Міністерство освіти і науки України
Сумський державний університет

Кваліфікаційна наукова праця
на правах рукопису

УДК: 330.342:338.28:004.738.5.056(043.5)

КУШНЕРЬОВ ОЛЕКСАНДР СЕРГІЙОВИЧ

ДЕТЕРМІНАНТИ ПОШИРЕННЯ ТА ЛОКАЛІЗАЦІЇ КІБЕРЗАГРОЗ В УМОВАХ ЦИФРОВІЗАЦІЇ НАЦІОНАЛЬНОЇ ЕКОНОМІКИ

Спеціальність 051 Економіка
галузь знань: 05 Соціальні та поведінкові науки

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень.
Використання ідей, результатів і текстів інших
авторів мають посилання на відповідне джерело _____ О.С. Кушнерьов

Науковий керівник –
Бойко Антон Олександрович,
доктор економічних наук, професор

Суми – 2023

АНОТАЦІЯ

Кушнерьов О.С. Детермінанти поширення та локалізації кіберзагроз в умовах цифровізації національної економіки. – Рукопис.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 051 Економіка (галузь знань: 05 Соціальні та поведінкові науки). Сумський державний університет Міністерства освіти і науки України, Суми, 2023.

У дисертації наведено теоретичне узагальнення й запропоновано нове вирішення науково-прикладного завдання розвитку науково-методичних засад ідентифікації та локалізації кіберзагроз в умовах цифровізації національної економіки.

Динамічний аналіз кількості наукових публікацій з питань протидії кібершахрайствам та посилення рівня кібербезпеки, реалізований за допомогою інструментарію VOSviewer v.1.6.10 та Scopus Citation Overview tool засвідчив, що середньорічний темп зростання опублікованих наукових статей з цієї проблематики складає 20%. У 2022 році опубліковано 690 наукових публікацій з досліджуваної тематики, що на 88,5% більше порівняно з 2018 роком. Науковці з США, Великобританії та Індії є найбільш активними у дослідженні питання кібербезпеки та кіберзахисту. Результати бібліометричного аналізу засвідчили наявність чотирьох кластерів. За результатами контекстуально-часового аналізу з питань кібершахрайств встановлено, що протягом 2019-2020 років основна увага почала приділятися технологіям та засобам забезпечення кібербезпеки, а починаючи з 2021 року науковий інтерес був зміщений на дослідження кіберфізичних систем, використання технологій штучного інтелекту для протидії кібератакам, вивчення ролі кіберзахисту при впровадженні інтернету речей.

У роботі обґрунтовано трактувати кіберзагрозу як дію наявних та/або потенційно можливих дестабілізуючих факторів й умов навмисного або випадкового порушення безпеки функціонування громадянина, економічних

суб'єктів та держави у кіберпросторі. У роботі проведено змістове розмежування таких понять як «кіберзагроза», «кіберінцидент», «кібератака», «кіберзлочин». Розширено перелік об'єктів кібербезпеки за рахунок інформаційно-комунікаційних засобів фізичних осіб, які використовуються ними для реалізації суспільно та життєвоважливих потреб під час використання кіберпростору.

На основі результатів ретроспективного аналізу тенденцій поширення кіберзагроз визначено ключові драйвери стрімкого нарощення загроз та ризиків у кіберпросторі. Упродовж 2005-2020 років найбільша кількість кібератак (41,8% від загального обсягу) була ініційована злочинцями з Китаю, при цьому 40% з них були направлені на об'єкти критичної інфраструктури у сфері публічного управління та 36% – на об'єкти приватного сектору. Найбільш розповсюдженою формою кібератаки у світі є різні види фішингу, що передбачає викрадення важливої інформації за допомогою електронних листів із застосуванням соціальної інженерії та обману. Щодо України, то у 2022 році офіційно зареєстровано 415 кіберінцидентів, що в 2,8 рази більше порівняно з 2021 роком.

Розроблена методологія для типологізації країн за рівнем участі їх резидентів у здійсненні фінансових кібернетичних шахрайствах, яка передбачає врахування широкого кола індикаторів, що характеризують різні види злочинності та активність кримінальних угруповувань в країні, а також стану корупції, активності на даркнет-ринку, рівня кіберзлочинності та накладення на країну міжнародних санкцій. За результатами використання кластерного аналізу та побудови дерев класифікації обґрунтовано доцільність виокремлення двох груп країн. Для віднесення країни до першої групи необхідними та достатніми є наступні умови: значення змінної «ризик корупції та хабарів» має приймати значення більше 56,500 одиниць, значення змінної «загальний дохід, який отримано на даркнет-ринку» – менше 5,4100 одиниць, значення змінної «міжнародні санкції, які накладені на країну» – менше 0,05 одиниць, значення змінної інтегрального рівня активності

кримінальних угруповувань, яке приймає значення менше 0,504 одиниць, значення змінної інтегрального рівня характеристики різних видів злочинності – не більше 0,590 одиниць. За протилежних умов вищезазначених індикаторів країни віднесено до другої групи.

Удосконалено методичні засади обґрунтування факторів стрімкого поширення кіберзагроз в національній економіці, що відрізняються від існуючих системним поєднанням сигмоїдної моделі із застосуванням методів машинного навчання SVM та групового врахування аргументів Івахненка. На основі аналізу п'ятнадцяти індикаторів, що характеризують ступінь поширення різних видів кібершахрайств (шкідливе програмне забезпечення, програми-здирники, фішинг, атаки на відмову в обслуговуванні) розроблено узагальнюючий індекс кіберзагроз для економічних суб'єктів. За результатами емпіричного дослідження причин стрімкого поширення кібершахрайств у національній економіці встановлено, що основними драйверами зростання кібершахрайства є частка населення, яка користується онлайн банкінгом, рівень навичок в Інтернеті, інтенсивність онлайн діяльності.

Обґрунтовано методичні засади визначення кібервразливості економічних суб'єктів шляхом інтегрального врахування наступних показників: поінформованість про ознаки підозрілих кібершахрайств, способи кіберзахисту та канали інформування про кібератаки на основі системного поєднання методів головних компонент, узагальненого знижуючого градієнту та мультиплікативної згортки Кіні. Апробація запропонованого методичного підходу засвідчила, що рівень кібервразливості споживачів фінансових послуг у країнах Європи становить у середньому 11%, що дозволяє стверджувати про усвідомленість населенням європейський країн наявних загроз у віртуальному просторі, способів захисту від кіберзлочинності. Проте рівень кібервразливості споживачів фінансових послуг у розрізі країн ЄС не є однорідним, а саме найменшим ризик стати жертвою кібершахрайства мають громадяни таких країн як Данія, Нідерланди, Швеція. До країн з найвищими значеннями розрахованого рівня кібервразливості споживачів фінансових

послуг (18%) належать: Іспанія, Італія, Румунія. Отже, запропонований підхід дозволив сформувати рейтинг країн Європи за рівнем кібервразливості економічних агентів та визначити пріоритети й бенчмарки реалізації державної політики щодо захисту даних громадян у віртуальному просторі.

Набув подальшого вдосконалення методичний підхід до оцінювання та прогнозування ризику кібершахрайств у сфері фінансових послуг, що відрізняються від існуючих врахуванням закономірностей фінансових шахрайських транзакцій, ідентифікованих на основі побудови нейромережевої моделі. 54.2% власників банківських карток, за допомогою яких здійснювалися шахрайські транзакції, були жінки. Середній вік держателів банківських карток, які здійснювали шахрайські фінансові транзакції, становив 50 років. Проаналізувавши призначення підозрілих фінансових транзакцій, встановлено, що в основному вони спрямовані на придбання продуктів харчування та/або товарів. Для вчасної ідентифікації ризику шахрайства з банківськими платіжними картками проведено навчання нейронної мережі на основі тестової вибірки. Це дозволило розробити методичний базис для удосконалення системи протидії дестабілізації роботи інформаційних систем фінансових установ, запровадити систему попереджувальних заходів для скорочення кількості та частоти здійснення шахрайських платіжних операцій, а також захисту персональних даних споживачів фінансових послуг.

Удосконалено сценарний підхід до обґрунтування поведінки економічних агентів в умовах цифровізації національної економіки щодо забезпечення їх стійкості до зовнішніх та внутрішніх загроз шляхом ідентифікації критичних точок у ланцюзі «діджиталізація фінансового сектору-технологічний розвиток-кіберзагрози» шляхом системного застосування методу головних компонент та мультиплікативної згортки Кіні. За результатами дослідження встановлено, що 2019 рік був найбільш ризиковим для економічних агентів, оскільки прослідковувався недостатній рівень забезпечення діджиталізації фінансового сектора, існував

технологічний розвив. Проте вчасно ухвалені рішення економічних агентів у 2019 році щодо модернізацію технологічного забезпечення, інвестування коштів у кібербезпеку призвели до покращення системи протидії внутрішнім та зовнішнім шоками у національній економіці.

Удосконалено науково-методичний підхід до моделювання часових закономірностей впливу кібершахрайств на рівень довіри клієнтів до фінансових установ на основі аналізу популярності пошукових запитів користувачів в Google з використанням поліноміальної моделі розподіленого лагу Алмона. За результатами дискретного лагового моделювання підтверджено, що між кібервіктимізацією споживачів фінансових послуг та довірою до фінансових установ існує статистично значимий зв'язок з лаговою затримкою, а саме в Німеччині, США, Україна – один місяць, Польщі – три місяці. Отримані дані засвідчують, що ефект від фінансових кібершахрайств на зміну поведінкових патернів споживачів фінансових послуг присутній та наступає у короткостроковій перспективі.

З метою ефективної протидії кіберзагрозам і забезпечення стійкості фінансової системи доцільно прийняти комплекс заходів, направлених на моніторинг складових інформаційної безпеки фінансових установ, об'єднання зусиль національного регулятора та керівників фінансових установ щодо інформування про реальні та потенційні кібератаки, а також створення якісних компетенцій в сфері інформаційної безпеки шляхом підвищення кваліфікації працівників фінансових установ та національного регулятора.

Ключові слова: кіберзагрози, кіберстійкість, кіберризик, діджиталізація, безпека, стабільність, фінансові установи, платіжні технології, фінансовий моніторинг, фінансові інновації, цифровізація, національна економіка.

SUMMARY

Kushnerov O.S. Determinants of the spread and localization of cyber threats in terms of the national economy digitalization. – Manuscript.

Dissertation for obtaining the scientific degree of Doctor of Philosophy in 051 Economics (field of knowledge: 05 Social and Behavioural Sciences). Sumy State University of the Ministry of Education and Science of Ukraine, Sumy, 2023.

The dissertation provides a theoretical generalization and offers a new solution to the scientific and applied task of developing the scientific and methodological foundations of identification and localization of cyber threats in terms of digitalization of the national economy. A dynamic analysis of the number of scientific publications on countering cyber fraud and strengthening the level of cyber security, implemented using the VOSviewer v.1.6.10 toolkit and the Scopus Citation Overview tool, showed that the average annual growth rate of published scientific articles on this issue is 20%. In 2022, 690 scientific publications on the subject under study were published, which is 88.5% more than in 2018. Scientists from the USA, Great Britain and India are the most active in researching the issue of cyber security and cyber defence. The results of the bibliometric analysis proved the existence of four clusters. According to the results of a contextual and temporal analysis of cyber fraud issues, it was established that during 2019-2020, the main attention began to be paid to technologies and means of ensuring cyber security. Starting from 2021, scientific interest was shifted to the study of cyber-physical systems, the use of artificial intelligence technologies to counter cyber-attacks, as well as the study the role of cyber protection in the implementation of the Internet of Things.

It is justified in the study to interpret the cyber threat as the effect of existing and/or potentially possible destabilizing factors and conditions of intentional or accidental violation of the security of the functioning of the citizen, economic entities, and the state in cyberspace. A meaningful distinction of such concepts as “cyber threat”", “cyber incident”, “cyber-attack”, “cybercrime” is made. The list of

cyber security objects has been expanded due to the information and communication means of individuals, which are used by them to realize socially and vitally important needs when using cyberspace. Based on the results of a retrospective analysis of the trends in the spread of cyber threats, the key drivers of the rapid increase in threats and risks in cyberspace have been identified. During 2005-2020, the largest number of cyberattacks (41.8% of the total volume) was initiated by criminals from China, while 40% of them were directed to objects of critical infrastructure in the field of public administration, and 36% to objects of the private sector. The most widespread form of cyberattack in the world is various types of phishing, which involves the theft of important information with the help of e-mails using social engineering and deception. As for Ukraine, 415 cyber incidents were officially registered in 2022, which is 2.8 times more than in 2021.

A methodology has been developed for the typology of countries according to the level of participation of their residents in financial cyber fraud, taking into account a wide range of indicators characterizing various types of crime and the activity of criminal groups in the country, as well as the state of corruption, activity on the dark net market, the level of cybercrime and the imposition to the country of international sanctions. Based on the results of the use of cluster analysis and the construction of classification trees, the expediency of separating two groups of countries is substantiated. The following conditions are necessary and sufficient to assign a country to the first group: the value of the variable “risk of corruption and bribes” should be greater than 56,500 units, the value of the variable “total income received on the dark net market” should be less than 5,4100 units, the value of the variable “international sanctions imposed on the country” should be less than 0,05 units, the value of the variable of the integral level of the criminal groups activity, which takes a value of less than 0.504 units, the value of the variable of the integral level of the characteristics of various types of crime should be no more than 0.590 units. Under the opposite conditions of the above-mentioned indicators, the country is assigned to the second group.

Methodological principles for substantiating the factors of the rapid spread of cyber threats in the national economy have been improved, which differ from the existing ones by a systematic combination of the sigmoid model with the use of SVM machine learning methods and group consideration of Ivakhnenko's arguments. Based on the analysis of fifteen indicators characterizing the degree of spread of various types of cyber fraud (malware, ransomware, phishing, denial-of-service attacks), a generalizing index of cyber threats for economic entities was developed. According to the results of an empirical study of the reasons for the rapid spread of cyber fraud in the national economy, it was established that the main drivers of the growth of cyber fraud are the share of the population that uses online banking, the level of Internet skills, and the intensity of online activity.

Methodological principles for determining the cyber vulnerability of economic entities are substantiated by integrally taking into account the following indicators: awareness of the signs of suspicious cyber fraud, methods of cyber protection and channels for informing about cyber-attacks based on a systematic combination of the methods of principal components, the generalized decreasing gradient and the multiplicative Keene convolution. Approbation of the proposed methodological approach proved that the level of cyber vulnerability of consumers of financial services in European countries is on average 11%, which allows us to assert that the population of European countries is aware of existing threats in virtual space, ways to protect against cybercrime. However, the level of cyber vulnerability of consumers of financial services across EU countries is not homogeneous, namely citizens of countries such as Denmark, the Netherlands, and Sweden have the lowest risk of becoming a victim of cyber fraud. The countries with the highest values of the calculated level of cyber vulnerability of financial services consumers (18%) include: Spain, Italy, Romania. Therefore, the proposed approach made it possible to form a rating of European countries according to the level of cyber vulnerability of economic agents and to determine priorities and benchmarks for the implementation of state policy regarding the protection of citizens' data in virtual space.

The methodical approach to assessing and predicting the risk of cyber fraud in the financial services sector, which differs from the existing ones by taking into account the patterns of fraudulent financial transactions identified on the basis of the construction of a neural network model, has been further improved. 54.2% of the owners of bank cards, with the help of which fraudulent transactions were carried out, were women. The average age of bank card holders who made fraudulent financial transactions was 50 years. After analysing the destination of suspicious financial transactions, it was established that they are mainly aimed at purchasing food and/or goods. For the timely identification of the risk of fraud with bank payment cards, neural network training was carried out on the basis of a test sample. This made it possible to develop a methodical basis for improving the system for countering the destabilization of information systems of financial institutions, to introduce a system of preventive measures to reduce the number and frequency of fraudulent payment transactions, as well as to protect personal data of consumers of financial services.

The scenario approach to justifying the behaviour of economic agents in the conditions of digitalization of the national economy to ensure their resistance to external and internal threats has been improved by identifying critical points in the chain “digitalization of the financial sector-technological development-cyber threats” through the systematic application of the method of principal components and the multiplicative Keene convolution. According to the results of the study, it was established that 2019 was the riskiest year for economic agents, since the insufficient level of ensuring the digitization of the financial sector was monitored, and there was technological gap. However, the timely decisions of economic agents in 2019 regarding the modernization of technological support, investing funds in cyber security led to the improvement of the system of countering internal and external shocks in the national economy.

The scientific-methodical approach to modelling the temporal patterns of the impact of cyber fraud on the level of trust of customers in financial institutions has been improved based on the analysis of the popularity of users’ search queries in

Google using Almon's distributed lag polynomial model. According to the results of discrete lag modelling, it was confirmed that there is a statistically significant relationship between cyber victimization of consumers of financial services and trust in financial institutions with a lag, namely in Germany, the USA, Ukraine – one month, Poland – three months. The obtained data prove that the effect of financial cyber fraud on changing the behavioural patterns of consumers of financial services is present and occurring in the short term.

In order to effectively counter cyber threats and ensure the stability of the financial system, it is advisable to adopt a set of measures aimed at monitoring the components of information security of financial institutions, combining the efforts of the national regulator and managers of financial institutions to inform about real and potential cyber-attacks, as well as creating high-quality competences in the field of information security by improving the qualifications of employees of financial institutions and the national regulator.

Keywords: cyber threats, cyber resilience, cyber risk, digitalization, security, stability, financial institutions, payment technologies, financial monitoring, financial innovations, national economy.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ

Монографії

1. Доценко Т. В., Кушнерьов О. С. Використання гравітаційного моделювання при оцінюванні ризику використання банків з метою легалізації доходів, отриманих злочинним шляхом. *Теорія та практика забезпечення розвитку кіберпростору України* : монографія / за ред. О .В. Кузьменко, Г. М. Яровенко. Київ: Інтерсервіс, 2020. С. 110-131. (0,4 друк. арк.). *Особистий внесок: в обґрунтуванні необхідності удосконалення методичних підходів до ідентифікації ризику використання фінансових установ в протиправній діяльності (0,2 друк. арк.).*

2. Доценко Т. В., Кушнерьов О. С. Моделювання інтегрального індексу загрози національної економіки за допомогою метода Кернела. *Теорія та практика забезпечення розвитку кіберпростору України:* монографія / за ред. О .В. Кузьменко, Г. М. Яровенко. Київ: Інтерсервіс, 2020. С. 157-172. (0,3 друк. арк.). *Особистий внесок: у визначенні індикаторів для оцінювання рівня загроз для стабільного функціонування національної економіки (0,1 друк. арк.).*

Публікації в наукових фахових виданнях України

3. Золковер А. О., Кузьменко О. В., Кушнерьов О. С., Койбічук В. В. Бібліометричний аналіз досліджень кіберзлочинності в умовах цифровізації фінансового сектору економіки держави. *Вісник Хмельницького національного університету*. 2019. № 6, Том 2. С. 253-259. DOI: https://doi.org/10.31891/2307-5740-2019-276-6(2)-253-259 (0,4 друк. арк.). *Особистий внесок: у проведенні бібліометричного аналізу наукових публікацій, присвячених дослідженню кіберзлочинності в умовах цифровізації економіи (0,2 друк. арк.).*

4. Бойко А. О., Миненко С. В., Кушнерьов О. С., Хмелик О.С. Створення управлінських інформаційних систем виявлення фінансових операцій, що підлягають під ознаки внутрішнього фінансового моніторингу. *Вісник Сумського державного університету. Серія Економіка*. 2017. № 4. С. 58-66. DOI: https://doi.org/10.21272/1817-9215.2017.4-08 (0,38 друк. арк.). *Особистий внесок: у розробці алгоритму для виявлення фінансових*

транзакцій, що підпадають під ознаки внутрішнього фінансового моніторингу (0,2 друк. арк.).

5. Боженко В.В., Кушнерьов О.С., Кільдей А.Д. Детермінанти поширення кіберзлочинності у сфері фінансових послуг. *Економічний форум.* 2021. № 4. С. 116-121. DOI: https://doi.org/10.36910/6775-2308-8559-2021-4-16 (0,6 друк. арк.). *Особистий внесок: у визначенні причин стрімкого поширення кібершахрайств у та особливостей їх здійснення (0,4 друк. арк.).*

6. Кузьменко О. В., Доценко Т. В., Кушнерьов О. С. Удосконалення системи фінансового моніторингу: автоматизація процесу верифікації клієнтів банку. *Науковий погляд: економіка та управління*. 2021. № 2. С. 88-95. DOI: https://doi.org/10.32836/2521-666X/2021-72-13 (0,8 друк. арк.). *Особистий внесок: у обґрунтуванні доцільності запровадження автоматизації процесів ідентифікації та верифікації клієнтів при проведенні внутрішнього фінансового моніторингу (0,3 друк. арк.).*

7. Лєонов С. В., Кузьменко О. В., Койбічук В. В., Кушнерьов О. С. Розроблення моделі бізнес-процесу автоматизованого моніторингу фінансових операцій банком для протидії легалізації кримінальних доходів. *Вісник Сумського державного університету. Серія Економіка.* 2021. № 1. С. 9−16. DOI: https://doi.org/10.21272/1817-9215.2021.1-1 (0,4 друк. арк.). *Особистий внесок: у розробці моделі бізнес-процесу автоматизованої системи внутрішнього моніторингу економічних агентів (0,1 друк. арк.).*

8. Лєонов С. В., Кузьмено О. В., Кушнерьов О. С., Люльов О. В., Квілінський О. С. Теоретичні основи формування інформаційної бази дослідження ризику використання фінансових установ України з метою легалізації кримінальних доходів. *Вісник Сумського державного університету. Серія Економіка.*. 2020. С. 104-113. DOI: https://doi.org/10.21272/1817-9215.2020.3-11 (0,42 друк. арк.). *Особистий внесок: у визначенні індикаторів, які характеризують участь фінансових установ в нелегальних фінансових операціях (0,1 друк. арк.).*

9. Кузьменко О. В., Доценко Т. В., Кушнерьов О. С. Оцінювання ризику використання банків з метою легалізації кримінальних доходів на основі гравітаційного моделювання. *Проблеми і перспективи економіки та управління*. 2020. № 1 (21). С. 205-219. DOI: https://doi.org/10.25140/2411-5215-2020-1(21)-205-219 (0,72 друк. арк.). *Особистий внесок: у систематизації існуючих підходів у науковій літературі до оцінювання ризику шахрайств (0,4 друк. арк.).*

10. Кушнерьов О. С. Тенденції шахрайських операцій на банківському ринку та можливості протидії. *Інноваційна економіка*. 2019. № 3-4. С. 180–188 (0,6 друк. арк.).

