій агресора на банківський сектор України, одними із таких були:

1) Надсилання клієнтами банку SMS оповіщення із змістом про те, що банківська система вийшла із ладу;

2) Розсилка повідомлень між банківськими установами про те, що будівлі (офіси, філії банків) є замінованими;

3) DDoS-атаки, які були направлені на веб-ресурси найбільших українських банків, атаки на DNS-сервери, що не дало змогу користуватися офіційним веб-ресурсом НБУ.

Окрім цього, у березневий період 2022 року спостерігалися DDoS-атаки, для реалізації яких кіберзлочинці розміщували шкідливий код JavaScript (BrownFlood) у структурі веб-сторінок і файлів скомпрометованих сайтів (переважно під контролем WordPress[3], в результаті чого обчислювальні ресурси комп'ютерів відвідувачів таких веб-сайтів використовуються для генерації аномальної кількості запитів для атаки на цілі, URL-адреси яких статично визначені в шкідливому коді JavaScript. Іншими словами, відвідувачі сайту сформували новий ботнет, за допомогою якого зловмисники атакували, в тому числі банківські установи.

Для належного розвитку кіберстрахування в Україні, як одного з інструментів хеджування від кібер-ризику для банківських установ, потрібно розробити стратегію і план розвитку страхування від кібер-ризиків. Перед складанням стратегії, доцільно виділити основні проблеми з якими стикаються банківські установи в процесі вирішення доцільності користуванням послуг кіберстрахування (рис. 2).

Найчастіше страхову послугу дуже складно продати, через те, що покупець може не отримати вигоди від такої послуги, адже немає 100 % ймовірності того, що страховий випадок дійсно настане (Журавка, 2020). Окрім цього, через унікальну специфіку кібер-ризику та його ранню історію, страховик може включати у договір страхування додаткові пункти, які описують у разі чого саме страховик зобов'язується виплатити страхове відшкодування

---

[2] Exabeam Community. URL:https://community.exabeam.com/s/ (Accessed 1 May, 2023).

[3] CERT-UA. URL:https://cert.gov.ua/article/39923 (Accessed 1 May, 2023).

страхувальнику. Оскільки страхові премії часто розраховуються на основі статистичних даних, то саме в Україні виникає проблеми у цьому питанні, адже великої кількості статистичних даних із кіберінцидентів немає, тому зробити актуарні розрахунки, в таких умовах, дуже складно, що призводить до страхового тарифу сума якого, у рази більше ніж в інших видах страхування, через що, можна спостерігати велику вартість такого страхування.

Рис. 2. Основні проблеми (питання), які виникають в процесі укладання договору кіберстархування

Джерело: складено автором самостійно

На основі виявлених проблемних точок у процесі вирішення доцільності страхування від кібер-ризику та реальної актуальності кіберстрахування для банків, було складено загальну стратегію розвитку кіберстрахування в Україні, яку можна виділити в таких напрямках (рис. 3):

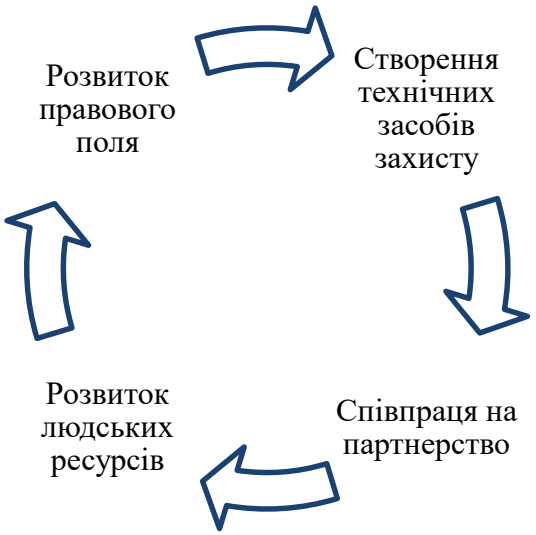

Рис. 3. Основні стратегічні напрямки розвитку кіберстрахування в Україні

Джерело: складено автором

Виходячи із рисунка 3, було зроблено детальний опис стратегічних напрямків розвитку кіберстрахування в Україні:

1) Розвиток правового поля:

- Визначення стандартів безпеки даних та приватності в Інтернеті;
- Визначення обов'язків страхових компаній щодо кібербезпеки та створення сприятливого регуляторного середовища.

2) Створення технічних засобів захисту:

- Розробка нових методів кіберзахисту та розробка протоколів безпеки;

- Впровадження інноваційних технологій для захисту персональних даних та обмеження доступу до них;
- Розробка кіберстрахових продуктів, які забезпечують комплексний захист від кібератак.