Публікації в зарубіжних виданнях

11. Kuzmenko O.V., Kubálek J., Bozhenko V.V., Kushneryov O.S., Vida I. An approach to managing innovation to protect financial sector against cybercrime Podejście do zarządzania innowacjami w celu ochrony sektora finansowego przed cyberprzestępczością. *Polish Journal of Management Studies*. 2021.№ 24. С. 276-291. DOI: https://doi.org/10.17512/pjms.2021.24.2.17 (1,0 друк. арк.). *Особистий внесок: у розробці науково-методичного підходу до визначення детермінаниів поширення кіберзагроз (0,7 друк. арк.).*

12. Kuzmenko O., Krukhmal O., Koibichuk V., Hrytsenko K., Kushneryov O., Hordiienko V., Pasemko G., Taran O., Smihunova O. Survival Analysis Methods for Assessing the Anti-Money Laundering System Effectiveness. *WSEAS Transactions on Business and Economics*. 2023. 20. P. 1185–1206. DOI: https://doi.org/10.37394/23207.2023.20.106 (1,5 друк. арк.). *Особистий внесок: в обґрунтуванні концепції оцінювання ефективності системи протидії легалізації кримінальних доходів (0,8 друк. арк.).*

Тези доповідей на наукових конференціях

13. Доценко Т. В., Миненко С. В., Кушнерьов О. С. Сплайн-моделювання взаємозалежності кібершахрайств, фінансових правопорушень

та легалізації кримінальних доходів України // Менеджмент, аудит та фінанси: стан, проблеми та перспективи розвитку : збірник тез наукових робіт учасників Міжнародної науково-практичної конференції для студентів, аспірантів та молодих учених, м. Київ, 24 квітня 2021 р. Київ: Аналітичний центр «Нова Економіка», 2021. С. 80-85. (0,2 друк. арк.). *Особистий внесок: в обґрунтуванні та аналізі індикаторів, що характеризують кібершахрайства (0,1 друк. арк.).*

14. Кушнерьов О. С., Радько В. В. Організаційні аспекти кібербезпеки платіжних систем у електронній комерційній діяльності. *Priority directions of science and technology development*: збірник тез доповідей V Міжнародної науково-практичної конференції (24-26 січня 2021 р.). С. 1476–1480. (0,14 друк. арк.). *Особистий внесок: у визначенні основних принципів забезпечення захисту інформації в електронних платіжних системах (0,07 друк. арк.).*

15. Лєонов С. В., Васильєва Т. А., Кузьменко О. В. Кушнерьов О. С., Скринька Л. О. Проблеми формування інформаційної бази оцінювання ризику легалізації кримінальних доходів в сучасних умовах розвитку фінансової системи України. *Проблеми та перспективи розвитку фінансово-кредитної системи України: збірник тез доповідей V Всеукраїнської науково-практичної on-line конференції*. Суми: Сумський державний університет, 2020. С. 260-265. (0,30 друк. арк.). *Особистий внесок: у визначенні особливостей формування інформаційної бази для оцінювання ризику фінансових шахрайств (0,05 друк. арк.).*

16. Кушнерьов О. С., Яценко В. В. Аналіз тенденцій проведення шахрайських операцій з транзакціями на банківському ринку України. *Проблеми та перспективи розвитку фінансово-кредитної системи України: збірник тез доповідей V Всеукраїнської науково-практичної on-line конференції.* Суми: Сумський державний університет, 2019. С. 156-160. (0,3 друк. арк.). *Особистий внесок: у дослідженні поточних тенденцій шахрайства у банківській сфері (0,15 друк. арк.).*

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Перехід людства до якісно нового етапу інноваційної економіки – Індустрії 4.0 супроводжується структурною перебудовою соціально-економічних відносин у країні. Проникнення цифрових технологій, автоматизація і використання технологій штучного інтелекту й машинного навчання, акумулювання великих даних, поширення Інтернету речей з однієї сторони відкривають нові можливості для інтенсивного розвитку держави, а з іншого – підвищують вразливість національної економіки перед зовнішніми викликами і загрозами цифрових трансформацій. Масова імплементація технологій у промислове виробництво та в організацію бізнес-процесів формує потенційну вразливість інформаційних систем до технологічних збоїв та кіберзагроз. За даними звітів Allianz Risk Barometer у 2022 та 2023 роках кіберінциденти є головними бізнес-ризиками у світі [56]. Економічні суб'єкти щоденно стикаються з численними кіберзагрозами, що походять як із зовнішніх, так і з внутрішніх джерел. Світова статистика засвідчує, що 64% компаній наражалися на спроби веб-атак, 62% – зазнавали атак фішингу та соціальної інженерії, 59% – стикалися зі шкідливим програмним забезпеченням і ботнетами, 51% – протистояли атакам типу «відмова в обслуговуванні». Застаріле програмне забезпечення, низький рівень цифрової гігієни працівників, недостатній рівень інвестицій у систему кіберзахисту корпоративних інформаційних систем та інші види вразливостей можуть призвести до значних матеріальних збитків, неавторизованого доступу до конфіденційної інформації, компрометації даних, репутаційних втрат тощо.

Виходячи з цього, у сучасних умовах забезпечення стійкості об'єктів критичної інфраструктури до кіберзагроз та підвищення культури безпекового поводження громадян в кіберпросторі є одним із ключових питань державної політики для регуляторних і наглядових органів.

Питанням запровадження ефективних механізмів протидії кіберзагрозам та підвищення рівня кібербезпеки на національному та корпоративному присвячено наукові праці вітчизняних і зарубіжних вчених: А. Ахмад, С. Маднік, Д. Бюрелл, С. Танг, Я. Мірковіч, П. Целеда, Я.Викопал, Х. Джаханхані, Дж. Хрістов, Г. Макгроу, Х. Шахріар, К. Ренауд, С. Кріс, Н. Кшетрі, Т. Хольт, М. Алазаб, І. Школьник, В. Маргасова, А.Бойко, В.Боженко, Г.Яровенко, О. Кузьменко, Ю. Кіндзерський, О. Пахненко, Н. Демчишак, С. Гончар, О. Ткаченко, І. Яковів, О.Трофименко, В.Биков, О. Буров, Ю. Хлапонін, М.Ковалів, Р.Скриньковський, О. Добржанська, В. Пядишев, В.Ємельянов, Г. Бондар.

Однак, ураховуючи існуючі наукові напрацювання провідних вітчизняних і зарубіжних учених із питань національної та корпоративної кібербезпеки, остаточно не вирішеною залишається низка теоретичних і прикладних проблем, що стосуються, зокрема, визначення детермінантів стрімкого поширення кіберзагроз а економіці, оцінювання рівня кібервразливості економічних суб'єктів, типологізації країн за рівнем участі їх резидентів у здійсненні кібернетичних та фінансових кібершахрайств, визначення критичних зон кіберзагроз для фінансового сектора економіки, визначення наявності зв'язку між фінансовими шахрайствами та довірою громадян до фінансового сектора, розробка комплексу заходів для швидкого реагування на кіберзагрози та удосконалення системи протидії їм. Усе вищезазначене обумовило актуальність дослідження, його мету, завдання і зміст.

Зв'язок роботи з науковими програмами, планами, темами. Тематика дисертаційної роботи узгоджується з програмою Європейського Союзу «Цифрове десятиліття до 2030 року» (рішення ЄС 2022/2481 від 14.12.2022 р.), програми ЄС з інформаційно-комунікаційних технологій («Цифровий компас» COM(2021)00118 від 09.03.2021 р. та «Цифрова Європа» (DIGITAL) від 02.06.2021 р.), Стратегією національної безпеки України (Указ Президента України № 392/2020 від 14.09.2020 р.), Стратегією кібербезпеки

України (Указ Президента України № 447/2021 від 14.05.2021 р.), Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури (постанова Кабінету Міністрів України № 518 від 19.06.2019 р.), Доктриною інформаційної безпеки України (Указ Президента України № 47/2017 від 25.02.2017 р.) тощо.

Основні положення дисертаційного дослідження узгоджуються з пріоритетними напрямками науково-дослідної роботи Сумського державного університету. У рамках науково-дослідної роботи «Data-Mining для протидії кібершахрайствам та легалізації кримінальних доходів в умовах цифровізації фінансового сектору економіки України» (номер д/р 0121U100467) визначено детермінанти поширення кібершахрайств та незаконних фінансових операцій, оцінено рівень кібервазливості економічних суб'єктів, розроблено методологію для типологізації країн за рівнем участі їх резидентів у здійсненні кібернетичних та фінансових шахрайств.

У межах науково-дослідної роботи «Моделювання механізмів детінізації та декорумпізації економіки для забезпечення національної безпеки: вплив трансформації фінансових поведінкових патернів» (номер д/р 0122U000783) оцінено вплив рівня цифровізації ринку фінансових послуг на ступінь поширення кіберзагроз.

У рамках науково-дослідної роботи «Національна безпека України через запобігання фінансовим шахрайствам та легалізації брудних грошей: воєнні та післявоєнні виклики» (номер д/р 0123U101945) проведено бібліографічний аналіз наукового доробку у сфері протидії кібершахрайствам.

У межах НДР «Фрактальна модель трансформації фондового ринку України: соціально-відповідальне інвестування для досягнення Цілей сталого розвитку» (номер д/р 0121U100473) запропоновано механізми удосконалення системи протидії кіберзагрозам в Україні в умовах цифрової трансформації національної економіки.

Мета і завдання дослідження. Мета дисертаційної полягає у розвитку існуючих та формуванні нових науково-методичних підходів до ідентифікації

кіберзагроз та пошуку методів їх локалізації в контексті цифрової трансформації економіки.

Для досягнення поставленої мети визначено наступні завдання:

− провести декомпозиційний аналіз змістовних аспектів кіберзагроз в системі економічних відносин;

− проаналізувати основні тенденції поширення кіберзагроз в Україні та світі;

− розробити методику для типологізації країн за рівнем участі їх резидентів у здійсненні кібернетичних та фінансових шахрайств;

− формалізувати основні передумови поширення кіберзагроз у національній економіці;

− оцінити рівень вразливості економічних суб'єктів у кіберпросторі;

− розробити методичний підхід д оцінювання ризику фінансових шахрайств;

− ідентифікувати критичні зони кіберзагроз для фінансового сектору економіки;

− проаналізувати наявність причинно-наслідкових зв'язків між рівнем кібершахрайств та довірою до фінансового сектору економіки;

− розробити шляхи удосконалення системи протидії кібершахрайствам.

Об'єктом дослідження є економічні відносини, що виникають між органами публічного управління, суб'єктами господарювання та громадянами в процесі запобігання, виявлення та усунення наслідків кіберінцидентів.

Предметом дослідження є теоретико-методичні засади та методичний інструментарій поширення та локалізації кіберзагроз в умовах цифровізації національної економіки.

Методи дослідження. Методологічну основу дисертаційної роботи складають фундаментальні положення економічної теорії, макро- і мікроекономіки, теорії фінансів та кредиту, теорії державного регулювання

економіки, економіко-математичного моделювання, наукові публікації з питань кібербезпеки та управління національною економікою.

Для вирішення поставлених завдань використано комплекс загальнонаукових і спеціальних методів дослідження: наукової абстракції, аналізу, синтезу, індукції, дедукції, узагальнення – для уточнення понятійно-категоріального апарату дослідження; комплексне поєднання бібліометричного та трендового аналізів – для дослідження змістовно-контекстуальних та еволюційно-просторових закономірностей публікаційної активності у сфері кібербезпеки; методи попарного порівняльного та статистичного аналізів – для характеристики поточного стану та тенденцій закономірностей розвитку кібершахрайств в Україні та світі; методи формально-логічного аналізу – для визначення основних передумов поширення кіберзагроз в економічній системі; кластерний, дисперсіний аналізи та дерева класифікації – при проведенні типологізації країн за рівнем участі їх резидентів у здійсненні кібернетичних та фінансових шахрайств; метод групового врахування аргументів Івахненка – при розрахунку інтегрального індексу кіберзагроз; метод опорних векторів – при формалізації ключових детермінантів активізації кіберзагроз; поєднання методів головних компонент та узагальненого знижуючого градієнту –при визначенні рівня кібервразливості економічних суб'єктів; нейромережева модель – при розрахунку ризику фінансових кібершахрайств; трансформована мультиплікативна згортка Кіні – при визначенні інтегральних показників для характеристики діджиталізації фінансового сектору, технологічного розвитку та ризику кіберзагроз; поліноміальна модель розподіленого лагу Алмона – при оцінюванні впливу фінансових та кібернетичних злочинів на рівень довіри до фінансового сектору. Практичні розрахунки та моделювання в дисертаційній роботі здійснено з використанням VOSviewer v. 1.6.10, Scopus Citation Overview tool, Google Trends, STATISTICA 12, EViews.

Інформаційну базу дослідження склали: закони України, міжнародні нормативно-правові акти, нормативно-правова база профільних міністерств та

відомств, звітно-аналітична інформація Державної служби статистики України; дані Міжнародного валютного фонду, Світового банку, Організації економічного співробітництва та розвитку, Євробарометр, результати наукових досліджень у сфері кібербезпеки та кіберзахисту.

Наукова новизна одержаних результатів полягає у розвитку існуючого та розробленні нового методичного інструментарію для запобігання та протидії кіберзагрозам у контексті цифровізації національної економіки:

вперше:

– розроблено методичні засади визначення кібервразливості економічних агентів шляхом інтегрального врахування показників щодо проінформованості про ознаки підозрілих кібершахрайств, способи кіберзахисту та канали інформування про кібератаки на основі системного поєднання методів головних компонент, узагальненого знижуючого градієнту та мультиплікативної згортки Кіні. Це дозволило сформувати рейтинг країн Європи за рівнем кібервразливості економічних суб'єктів та визначити пріоритети й бенчмарки реалізації державної політики щодо захисту даних громадян у віртуальному просторі.

удосконалено:

– науково-методичний підхід до моделювання часових закономірностей впливу кібершахрайств (тестування на наявність лагу до 12 місяців) на рівень довіри клієнтів до фінансових установ на основі аналізу популярності пошукових запитів користувачів в Google з використанням поліноміальної моделі розподіленого лагу Алмона. Це дозволило кількісно оцінити зміну поведінкових патернів споживачів фінансових послуг під впливом рівня їх віктимізації у кіберпросторі на різних часових горизонтах.

– сценарний підхід до обґрунтування поведінки економічних агентів в умовах цифровізації національної економіки щодо забезпечення їх стійкості до зовнішніх та внутрішніх загроз шляхом ідентифікації критичних точок у ланцюзі «діджиталізація фінансового сектору - технологічний розвиток -

кіберзагрози», що на відміну від існуючих, ґрунтуються на застосуванні методу головних компонент та мультиплікативної згортки Кіні. Це дозволило сформувати комплекс превентивних заходів для протидії негативним інформаційним впливам та посилення кіберстійкості економічних агентів.

– науково-методичне підґрунтя визначення рівня участі резидентів країни у здійсненні фінансових та кібернетичних шахрайств, що відрізняється від існуючих поєднанням кластерного аналізу (за допомогою ітеративного дивізівного методу k-середніх) та побудови дерев класифікації з використанням методу одномірного розгалуження CART. Це дозволило визначити список країн, з якими рекомендовано посилити перевірку клієнтів та їх бенефіціарних власників в контексті реалізації превентивних заходів протидії незаконної та сумнівної діяльності.

набули подальшого розвитку:

– методичний підхід до обґрунтування факторів стрімкого поширення кіберзагроз в національній економіці, що відрізняються від існуючих системним поєднанням сигмоїдної моделі із застосуванням методів машинного навчання SVM та групового врахування аргументів Івахненка. Це дозволило окреслити фінансові та соціальні драйвери та інгібітори, коригування яких сприятиме підвищенню стійкості національної економіки до кіберзагроз.

– методологічні засади інтегрального оцінювання та прогнозування ризику кібершахрайств у сфері фінансових послуг, що відрізняються від існуючих врахуванням закономірностей фінансових шахрайських транзакцій, ідентифікованих на основі побудови нейромережевої моделі. Це дозволить удосконалити систему протидії дестабілізації роботи інформаційних систем фінансових установ, запровадити систему попереджувальних заходів для скорочення кількості та частоти здійснення шахрайських платіжних операцій, а також захисту персональних даних споживачів фінансових послуг.

– теоретичні засади дослідження наукового ландшафту визначення трендів і векторів наукових досліджень з питань протидії кіберзазрозам та

забезпечення кібербезпеки, що відрізняються від існуючих базуються на результатах структуризації наявного дослідницького доробку за допомогою інструментарію VOSviewer v. 1.6.10 та Scopus Citation Overview tool. Це дозволило визначити еволюційно-контекстуальні та часові закономірності трансформації дослідницького інтересу до питань у сфері протидії кіберзагрозам в умовах цифровізації національної економіки.

Практичне значення одержаних результатів полягає в тому, що основні положення дисертації доведено до рівня методичних розробок і практичних рекомендації, що можуть бути використані: − органами державного регулювання: – при розробці програмних, нормативно-правових документів, які спрямовані на посилення кібербезпеки інформаційної інфраструктури та кіберзахисту інформаційних ресурсів, а також запобігання, виявлення та усунення наслідків кіберінцидентів щодо економічних суб'єктів; – профільними міжнародними інституціями – для обміну технологіями, знаннями та іншими здобутками у сфері кіберзахисту; суб'єктами господарювання – під час розроблення корпоративних політик забезпечення інформаційної безпеки; громадянами – при виборі ефективних інструментів захисту персональної інформації.

Результати дисертації використані вченими Сумського державного університету під час підготовки та викладання дисциплін «Програмне забезпечення математичного та статистичного аналізу» та «Прикладна статистика».

Особистий внесок здобувачки. Дисертаційна робота є самостійно виконаною науковою працею, в якій автором розроблено низку нових, а також поглиблено існуючі науково-методичні засади дослідження детермінантів поширення та протидії кіберзагрозам в умовах цифровізації національної економіки. Наукові положення, висновки та рекомендації, що виносяться на захист, одержані автором самостійно. Особистий внесок у працях, опублікованих у співавторстві, зазначено у списку публікацій.

Апробація результатів дисертації. Основні положення дисертаційної роботи апробовані на наукових та науково-практичних конференціях різних рівнів, зокрема: Міжнародна науково-практична конференція «Менеджмент, аудит та фінанси: стан, проблеми та перспективи розвитку» (м. Київ, Україна, 2021 р.), Міжнародній науково-практичній конференції «Priority directions of science and technology development» (м. Київ, Україна, 2021 р.), Всеукраїнської науково-практичної on-line конференції Проблеми та перспективи розвитку фінансово-кредитної системи України (м. Суми, Україна, 2019, 2020 рр.).

Публікації. Основні результати дисертаційної роботи опубліковано в 16 наукових працях, загальним обсягом 8,46 друк. арк., із яких особисто авторці належить 4,47 друк арк., зокрема 2 підрозділи у колективній монографії, 8 статей у наукових фахових виданнях України, 1 статі у виданнях, що індексується міжнародною наукометричною базою Scopus, 4 публікації у збірниках матеріалів конференцій.

Структура та обсяг дисертації. Дисертація складається з вступу, трьох основних розділів, списку використаних джерел. Повний обсяг дисертації становить 205 сторінок, зокрема обсяг основного тексту – 159 сторінок, 27 таблиць, 51 рисунок, 5 додатків, список використаних джерел містить 159 найменувань.

РОЗДІЛ 1 ТЕОРЕТИЧНІ ЗАСАДИ ВИЗНАЧЕННЯ ЗМІСТУ КІБЕРЗАГРОЗ ТА ТЕНДЕНЦІЇ ЇХ ПОШИРЕННЯ

1.1. Декомпозиційний аналіз змістовних аспектів кіберзагроз в системі економічних відносин

Швидкі темпи цифровізації економічних відносин, автоматизація бізнес-процесів, перехід на електронне урядування ставить нові виклики безпеки у кіберпросторі перед урядами багатьох країн. Анонімність, невизначеність географічної зони здійснення кіберзлочину, постійне удосконалення способів здійснення кібератак відрізняє кіберзагрози від традиційних загроз стабільного функціонування національної економіки.

На сьогодні протидія кіберзагрозам є однією із головних тем для обговорення на міжнародних економічних форумах і конференціях, дана проблематика широко висвітлена у працях зарубіжних та вітчизняних науковців. Кібершахрайство представляє загрозу економічній безпеці будь-якої країни, вона набуває глобального характеру, оскільки різні способи кібератак доволі часто мають транскордонний характер. Саме тому розвиток сучасної економічної науки неможливий в межах ізольованої території окремої країни. Виходячи з цього, джерелом даних про наукові публікації для проведення бібліометричного аналізу виступила міжнародна наукометрична база даних Scopus.

Для пошуку публікацій у сфері кіберзахисту та кібербезпеки у контексті розвитку національної економіки обрано декілька ключових слів. Зауважимо, до для бібліографічного аналізу відібрано тільки наукові статті, які опубліковані протягом 2012-2022 років та входять до трьох галузей знань «соціальні науки», «бізнес, управління та облік» та «економіка, економетрика та фінанси». Результати проведеного пошуку наукових публікацій у наукометричній базі Scopus подано в таблиці 1.1.

Таблиця 1.1 – Динаміка наукових публікацій, присвячених вивченню питання кіберзагроз та інших споріднених понять у системі економічних відносин, одиниць

Ключові слова для пошуку	Рік											
	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	ВСЬОГО
1. Cyber AND threat*	29	51	46	60	74	97	123	165	211	235	246	1337
2. Cyber AND attack*	34	71	59	52	83	117	154	196	214	267	306	1553
3. Cyber AND security	64	106	105	125	137	193	267	373	400	472	507	2749
4. Cyber AND crime	53	60	46	55	69	96	108	133	128	152	139	1039
5. Cyber AND threat* OR attack* OR security OR crime	111	164	152	173	211	299	366	491	552	648	690	3857

Джерело: складено автором на основі наукометричної бази Scopus

Дані таблиці 1.1 демонструють, що протягом останніх десяти років науковий інтерес до вивчення питань кіберзагроз постійно та динамічно зростає. Зокрема, близько половини наукових статтей з досліджуваної проблематики опублікована протягом останніх трьох років (2020-2022): напрямок «cyber threat» – 692 публікації або 51,8% від загального обсягу протягом 2012-2022 рр.; напрямок «cyber attack» – 787 публікації або 50,7%; напрямок «cyber security» – 1379 публікації або 50,2%; напрямок «cyber crime» – 419 публікації або 40,3%.

Для уникнення дублювання наукових статей, які будуть використані для подальшого бібліографічного аналізу, пошуковий запит сформульовано наступним чином «Cyber AND threat* OR attack* OR security OR crime». За цим запитом відібрано 3857 науковий публікацій із середньорічним темпом зростання опублікованих наукових статей на рівні 20%. Щодо резиденства наукових авторів, якими найбільше опубліковано статей з цієї проблематики, то це США – 1174 статті (або 30,4% від загального обсягу), Великобританія – 509 статей (або 13,2%), Індія – 282 статті (або 7,3%). Зауважимо, що науковцями з України протягом 2012-2022 років опубліковано 67 статей. Дані цифри наочно демонструють, що протидія кіберзагрозам залишається

пріоритетним для будь-яких країн світу незалежно від рівня економічного її розвитку.

З метою проведення більш ґрунтовного дослідження визначення підходів до виявлення та протидії кіберзагрозам проведено бібліометричний аналіз за допомогою інструментарію VOSViewerv.1.6.10, що дозволяє ідентифікувати взаємозв'язки між об'єктами, проводити кластеризацію і візуалізацію наукометричних даних. Особливістю кластерного бібліографічного аналізу полягає в тому, що чим схожишіми є ключові слова у кластері, тим сильнішим є їх взаємозв'язок і більше науковий статей, в яких зустрічаються дані ключові слова. Об'єктом бібліометричного аналізу обрано 3857 наукові статті у виданнях, що індексуються наукометричною базою даних Scopus, які відповідають одночасному врахуванні в пошуковому запиті таких категорій як «кібер загрози», «кібер атаки», «кібер безпека», «кіберзлочин» за період 2012–2022 рр.