3) Співпраця та партнерство:

- Співпраця між страховими компаніями та іншими суб'єктами, які мають досвід у кібербезпеці, зокрема з виробниками програмного забезпечення;
- Розробка нових видів страхування, що враховують кібер-ризики та виклики.

4) Розвиток людських ресурсів:

- Навчання страхових працівників та фахівців у сфері кібербезпеки;
- Проведення навчальних заходів для широкого загалу з питань кіберзахисту та кіберстрахування;
- Проведення просвітницької роботи щодо кібербезпеки та кіберзахисту.

Розвиток правового поля, та визначення термінів стандартів безпеки баз даних стане підставою для банківських установ використовувати найкращі стандарти кібербезпеки, якими користуються банки в інших країнах. Відповідно до цього, держава повинна розуміти, що банки є ключовим суб'єктом через який проходять всі операції бізнесу, оскільки ці операції майже на 100% проходять за допомогою систем ІКТ **(**Рудевська, 2020**)**, тому доцільно зробити страхування від кібер-ризиків для банків обов'язковим, адже потенційні збитки від таких атак можуть зробити банк неплатоспроможним, що порушить його фінансову стійкість до у кінцевому випадку, може призвести до банкрутства.

Окрім цього, страховик повинен досліджувати нові зміни та інновації у сфері кіберзахисту. для того, щоб мати можливість пропонувати банкам створити або оновити технічні засоби захисту від кібератак. Наприклад, встановити нове програмне забезпечення, або оновити програми антивірусу та інші, які мають вищі сертифікати та протоколи захисту (Завгородня, 2021). Тобто, страховик повинен бути зацікавлений в тому, що банк надійно захищений від кібератак, а дотримуючись порад страховика, банківські установи можуть отримувати знижки на страхові тарифи за кіберстрахуванням.

Розвиток людських ресурсів є ключовим питанням у сфері кіберстрахування, адже навчання працівників банку від захисту, моніторингу, превентивних дій від кібератак є запорукою успіху та зменшення ймовірності настання страхового випадку (Арсенович, 2022, С. 7-27). Тому у страховика є можливість включити у договір страхування пункт про періодичні тренінги для працівників банку на тему кібербезпеки банку, що може, у свою чергу, зменшити вартість страхового тарифу, але навчання співробітників потенційно зменшує ймовірність настання кібер-ризику. Наприклад, організація ISACA, яка працює із користувачами інтернет-технологій та підтримує довіру до інформації та інформаційних систем, поширює різні сертифікації, а також надає доступ до широкого спектра навчальних ресурсів Cybersecurity Nexus [4].

Становлення кіберстрахування в Україні є надзвичайно важливим для прийняття сучасних ризиків. На сучасному етапі ринку кіберстрахування в Україні, цей вид страхування є новим і зараз йде етап його впровадження на ринок, страховикам важлива підхопити цю тенденцію, адже ця динаміка базується на змінах у попиті населення (в цьому випадку бізнесу). Великим плюсом є те, що страхування від кібер-ризиків є актуальним не лише для банківського сектору, але й для середнього та великого бізнесу, міжнародних компаній, акціонерних товариств тощо (Приказюк Н.В., 2020). Але в реаліях того, що кібер-ризик та збитки від нього можуть призвести банк до банкрутства, актуальність кіберстрахування саме для банківського сектору є нагальним питанням, яке повинно бути розглянуто, як банками, страховими компаніями так і державою.

[4] ISACA. URL: https://www.isaca.org/training-and-events/cybersecurity (Accessed 1 May, 2023).

Висновки. У статті було проведено дослідження та аналіз банківського сектору Україна, на основі динаміки доходів банків, яке показало, що банківський сектор з кожним роком отримує все більше грошей від населення та акумулює їх на своїх рахунках, за рахунок чого має можливість проводити операційну діяльність та отримувати дохід і нарощувати ресурси, навіть, попри військову ситуацію в Україні. Окрім цього було проаналізований зв'язок між ймовірністю настання кіберінциденту та збитками яких він може завдати, в результаті цього аналізу виявилося, що не завжди найчастіший кіберінцидент (інцидент із найбільшим відсотком ймовірності), завдає найбільшу шкоду для банку та банківській системі.

Розгляд основних проблем на етапі укладання договору кіберстрахування, дали поштовх до виявлення перешкод у сфері кіберстрахування на етапах становлення та розвитку в українському ринку страхування. На основі виявлених проблем та за допомогою подальших досліджень було запропоновано стратегію розвитку кіберстрахування в Україні, що є потенційно важливим на наступні декілька років.

Банки мають велику кількість конфіденційної інформації про своїх клієнтів, таку як особисті дані, фінансову історію та іншу важливу інформацію. Ця інформація може бути скомпрометована в результаті кібератаку або витоку даних, які можуть призвести до значних фінансових втрат та зниження репутації банку. Крім того, банки є показовими мішенями для кіберзлочинців через використання електронних платіжних систем, мобільного та інтернет-банкінгу. У разі кібератаки банки можуть втратити контроль над своїми системами та фінансовими активами, а також постраждати від поганих відгуків клієнтів. Отже, кіберстрахування банків зменшує ризики втрати конфіденційної інформації та запобігає негативним наслідкам, пов'язаним з кібератаками. Враховуючи швидке зростання кіберзлочинності, кіберстрахування стає все актуальнішим для банків та інших компаній, які користуються фінансовими послугами.

Список використаних джерел.

1. Дубіна М. В., Середюк І. О., Білоус Н. В. Роль кіберстрахування в системі ризик-менеджменту банківських установ. *Проблеми і перспективи економіки та управління.* 2020. № 1(21). С. 183–196. https://doi.org/10.25140/2411-5215-2020-1(21)-183-196.
2. Kloba L., Kloba T. Cyber threats of the banking sector inthe conditions of the war in Ukraine. *Financial and credit activity problems of theory and practice*. 2022. No. 5, № 46. Pp. 19–28. https://doi.org/10.55643/fcaptp.5.46.2022.3883.
3. Doerr S. et al. Cyber risk in central banking. *BIS Working Papers*. 2022. No. 1039. URL: https://www.bis.org/publ/work1039.pdf.
4. Gatzert N., Schubert M. Cyber risk management in the US banking and insurance industry: a textual and empirical analysis of determinants and value. *Journal of risk and insurance*. 2022. https://doi.org/10.1111/jori.12381.
5. Shinichi K., Kang Jun-Koo, Kim J., Andreas M., René M. Stulz. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of financial economics*. 2020. https://doi.org/10.1016/j.jfineco.2019.05.019.
6. Рекуненко І.І., Шалда А.А., Чийпеш В.О. Роль банківського сектору в розвитку фондового ринку України. *Ефективна економіка.* 2021. №12. URL: http://www.economy.nayka.com.ua/pdf/12_2021/7.pdf.
7. Швачич Г.Г., Толстой В.В., Петречук Л.М., .Іващенко Ю.С., Гуляєва О.А, Соболенко О.В. Сучасні інформаційно-комунікаційні технології. *Навчальний посібник.* 2017. С. 75-78. URL: https://nmetau.edu.ua/file/ikt_tutor.pdf.
8. Содома Р., Агрес О., Шматковська Т. Платіжні системи в умовах діджиталізації. *Вісник Львівського національного аграрного університету. Економіка АПК*. 2020. №27. С. 87-91. https://doi.org/110.31734/economics2020.27.087.

9. Чкан І.О., Чкан А.С. Електронний банкінг для бізнесу і населення як запорука розвитку ринкової інфраструктури. *Ефективна економіка*. 2020. № 4. URL: http://www.economy.nayka.com.ua/pdf/4_2020/60.pdf.

10. Прищепа О., Доценко О. Огляд статичних методів аналізу зловмисного програмного забезпечення. *Комп'ютерні науки та кібербезпека*. 2020. №2. С. 15-24. URL: https://periodicals.karazin.ua/cscs/article/view/16771/15469.

11. Бараненко Р.В. Кібератаки як одна з форм кібертероризму. *Вчені записки Таврійського національного університету імені В. І. Вернадського*. 2021. Том 32 (71) ч 1.№ 1. https://doi.org/10.32838/2663-5941/2021.1-1/07.

12. Журавка О.С., Бухтіарова А.Г., Пахненко О.М. Страхування. Н*авчальний посібник. Сумський державний університет.* 2020. С. 72-83. URL: https://core.ac.uk/download/pdf/324218949.pdf.

13. Рудевська В. І. Теоретичні підходи до визначення сутності банківської діяльності. *Підприємництво та інновації*. 2020. № 12. С. 194–199. https://doi.org/10.37320/2415-3583/12.34.

14. Завгородня Ю. В. Кібербезпека як інноваційний захист у політичному просторі України. *Вісник Національного технічного університету України "Київський політехнічний інститут""Політологія соціологія право".* 2021. № 4(52). С. 33-38. https://doi.org/10.20535/2308-5053.2021.4(52).248130.

15. Арсенович Л. Удосконалення механізмів формування системи підготовки кадрів у сфері кібербезпеки в умовах державно-приватної взаємодії. *Науковий вісник: Державне управління.* 2022. No 1(11). С. 6-27. URL: https://nvdu.undicz.org.ua/index.php/nvdu/article/view/212/225 https://doi.org/10.33269/2618-0065-2022-1(11)-6-27.

16. Приказюк Н.В., Гуменюк Л.С. Кібер-страхування як важливий інструмент захисту підприємств в умовах цифровізації економіки. *Ефективна економіка*. 2020. №4. URL: http://www.economy.nayka.com.ua/pdf/4_2020/8.pdf.