Проаналізувавши ключові слова в анотаціях відібраних наукових статей виявлено значну кількість дублювань понять (наприклад, «cyber-attack», «cyberattack», «cyberattacks», «cyber attack» тощо). Для усунення цієї проблеми було складено спеціальний тезаурус, щоб об'єднати схожі терміни та усунути помилки у ключових словах.

За результатами бібліографічного аналізу було виявлено 14 838 спільних ключових слів, які зустрічаються в анотаціях та назвах наукових статей. Для візуалізації спільного використання ключових слів встановлено порогове значення на рівні 7 повторень, що дозволило відфільтрувати 200 ключових слів. Графічна візуалізація результатів бібліометричного аналізу за допомогою інструментарію VOSviewer представлена на рисунку 1.1.

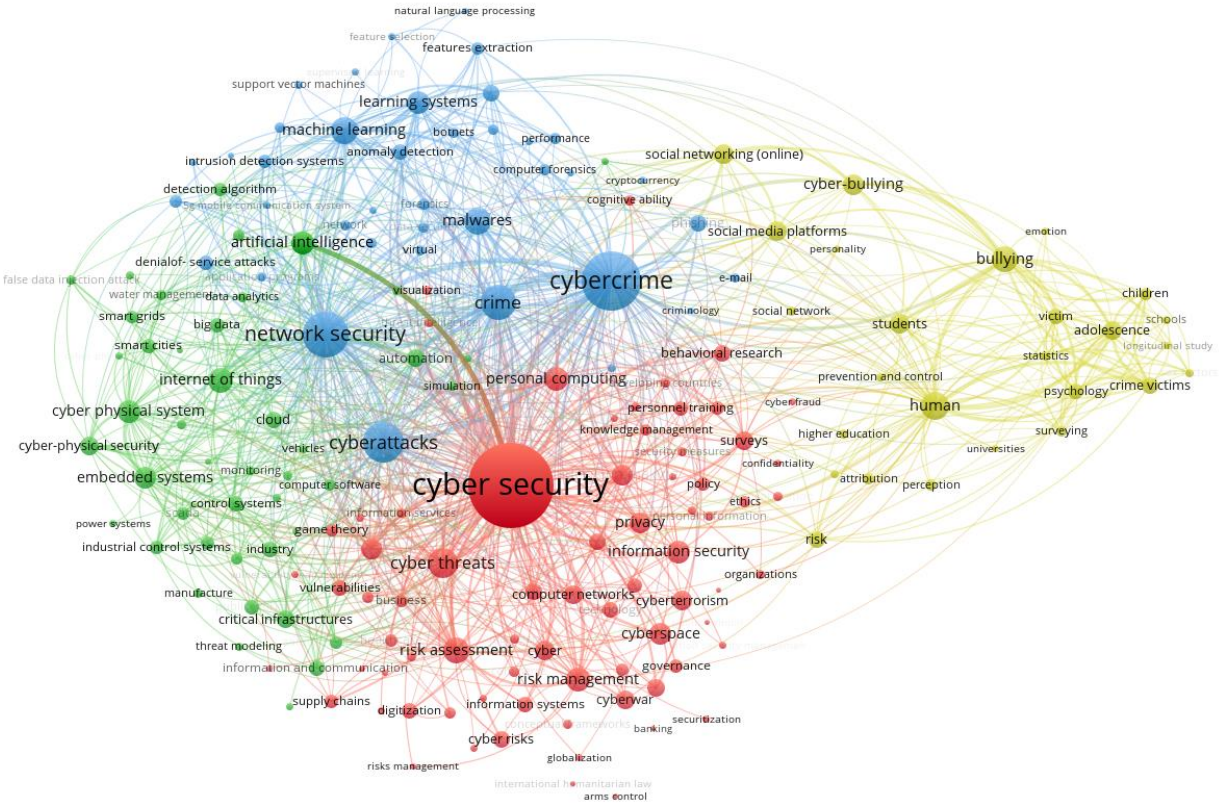


Рисунок 1.1 – Результати бібліометричного аналізу наукових праць з питань кібербезпеки в економічному вимірі у виданнях, що індексуються наукометричною базою даних Scopus

Джерело: складено автором з використанням інструментарію VOSViewerv.1.6.10

За результатами аналізу частоти використання ключових слів з цієї проблематики у наукових статтях виокремлено чотири кластери:

Науковий кластер 1 (червоний колір) присвячений вивченню кібербезпеки та складові її забезпечення (74 ключові слова). Основними ключовими словами цього кластеру є: кібер безпека, кібер загрози, компю’ютерні мережі, управління ризиком, інформаційна безпека, управління знаннями, технології, приватність, ланцюги поставок, діджиталізація тощо.

Науковий кластер 2 (синій колір) сфокусований на дослідженні та пошуку засобів та технологій ідентифікації кіберзагроз, а також протидії кібератакам (39 ключових слів). До кластеру включено наукові статті, ключовими словами яких є: кібер атаки, кібер злочин, машинне навчання,

нейронні мережі, візуалізація, автоматизація, мережева безпека, кіберкриміналістика, розслідування, виявлення аномалій тощо.

Науковий кластер 3 (зелений колір) має спеціалізацію щодо дослідження об’єктів кіберзахисту, які мають пріоритетне значення в умовах діджиталізації економіки (44 ключових слів). Основними ключовими словами даного кластеру є: кіберфізична система, критична інфраструктура, хмарні технології, виробництво, «розумні» міста, управління водними ресурсами, розумні системи електропостачання, інтернет речей тощо.

Науковий кластер 4 (жовтий колір) присвячений дослідженню впливу кіберзагроз на життєдіяльність людини (26 ключових слів). Ключовими словами даного кластеру є: кібер булінг, підлітковий вік, людина, кібер жертва, психологія, соціальні мережі, емоції, студенти тощо.

Більш детальніше проаналізуємо окремі наукові праці у розрізі кожного з виділених кластерів.

Науковий кластер 1.

Найбільш цитованою працею даного кластеру є стаття Von Solms & Van Niekerk (2013), в якій представлено фундаментальну роль кібербезпеки у суспільстві та її критичні відмінності від інформаційної безпеки [148]. Зокрема, кібербезпека виходить за рамки традиційної інформаційної безпеки, включаючи захист не лише інформаційних ресурсів, а й інших активів, включаючи саму особу.

Однією з найбільш поширених кібератак є фішинг, метою якого є викрадення конфіденційної персональної та фінансової інформації. Науковцями [55] запропоновано модель класифікатора фішингової електронної пошти, яка застосовує алгоритми глибокого навчання з використанням згорткової мережі графів (GCN). Експериментальні тести підтвердили, що класифікатор ідентифікував фішингові листи з точністю 98,2%.

У роботі [54] представлено результати опитуваннння керівників інформаційних служб та служб інформаційної безпеки, що дозволило

виокремити основні виклики, з якими стикаються малі, середні та великі підприємства в галузі фінансових послуг щодо безпеки даних та надання відповідних інструментів і стратегій для їх захисту.

Науковий кластер 2.

На сьогодні активно впроваджують методи машинного навчання у системи захисту інформації та забезпечення кібербезпеки, які дозволяють ефективно вирішувати завдання аналізу, класифікації та прогнозування широкого класу даних. Колектив авторів (Ying та ін., 2018) у своєму тематичному дослідженні довели, що блокчейн здатний захистити конфіденційну інформацію, а також усунути посередництво будь-яких установ [158].

У роботі [57] проаналізовано сфери практичного застосування нейронних мереж та генетичних алгоритмів в системі управління інформаційною безпекою комерційних банків. У роботі [114] побудовано фазові профілі кібершахраїв на основі аналізу моделей їх атак шляхом використання техніки розподільної семантики обробки природної мови. А. Бердюгін та П.Ревенков [62] розробили за допомогою Borland Delphi програмне забезпечення для кількісної оцінки ймовірності ризику кібератак на технології електронного банківського обслуговування.

У роботі [109] обґрунтовано необхідність посилення інформаційної безпеки серед працівників фінансових установ. Yerdon [156] запропоновано використовувати активні індикатори відстеження очей для визначення кібершахраїв з числа працівників великих компаній.

Науковий кластер 3.

Протягом останнього десятиріччя інфраструктура Інтернету речей розвивається стрімкими темпами, що трансформує традиційні системи надання суспільних послуг, організацію бізнес-процесій та побуту населення. Крім можливостей та зручностей, що привносить концепція «інтернет речей» у суспільстві, посилюється питання кіберзахисту цих технологій та пристроїв. У роботі Chen et al (2021) представлено детальний аналіз моделей глибокого

навчання для покращення рівня кіберзахисту на систему «розумного міста», а саме машини Больцмана, обмежені машини Больцмана, мережі глибоких переконань, рекурентні нейронні мережі, згорткові нейронні мережі та генеративні змагальні мережі [73]. Зокрема, Singh et al (2020) запропоновано орієнтовану на IoT інфраструктуру на основі глибокого навчання для безпечного розумного міста, де блокчейн забезпечує розподілене середовище на етапі зв'язку CPS, а програмно-визначена мережа встановлює протоколи для пересилання даних у мережі [136136].

Науковцями С. Твенебоа-Кодуа & С. Тосун [145], М. Аркурі [59] оцінено вплив кібератак на динаміку зміни вартості цін на акції компаній залежно від їх галузевої приналежності. Доведено, що кібератака на фінансові компанії призводить до значної волатильності їх акцій протягом тривалого періоду часу [145].

Науковий кластер 4.

Різке зростання використання соціальних мереж кинуло виклик традиційним суспільним структурам і перемістило значну частину міжособистісного спілкування з фізичного світу в кіберпростір [107]. Найчастішою причиною зараження шкідливим програмним забезпеченням і порушення конфіденційності є соціальні мережі [115].

На думку П. Андреу і С. Аніфантакі [58] одним із факторів стрімкого поширення кіберзагроз є низький рівень цифрової та фінансової грамотності, а також недостатня обізнаність населення про кібератаки та їх потенційні руйнівні наслідки. Зокрема, у роботі [68] визначено набір навичок кібербезпеки не-IT-спеціалістів, які дозволяють зменшити ризики інформаційній безпеці компанії.

Розширюючи дослідження, проаналізуємо контекстуально-часовий блок бібліометричного аналізу (рисунок 1.2). Насиченість кольору на рисунку 1.2 змінюється від темно-синього кольору (ранні публікації) до жовтого кольору (сучасні публікації).

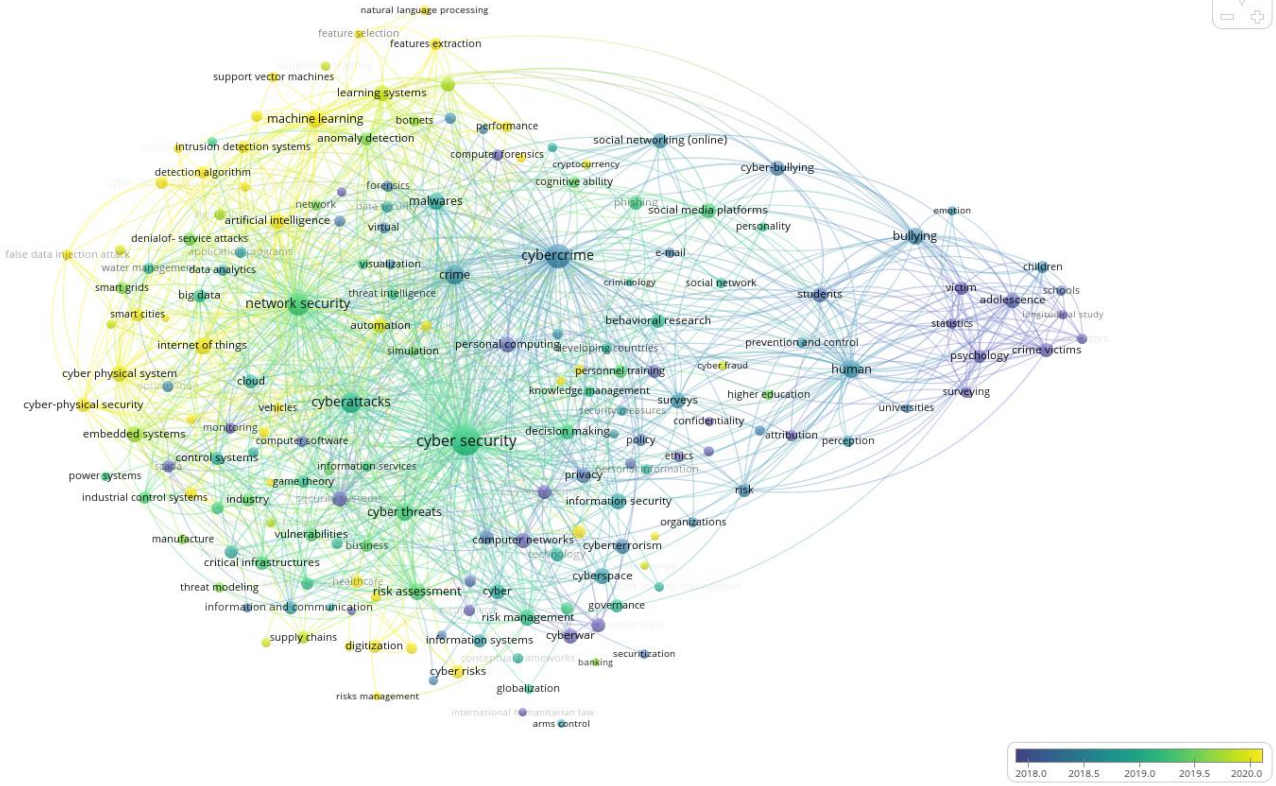


Рисунок 1.2 – Візуалізаційна карта контекстуально-часового виміру досліджень з питань кібербезпеки в контексті економічних відносин

Джерело: складено автором з використанням інструментарію VOSViewerv.1.6.10

Отже, за результатами контекстуально-часового аналізу з питань кібершахрайств встановлено, що протягом 2017-2018 років науковці активно досліджували питання кібербулінгу, кіберзлочинів, персонального захисту в кіберпросторі. У період з 2019 по 2020 роки з розвитком електронних коштів і блокчейну основна увага почала приділятися технологіям та засобам забезпечення кібербезпеки у сучасних реаліях. Починаючи з 2021 року науковий інтерес був зміщений на дослідження кіберфізичних систем, використання технологій штучного інтелекту для протидії кібератакам, вивчення ролі кіберзахисту при реалізації «розумних» технологій для управління електропостачанням, комунальними послугами та транспортною інфраструктурою.

Отже, за результатами обробки бібліографічних даних, їх візуалізації та co-occurrence-аналізу, можемо зробити наступні висновки:

–дослідження в сфері кібербезпеки є мультидисциплінарними та охоплюють широке коло питань технічного, фінансово-економічного, соціального характеру;

–кількість наукових публікацій, присвячених питанням кібербезпеки, динамічно зростає з кожним роком. Нині найбільш актуальними напрямками у даній тематиці є використання технологій штучного інтелекту та машинного навчання для вчасної ідентифікації кіберзагроз та побудови ефективної системи кіберзахисту, а також механізми посилення кіберзахисту розумних технологій в сучасній екосистемі.

–географія локація дослідницьких груп в основному зконцентрована в наукових школах та центрах таких країн як США, Великобританія Індія та Китай;

– забезпечення кіберзахисту відіграє фундаментальну роль стабільного розвитку національної економіки з урахуванням стрімких темпів впровадження цифрованих інновацій та технологій в екосистему.

З метою ефективної реалізації державної політики щодо захисту економічних агентів у кіберпросторі та понесення відповідальності за вчинення протиправних кібернетичних дій доцільно чітко визначити зміст «кіберзагроз» та інших споріднених понять: «кібершахрайство», «інтернет-злочин», «комп'ютерний злочин», «кіберризик», «кіберінцидент», «кіберзлочин», «кіберінцидент», «кібератака» тощо.

Першочергово доцільно проаналізувати зміст цього питання в чинному вітчизняному законодавстві. Основним нормативно-правовим актом, що легітимізує законодавчі дефініції у сфері кіберзахисту є Закон України «Про основні засади забезпечення кібербезпеки України» [44], в якому визначено сутність таких основних понять як «кіберзагроза», «кіберінцидент», «кібератака», «кіберзлочин». Зокрема, «кіберзагроза - наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим

національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів». На нашу думку, зазначене визначення є фрагментарним, та охоплює виключно захист кібербезпеки держави та її об'єктів, при цьому залишаючи поза увагу захист громадян країни. Водночас міжнародними стандартами ISO/IEC TS 27100:2020 визначення «кіберзагроз» є більш загальним, а саме як «потенційні причини небажаного кіберінциденту, який може завдавати збитків системі, людині, суспільству, організації чи іншим суб'єктам у кіберпросторі» [100].

Заслуговує на увагу й визначення «кіберзагроз» у роботі Li & Liu (2023), що трактується як будь-яка подія, що може завдати шкоди національним кіберактивам через інформаційну систему, несанкціонований доступ, знищення, розголошення, зміну інформації та/або перешкоджання наданню послуг [106]. Компанії, які працюють у галузі цифрової безпеки, в основному розглядають кіберзагрозу як зловмисну дію, спрямована на викрадення чи пошкодження даних або порушення цифрового добробуту та стабільності суб'єкта господарювання.

На основі аналізу існуючих підходів до визначення «кіберзагроз», запропонуємо власне трактування цього поняття як «дію наявних та/або потенційно можливих дестабілізуючих факторів та умов навмисного або випадкового порушення безпеки функціонування громадянина, економічних суб'єктів та держави у кіберпросторі». Зауважимо, що кіберзагрози можуть виникати випадково (із-за низької якості аутентифікації сторони, інші слабкі місця в безпеці) або результатом спланованих дій зацікавленої сторони.

Наступною парою понять, які доволі часто ототожнюються у науковій літературі та практичній діяльності – це «кібератака» та «кіберінцидент».

Фахівцями IBM запропоновано трактувати кібератаки як будь-яку навмисну спробу викрасти, викрити, змінити, вивести з ладу або знищити дані, програми чи інші активи шляхом несанкціонованого доступу до мережі, комп'ютерної системи чи цифрового пристрою [151]. У роботі [108] кібератаки розглянуто як дії, що здійснюються країнами з метою проникнення

в комп’ютери чи інформаційні мережі інших країн з метою нанесення шкоди або збою у функціонування їх систем. Фактично дане визначення враховує частину кібератак, які ініційовані урядами інших країн, залишаючи поза увагою інших суттєвих учасників – кіберзловмисники, терористичні групи, хактивісти, перснонал компанії тощо.

Визначення «кібератаки», що представлено в Законі України «Про основні засади забезпечення кібербезпеки України», є змістовним та повним, оскільки у трактуванні даного терміну зазначено інструменти й засоби здійснення кібератак, мету цих протизаконних дій у кіберпросторі та наслідки для держави й суспільства.

Кібератака зазвичай вважається передвісником кіберінциденту. Встановлення факту кіберінциденту відбувається тоді, коли кібератака фактично вплинула на конфіденційність, цілісність або доступність ІТ-системи. Суб’єкти національної системи кібербезпеки, інших державних органів, а також критичної інфраструктур, мають повідомляти про кіберінциденти у встановлений спосіб. Беручи до уваги рекомендації Європейської агенції з кібербезпеки та Європейського центру боротьби з кіберзлочинністю Європолу, урядова команда реагування на комп’ютерні надзвичайні події України, яка функціонує в складі Державної служби спеціального зв’язку та захисту інформації України (CERT-UA), сформувала перелік 10 категорій кіберінцидентів [40].

Наступною групою понять, трактування яких викликає дискусії серед науковців та практиків, є «кіберзлочин» та «комп’ютерний злочин». Зокрема, у Законі України «Про основні засади забезпечення кібербезпеки України» дані поняття ототожнюються та розглядаються як «суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України». Оскільки кіберзлочинність – будь-яке протиправне діяння, пов’язане з використанням як комп’ютерів, так і інформаційно-комунікативних засобів та технологій, тоді

як «комп’ютерна злочинність» належить до правопорушень, де комп’ютер або комп’ютерні дані є основною метою злочинців [12]. І тому, поняття «кіберзлочинність» є більш ширшим порівняно з поняттям «комп’ютерна злочинність».

У Кримінальному Кодексі України зазначено, що правопорушення вважалося злочином, воно повинно містити в собі такі ознаки: кримінальна протиправність, суспільна небезпека, винність, караність [22]. Відповідно до Кримінального Кодексу України можна набути кримінальну відповідальність за:

1) злочини, що вчиняються за допомогою комп’ютерних технологій: порушення авторського права і суміжних прав (ст. 176), шахрайство (ст. 190), незаконні дії з документами на переказ, платіж. картками, банк. рахунками (ст. 200), незаконне збирання відомостей, що становлять комерційну або банківську таємницю (ст. 231), ввезення, виготовлення, збут і розповсюдження порнографічних матеріалів (ст. 301)

2) злочини у сфері використання комп’ютерів, систем та мереж: несанкціоноване втручання в роботу комп'ютерів (ст. 361), створення шкідливих програмних чи технічних засобів (ст. 361-1), несанкціоновані збут або розповсюдження інформації з обмеженим доступом (ст. 361-2), несанкціоновані дії з інформацією, яка оброблюється комп'ютерах (ст.362), порушення правил експлуатації комп'ютерів (ст. 363), перешкоджання роботі комп'ютерів шляхом розповсюдження повідомлень електрозв'язку (ст. 363-1).

Крім кримінальної відповідальності, існує й адімністративна відповідальність – особа, яка набула майно або зберегла його у себе за рахунок іншої особи без достатньої правової підстави, зобов’язана повернути потерпілому це майно (ст. 1212 Цивільного кодексу України) [51].

Кіберінцидент переходить в категорію «кіберзлочин» за умови кваліфікації правопорушення відповідно до чинного законодавства. Проте специфікою кіберзлочинів є їх транскордонний та організований характер, анонімність, постійне удосконалення способів здійснення кібератак, що

ускладнює проведення як розшукових, так і процесуальних заходів [20]. Тому виникає ситуація, коли офіційна статистика щодо кіберзлочинів фактично в рази нижча, ніж реальна ситуація в країні.

Проаналізувавши сутнісні характеристики ключових понять у сфері кібербезпеки, представимо структурно-логічну схему розуміння основних кібер- понять (рисунок 1.3) .

Рисунок 1.3 – Структурно-логічна схема співвідношення основних кібер-понять

Джерело: складено автором

Для успішної ідентифікації та локалізації кіберзагроз у контексті стабільного розвитку національної економіки доцільно проаналізувати суб’єктно-об’єктну парадигму системи кіберзахисту та ініціаторів-виконавців кібератак.

Унаслідок всепроникності кіберзагроз та їх потенційний вплив на різноманітні аспекти життя й галузі господарювання, питання кіберзахисту має фундаментальне значення для стабільного розвитку національної економіки. Саме тому координація діяльності у сфері кібербезпеки

здійснюється Президентом України через Раду національної безпеки і оборони України. Основними суб'єктами, які задіяні до забезпечення кібербезпеки, є: міністерства та інші центральні органи виконавчої влади, органи місцевого самоврядування; правоохоронні та інші суб'єкти оперативно-розшукової діяльності; військові формування; підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури, Національний банк України; суб'єкти господарювання та громадяни, які взаємодіють з іншими суб'єктами у кіберпросторі; міжнародні організації (НАТО, Європол, Комп'ютерна група реагування на надзвичайні ситуації (CERT, Робочої групи команд реагування на інциденти безпеки); спеціалізованими установами з кіберзахисту інших країн світу.

У Законі України «Про основні засади забезпечення кібербезпеки України» [44] визначено три об'єкта кібербезпеки:

– інформаційно-комунікаційні системи суб'єктів господарювання всіх форм власності, через які здійснюється обмін інформацією з органами державної влади та місцевого самоврядування, іншими органами публічного управління;

– інформаційно-комунікаційні системи, які використовуються у сферах електронного урядування, електронних державних послуг, електронної комерції та інших сферах для задоволення суспільних потреб (система охорони здоров'я, освіти, соціального забезпечення тощо);

– інформаційно-комунікаційні системи об'єктів критичної інфраструктури.

Беручи до уваги, всеохоплюючий характер кіберзагроз та їх деструктивний вплив на функціонування не лише суб'єктів господарювання, а також й життєдіяльність громадян країни, то доцільно включити до складу об'єктів кібербезпеки також інформаційно-комунікаційні засоби фізичних осіб, які використовуються ними для реалізації суспільно та життєвоважливих потреб під час використання кіберпростору.

Важливим завданням державної політики у сфері інформаційної безпеки на всіх рівнях є підвищити рівень резильєнтності до кіберзагроз, а також швидко адаптуватися до змін безпекового середовища, що сприятиме стабільному розвитку національної економіки. У рамках даного дослідження доцільно проаналізувати ключові кіберзагрози, які матимуть потенційний вплив на функціонування окремих галузей господарювання або національної економіки загалом.

У науковій літературі [39, 28] та профільних звітах компаній, які спеціалізуються на інформаційній безпеці, відбувається ототожнення «видів кіберзагроз» та «видів кібератак». Ґрунтуючись на вищенаведеному змістовному аналізі понять, на рисунку 1.4 наведені основні види «кіберзагроз», «кібератак», «кіберінцидентів».

Досліджуючи сутнісні характеристики кіберзагроз у системі економічних відносин, доцільно проаналізувати основних ініціаторів шахрайських дій і кіберпросторі. Базовим завданням для зловмисників є отримання доступу до пристроїв і мереж, що дозволить в подальшому незаконно використовувати процесорну потужність комп’ютерів, викрасти або маніпулювати інформацією, вимагати отримати фінансової винагороди. Загалом кожна категорія суб’єктів кіберзагрози має власну мотивацію в здійсненні протиправної діяльності. Отже, до основних ініціаторів кібератак варто віднести [113]:

– хакерів та хактивістів, мотивами яких є цікавість, привернення уваги, помста, порушення норм соціальної справедливості тощо. Хакери зазвичай використовують вже наявний інструментарій, базові сценарії або веб-ресурси;

– злочинців та шахраїв, які націлені виключно на отримання фінансових ресурсів. Дана група шахраїв можуть розробляти власні програмні інструменти для здійснення кіберзлочину;

– держава та її шпигуни, які здійснюють незаконну діяльність з метою викрадення конфіденційних даних, збору конфіденційної інформації або порушення критичної інфраструктури іншого уряду, встановлення

геополітичних інтересів, впливу на громадську думку на національному на міжнародному рівнях та інше Основними способами кібератак національних урядів є шпигунство або кібервійна;

Рисунок 1.4 – Види кіберзагроз та кібератак

* кібератака фактично вплинула на конфіденційність, цілісність або доступність даних

Джерело: складено автором на основі 16, 40, 86, 102, 146, 157

– інсайдерів, мотивами зловмисної діяльності яких є отримання фінансової винагороди, збір та передача конфіденційної інформації, завдати шкоду діловій репутації організації [35]. Крім цього , суб’єкти внутрішньої загрози не завжди мають зловмисні наміри. Деякі завдають шкоди своїм

компаніям через людську помилку – через мимовільне встановлення шкідливого програмного забезпечення або втрату пристрою, виданого компанією, який кіберзлочинець знаходить і використовує для доступу до мережі.

Незалежно від ініціатора кібератак вони є постійною загрозою в усьому світі як для урядів, компаній, так і для окремих осіб. Публічне визнання порушення зазвичай несе значну репутаційну шкоду на додаток до втрат через викрадені дані та інтелектуальну власність, пошкоджені системи. До основних наслідків кіберінцидентів можно віднести: крадіжка грошових коштів як економічних суб'єктів; несанкціоноване розголошення особистої інформації третіх осіб; репутаційні втрати, спричинені розкриттям комерційної таємниці, викрадення конфіденційної інформації або її шифрування, додаткові витрати на розслідування інциденту та відновлення після кібератак; втрата довіри стейкхолдерів до суб'єктів господарювання; витрати на юридичні позови від постраждалих клієнтів. У сучасних умовах для захисту економічних суб'єктів у кіберпросторі доцільно інвестувати кошти у придбанні складніших засобів захисту для забезпечення належного рівня інформаційної безпеки, а також постійно удосконалювати навички та знання існуючого персоналу та здійснювати пошук кваліфікованих спеціалістів для вирішення поточних та майбутніх прогалин у системі інформаційної безпеки економічних суб'єктів.

Підсумовуючи, зазначимо, що кібербезпека є безперервним і вкрай актуальним процесом для стабільного функціонування економічних суб'єктів з урахуванням цифрових трансформацій. У сучасних умовах розвитку вкрай важливо для суб'єктів кібербезпеки вчасно запобігати кібератакам на ранньому етапі та здійснювати комплекс превентивних заходів для підвищення рівня їх кіберзахисту.

1.2. Сучасні тенденції поширення кіберзлочинності в Україні та світі

Цифровізація сучасного світу, розвиток інформаційних технологій, поширення Internet, комп'ютерні мережі, використання кіберпростору, наразі виступають основою сучасного суспільства. Оскільки використання Інтернету та підключених до мережі комп'ютерів зростає, а також відбувається інтенсивний розвиток інноваційних технологій, що в кінцевому підсумку сприяє зростанню кіберзагроз. Зростання кількості кібератак є результатом стрімкого використання інноваційних цифрових технологій у діяльності економічних суб'єктів, появою фінтех компаній, а також збільшенням попиту на цифрові фінансові продукти та розвитком електронної комерції із-за пандемії COVID-19. Зокрема, під час пандемії кількість порушень у сфері кібербезпеки серед FinTech компаній в середньому збільшився на 17% [142].

У 2020 році збитки від кіберзлочинів у США оцінювалися на рівні 4,2 млн дол США, що вдвічі більше порівняно з 2018 роком (2,7 млн дол США). При цьому впродовж останніх років виробнича сфера та сфера фінансових послуг були та залишаються основними таргетами для кіберзлочинців. IBM щорічно визначає індекс загроз (X-Force Threat Intelligence Index), який відображає ландшафт кіберзагроз у світі (табл. 1.2).

Таблиця 1.2 – Рейтинг вразливості сфер діяльності до кіберзлочинів у період з 2018 по 2022 рр.

Сфери діяльності	Рік					Зміна, 2022/2018
	2018	2019	2020	2021	2022	
Фінансові послуги	19	17	23	22,4	18,9	0
Виробництво	10	8	17,7	23,2	24,8	+15
Енергетика	6	6	11,1	8,2	10,7	+5
Роздрібна торгівля	11	16	10,2	7,3	8,7	-2
Професійні послуги	12	10	8,7	12,7	14,6	+3
Охорона здоров'я	6	3	6,6	5,1	5,8	0
Медіа	8	10	5,7	2,5	0,5	-8
Транспорт	13	13	5,1	4	3,9	-9
Освіта	6	8	4	2,8	7,3	+1
Інші	9	9	7,9	12	4,8	+4

Джерело: складено автором на основі даних IBM Security [154]

На основі даних про атаки та інциденти з порушення інформаційної безпеки з керованих мереж X-Force, а також про публічно розкриті кіберзлочини фахівцями IBM встановлено, що протягом 2018-2022 років найбільший приріст зафіксовано по сфері виробництва, при цьому зменшився інтерес кіберзлочинців до транспортної галузі та медіа. Варто відзначити, що протягом останніх п’яти років сфера фінансових відносин має високий рівень вразливості до кіберзлочинів. Це пояснюється тим, що банки – це фактично «кровоносна система» національної економіки, через яку здійснюється обслуговування інтересів держави (виконання державного і місцевих бюджетів, отримання міжнародної допомоги, надання субсидій тощо), суб’єктів господарювання різних галузей економіки, а також громадян суспільства. З урахуванням цього, банківські установи акумулюють значну за обсягом інформацію від своїх клієнтів. У разі порушення інформаційної безпеки фінансових установ конфіденційні дані можуть бути використані для здійснення протиправної діяльності або продані на темних веб-майданчиках, що може призвести до втрати ділової репутації як фінансових установ, так і їх клієнтів [2].

У таблиці 1.3 представлено найбільші кіберзлочинні угруповання, які атакують фінансові установи в світі.

Таблиця 1.3 – Найбільші кіберзлочинні угруповання, які здійснюють атаки на фінансові установи, у світі

Назва	Рівень складності кібератак	Жертви	Особливості кібератак
Money Taker (Російська Федерація)	група використовує власні інструменти кібератак, шкідливе програмне забезпечення, яке працюватиме і після перезавантаження. здійснює налаштування загальнодоступних інструментів для своїх потреб.	банки, компанії, що надають послуги та/або технології фінансовим установам	більше 20 успішних атак на банки, фінансові установи та юридичні компанії в США, Великобританії та Росії.

Продовження таблиці 1.3

Назва	Рівень складності кібератак	Жертви	Особливості кібератак
Carbanak (Російська Федерація)	угруповання використовує шкідливе програмне забезпечення, яке надає широкий спектр можливостей: авторизація, зчитування даних банківських карток, особистої інформації.	Банки, фінансові компанії, компанії з електронної комерції / роздрібної торгівлі	понад 300 успішних атак на банки, фінансові установи та роздрібних торговців, у тому числі на систему Oracle
Lazarus Group (Північна Корея)	група має потужні можливості, а саме технології ухилення корпоративних систем кіберзахисту, трирівневі атакуючі сервери, зашифровані комунікації.	Банки, фінансові компанії, урядові структури	атака на Sony Pictures, розробник програми, атака на SWIFT (1 млн дол США), Центральний банк Бангладеша (81 млн дол США) ті інші.

Джерело: складено автором на основі даних компанії Insights [144]

Кіберзагрози досягли безпрецедентного розмаху, що спричинено дією наступних потенційних чинників:

– потужний розвиток електронних обчислювальних машин, мобільних пристроїв дозволив підвищити швидкість обробки даних та отримати постійний доступ до фінансових послуг. Так, у 2019 році у світі нараховувалося близько 5,2 млрд мобільних користувачів, що охоплює 67% населення світу, тоді як у 2015 р.– 4,66 млрд, 2010 р. – 3,219 млрд осіб [143].

– збільшення кількості пристроїв, підключених до мережі Інтернет. У 2019 р. 39% громадян ЄС, які користувалися Інтернетом, зіткнулися з проблемами безпеки у віртуальному просторі. Значення даного показника значною мірою коливається в різних державах-членах: більше 50% у Великобританії та 10% у Литві[88].

– неможливість відслідкувати територію / країну здійснення кібератаки, що дозволяє анонімно здійснювати інтернаціональну протиправну діяльність;

– збільшення кількості користувачів соціальних мереж, які містять персональні дані. Відповідно до Emarketer рівень проникнення соціальних

мереж у світі у 2020 р. становив 41,9% від загальної кількості населення або 3,23 млрд користувачів. Для порівняння: у 2017 р. – 2,3 млрд користувачів або 31,2%, у 2013 р. – 1,6 млрд користувачів або 22,8% [95];

– використання застарілого та неліцензійного програмного забезпечення;

– стрімке зростання технологій Інтернет речей, які використовуються у різних системах господарювання та побуті. Зокрема, у країнах Європейського Союзу у 2021 р. майже третина суб'єктів господарювання користуються на практиці можливостями Інтернет речей, тоді у Австрії – 51% компаній від загального обсягу, Словенія – 49%, Фінляндія та Швеція – по 40% [90];

– збільшення питомої ваги бізнес-процесів, які передаються на управління третім особам, у тому числі й закордон;

– використання хмарних технологій для зберігання та передачі даних. У 2021 році У 2021 році у середньому 41% підприємств ЄС використовували хмарні обчислення, переважно для електронної пошти та зберігання файлів. Проте між країнами можна спостерігати значні відмінності: у Швеції (75 % підприємств використовували хмарні обчислення), Фінляндії (75 %), Нідерландах (65 %), Данії (65 %), тоді як у Румунії (14 %), Болгарії (13 %), Польща (29%), Україна (10,1%) [89]. Проте протягом 2023-2030 рр. очікується збільшення використання хмарних технологій у бізнес-процесах приблизно на 14,1% [74].

– розширене використання робототехніки або алгоритмів для здійснення автоматичної торгівлі та розробки додатків. У 2019 році на європейських виробничих компаніях на 10 000 працівників припадає 500 роботів, США – 293 роботи на 10 000 працівників, а в Сінгапурі – 918 на 10 000 працівників [153].

– збільшення використання віртуальних та цифрових валют. Сумарна капіталізація ринку криптовалют всього за одне десятиліття збільшилася до позначки 1.2 трильйона дол.

Забезпечення кібербезпеки є динамічним процесом швидкого реагування та адаптації до швидко змінюваних кіберзагроз, що обумовлено використанням нових технологій зловмисниками при реалізації кібератак. Проаналізуємо основні патерни кіберзагроз у світі протягом 2005-2020 років. Джерелом даних про кіберінциденти слугувала база даних Європейського репозитарію кіберінцидентів (European Repository of Cyber Incidents, EuRepoC) [87]. Дослідження ландшафту кіберзагроз у світі проведено на основі 785 кіберінцидентів, які призвели до значущих змін у стабільному функціонування національної економіки (атака на центральні банки, державні установи, міжнародні компанії тощо). При цьому зазначимо, що щодня відбувається близько 4000 нових кібератак. Кожні 14 секунд компанія стає жертвою атаки програм-вимагачів, що може призвести до катастрофічних фінансових втрат [121]. Дані щодо кіберінцидентів згруповані за наступними характеристиками: за країною-ініціатором, за країною-жертвою, типом кібератак (шпіонаж, відмова в обслуговуванні, пошкодження або знищення інформації, дефейс, фінансова крадіжка, доксинг, саботаж), за сферою госпдарювання (публічний та приватний сектор, військовий сектор, громадянське суспільство), за датою проведення кібератаки (у розрізі років, місяців, днів тижня, днів). Динаміка аналізованих кіберінцидентів по роках представлена на рисунку 1.5.

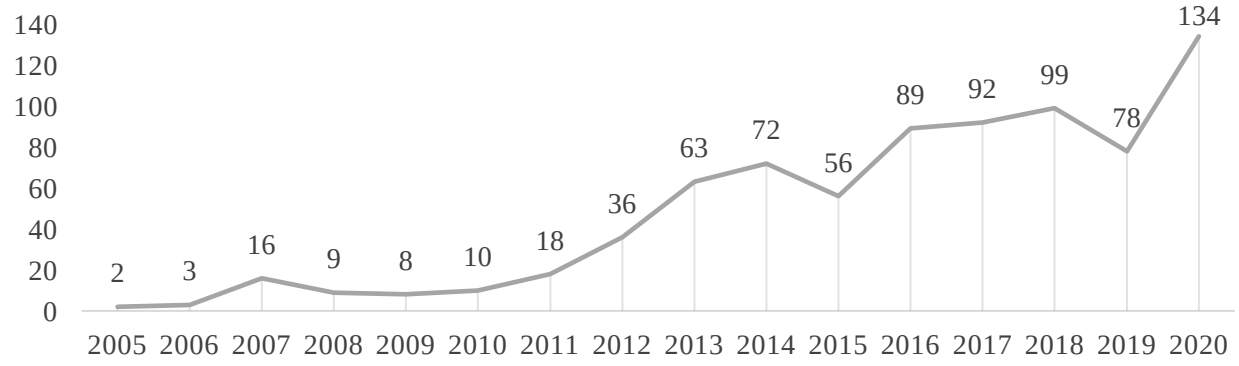


Рисунок 1.5 – Динаміка значущих кіберінцидентів у світі протягом 2005-2020 років

Джерело: складено автором на основі база даних Європейського репозитарію кіберінцидентів [87]

Дані рисунку 1.5 наочно демонструють, що у 2020 році у світі було зафіксовано 134 кіберінциденти, які ймовірно заподіяли суттєвої шкоди об'єктам критичної інфрастурктури, що майже вдвічі більше порівняно з 2019 роком (78 кіберінцидентів).

У період з 2005 по 2020 роки 41,8% кіберіндидентів здійснено резидентами з Китаю, при цьому 40% з них були направлені на об'єкти критичної інфраструктури у сфері публічного управління та 36% – на об'єкти приватного сектору (рис. 1.6). Пріоритетними країнами-цілями для Китаю є США (питома вага – 25%), світ (13%). Крім Китаю, найбільшими спонсорами кібератак у світі є росія та Іран, сукупно на ці три країни припадає 78,5% від всіх кіберінцидентів. Рівень концентрації кіберінцидентів у розрізі країн-жертв є значно нижчим порівняно з країнами-спонсорами. Так, найбільше атакуються у кіберпросторі об'єкти критичної інфраструктури США (149 інцидентів або 18,9% від загального обсягу).

Рисунок 1.6 – Топ країни, які є найбільшими спонсорами та жертвами кібернцидентів у світі

Джерело: складено автором на основі база даних Європейського репозитарію кіберінцидентів [87]

Стосовно України, то протягом 2005-2020 рр. зафіксовано 22 кіберінциденти, ініціатором яких виступала росія, 10 з яких були направлені на злам урядових структур та 9 – на об'єкти приватного сектору.

Переважна більшість кібератак були здійснені у формі шпіонажу, що передбачає здійснення розвідувальної діяльності для збору конфіденційної інформації у публічному та приватному секторах (рис. 1.7).

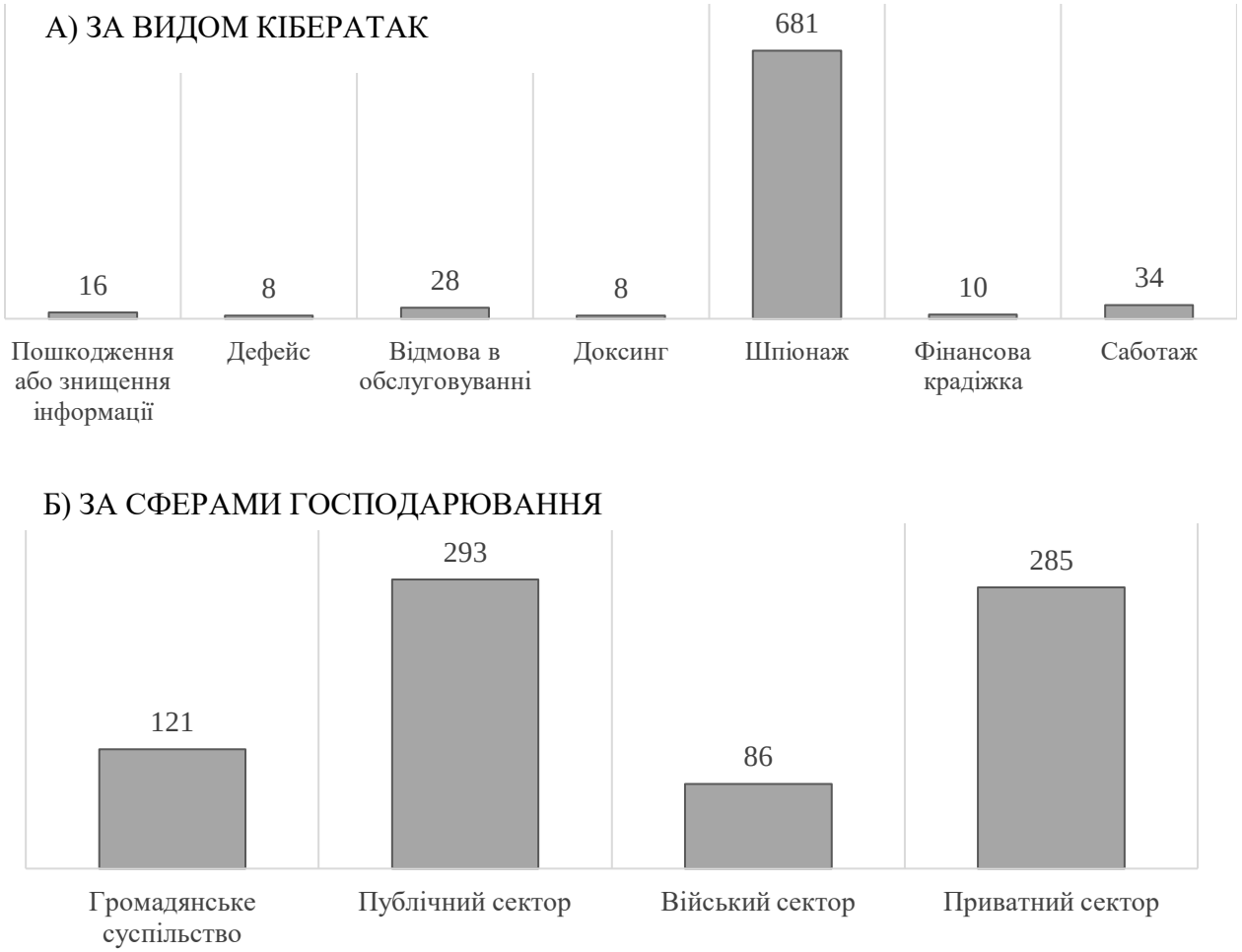


Рисунок 1.7 – Структура кіберінцидентів у період з 2005 по 2020 роки (а – за видом кібератак; б – за сферами господарювання)

Джерело: складено автором на основі база даних Європейського репозитарію кіберінцидентів [87]

У межах даного дослідження також вирішено більш детальніше проаналізувати дати здійснення кібератак (рис. 1.8). Це обумовлено тим, що у багатьох дослідження [63, 98, 120] вже емпірично доведено, що часова концентрація є стійкою ознакою різних видів злочинності.