References.

1. Dubina, M. V., Serediuk, I. O. and Bilous, N. V. (2020), "The role of cyber insurance in the risk management system of banking institutions", *Problemy i perspektyvy ekonomiky ta upravlinnia,* vol.1(21), pp. 183–196. https://doi.org/10.25140/2411-5215-2020-1(21)-183-196.

2. Kloba, L. and Kloba, T. (2022), "Cyber threats of the banking sector inthe conditions of the war in Ukraine", *Financial and credit activity problems of theory and practice,* no. 5, vol. 46, pp. 19–28. https://doi.org/10.55643/fcaptp.5.46.2022.3883.

3. Doerr, S. et al. (2022), "Cyber risk in central banking", *BIS Working Papers*, vol. 1039. Retrieved from: https://www.bis.org/publ/work1039.pdf.

4. Gatzert, N. and Schubert, M. (2022), "Cyber risk management in the US banking and insurance industry: a textual and empirical analysis of determinants and value", *Journal of risk and insurance*. https://doi.org/10.1111/jori.12381.

5. Shinichi, K., Kang, Jun-Koo, Kim, J., Andreas, M. and René M. Stulz. (2020), "Risk management, firm reputation, and the impact of successful cyberattacks on target firms", *Journal of financial economics.* https://doi.org/10.1016/j.jfineco.2019.05.019.

6. Rekunenko, I.I., Shalda, A.A. and Chyipesh, V.O (2021), "The role of the banking sector in the stock market of Ukraine", *Efektyvna ekonomika*, vol. 12. http://www.economy.nayka.com.ua/pdf/12_2021/7.pdf.

7. Shvachych, H.G., Tolstoy, V.V., Petrechuk, L.M., Ivashchenko, Yu.S., Gulyaeva, O.A. and Sobolenko, O.V. (2017), *Suchasni informatsiino-komunikatsiini tekhnolohii* [Modern information and communication technologies], Navchalnyi posibnyk, Dnipo, Ukraine.

8. Sodoma, R., Ahres, O. and Shmatkovska, T. (2020), "Payment systems in the

conditions of digitalization", *Visnyk Lvivskoho natsionalnoho ahrarnoho universytetu,* vol. 27, pp. 87-91. https://doi.org/110.31734/economics2020.27.087.

9. Chkan, I.O. and Chkan, A.S. (2020), "E-banking for business and population as a guarantee for market infrastructure development", *Efektyvna ekonomika,* vol. 4. http://www.economy.nayka.com.ua/pdf/4_2020/60.pdf.

10. Pryshchepa, O., Dotsenko, O. (2020), "Overview of static methods of analysis malicious software", *Kompiuterni nauky ta kiberbezpeka,* vol. 2, pp. 15-24. https://periodicals.karazin.ua/cscs/article/view/16771/15469.

11. Baranenko, R.V. (2021), "Cyber attacks as a form of cyber terrorism", *Vcheni zapysky Tavriiskoho natsionalnoho universytetu imeni V. I. Vernadskoho,* no, 32 (71) part 1, vol.1. https://doi.org/10.32838/2663-5941/2021.1-1/07.

12. Zhuravka, O.S., Bukhtiarova, A.G. and Pakhnenko, O.M (2020), *Strakhuvannia* [Insurance], Navchalnyi posibnyk, Sumskyi derzhavnyi universytet, Sumy, Ukraine.

13. Rudevska, V. I. (2020), "Theoretical approaches to determining the essence of banking", *Pidpryiemnytstvo ta innovatsii,* vol. 12, pp. 194–199. https://doi.org/10.37320/2415-3583/12.34.

14. Zavhorodnia, Yu. V. (2021), "Cyber security as an innovative protection in the political space of Ukraine", *Visnyk Natsionalnoho tekhnichnoho universytetu Ukrainy "Kyivskyi politekhnichnyi instytut" "Politolohiia sotsiolohiia pravo",* vol. 4(52), pp. 33-38. https://doi.org/10.20535/2308-5053.2021.4(52).248130.

15. Arsenovych, L. (2022), "Improving the mechanisms for forming a system of training in the field of cybersecurity in terms of public-private interaction", *Naukovyi visnyk: Derzhavne upravlinnia,* no. 1(11), pp. 6-27. https://nvdu.undicz.org.ua/index.php/nvdu/article/view/212/225.

16. Prykaziuk, N.V. and Humeniuk, L.S. (2020), "Cyber-insurance as an important tool of enterprise protection in the digitization economy", *Efektyvna ekonomika,* vol. 4. http://www.economy.nayka.com.ua/pdf/4_2020/8.pdf

Стаття надійшла до редакції 10.05.2023 р.
Рецензовано 20.05.2023 р.
Опубліковано 30.05.2023 р.