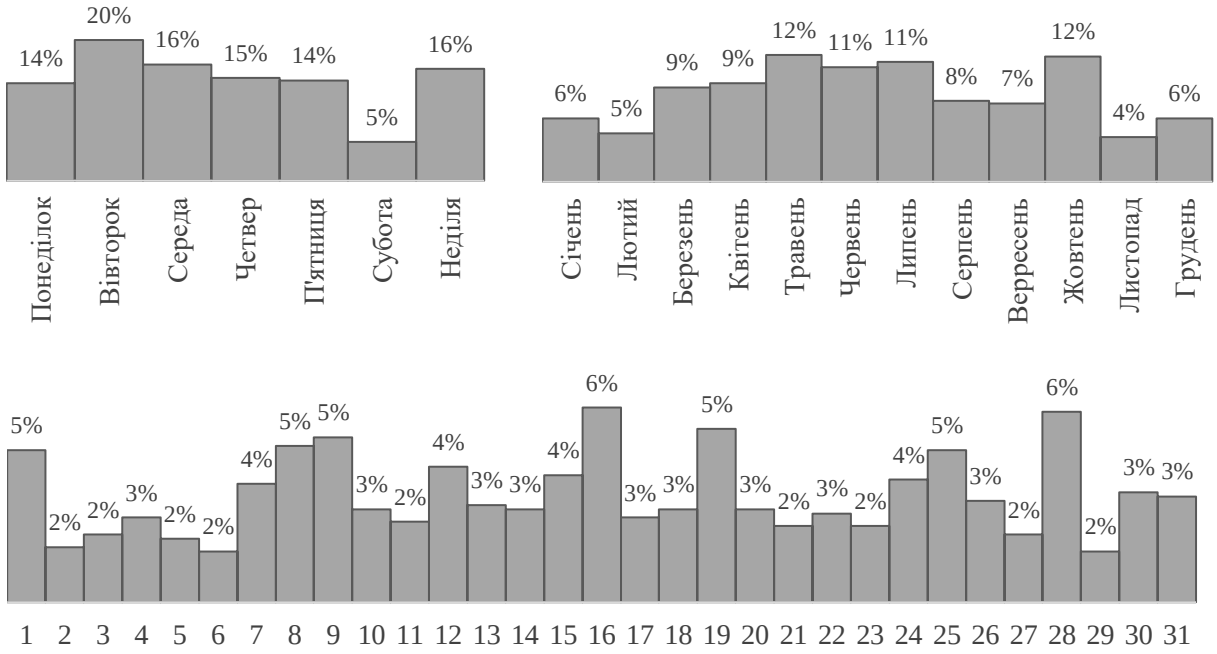


Рисунок 1.8 – Часова концентрація кіберзагроз у розрізі місяців, днів тижня та днів

Джерело: складено автором на основі база даних Європейського репозитарію кіберінцидентів [87]

Дані, представлені на рисунку 1.8, засвідчують про достатню однорідність розподілу кіберіндицентів. Найбільша кількість кіберінцидентів у світі була реалізована у вівторок, при цьому фіксуючи збільшення даних протиправних дій у такі дні як 19,24,25. Найменша кількість кіберінцидентів була здійснена у суботу. Стосовно місяців, то найбільш інтенсивно кіберзлочинці здійснювали атаки у травні, жовтні, червні та липні. Щодо днів тижня, то збільшення кількості кіберінцидентів фіксувалося 16 та 28 числа.

Забезпечення безпеки інформаційних технологій установ та їх баз даних є постійно зростаючим викликом для топ-менеджменту установ, так і національного регулятора. Хоча програмне забезпечення поступово стає все більш безпечним, а розробники створюють нові підходи до кібербезпеки, зловмисники також удосконалюють технології здійснення зловмисних діянь. Найбільш поширеними формами здійснення кібератак є програма – фішинг,

експлуатація загальнодоступних програм, програми-здирники. У таблиці 1.4 наведено найбільш поширені способи здійснення кібератак у світі у розрізі сфер господарювання.

Дані таблиці 1.4 засвідчують, способи здійснення атак кіберзлочинцями є різноманітними залежно від приналежності об'єкта до відповідної сфери господарювання. Проте найбільш розповсюдженою формою кібератаки є різні види фішингу, який передбачає викрадення важливої інформації за допомогою електронних листів із застосуванням соціальної інженерії та обману.

Таблиця 1.4 – Найбільш поширені види кібератак у розрізі сфер господарювання

Сфери діяльності	Види кібератак	Географія поширення
Фінансові послуги	Фішингові вкладення – 53% атак, експлуатація загальнодоступних програм – 18%, а фішингові посилання – 12%.	Європа – 33% усіх атак, Азіатсько-Тихоокеанський регіон – 31%, Латинська Америка – 15%, Північна Америка – 10%, Близький Схід і Африка – 10%.
Виробництво	Фішингові вкладення – 28%, експлуатація загальнодоступних програм – 28%, атаки з боку зовнішніх віддалених служб – 14%, фішингові посилання –10.	Азіатсько- Тихоокеанський регіон – 61%, Європа – 14%, Північна Америка – 14%, Латинська Америка – 8%, Близький Схід і Африка – 4%.
Енергетика	Фішингові посилання – 20%, атаки з боку зовнішніх віддалених служб – 20%. ботнети – 19%, а програми-здирники та BEC-атаки – 15%	Північна Америка – 46%, Європа – 23%, Латинська Америка – 23%, Азіатсько- Тихоокеанський регіон – 4%, Близький Схід і Африка – 4%.
Роздрібна торгівля	Програми-здирники – 18%, бекдори – 18%, BEC-атаки – 18%, «хробак» –10.	Північна Америка – 39%, Латинська Америка – 39%, Європа – 22%.
Професійні послуги	Програми-здирники – 18%, бекдор-атаки – 18%, експлуатація загальнодоступних програм – 23%, атаки з боку зовнішніх віддалених служб –23%, фішингові вкладення та дійсні локальні облікові записи – 15%	Європа – 47%, Північна Америка – 33%, Азіатсько- Тихоокеанський регіон – 10%, Близький Схід і Африка – 7%. Латинська Америка – 3%.

* експлуатація загальнодоступних програм виникає коли зловмисник використовує вразливість загальнодоступної програми для отримання несанкціонованого доступу до цільової мережі; BEC-атаки – компроментація ділової електронної пошти
Джерело: складено авторами на основі даних IBM Security [154]

Одним з найбільш розповсюджених методів для викрадення грошей безпосередньо з рахунків компаній - це BEC-афера (business email compromise). Принцип роботи BEC-афери наступний: кіберзлочинець вводить в оману співробітника компанії, який має доступ до конфіденційної інформації, з вимогою зробити переказ коштів на рахунок, який начебто належить клієнту, або контрагенту компанії, проте кошти перенаправляються на рахунок кримінальної організації. У 2020 році збитки від BEC-афер та EAC-афер (компрометація облікового запису, email account compromise), які є аналогом BEC-афер для фізичних осіб, у США оцінені на рівні 1,8 млрд дол США (або 36% від загальної суми збитків від кіберзлочинів), тоді як у 2019 році – 1,7 млрд дол США (або 48,57% від загальної суми) [101].

Динамічна цифровізація економіки робить банківські та небанківські фінансові установи більш вразливими до кіберзлочинності. По-перше, банки – це фактично «кровоносна система» національної економіки, через яку здійснюється обслуговування інтересів держави (виконання Державного і місцевих бюджетів, отримання міжнародної допомоги, надання субсидій тощо), суб'єктів господарювання різних галузей економіки, а також громадян суспільства. По-друге, доволі поширеною практикою є передача управління інформаційною системою фінансових установ спеціалізованим компаніям, що вимагає від останніх здійснення додаткових заходів щодо захисту своїх ресурсів від кібератак [2].

Шахрайство у банківській сфері є достатньо різноманітним. Існує безліч видів шахрайства в банківській сфері і серед них можна виділити чотири основні групи. Першу групу утворюють схеми розкрадання грошових коштів шляхом їх отримання за підробленими банківськими документами і цінними паперами, наприклад: розрахунковими чеками, векселями, депозитними сертифікатами і т.д. Другу групу складають розкрадання грошових коштів вкладників і інвесторів, отриманих під обіцянку виплати високих відсотків або виконання інших зобов'язань (за принципом фінансових пірамід чи інших «пірамід»). Суть такого шахрайства полягає в тому, що зобов'язання перед

новими вкладниками виконуються на першому етапі за рахунок надходження коштів нових інвесторів і їх обману. До наступної групи відноситься кредитне шахрайство, яке представляє собою розкрадання грошових коштів шляхом отримання різних кредитів з наданням підробленої документації. В цьому випадку обман полягає в: поданні завідомо неправдивих відомостей; поданні завідомо недостовірних відомостей; поданні завідомо неправдивих і недостовірних відомостей. Даний вид шахрайства в банківській сфері є найпоширенішим і зловмисники використовують його частіше за інших. Потенційний позичальник надає банку або іншому кредитору завідомо неправдиві і (або) недостовірні відомості у вигляді документів, що підтверджують його уявну платоспроможність, які в подальшому повинні бути ретельно перевірені кредитною організацією. Четверту групу утворює шахрайство з використанням банківських карт (чужих або підроблених кредитних, розрахункових чи інших платіжних). Даний вид шахрайства є порівняно новим і активно розвивається.

Найбільш розповсюдженими шахрайствами у сфері фінансових послуг є саме методи соціальної інженерії. Ці методи спираються на здійснення психологічного впливу на жертву з метою підштовхування останньої до здійснення необхідних для зловмисників дій. За даними ЄМА (Української міжбанківської асоціації членів платіжних систем) на кінець 2018 р. близько 70% – це шахрайські операції, пов’язані з соціальною інженерією та здійснені за допомогою мережі Інтернет [71]. Банкоматне шахрайство складає приблизно четверту частину від усієї кількості шахрайських операцій та має тенденцію до зниження своєї частки у зв’язку з удосконаленням банківських технологій захисту банкоматів. Протягом 2017–2018 рр. значно зменшилася й до цього незначна частка шахрайських операцій через POS-термінали та дещо зросла частка випадків шахрайства при дистанційному банківському обслуговуванні. Не варто виключати і можливостей співучасті в тій чи іншій шахрайській схемі з боку працівників банків. Це – ще один з напрямків «роботи» шахрайських схем. Працівники банку можуть не лише надавати

зловмисникам дані клієнтів за грошову винагороду, але й бути активними учасниками схем, а подекуди – й організаторами. Величезним сегментом шахрайства є технологічний сегмент. Тобто, за допомогою застосування технологічних рішень зловмисники отримують дані клієнтів банків, або й безпосередній доступ до банківських рахунків жертв (цю «задачу» виконують, як правило, фішингові технології) [36]. З 2016 р. VISA і MasterCard ввели принцип нульової відповідальності в Україні та на глобальному рівні. Це означає, що якщо власник карт цих платіжних систем став жертвою шахраїв і зміг це довести, то банки повинні компенсувати йому кошти. Це ставить проблему запобігання шахрайським операціям з боку банків. Отже, даний аспект є позитивним для клієнтів банків не лише з огляду на можливість компенсації навіть безнадійно втрачених коштів, а й, що найбільш важливо, з огляду на те, що інвестиції банків у технології захисту від шахрайства є вже об’єктивно обумовленими інтересами самих банків. Отже, постійна робота з боку банків над удосконаленням систем безпеки транзакцій та систем захисту даних своїх клієнтів буде тривати й надалі.

Щодо можливостей протидії шахрайським операціям, варто відзначити, що існує два напрямки: технічний та соціальний, в залежності від сфери застосування шахрайських технологій. Технічний шлях запобігання банківському шахрайству активно удосконалюється, постійно розвиваються технічні інструменти безпеки банківських транзакцій, розкриваються нові шахрайські схеми. Цей напрямок «приречений» на постійну еволюцію. З наведених вище даних щодо тенденцій шахрайства можна бачити, що невдовзі варто очікувати збільшення обсягу шахрайства в сфері електронної комерції. Також вкрай важливо звернути увагу на сегмент мобільних і безконтактних платежів.

З урахуванням постійно зростаючих загроз у кіберпросторі, національні регулятори розробляють стратегії щодо підвищення кіберзахисту національних економік, обмінюються кращими практиками протидії кіберзагрозам з іншими країнами та розробляються міжнародні рекомендації

для підвищення кіберрезильєнтності економічних суб'єктів та урядових структур. Для моніторингу поточного стану готовності України та інших країн світу до запобігання кіберзагрозам та управління кіберінцидентами проаналізуємо Національний індекс кібербезпеки (National Cyber Security Index), що розраховується естонською Академією електронного урядування. У 2018 році експертами було оцінено кібербезпеку в Україні на рівні 58% з поміж 100%, проте вже у 2022 році – 75% за рахунок удосконалення кібербезпеки у військовій сфері, кіберзахисту у сфері надання цифрових послуг, системи управління кіберризиками тощо.

На сьогодні кіберзахист критично важливих об'єктів інфраструктури є пріоритетним завданням для держави, оскільки використання шкідливих програм є елементом сучасної стратегії гібридної війни. За даними Оперативного центру реагування на кіберінциденти Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України у 2022 році отримано 58 млрд подій, які опрацьовані за допомогою засобів моніторингу. За результатами первинного та вторинного аналізу підозрілих подій для інформаційної безпеки у 2022 році офіційно зареєстровано 415 кіберінцидентів, що в 2,8 рази більше порівняно з 2021 роком [18]. За підсумками I кварталу 2023 року зафіксовано та оброблено безпосередньо аналітиками безпеки 202 кіберінциденти, що у 5 разів більше порівяно з аналогічним періодом 2022 року (40 кіберінцидентів) [18].

Таким чином, збільшення частоти та масштабів кібершахрайств у фінансовому секторі може призвести до несанкціонованого розповсюдження персональної фінансової інформації про клієнтів, отримання значних збитків та репутаційних втрат фінансовими установами і навіть мати системні наслідки для економіки країни, оскільки загрози можуть швидко поширюватися по різних секторах економіки. За цих умов вчасно ідентифікувати ознаки кібершахрайства та швидко прийняти рішення щодо їх нейтралізації.

1.3. Проведення типологізації країн за рівнем участі їх резидентів у здійсненні кібернетичних та фінансових шахрайств

Протягом останніх років відбувається динамічне поширення кібершахрайств та фактично набула характеристик організованої злочинної діяльності у кіберпросторі. Враховуючи транснаціональний характер злочинів, пов'язаних із протиправним, несанкціонованим створенням, зберіганням, обробкою, пошкодженням або знищенням об'єктів інформаційної інфраструктури, ефективна протидія цим діям потребує розробки системних заходів для посилення перевірки та контролю задля протидії шахрайським операціяv у мережі Інтернет.

Для ефективної організації системи кібербезпеки на як рівні окремих суб’єктів господарювання, так і держави загалом доцільним є запровадження двостороннього підходу, який передбачає поєднання дієвих превентивних заходів та постійного моніторингу стану інформаційної системи. З одного боку в умовах постійного збільшення кількості кіберзагроз та зростання складності їх проведення та, з іншого боку, нарощення обсягів транскордонної торгівлі товарів та послуг, вкрай важливо суб’єктам господарювання проводити процедуру експрес-перевірки клієнтів та контрагентів без безпосередньої взаємодії з ним. Це може бути реалізовано шляхом розробки списку ризикових держав (юрисдикцій), резиденти яких можуть мати фактичний або потенційний несприятливий вплив через ланцюги відносин на функціонування суб’єктів національної економіки. Виходячи з цього, запропоновано науково-методичний підхід до багатокритеріального оцінювання ступеня залученості ділового партнера до фактичного або ймовірного у перспективі несприятливого впливу на безпеку об'єктів інформаційної інфраструктури. Для вирішення поставленого завдання використано алгоритм машинного навчання без нагляду на основі змінних на рівні країн, який може класифікувати країни за рівнем їх фактичної або ймовірної участі у протиправних кібернетичних правопорушеннях.

Основними етапами розробленого науково-методичного підходу є:

– формування вхідної статистичної бази дослідження;

– приведення значень показників до єдиного співставного вигляду;

– визначення узагальненої оцінки окремим складовим протиправної діяльності в країні;

– поділ країни на кластери за рівнем їх фактичної або ймовірної участі у протиправних кібернетичних правопорушеннях;

– формалізація сутнісних характеристик кластерів країн на основі використання дерев класифікації.

Перший етап передбачає формування інформаційної та статистичної бази дослідження. Соціальні та економічні чинники відображають рівень добробуту громадян та умов для їх стабільного функціонування, слугуючи основним контекстом, у якому виникає кіберзлочинність. Людські та соціальні чинники відіграють значну роль у формуванні агломерацій кіберзлочинності (Waldrop, 2016) [149]. Особливістю розробленого авторського підходу є розробка інтегрального показника, який буде відображати не тільки частоту й масштаби кібератак, ініційованих резидентами відповідної країни, а також врахувати стан дотримання норм доброчесності у бізнес-середовищі, доступу резидентів до анонімної мережі даркнету та інтенсивність її використання, а також загальну криміногенну ситуацію в регіоні, що в сукупності опосередковано визначають ступінь залученості громадян відповідної країни до протиправної діяльності у кіберпросторі.

Для побудови інтегрального показника рівня фактичної або ймовірної участі резидентів країни у протиправних кібернетичних правопорушеннях обрано наступні групи показників, які подані а таблиці 1.5.

Дві групи показників, які характеризують різні види злочинності (X1) та активність кримінальних угруповувань (X2), визначалися на основі двоетапного опитування експертів у рамках проекту Глобальної ініціативи проти транснаціональної організованої злочинності. Дане опитування проходило у межах розрахунку Глобального індексу організованої злочинності (Global

Organized Crime Index) [93]. Для апробації розробленого науково-методичного підходу використано вхідну статистичну базу 34 країн світу, яка подана в таблиці 1.6. Системне та грубе недотримання суб'єктом господарювання норм міжнародного права може призвести до запровадження міжнародних штрафних санкцій та обмежень як до окремого економічного суб'єкта, так і держави загалом.

Таблиця 1.5 – Перелік індикаторів для типологізації країн за рівнем участі їх резидентів у здійсненні фінансових кібернетичних шахрайств

Показник		Одиниця вимірювання	Умовне позначення	Межі коливання
Група показників, які характеризують різні види злочинності (X1)	контрабанда людей	бал	X1_1	0-10
	торгівля зброєю	бал	X1_2	0-10
	злочини проти флори	бал	X1_3	0-10
	злочини проти фауни	бал	X1_4	0-10
	злочини проти невідновлюваних ресурсів	бал	X1_5	0-10
	торгівля героїном	бал	X1_6	0-10
	торгівля кокаїном	бал	X1_7	0-10
	торгівля канабісом	бал	X1_8	0-10
	торгівля синтетичними наркотиками	бал	X1_9	0-10
Група показників, які відображають активність	мафіозні угруповання	бал	X2_1	0-10
	злочинні мережі	бал	X2_2	0-10
	державні суб'єкти	бал	X2_3	0-10
	іноземні суб'єкти	бал	X2_4	0-10
Ризик корупції та хабарів		ум.од.	X3	0-100
Питома вага кібератак у світі, ініціатором якої виступила країна		%	X4	0-100
Загальний дохід, який отримано на даркнет-ринку		євро на душу населення	X5	0;∞
Міжнародні санкції, які накладені на країну		ум.од.	X6	0-1

Джерело: складено автором

У роботі зроблено припущення, що ті суб'єкти господарювання, які перебувають у зоні високого ризику потрапляння під міжнародні санкції, можуть функціонувати ірраціонально та здійснювати злочинну діяльність. Зауважимо, що індикатор «міжнародні санкції, які накладені на країну» визначено на основі аналізу 10 діючих режимів санкцій, спрямованих на протидію легалізації доходів, отриманих незаконним шдяхом: US OFAC, UN Security Council, EU restrictive measures, EU non-cooperative tax jurisdictions, EU high-risk third countries,UK high-risk third countries, UK financial sanctions, FATF

increased monitoring (сірий список), FATF call for action (чорний список), Australian sanctions.

Таблиця 1.6 – Вхідна статистична база для дослідження

Країна	X1_1	X1_2	X1_3	X1_4	X1_5	X1_6	X1_7	X1_8	X1_9	X2_1	X2_2	X2_3	X2_4	X3	X4	X5	X6
Албанія	6,5	4,5	4,5	3,5	5,5	6,0	7,0	7,0	3,0	7,0	7,5	7,0	2,5	35	0,0	2,9	0,2
Білорусь	5,5	6,5	3,0	2,0	5,0	4,0	2,0	4,0	5,0	4,0	5,0	9,0	5,0	41	0,7	13,7	0,3
Хорватія	6,0	3,5	5,0	2,5	4,5	5,0	5,5	5,5	5,5	4,0	6,5	6,5	4,5	47	0,0	7,7	0,0
Кіпр	6,0	2,5	2,5	3,0	2,0	2,0	4,5	4,0	3,0	3,5	5,0	4,0	7,0	53	0,0	14,3	0,0
Чехія	5,0	4,5	3,0	5,5	3,0	4,5	4,5	6,0	6,5	3,0	5,0	5,5	4,5	54	0,0	13,6	0,0
Данія	4,5	4,0	1,5	2,0	2,0	5,0	5,5	5,0	5,0	5,0	4,0	2,0	4,5	88	0,0	9,0	0,0
Єгипет	5,5	7,0	1,0	5,0	4,0	5,5	2,0	7,0	7,0	3,0	5,5	8,0	5,0	33	0,1	0,7	0,0
Естонія	3,0	3,0	1,5	1,5	3,0	3,0	3,5	5,0	6,5	3,0	5,0	2,0	5,0	74	0,0	21,7	0,0
Фінляндія	2,5	2,5	1,0	1,5	2,0	3,5	4,0	3,5	4,5	3,0	3,0	1,5	3,0	88	0,0	18,3	0,0
Франція	6,5	6,0	4,0	5,5	4,5	6,0	6,5	6,5	5,5	6,0	6,5	3,0	7,0	71	0,1	5,8	0,0
Грузія	2,0	2,0	3,5	3,5	3,0	3,5	2,0	3,5	4,0	2,5	3,0	3,0	3,0	55	0,0	9,0	0,0
Німеччина	7,0	6,0	1,5	3,5	2,5	4,5	6,5	5,0	6,0	5,0	6,5	2,0	6,5	80	0,0	6,5	0,0
Греція	7,5	3,5	2,0	2,5	3,0	6,0	3,5	5,0	2,5	3,0	6,5	7,5	6,0	49	0,1	4,1	0,0
Угорщина	6,0	3,5	3,5	4,5	3,5	4,5	5,0	5,5	5,5	1,0	4,0	7,0	5,0	43	0,0	5,1	0,0
Італія	6,5	5,5	2,5	3,5	5,5	4,5	7,5	5,0	5,0	9,0	3,0	6,5	7,0	56	0,0	2,9	0,0
Йорданія	5,5	6,5	3,5	3,5	1,5	3,5	3,0	6,0	6,0	1,5	7,0	6,5	4,5	49	0,1	1,4	0,3
Латвія	3,5	3,5	1,0	2,0	2,0	4,5	5,0	5,5	5,0	3,5	3,5	2,0	4,5	59	0,0	30,8	0,0
Литва	2,5	2,5	1,0	2,0	2,0	4,0	4,5	4,0	4,0	3,5	4,0	4,0	3,0	61	0,0	16,4	0,0
Мальта	4,0	2,5	1,0	5,0	5,0	3,0	5,0	4,5	5,5	1,5	7,0	7,5	5,0	54	0,0	17,1	0,0
Молдова	4,0	5,0	2,5	2,0	3,0	3,0	2,5	4,5	5,0	4,0	4,0	7,0	5,0	36	0,0	14,4	0,1
Морокко	6,5	3,0	3,0	4,5	3,0	3,0	6,0	9,0	6,0	1,0	6,5	7,0	4,0	39	0,1	1,4	0,2
Нідерланди	4,5	5,0	3,0	4,0	4,0	4,0	7,0	5,5	7,5	4,5	6,0	2,5	4,5	82	0,1	16,8	0,0
Норвегія	3,5	3,5	2,5	4,0	3,5	5,0	4,5	4,0	4,5	4,5	4,0	2,0	4,0	85	0,0	16,3	0,0
Польща	4,5	3,5	2,0	2,5	5,5	4,0	4,5	5,5	6,5	2,0	5,5	3,5	3,5	56	0,1	6,4	0,0
Португалія	4,0	4,0	3,5	3,5	3,0	4,5	5,0	4,5	4,5	4,5	6,0	4,5	5,0	62	0,0	7,5	0,0
Росія	6,0	4,5	7,5	7,5	5,0	7,0	4,5	5,0	7,5	4,5	7,5	8,5	5,0	29	22,6	8,7	0,5
Сербія	6,5	7,5	4,0	4,0	4,0	7,0	5,5	6,0	6,0	6,0	7,0	8,0	6,5	38	0,0	5,1	0,3
Словенія	5,5	3,5	2,0	3,0	2,5	4,0	4,5	5,0	5,5	3,0	4,5	6,0	5,0	57	0,0	23,5	0,0
Іспанія	7,0	4,0	3,5	5,0	2,0	6,5	7,0	7,0	4,0	6,0	6,5	5,0	7,5	61	0,3	5,7	0,0
Швеція	5,5	6,0	2,0	3,5	2,0	4,0	4,5	5,0	5,5	5,5	5,5	2,5	6,0	85	0,0	19,1	0,0
Туніс	7,0	5,0	3,5	3,5	5,0	2,0	3,0	5,0	4,0	1,0	4,0	5,5	3,0	44	0,0	1,7	0,1
Турція	9,0	9,0	4,0	3,0	9,5	8,0	4,0	5,0	5,5	8,0	7,5	9,0	5,0	38	0,1	4,8	0,3
Україна	6,5	8,0	6,5	4,0	7,0	5,0	3,5	5,0	3,5	6,0	7,0	8,0	6,0	32	0,7	18,8	0,3
Великобританія	5,0	3,5	2,5	4,0	2,0	4,5	6,5	4,5	5,5	4,0	6,5	3,0	8,0	78	0,3	9,0	0,0

Джерело: складено на основі даних Центр стратегічних і міжнародних досліджень [133], Глобального індексу організованої злочинності [93], Transparency International, Chainalysis

Оскільки для характеристики злочинності в країні використано 9 індикаторів, тому виникає об’єктивна необхідність визначення проміжного узагальненого показника для використання його в подальших розрахунках. Аналогічну процедуру доцільно провести й для оцінки узагальненого рівня активності кримінальних угрупувань, що включатиме 4 індикатори.

2 етап. Агрегування показників першої та другої груп в інтегральні показники за допомогою попереднього проведення нормалізації за допомогою методу Харрінгтона з подальшим формуванням узагальнюючих показників шляхом застосування функції Fonseca-Fleming.

Приведення показників вхідної статистичної бази дослідження в розрізі 1-ої та 2-ої груп по співставного вигляду відбувається за допомогою застосування методу Харрінгтона, тобто наступного співвідношення:

$$P_{qi}^{N} = \frac{2 \cdot P_{qi} - \left(\max\limits_{q}\{P_{qi}\} + \min\limits_{q}\{P_{qi}\}\right)}{\max\limits_{q}\{P_{qi}\} - \min\limits_{q}\{P_{qi}\}} \qquad (1.1)$$

де P_{qi}^{N} – нормалізоване значення і-го показника для q-ої країни;

P_{qi} – фактичне значення і-го показника для q-ої країни.

На основі формули 1.1 визначено нормалізовані показники, які подані в таблиці А.1., додатку А.

З метою згортки нормалізованих показників в єдиний інтегральний показник використовується функція Fonseca-Fleming, яка набуває наступного вигляду (формула 1.2).

$$I_q^G = \min_{P_{qi} \epsilon R^n} \begin{pmatrix} 1 - exp\left(-\sum_{i=1}^{n}\left(P_{qi} - \frac{1}{\sqrt{n}}\right)^2\right) \\ 1 - exp\left(-\sum_{i=1}^{n}\left(P_{qi} + \frac{1}{\sqrt{n}}\right)^2\right) \end{pmatrix} \quad (1.2)$$

де I_q^G – інтегральний показник для q-ої країни в розрізі G-ої групи показників;

n- кількість показників в розрізі G-ої групи.

Результати розрахунку інтегральних показників для відображення загального рівня злочинності в країні та активності криміногенних угрупувань, використовуючи формулу Fonseca-Fleming (1.2), подано в таблиці 1.7.

Таблиця 1.7 – Інтегральні показники рівня злочинності та активності криміногенних угрупувань в окремих країнах світу

Країна	Рівень злочинності (X1)	Рівень активності криміногенних угрупувань (X2)	Країна	Рівень злочинності (X1)	Рівень активності криміногенних угрупувань (X2)
Албанія	0,9203	0,8965	Литва	0,8404	0,2489
Білорусь	0,7942	0,6872	Мальта	0,8152	0,8517
Хорватія	0,7738	0,5309	Молдова	0,6215	0,5300
Кіпр	0,8380	0,6290	Морокко	0,9771	0,8488
Чехія	0,7955	0,2140	Нідерланди	0,9583	0,4787
Данія	0,7588	0,3615	Норвегія	0,4694	0,3242
Єгипет	0,9761	0,6617	Польща	0,7391	0,3817
Естонія	0,8769	0,3432	Португалія	0,3502	0,4313
Фінляндія	0,8919	0,6839	Росія	0,9436	0,6734
Франція	0,5111	0,6391	Сербія	0,7215	0,3156
Грузія	0,8513	0,5664	Словенія	0,5751	0,3100
Німеччина	0,9370	0,8011	Іспанія	0,9592	0,3633
Греція	0,8798	0,5590	Швеція	0,6731	0,6074
Угорщина	0,6049	0,6966	Туніс	0,7066	0,5889
Італія	0,9241	0,9011	Туреччина	0,9739	0,7113
Йорданія	0,8109	0,8614	Україна	0,9362	0,3080
Латвія	0,7592	0,3858	Великобританія	0,8348	0,8183

Джерело: розрахунки автора

Наступним етапом є кластеризація країн за рівнем участі їх резидентів у фінансових кібершахрайствах. Крім вищерозрахованих двох індикаторів загального рівня злочинності та активності криміногенних угрупувань, поділ країн на кластери буде здійснюватися також з урахуванням даних про рівень корупції, рівень участі країни в кібератаках, обсягу доходу, який закумульвано на площадках даркнет-ринку, а також про рівень включення країни до міжнародних санкційних списків.

Для кластеризації країн використано агломеративні методи мінімальної дисперсії (ітеративний дівізівний метод k-середніх). Використання методу k-середніх передбачає розрахунок та аналіз наступних показників: середні величини для кожного кластера (усереднення проводиться всередині кластера), евклідові відстані та квадрати евклідових відстаней між кластерами. У розрізі початкових центрів кластерів запропоновано обрати підхід сортування відстані і вибору спостереження на постійних інтервалах. Для розрахунків використано програмний статистичний продукт Statistica 8.

Ключовим моментом кластерного аналізу є визначення обґрунтованої кількості груп країн світу (дві або три), що здійснюється на основі результатів дисперсійного аналізу. У таблиці 1.8 та 1.9 представлені значення міжгрупових (Between SS) та внутрішньогрупових (Within SS) дисперсій ознак.

Про якість даної кластеризації свідчить виконання наступних критеріїв:

– мінімізація значення внутрішньогрупової дисперсії та максимізація значення міжгрупової дисперсій. Виконання даної умови засвідчує рівень належності країн до відповідного кластеру в розрізі кожного індикатора, а також якість проведеної кластеризації;

– максимізація значення критерію Фішера (F) та спрямування до нульового значення ймовірності відхилення нульової гіпотези (p), тобто недоцільність використання певного індикатора для визначення ступеня належності країни до відповідного кластеру.

Таблиця 1.8 – Результати дисперсійного аналізу кластеризації країн світу на 2 групи

Індикатор	Between SS	df	Within SS	df	F	sign. p
X1	0,063	1	0,749	32	2,70462	0,109848
X2	0,143	1	1,571	32	2,91429	0,097485
X3	7211,954	1	3244,164	32	71,13775	0,000000
X4	11,468	1	482,139	32	0,76117	0,389462
X5	409,008	1	1389,547	32	9,41908	0,004352
X6	0,139	1	0,462	32	9,63993	0,003968

Джерело: розрахунки автора

Таблиця 1.9 – Результати дисперсійного аналізу кластеризації країн світу на 3 групи

Індикатор	Between SS	df	Within SS	df	F	sign. p
X1	0,033	2	0,779	31	0,6615	0,523226
X2	0,147	2	1,566	31	1,4582	0,248179
X3	9548,153	2	907,964	31	162,9980	0,000000
X4	24,114	2	469,494	31	0,7961	0,460094
X5	406,276	2	1392,279	31	4,5230	0,018899
X6	0,284	2	0,317	31	13,8818	0,000050

Джерело: розрахунки автора

Таким чином, аналіз результатів групування країн на 2 кластери свідчить про якісно проведену кластеризацію, оскільки значення p-значення в розрізі трьох індикаторів (X1, X2, X4) перевищує допустимий для економічних досліджень рівень 0,05, а для всіх інших інтегральних показників характеристики груп приймає граничний до допустимого рівень. Перехід від двох до трьох кластерів призводить до погіршення якості кластеризації. Отже, неадекватність групування країн світу на 3 кластери призводить до необхідності розгляду 2-кластерного групування досліджуваних об’єктів.

Обґрунтувавши доцільність виділення саме 2 кластерів країн, визначимо склад кожного із виділених кластерів (таблиця 1.10).

Таким, структура країн за кластерами представлена наступним чином: 1 кластер – 14 країн; 2 кластер – 20 країн. Візуалізацію проведеної процедури групування країн світу представлено на рисунку 1.9.

Таблиця 1.10 – Розподіл країн у розрізі 2 виокремлених кластерів

Кластер 1		Кластер 2	
Країна	Відстань від центру кластера	Країна	Відстань від центру кластера
Данія	6,304783	Албанія	4,21450
Естонія	2,847356	Білорусь	2,74840
Фінляндія	6,041784	Хорватія	1,30750
Франція	3,811374	Кіпр	4,57046
Німеччина	4,260769	Чехія	4,75683
Латвія	8,861327	Єгипет	5,36010
Литва	5,204945	Грузія	4,53325
Нідерланди	3,520315	Греція	2,53516
Норвегія	4,679923	Угорщина	1,25265
Португалія	5,605646	Італія	5,27588
Словенія	7,673571	Йорданія	3,30724
Іспанія	6,336485	Мальта	5,60651
Швеція	4,970037	Молдова	4,30121
Великобританія	2,956365	Мороко	3,31009
		Польща	4,93041
		Росія	10,68329
		Сербія	2,74289
		Туніс	2,48588
		Туреччина	2,76711
		Україна	6,70613

Джерело: розрахунки автора

Переходячи до аналізу описових статистик виділених 2 кластерів (рисунок 1.9 – 1 фрагмент) в розрізі середніх значень прослідковуються наступні характерні особливості: середні значення за індикаторами в країнах 1-го кластеру є вищими у порівнянні з 2-им кластером країн.

Variable	Cluster Means (Spreadsheet2.sta)	
	Cluster No. 1	Cluster No. 2
Var1	0,74252	0,83018
Var2	0,49934	0,63113
Var3	73,64286	44,05000
Var4	0,05669	1,23677
Var5	14,72786	7,68050
Var6	0,00000	0,13000

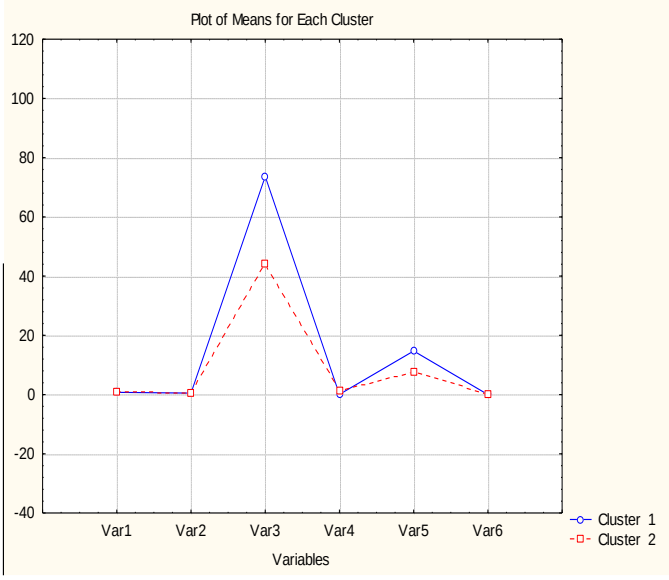


Рисунок 1.9 – Скріншот фрагменту середніх значень вхідних показників кластеризації

Джерело: розрахунки автора

Variable	Descriptive Statistics for Cluster 1 (Spreadsheet2.sta) Cluster contains 14 cases		
	Mean	Standard Deviation	Variance
Var1	0,74252	0,19715	0,0389
Var2	0,49934	0,20562	0,0423
Var3	73,64286	11,61304	134,8626
Var4	0,05669	0,09999	0,0100
Var5	14,72786	7,69965	59,2846
Var6	0,00000	0,00000	0,0000

Variable	Descriptive Statistics for Cluster 2 (Spreadsheet2.sta) Cluster contains 20 cases		
	Mean	Standard Deviation	Variance
Var1	0,83018	0,113201	0,01281
Var2	0,63113	0,231809	0,05374
Var3	44,05000	8,858389	78,47105
Var4	1,23677	5,036755	25,36889
Var5	7,68050	5,707094	32,57092
Var6	0,13000	0,155935	0,02432

Рисунок 1.10 – Скріншот фрагменту описової статистики кластеризації європейських країн на 2 кластери

Джерело: розрахунки автора

Дані рисунків 1.9-1.10 наочно демонструють, що найбільший ефект у розподіл країн на кластери за рівнем ймовірної участі їх резидентів в протиправній діяльності в кіберпросторі є індикатор «питома вага кібератак у світі, ініціатором якої виступила країна» (X4). Зокрема, середнє значення даного показника в кластері 1 становить 0,06 %, тоді як у кластері 2 – 1,24%.

Наступний (четвертий) етап розробленого науково-методичного підходу є побудова дерев класифікації на основі методу одномірного розгалуження

CART, що дозволить визначити тригерні показники та їх значення, на основі яких відбувалося поділ країн світу на кластери

Провівши кластеризацію країн, при реалізації даного етапу постає необхідність у формалізації портретів кластерів країн на основі використання дерев класифікації – методу, що дозволяє передбачати приналежність об'єктів (країн) до відповідного класу категоріальної змінної (кластер 1, 2) залежно від значень однієї чи більше незалежних вхідних предикторів.

Процес побудови дерев класифікації включає здійснення чотирьох кроків:

1.Процедура вибору критеріїв точності прогнозу на основі використання методу однакової апріорної ймовірності.

2. Процедура вибору варіантів розгалуження на основі активізації CART-методу, тобто програми дерев класифікації, яка при побудові дерева здійснює повний перебір усіх можливих варіантів одномірного розгалуження. В якості критерія узгодженості обрано міру Джині, що представляє собою суму усіх попарних добутків відносних розмірів класів, представлених у розглянутій вершині дерев. Значення міри Джині будуть максимальними у випадку однакових розмірів усіх класів.

3. Ідентифікація тригерної точки, за якої необхідно зупинити процедуру розгалуження на основі обраної прямої зупинки процедури розгалуження за методом FACT. Так, розгалуження за предикторними змінними продовжується до того часу, коли кожна термінальна вершина не буде містити не одного неправильно класифікованого об'єкту (країни).

4. Визначення необхідного розміру дерева класифікації за методом глобальної крос-перевірки, коли кількість ітерацій встановлюється за замовчуванням рівною трьом.

Використання методичного інструментарію дерев класифікації в дослідженні здійснюється на основі програмного забезпечення Statistica. Дерева класифікації побудовано для шести ключових індикаторів (X1-X6), які

використані для типологізації країн за рівнем фактичної або ймовірної участі резидентів країни у протиправних кібернетичних правопорушеннях

Першим індикатором є «рівень злочинності» (X1). На рисунку 1.11 показано результат побудови дерева класифікації для даного індикатора. Будь-яек дерево класифікації містить інформацію про номера вершин (node), номера дочірніх вершин на лівій та правій гілках, кількість об'єктів у класах та умову розгалуження (split variable).

Tree Structure (Spreadsheet2.sta)
Child nodes, observed class n's,
predicted class, and split condition for each node

Node	Left branch	Right branch	n in cls 2G	n in cls 1G	Predict. class	Split constant	Split variable
1	2	3	20	14	2G	-0,590035	Var1
2			0	4	1G		
3			20	10	2G		

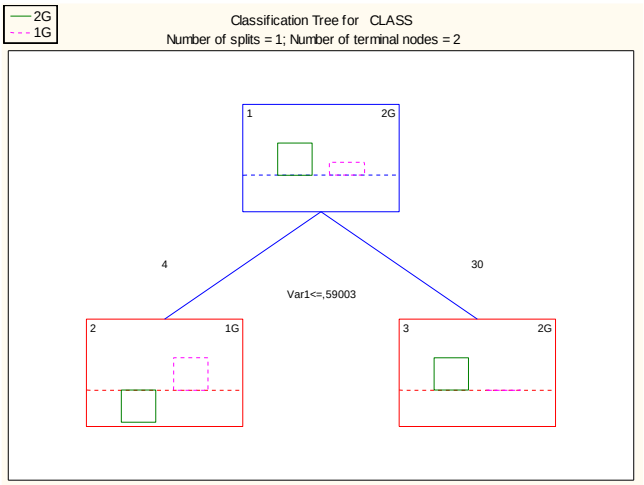


Рисунок 1.11 – Скріншот фрагменту структури дерева класифікації країн в розрізі індикатора «рівень злочинності» (X1)

Джерело: розрахунки автора

На основі аналізу рисунку 1.11 можна зробити висновок, що ліва гілка містить один вузол під номером 2, права – теж один вузол під номером 3. На основі першого рядка рисунку 5 видно, що у першій вершині 20 країн класифіковані до 2 кластеру, 14 до 1 кластеру. Для розгалуження країн за вершинами 2 і 3 використовується значення змінної інтегрального рівня злочинності, яке приймає значення більше «0,590» для країн кластеру 2 і значення не більше «0,590» для країн кластеру 1.

На рисунку 1.12 представлено дерево класифікації для індикатора «рівень активності кримінальних угруповувань» (X2).

Node	Left branch	Right branch	n in cls 2G	n in cls 1G	Predict. class	Split constant	Split variable
1	2	3	20	14	2G	-0,504391	Var2
2			4	9	1G		
3			16	5	2G		

Tree Structure (Spreadsheet2.sta)
Child nodes, observed class n's,
predicted class, and split condition for each node

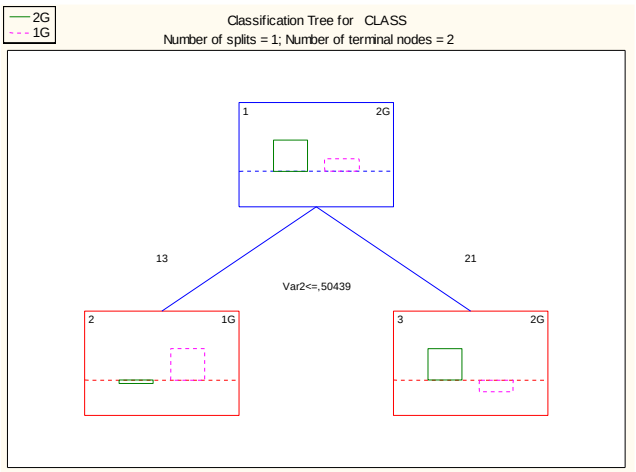


Рисунок 1.12 – Скріншот фрагменту структури дерева класифікації країн в розрізі індикатора «рівень активності кримінальних угруповувань»

Джерело: розрахунки автора

На основі аналізу рисунку 1.12 можна зробити висновок, що ліва гілка містить один вузол під номером 2, права – теж один вузол під номером 3. На основі першого рядка рисунку 5 видно, що у першій вершині 20 країн класифіковані до 2 кластеру, 14 до 1 кластеру. Для розгалуження країн за вершинами 2 і 3 використовується значення змінної інтегрального рівня активності кримінальних угруповувань, яке приймає значення більше «0,504» для країн кластеру 2 і значення не більше «0,504» для країн кластеру 1.

Розрахункові результати, що показані на рисунку 1.13, включають інформацію про дерева класифікації для індикатора «ризик корупції та хабарів» (X3).

Node	Tree Structure (Spreadsheet2.sta) Child nodes, observed class n's, predicted class, and split condition for each node Left branch	Right branch	n in cls 2G	n in cls 1G	Predict. class	Split constant	Split variable
1	2	3	20	14	2G	-56,5000	Var3
2			20	0	2G		
3			0	14	1G		

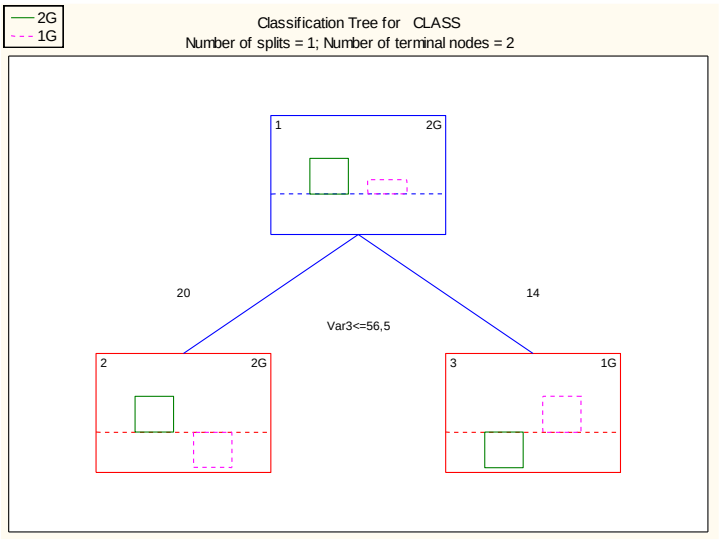


Рисунок 1.13 – Скріншот фрагменту структури дерева класифікації країн в розрізі індикатора «ризик корупції та хабарів» (X3)

Джерело: розрахунки автора

На основі аналізу рисунку 1.13 можна зробити висновок, що ліва гілка містить один вузол під номером 2, права – теж один вузол під номером 3. На основі першого рядка рисунку 5 видно, що у першій вершині 20 країн класифіковані до 2 кластеру, 14 до 1 кластеру. Для розгалуження країн за вершинами 2 і 3 використовується значення змінної «ризик корупції та хабарів», яке приймає значення не більше «56,500» для країн кластеру 2 і значення більше ««56,500» для країн кластеру 1.

Для формування профілей кластерів країн, розглянемо результати побудови дерев класифікації в розрізі індикатора «загальний дохід, який отримано на даркнет-ринку» (X5).

Node	Tree Structure (Spreadsheet2.sta) Child nodes, observed class n's, predicted class, and split condition for each node						
	Left branch	Right branch	n in cls 2G	n in cls 1G	Predict. class	Split constant	Split variable
1	2	3	20	14	2G	-5,41000	Var5
2			10	0	2G		
3	4	5	10	14	1G	-0,05000	Var6
4			6	14	1G		
5			4	0	2G		

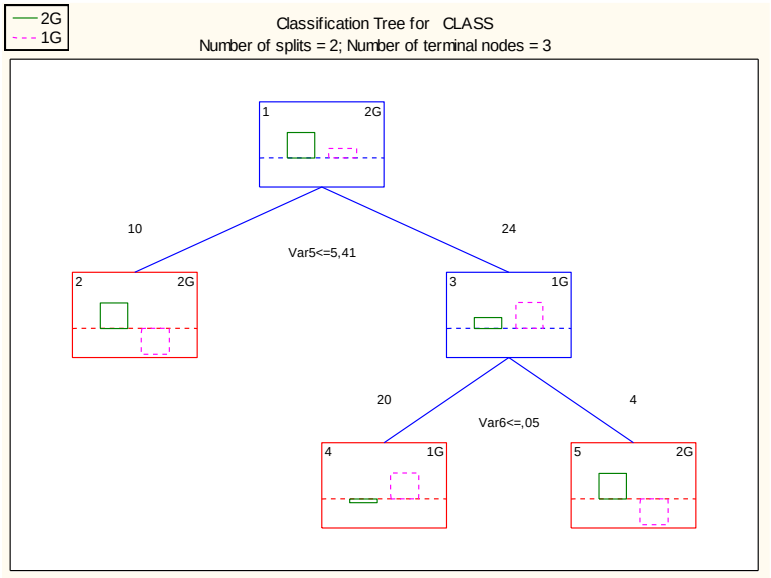


Рисунок 1.14 – Скріншот фрагменту структури дерева класифікації країн в розрізі індикаторів «загальний дохід, який отримано на даркнет-ринку» (X5) та «міжнародні санкції, які накладені на країну» (X6)

Джерело: розрахунки автора

На основі аналізу рисунку 1.14 можна зробити висновок, що ліва гілка містить один вузол під номером 2, права – теж один вузол під номером 3. Для розгалуження країн за вершинами 2 і 3 використовується значення змінної «загальний дохід, який отримано на даркнет-ринку» (X5), яке приймає значення не більше «5,4100» для країн кластеру 2 і значення більше «5,4100» для країн кластеру 1. Подальше виділення країн кластеру 1 відбувається на основі застосування змінної «міжнародні санкції, які накладені на країну» (X6), яка має приймати значення не менше «0,05», та віднесення країн до кластеру 2 в іншому випадку.

Отже, за результатами побудови дерев класифікації отримані основні результати, які представлені в таблиці.

Таблиця 1.11 – Результати побудови дерев класифікації

Назва індикатора	1 кластер	2 кластер
Рівень злочинності (X1)	< 0,590	> 0,590
Рівень активності кримінальних угруповувань (X2)	< 0,504	> 0,504
Ризик корупції та хабарів (X3)	> 56,500	< 56,500
Питома вага кібератак у світі, ініціатором якої виступила країна (X4)		
Загальний дохід, який отримано на даркнет-ринку (X5)	< 5,410	> 5,410
Міжнародні санкції, які накладені на країну (X6)	< 0,05	> 0,05

Джерело: розрахунки автора

П’ятий етап розробленого науково-методичного підходу є визначення інтегрального показника на основі згортки нормалізованих показників за допомогою методу Харрінгтона (рис. 1.15).

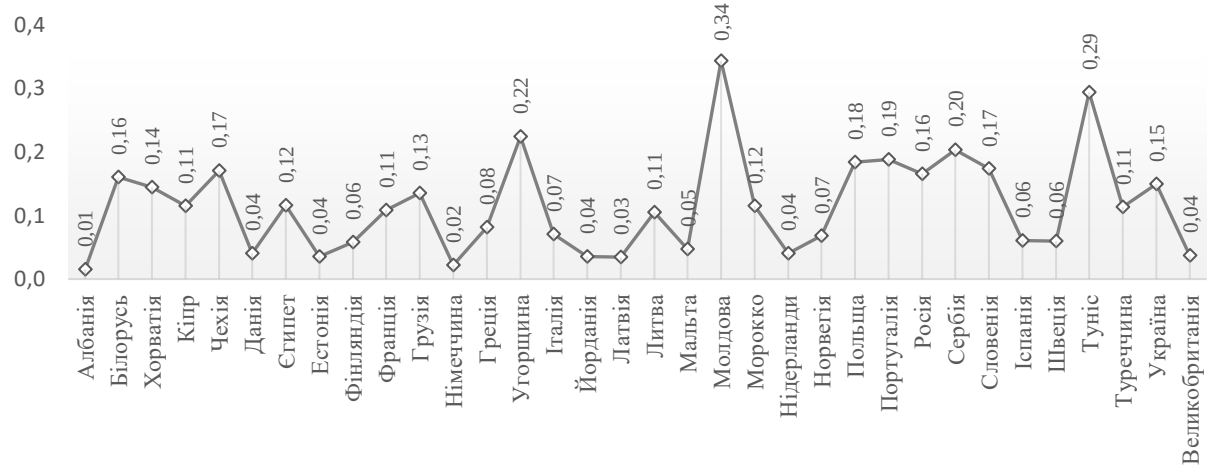


Рисунок 1.15 – Інтегральний рівень участі резидентів країни у здійсненні фінансових кібернетичних шахрайств

Джерело: розрахунки автора

Дані рисунку 1.15 демонструють, що з поміж 34 аналізованих країни світу найвищий рівень участі резидентів у здійсненні фінансових кібернетичних шахрайств має Молдова (0,34 ум.од.), Туніс (0,29 ум.од.) та Угорщина (0,22 ум.од.). Скандинавські країні (Данія – 0,04 ум.од, Фінляндія – 0,06 ум.од., Норвегія – 0,07 ум.од.) та інші високорозвинуті країни (Німеччина

– 0,02 ум.од., Нідерланди – 0,04 ум.од., Великобританія – 0,04 ум.од.) мають низький ступінь залученості громадян до протиправних шахрайських діянь у кіберпросторі.

Варто відзначити, що розширення переліку країн світу для практичної дозволило б масштабувати цей науково-методичний підхід та отримати загальний стан рівня залученості резидентів країни в протиправну діяльність у кіберпросторі на світовому рівні.

Підсумовуючи, зазначимо, що розроблений науково-методичний підхід до визначення ступеня залученості резидентів країни до здійснення фінансових кібернетичних шахрайств дозволяє визначити перелік країн світу, з резидентами яких має бути посилений регуляторний контроль з боку контролюючих та наглядових органів. Крім цього, співпраця з резидентами тих країн, які мають високий ступінь залученості до протиправних шахрайських дій у кіберпросторі, також несе репутаційні ризики для іншої країни.

Висновки до розділу 1

На основі проведеного бібліометричного аналізу наукових публікацій присвячених вивченню питання кіберзагроз та інших споріднених понять у системі економічних відносин виявлено, що протягом останніх десяти років науковий інтерес до вивчення питань кіберзагроз постійно та динамічно зростає. Основою бібліометричного аналізу виступила міжнародна база даних наукових публікацій Scopus. У 2022 році опубліковано 690 наукових публікацій з досліджуваної тематики, що на 88,5% більше порівняно з 2018 роком. Науковці з США, Великобританії та Індії є найбільш активними у дослідженні питання кібербезпеки та кіберзахисту.

За результатами аналізу частоти використання ключових слів у наукових статтях, присвячених питанням кібербезпеки в економічному вимірі та проіндексованих у наукометричній базі даних Scopus, у роботі сформовано 4 наукових кластери: 1) кластер, присвячений вивченню кібербезпеки та складові її забезпечення; 2) кластер, сфокусований на дослідженні та пошуку засобів та технологій ідентифікації кіберзагроз, а також протидії кібератакам; 3) кластер, який спеціалізується на вивченні об'єктів кіберзахисту, які мають пріоритетне значення в умовах діджиталізації економіки; 4) кластер, присвячений дослідженню впливу кіберзагроз на життєдіяльність людини. За результатами контекстуально-часового аналізу з питань кібершахрайств встановлено, що протягом 2019-2020 років основна увага почала приділятися технологіям та засобам забезпечення кібербезпеки, а починаючи з 2021 року науковий інтерес був зміщений на дослідження кіберфізичних систем, використання технологій штучного інтелекту для протидії кібератакам, вивчення ролі кіберзахисту при впровадженні інтернету речей.

Кіберзагрозу запропоновано розглядати як дію наявних та/або потенційно можливих дестабілізуючих факторів та умов навмисного або випадкового порушення безпеки функціонування громадянина, економічних суб'єктів та держави у кіберпросторі. У роботі проведено змістову розмежування таких понять як «кіберзагроза», «кіберінцидент», «кібератака», «кіберзлочин». Розширено перелік об'єктів кібербезпеки за рахунок інформаційно-комунікаційних засобів фізичних осіб, які використовуються ними для реалізації суспільно та життєвоважливих потреб під час використання кіберпростору.

У роботі визначено основні чинники та передумови зростання кіберінцидентів на глобальному рівні, а саме: потужний розвиток електронних обчислювальних машин, мобільних пристроїв, збільшення кількості пристроїв, підключених до мережі Інтернет; неможливість відслідкувати територію / країну здійснення кібератаки; збільшення кількості користувачів соціальних мереж, які містять персональні дані; використання застарілого та

неліцензійного програмного забезпечення; стрімке зростання технологій Інтернет речей; збільшення питомої ваги бізнес-процесів, які передаються на управління третім особам; використання хмарних технологій для зберігання та передачі даних; розширене використання робототехніки або алгоритмів для здійснення автоматичної торгівлі та розробки додатків; збільшення використання віртуальних та цифрових валют.

Аналіз значущих кіберінцидентів у світі протягом 2005-2020 рр. виявлено, що 41,8% кіберіндидентів здійснено резидентами з Китаю, при цьому 40% з них були направлені на об'єкти критичної інфраструктури у сфері публічного управління та 36% – на об'єкти приватного сектору. Крім Китаю, найбільшими спонсорами кібератак у світі є росія та Іран, сукупно на ці три країни припадає 78,5% від всіх кіберінцидентів. Встановлено, що переважна більшість кібератак були здійснені у формі шпіонажу. Найбільша кількість кіберінцидентів у світі була реалізована у вівторок, при цьому фіксуючи збільшення даних протиправних дій у такі дні як 19,24,25.

У роботі проведено типологізацію країн за рівнем участі їх резидентів у здійсненні фінансових кібернетичних шахрайств на основі аналізу показників, що характеризують різні види злочинності та активність кримінальних угруповувань в країні, а також стану корупції, активності на даркнет-ринку, рівня кіберзлочинності та накладення на країну міжнародних санкцій. За результатами використання ітеративного дивізівного методу k-середніх та дерев класифікацій виокремлено 2 групи кластерів: 1-й кластер (14 країн: Данія, Естонія, Фінляндія, Франція, Німеччина, Латвія та інші) та 2 -й кластер (20 країн: Албанія, Білорусь, Кіпр, Угорщина, Молдова, Морокко, Україні та інші).

Для віднесення країн до кластеру 1 необхідними та достатніми є наступні умови: значення змінної «ризик корупції та хабарів» має приймати значення більше 56,500, значення змінної «загальний дохід, який отримано на даркнет-ринку» – менше 5,4100, значення змінної «міжнародні санкції, які накладені на країну» – менше 0,05, значення змінної інтегрального рівня

активності кримінальних угруповувань, яке приймає значення менше 0,504, значення змінної інтегрального рівня характеристики різних видів злочинності – не більше 0,590. За протилежних умов вищезазначених індикаторів країни віднесено до кластеру 2.

Основні положення першого розділу дисертаційної роботи опубліковано автором в роботах [2, 19, 29, 34].

РОЗДІЛ 2 РОЗВИТОК МЕТОДИЧНОГО ІНСТРУМЕНТАРІЮ ОЦІНЮВАННЯ ПЕРЕДУМОВ ТА ПОТОЧНОГО СТАНУ КІБЕРЗАГРОЗ В УМОВАХ ДІДЖИТАЛІЗАЦІЇ ЕКОНОМІКИ

2.1. Методичний підхід до визначення детермінантів поширення кібершахрайств в умовах цифровізації економіки

Карантинні заходи, спричинені пандемією, спровокували збільшення розрахунків в мережі Інтернет, зростання обсягів електронних фінансових послуг, нарощення використання криптовалют та альткоїнів як платіжного засобу та інвестиційного інструменту. Дані тенденції вказують на прискорення темпів цифровізації економіки та трансформації підходів до організації бізнес-процесів. За цих умов цифрова трансформація відкриває як нові можливості для підвищення ефективності суб'єктів господарювання і зниження їх витрат за рахунок оптимізації транзакцій, так і загрози для стабільного їх функціонування – поширення кібератак та зростання частоти їх здійснення. У 2020 році в Україні зафіксовано близько мільйона випадків, пов'язаних з кіберзагрозами, сформовано достатньо сприятливі умови для "відмивання" брудних грошей (67 позиція з поміж 141 країни світу за даними Базельського індексу протидії легалізації), що має значущий дестабілізаційний ефект на функціонування національної економіки та враховуючи швидке перетікання із одної галузі господарювання до іншої, що в кінцевому підсумку виступає загрозою для національної безпеки держави [5]. Не зважаючи на велику кількість публікацій, присвячених окресленій проблематиці, у науковій літературі досі не здійснена спроба формалізації детермінант поширення кібер шахрайства у сфері фінансових послуг.

За результатами виконання науково-дослідної роботи розроблено науково-методичний підхід до формалізації факторів стрімкого поширення кібершахрайств на основі методів машинного навчання SVM. Реалізація запропонованого підходу передбачає покрокове виконання наступних етапів:

– збір та обробка статистичних даних, що характеризують обсяг кіберзлочинних операцій у розрізі різних методів здійснення кібератаки;

– приведення вхідних показників до єдиного співтавного вигляду;

– побудова інтегрального індексу кіберзагроз методом групового врахування аргументів Івахненка, де в якості опорної функції використовується адитивно-мультиплікативна згортка суми сум квадратів стандартизованих значень вхідних індикаторів;

– визначення потенційних факторів впливу на поширення кібершахрайств та збір по ним статистичних даних;

– визначення специфічних особливостей інтегрального індексу кіберзагроз та детермінант поширенння кіберзагроз на основі методів описової статистики;

– побудова SVM-моделі машинного навчання двох типів (epsilon-SVM regression та nu-SVM regression) в розрізі чотирьох специфікацій опорних векторів: лінійні, поліноміальні, радіально-базисні функції (RBF) та сигмоподібні.

Перший етап передбачає проведення збору та систематизації статистичних даних, що характеризують фактичні кібератаки, проведені у 2020 році. Об'єктом дослідження слугували 21 країна Європи. Джерелом первинної інформації слугували дані компанії Comparitech [152]. Для відображення інтенсивності здійснення кібератак у розрізі країн Європи використано наступні індикатори: частка мобільних пристроїв, заражених шкідливим програмним забезпеченням, % (I_1); частка користувачів, атакованих вірусами троян через інтернет банкінг, % (I_2); частка користувачів, атакованих мобільними троянами-вимагателями, % (I_3); частка користувачів, атакованих банківським шкідливим програмним забезпеченням, % (I_4); частка користувачів, атакованих троянськими програмами-вимагателями, % (I_5); частка комп'ютерів, заражених принаймні однією атакою зловмисного програмного забезпечення (в Інтернеті), % (I_6); частка комп'ютерів, які стикаються принаймні з однією локальною атакою шкідливого програмного забезпечення, % (I_7); частка мобільних користувачів, атакованих через веб-

джерела, % (I_8); частка атак на Telnet протокол, % (I_9); частка атак з боку криптомайнерів, % (I_{10}); частка атак на SSH протокол, % (I_{11}); частка спам-листів за країною відправника (за рік), % (I_{12}); частка країн, на які націлені зловмисні розсилки (щороку), %(I_{13}); частка комп'ютерів, атакованих фішингом (щорічно), % (I_{14}); загальна кількість виявлених шкідливих файлів, пов'язаних із Covid 19 (I_{15}). Зведена статистична інформація щодо випадків кібершахраства у розрізі різних методів для країн Європи представлена у додатку Б (таблиця Б.1), а основні результати подано в таблиці 2.1.

Таблиця 2.1 – Інформація щодо стану кіберзлочинності в європейських країнах у 2020 році у розрізі методів та способів їх здійснення

Показник	Топ-3 країн з найвищими показниками			Топ-3 країн з найнижчими показниками		
	1 місце	2 місце	3 місце	1 місце	2 місце	3 місце
Частка мобільних пристроїв, заражених шкідливим програмним забезпеченням (I_1)	Румунія (5,04%)	Іспанія (4,31%)	Словаччина (3,5%)	Фінляндія (1,06%)	Данія (1,33%)	Німеччина (1,63%)
Частка користувачів, атакованих банків-ським шкідливим програмним забезпеченням (I_4)	Португалія (0,9%)	Греція (0,5%)	Болгарія (0,5%)	Ірландія (0,1%)	Данія (0,1%)	Угорщина (0,2%)
Частка комп'ютерів, заражених принаймні однією атакою шкідливого програмного забезпечення (I_6)	Латвія (7,31%)	Франція (6,71%)	Іспанія (5,92%)	Данія (1,33%)	Ірландія (1,35%)	Швеція (1,435%)
Частка атак з боку криптомайнерів (I_{10})	Латвія (0,73%)	Болгарія (0,56%)	Словаччина (0,5%)	Данія (0,11%)	Німеччина (0,12%)	Румунія (0,14%)
Частка спам-листів за країною відправника (I_{12})	Німеччина (10,97%)	Франція (5,97%)	Нідерланди (4,00%)	Данія (0,07%)	Словаччина (0,19%)	Швеція (0,19%)
Частка комп'ютерів, атакованих фішингом (I_{14})	Португалія (19,73%)	Франція (17,9%)	Бельгія (16,4%)	Данія (3,26%)	Швеція (3,35%)	Ірландія (3,42%)
Загальна кількість виявлених шкідливих файлів, пов'язаних із Covid 19 (I_{15})	Іспанія (1825476)	Італія (578779)	Німеччина (314459)	Латвія (78)	Болгарія (301)	Словаччина (450)

Джерело: складено автором на основі даних компанії Comparitech [152]

На основі аналізованих у таблиці 2.1 видів кібератак, зауважимо, що найбільшими країнами-жертвами у 2020 році були Іспанія, Португалія та Латвія, тоді як найменша кількість кібератак зафіксована у таких країнах як Данія, Швеція та Ірландія. Зокрема, 19,73% комп'ютерів у Португалії були атаковані таким інтернет-шахрайством як фішинг, тоді як у Данії – лише 3,26%. Перехід на дистанційний режим роботи та інтенсивне користування електронними послугами, спричиненого пандемією COVID-19, призвів до збільшення масштабів кібершахрайства у світі. Щодо країн Європи, то найбільша кількість виявлених шкідливих файлів, пов'язаних із пандемією Covid 19 виявлена у Іспанії, Італії та Німеччині.

Другий етап передбачає визначення інтегрального індексу кіберзагроз методом групового врахування аргументів Івахненка, який ґрунтується на застосуванні індуктивних алгоритмів математичного моделювання багатопараметричних даних. В основі даного методу лежить рекурсивна селективна процедура здійснення відбору математичних моделей, на базі яких формалізуються більш складні моделі, при цьому точність та адекватність процесу моделювання поступово збільшується на кожному наступному кроці шляхом ускладнення вихідної моделі. Для побудови інтегрального індексу в якості опорної функції розглядається сума сум квадратів стандартизованих значень вхідних індикаторів.

Крок 2.1. Проведення стандартизації вхідних індикаторів на основі застосування програмного пакету Statistica інструментарію Data/ Standartize. В основі даного підходу обробки вхідних даних лежить метод Z-нормалізації, який передбачає зважження відхилення фактичного рівня кожного показника від середнього рівня за множиною розглянутих країн до середньоквадратичного відхилення, за наступним співвідношенням (формула 2.1.).

$$k_{cj} = \frac{I_{cj} - \overline{I_J}}{\sigma_j} \quad (2.1)$$

де k_{cj} – стандартизоване значення j-го індикатора поширення кіберзагроз в розрізі с-ої країни;

I_{cj} – фактичне значення j-го індикатора поширення кіберзагроз в розрізі с-ої країни;

$\overline{I_J}$ – середнє арифметичне значення j-го індикатора поширення кіберзагроз на множині значень розглянутої сукупності країн;

σ_j – середнє квадратичне відхилення в розрізі j-го індикатора поширення кіберзагроз на множині значень розглянутої сукупності країн.

Використовуючи формулу 2.1, розраховано стандартизовані значення показників, що характеризують рівень кіберзагроз в країнах Європи, подано в таблиці 2.2.

Таблиця 2.2 – Стандартизовані значення детермінант поширення кіберзагроз станом на 2020 рік

Країни	I1	I2	I3	I4	I5	I6	I7	I8	I9	I10	I11	I12	I13	I14	I15
AUS	-0,7	-0,9	-0,5	-0,5	-0,4	-0,2	-0,3	-0,7	-0,9	-0,5	-0,5	-0,4	-0,2	-0,3	-0,7
BEL	-0,6	-0,6	-0,5	-0,5	-0,5	1,1	-0,2	-0,6	-0,6	-0,5	-0,5	-0,5	1,1	-0,2	-0,6
BGR	-0,4	1,5	-0,5	-0,4	-0,5	0,1	-0,3	-0,4	1,5	-0,5	-0,4	-0,5	0,1	-0,3	-0,4
HRV	-0,6	0,3	-0,5	-0,1	-0,5	-0,4	-0,3	-0,6	0,3	-0,5	-0,1	-0,5	-0,4	-0,3	-0,6
DNK	-0,7	-1,2	-0,6	-0,6	-0,6	-1,6	-0,3	-0,7	-1,2	-0,6	-0,6	-0,6	-1,6	-0,3	-0,7
FIN	-0,7	0,3	-0,6	-0,5	-0,6	-0,8	-0,3	-0,7	0,3	-0,6	-0,5	-0,6	-0,8	-0,3	-0,7
FRA	0,0	-0,9	2,5	1,7	-0,2	1,4	-0,3	0,0	-0,9	2,5	1,7	-0,2	1,4	-0,3	0,0
DEU	0,3	-1,1	3,0	3,6	2,4	-0,3	0,4	0,3	-1,1	3,0	3,6	2,4	-0,3	0,4	0,3
GRC	3,4	1,1	-0,5	-0,5	0,1	1,0	-0,3	3,4	1,1	-0,5	-0,5	0,1	1,0	-0,3	3,4
HUN	-0,3	0,7	-0,4	-0,3	-0,5	0,8	-0,3	-0,3	0,7	-0,4	-0,3	-0,5	0,8	-0,3	-0,3
IRL	-0,7	-0,7	-0,4	-0,5	-0,6	-1,5	-0,3	-0,7	-0,7	-0,4	-0,5	-0,6	-1,5	-0,3	-0,7
ITA	1,8	-0,5	0,4	-0,2	1,6	0,9	1,1	1,8	-0,5	0,4	-0,2	1,6	0,9	1,1	1,8
LVA	-0,6	2,5	-0,6	-0,3	-0,5	0,4	-0,3	-0,6	2,5	-0,6	-0,3	-0,5	0,4	-0,3	-0,6
NLD	-0,3	-0,7	0,8	0,9	-0,5	-1,2	-0,3	-0,3	-0,7	0,8	0,9	-0,5	-1,2	-0,3	-0,3
POL	0,2	0,4	-0,3	0,2	-0,3	0,3	-0,3	0,2	0,4	-0,3	0,2	-0,3	0,3	-0,3	0,2
PRT	-0,6	0,8	-0,5	-0,5	0,2	1,8	-0,3	-0,6	0,8	-0,5	-0,5	0,2	1,8	-0,3	-0,6
ROU	0,2	-1,0	-0,4	-0,4	-0,2	-1,0	-0,3	0,2	-1,0	-0,4	-0,4	-0,2	-1,0	-0,3	0,2
SVK	-0,6	1,1	-0,6	-0,5	-0,6	0,4	-0,3	-0,6	1,1	-0,6	-0,5	-0,6	0,4	-0,3	-0,6
ESP	0,4	0,3	-0,1	0,4	2,9	0,5	4,1	0,4	0,3	-0,1	0,4	2,9	0,5	4,1	0,4
SWE	-0,3	-0,7	-0,3	-0,5	-0,6	-1,5	-0,3	-0,3	-0,7	-0,3	-0,5	-0,6	-1,5	-0,3	-0,3
GBR	0,7	-0,6	0,7	-0,2	-0,2	-0,2	-0,3	0,7	-0,6	0,7	-0,2	-0,2	-0,2	-0,3	0,7

Джерело: розрахунки автора

Крок 2.2 Агрегування стандартизованих рівнів індикаторів поширення кіберзагроз до єдиного інтегрального показника методом групового врахування аргументів Івахненка, тобто розрахунку суми сум квадратів стандартизованих значень вхідних індикаторів наступним чином:

$$IK_c = \sum_{j=1}^{J} \sum_{j=1}^{J} (k_{cj})^2 \qquad (2.2)$$

де IK_c – інтегральний індекс кіберзагроз в розрізі с-ої країни.

Результати обчислень за формулою (2.2) візуалізуємо на рисунку 2.1, де представимо динаміку індексу кіберзагроз у розрізі розглянутих країн Європи станом на 2020 рік, у тому числі з урахуванням впливу пандемії на захищеність інформаційного простору.

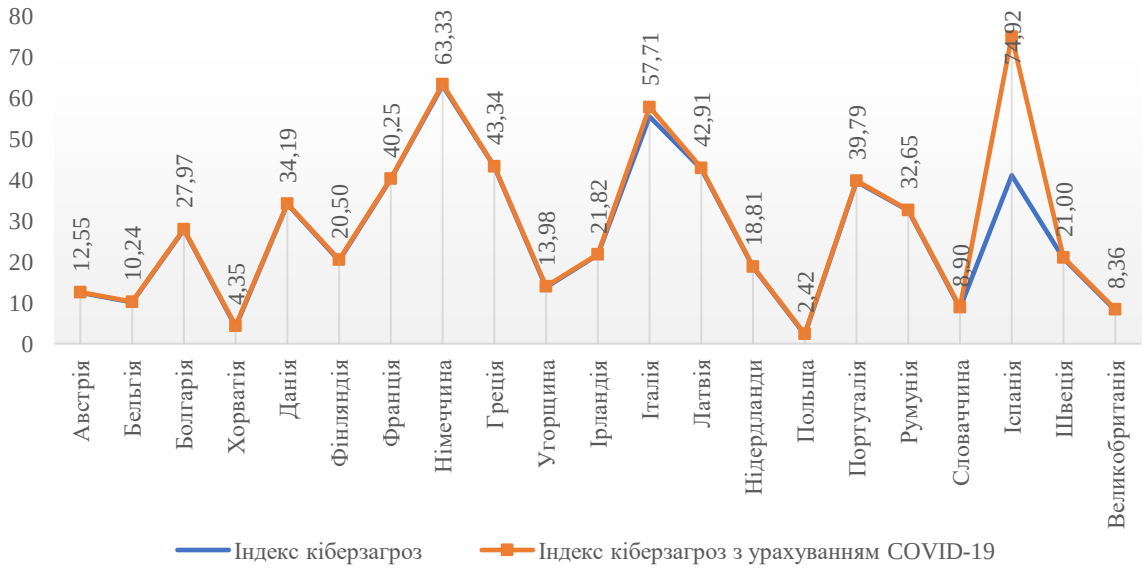


Рисунок 2.1 – Динаміка індексу кіберзагроз у розрізі країн Європи, а також з урахуванням впливу пандемії Covid 19 станом на 2020 рік

Джерело: розрахунки автора

Проведені розрахунки засвідчили, що нерівномірність здійснення кібератак у розрізі країн Європи, оскільки індекс кіберзагроз у 2020 році

варіюється від 2,4 ум. од до 74,9 ум.од. На основі агрегування 15 вхідних індикаторів, що характеризують різні способи здійснення шахрайства в інформаційному просторі, отримано, що найбільший рівень кіберзагроз у 2020 році спостерігається у таких країнах як Іспанія (74,9 ум.од.), Німеччина (63,3 ум.од.), Італія (57,7 ум.од.), Латвія (42,9 ум.од.) та Франція (40,2 ум.од.).

З метою детального аналізу динаміки інтегрального оцінювання рівня кіберзагроз у розрізі країн Європи розглянемо таблицю частот (рисунок 2.2). Так, найбільша кількість країн серед розглянутої множини характеризуються рівнем індексу кіберзагроз в межах від 0 до 10, від 10 до 20 та від 20 до 30 (по 4 країни, тобто 19,05% вибірки відповідно), що свідчить про низький рівень досліджуваного показника. Лише незначна кількість країн (всього 3 серед досліджуваної множини країн Європи) з рівнями від 50 до 60, від 60 до 70 та від 70 до 80, що свідчить про високий рівень кібернебезпеки.

	Frequency table: cyber threat index (cyber threat index SVM.sta) K-S d=,15528, p> .20; Lilliefors p<,15					
Category	Count	Cumulative Count	Percent of Valid	Cumul % of Valid	% of all Cases	Cumulative % of All
-10,0000<x<=0,000000	0	0	0,00000	0,0000	0,00000	0,0000
0,000000<x<=10,00000	4	4	19,04762	19,0476	19,04762	19,0476
10,00000<x<=20,00000	4	8	19,04762	38,0952	19,04762	38,0952
20,00000<x<=30,00000	4	12	19,04762	57,1429	19,04762	57,1429
30,00000<x<=40,00000	3	15	14,28571	71,4286	14,28571	71,4286
40,00000<x<=50,00000	3	18	14,28571	85,7143	14,28571	85,7143
50,00000<x<=60,00000	1	19	4,76190	90,4762	4,76190	90,4762
60,00000<x<=70,00000	1	20	4,76190	95,2381	4,76190	95,2381
70,00000<x<=80,00000	1	21	4,76190	100,0000	4,76190	100,0000
Missing	0	21	0,00000		0,00000	100,0000

Рисунок 2.2 – Таблиця частот індексу кіберзагроз на множині розглянутих країн світу станом на 2020 рік

Джерело: розрахунки автора

Третім етапом запропонованого підходу є визначення детермінант поширенння кіберзагроз. У межах даної роботи для математичної формалізації детермінант поширення кібершахрайств запропоновано використати наступні змінні:

– частка населення, яка користується послугами онлайн банкінгу (Z1);

– індикатор розвитку мобільного широкосмугового доступу, розрахований як середнє зважене нормалізованих показників: рівень покриття 4G (25%), рівень використання мобільного широкосмугового доступу (25%) і рівень готовності впроваджувати 5G (50%) (Z2);

– індикатор рівня навичок в Інтернеті, розрахований як середнє зважене нормалізованих показників: базові цифрові навички (33%), Вищі базові навички роботи в Інтернеті (33%) і базові навички програмного забезпечення (33%) (Z3);

– індикатор поглиблених навичок та вмінь розрахований як середнє зважене нормалізованих показників: частка фахівців у сфері інформаційно-комунікаційних технологіях (33%), частка фахівців-жінок у сфері інформаційно-комунікаційних технологіях (33%) і кількість випускників зі сфери інформаційно-комунікаційних технологій (33%) (Z4);

– індикатор онлайн діяльності розраховується як середньозважена сума нормованих показників: новини (16,6%), музика, відео та ігри (16,6%), відео на вимогу (16,6%), відеодзвінки (16,6%), соціальні мережі (16,6%)), і проведення онлайн-курсів (16,6%) (Z5);

– індикатор ділової онлайн активності, що визначається як середньо зважена сума нормалізованих показників: обмін електронною інформацією (16,7%), соціальні медіа (16,7%), великі дані (33,3%) і хмарні технології (33,3%) (Z6).

Станом на 2020 рік значення вищеперерахованих показників у розрізі країн Європи подано в таблиці 2.3.

Таблиця 2.3 – Детермінанти поширення кіберзагроз кіберзагроз на множині розглянутих країн світу станом на 2020 рік

Country	Banking	Mobile broadband	Internet User Skills	Advanced Skills and Development	Activities online	Business digitisation
	Z1	Z2	Z3	Z4	Z5	Z6
AUS	71,54	50,15	64,49	48,97	41,82	35,75
BEL	78,85	34,16	58,29	42,49	48,29	67,34
BGR	12,62	31,33	25,80	42,03	40,90	20,54
HRV	58,75	33,70	54,31	44,00	53,85	39,57
DNK	93,53	57,93	71,29	51,26	65,33	65,57
FIN	95,20	76,59	76,46	80,42	69,34	79,35
FRA	73,33	51,50	54,74	40,13	33,39	46,93
DEU	65,72	65,31	66,92	45,92	45,46	38,95
GRC	40,33	33,02	47,25	22,33	49,34	34,48
HUN	58,11	61,13	45,91	37,76	53,92	21,78
IRL	74,59	50,82	53,32	59,48	53,39	64,66
ITA	48,05	63,36	40,08	24,83	40,11	34,11
LVA	83,10	56,13	41,30	28,74	45,53	30,45
NLD	94,36	34,45	78,17	50,15	63,36	75,68
POL	58,76	46,32	40,93	33,61	41,46	25,03
PRT	55,67	35,42	51,80	23,73	48,53	40,50
ROU	11,35	40,73	27,23	39,08	35,70	25,41
SVK	66,11	48,81	50,15	33,47	40,57	33,25
ESP	60,50	49,39	57,06	38,06	56,31	43,44
SWE	86,59	49,43	71,90	71,55	68,78	62,11
GBR	81,30	46,77	74,46	51,55	62,98	58,61

Джерело: складено на основі даних European Commission [82]

Провести більш детальний ґрунтовний детермінант поширення кіберзагроз дозволить побудова діаграма (рис. 2.3), яка свідчить про найбільшу волатильність індикатора Z1 (частка населення, яка користується послугами онлайн банкінгу), значення якого за 21 країнами світу коливається в межах від 11 до 95. В той же час, найменшу волатильність має індикатор Z5 (індикатор онлайн діяльності), що приймає значення в межах від 33 до 69. Зазначені висновки можна також зробити, проаналізувавши описові статистики детермінант поширення кіберзагроз у розрізі країн Європи станом на 2020 рік, представлені на рисунку 2.4.

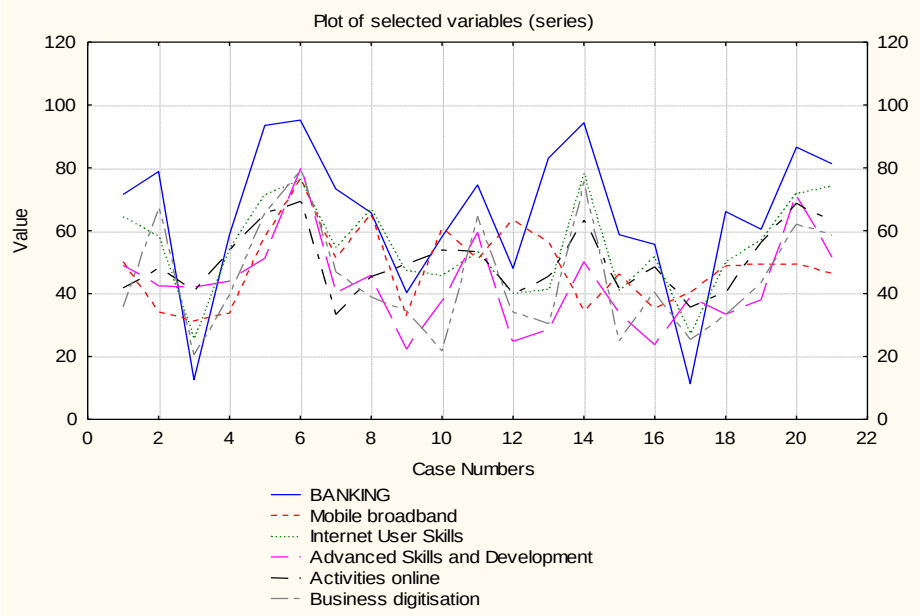


Рисунок 2.3 – Варіація значень детермінант поширення кіберзагроз на множині розглянутих країн світу станом на 2020 рік

Джерело: розрахунки автора

Variable	Descriptive Statistics (cyber threat index SVM.sta)								
	Valid N	Mean	Median	Mode	Sum	Minimum	Maximum	Std.Dev.	Coef.Var.
Banking	21	65,15940	66,10540	Multiple	1368,348	11,34820	95,20090	23,23360	35,65656
Mobile broadband	21	48,40275	49,38920	Multiple	1016,458	31,33480	76,58660	12,27426	25,35860
Internet User Skills	21	54,85063	54,30810	Multiple	1151,863	25,80109	78,17180	15,14183	27,60557
Advanced Skills and Development	21	43,31189	42,03000	Multiple	909,550	22,32950	80,42470	14,68059	33,89505
Activities online	21	50,39805	48,53089	Multiple	1058,359	33,38751	69,33851	10,77735	21,38445
Business digitisation	21	44,92810	39,56651	Multiple	943,490	20,54443	79,34860	18,14500	40,38675
cyber threat index	21	28,57143	21,82482	Multiple	600,000	2,41716	74,92434	20,09377	70,32818

Рисунок 2.4 – Описові статистики детермінант поширення кіберзагроз на множині розглянутих країн світу станом на 2020 рік

Джерело: розрахунки автора

На основі рисунку 2.4 можна стверджувати, що серед розглянутих 7 детермінант поширення кіберзагроз в розрізі лише 3 (рівень розвитку мобільного широкосмугового доступу, рівень навичок населення в Інтернеті, обсяг онлайн діяльності) спостерігається однорідність розглянутої вибірки країн, оскільки значення коефіцієнту варіації не перевищує рівня 33%. В розрізі інших детермінант, а особливо інтегрального індексу кібербезпеки спостерігається досить висока нерівномірність та різновекторність країн.

Наступним етапом запропонованого науково-методичного підходу є побудова SVM-моделей машинного навчання двох типів (epsilon-SVM regression та nu-SVM regression) в розрізі чотирьох специфікацій опорних векторів: лінійні, поліноміальні, радіально -базисні функції (RBF) та сигмоподібні на базі даних вибіркової сукупності країн світу. Для реалізації даного етапу розглянемо спочатку математичне підґрунтя побудови та специфікацію зазначених моделей.

У регресії необхідно оцінити функціональну залежність залежної змінної y від набору незалежних змінних x. Він передбачає, як і інші задачі регресії, що зв'язок між незалежною та залежною змінними задається детермінованою функцією f з урахуванням деяких адитивних шумів:

$$y = f(x) + noise \tag{2.3}$$

Завдання полягає в тому, щоб знайти функціональну форму для f, яка може правильно передбачити нові випадки, які раніше не були представлені методлм опроних векторів. Цього можна досягти шляхом навчання SVM-моделі на вибірковому наборі, що передбачає послідовну оптимізацію функції помилки. Залежно від визначення цієї функції помилки можна розпізнати два типи моделей SVM:

Тип SVM регресії 1. Для цього типу SVM модель:

$$\frac{1}{2}w^T w + C\sum_{i=1}^{N}\xi_i + C\sum_{i=1}^{N}{\xi_i}^* \to min \tag{2.4}$$

$$\begin{cases} w^T\phi(x_i) + b_i - y_i \le \varepsilon + {\xi_i}^* \\ y_i - w^T\phi(x_i) - b_i \le \varepsilon + \xi_i \\ {\xi_i}^*, \xi_i \ge 0, i = 1, \dots, N \end{cases}$$

де C – параметр ємності (використовується для перехресної перевірки сітки);

Тип SVM регресії 2. Для цього типу SVM модель:

$$\frac{1}{2}w^T w - C\left(v\varepsilon + \frac{1}{N}\sum_{i=1}^{N}(\xi_i + \xi_i^*)\right) \to min \tag{2.5}$$

$$\begin{cases} w^T\phi(x_i) + b_i - y_i \le \varepsilon + \xi_i \\ y_i - w^T\phi(x_i) - b_i \le \varepsilon + \xi_i^* \\ \xi_i^*, \xi_i \ge 0, i = 1, \dots, N, \varepsilon \ge 0 \end{cases}$$

Використовуючи метод опорних векторів, можливим є побудова різних типів функціональної залежності між зімнними (лінійна, поліноміальна, радіальна базисна. Сигмовидна):

$$\phi = \begin{Bmatrix} x_i \cdot x_j \quad Linear \\ (\gamma x_i \cdot x_j + coefficient)^d \quad Polynomial \\ exp\left(-\gamma(x_i - x_j)^2\right) \quad RBF \\ tanh(\gamma x_i \cdot x_j + coefficient) \quad Sigmoid \end{Bmatrix} \tag{2.6}$$

де d – ступінь поліноміального ядра;

γ – гамма-параметр для поліномінального, RBF і сигмоподібного ядер;

коефіцієнт – коефіцієнт для поліномінального та сигмоподібного ядер.

Отже, побудуємо 8 SVM-моделей машинного навчання: двох типів (epsilon-SVM regression та nu-SVM regression) в розрізі чотирьох специфікацій опорних векторів: лінійні, поліноміальні, радіально -базисні функції (RBF) та сигмоподібні на базі даних вибіркової сукупності країн Європи. На базі порівняння фактичних та прогнозних рівнів досліджуваних детермінант поширення кібербезпеки та інтегрального індексу кіберзагроз для тестової вибірки країн обчислимо середнє квадратичне відхилення (остання графа таблиці 2.4). Таким чином, найбільш точною виступає сигмоїдної nu-SVM регресійна модель машинного навчання, яка має наступні характеристики:

SVM: Regression type 2 (C=10,000, nu=0,500), Kernel: Sigmoid (gamma=0,167, coefficient=0,000) Number of support vectors= 9 (3 bounded).

Таблиця 2.4 – Порівняння 8 побудованих SVM-моделей

Специфікація SVM-моделей	DEU	ITA	LVA	NLD	SVK	ESP	Середньо-квадратичне відхилення
cyber threat index	63,33	57,71	42,91	18,81	8,90	74,92	
SVM: Regression type 1 (C=10,000, epsilon=0,100), Kernel: Linear Number of support vectors= 14 (8 bounded)	23,92	32,11	9,87	36,23	19,74	32,50	21,15
SVM: Regression type 1 (C=10,000, epsilon=0,100), Kernel: Polynomial (degree=3,000, gamma=0,167, 0,000(null) Number of support vectors= 14 (11 bounded)	24,08	26,02	25,38	17,44	25,21	24,81	20,69
SVM: Regression type 1 (C=10,000, epsilon=0,100), Kernel: Radial Basis Function (gamma=0,167) Number of support vectors= 14 (9 bounded)	17,09	27,93	19,68	23,59	21,38	22,23	21,24
SVM: Regression type 1 (C=10,000, epsilon=0,100), Kernel: Sigmoid (gamma=0,167, coefficient=0,000) Number of support vectors= 15 (13 bounded)	27,69	32,03	22,62	21,15	24,34	29,82	20,15
SVM: Regression type 2 (C=10,000, nu=0,500), Kernel: Linear Number of support vectors= 10 (4 bounded)	33,39	42,77	21,84	16,20	25,87	27,74	20,51
SVM: Regression type 2 (C=10,000, nu=0,500), Kernel: Polynomial (degree=3,000, gamma=0,167, 0,000(null) Number of support vectors= 9 (5 bounded)	26,03	26,03	25,98	15,91	25,39	24,52	20,71
SVM: Regression type 2 (C=10,000, nu=0,500), Kernel: Radial Basis Function (gamma=0,167) Number of support vectors= 10 (3 bounded)	29,48	37,48	28,72	16,45	28,24	24,30	20,20
SVM: Regression type 2 (C=10,000, nu=0,500), Kernel: Sigmoid (gamma=0,167, coefficient=0,000) Number of support vectors= 9 (3 bounded)	27,84	33,34	28,04	19,77	27,46	25,30	20,00

Джерело: розрахунки автора

Наступним етапом є проведення визначення детермінант поширення кіберзагроз на основі методів машинного навчання SVM за допомогою сигмоїдної nu-SVM regression моделі, яка була ідентифікована як найбільш

точна та адекватна на базі країн світу тестової сукупності. Отримані результати представимо у наведених нижче рисунках 2.5-.2.7.

	Model summary (Support Vector Machine),
Model specifications	Value
Number of independents	6
SVM type	Regression type 1
Kernel type	Sigmoid
Number of SVs	9 (3 bounded)

Рисунок 2.5 – Специфікація SVM-моделі кіберзагроз на множині розглянутих країн світу станом на 2020 рік

Джерело: розрахунки автора

Аналіз рисунку 2.5 дозволяє констатувати наступні характеристики сигмоїдної nu-SVM regression моделі машинного навчання: кількість незалежних змінних в моделі 6, тип моделі - nu-SVM regression, Kernel type – сигмоїдна, кількість опорних векторів, які дозволяють здійснити алгоритм розпізнавання образів – 9, серед яких граничними є 3.

	SVM model specifications (coefficients and support vectors), (cyber threat index SVM.sta) SVM: Regression type 2 (C=10,000000,nu=0,500000) Kernel: Sigmoid (gamma=0,166667,coefficient=0,000000)						
Support vector	Weights 1	Support vector Banking	Support vector Mobile broadband	Support vector Internet User Skills	Support vector Advanced Skills and Development	Support vector Activities online	Support vector Business digitisation
1	-9,9177	0,805002	0,062415	0,641306	0,346965	0,414561	0,795790
2	-10,0000	0,565335	0,052366	0,562736	0,373029	0,569233	0,323482
3	9,2885	0,980021	0,587784	0,897963	0,498039	0,888589	0,765671
4	9,2038	0,739172	0,445688	0,571192	0,306323	0,000000	0,448700
5	10,0000	0,345569	0,037336	0,423460	0,000000	0,443834	0,236902
6	-1,8307	0,557622	0,658421	0,396959	0,265601	0,571006	0,021026
7	-10,0000	0,565475	0,331067	0,298698	0,194190	0,224454	0,076249
8	9,0077	0,528589	0,090176	0,513257	0,024084	0,421223	0,339315
9	-5,7516	0,834259	0,340994	0,960563	0,502928	0,823048	0,647347

Рисунок 2.6 – Специфікація SVM-моделі визначення детермінант поширенння кіберзагроз

Джерело: розрахунки автора

Аналіз рисунку 2.6 дозволяє констатувати наступне: серед 9 побудованих опорних векторів, найбільшу за абсолютним значенням вагу мають 2, 5 та 7 вектори. Саме тому, для визначення детермінант поширенння кіберзагроз обчислимо в розрізі кожного опорного вектора середнє

арифметичне значення за трьома обраними опорними векторами. Отже, отримаємо наступний рейтинг важливості детермінант поширенння кіберзагроз:

– частка населення, яка користується онлайн банкінгом (Z1) – 0,49;
– індикатор рівня навичок в Інтернеті (Z3) – 0,42;
– індикатор онлайн діяльності (Z5) – 0,41;
– індикатор ділової онлайн активності (Z6) – 0,21;
– індикатор поглиблених навичок та вмінь (Z4) –0,18;
– індикатор розвитку мобільного широкосмугового доступу (Z2) – 0,14.

У полі «Резюме» у верхній частині діалогового вікна «Результати» наведено специфікацію SVM-моделі, включаючи кількість опорних векторів та їх типи, а також ядра та їх параметри. Крім цього, відображаються й інші специфікації, створені в діалоговому вікні «Машини опорних векторів»: список залежних і незалежних змінних, значення навчальних констант (ємність, епсилон і nu), результати перехресної перевірки (якщо застосовно), а також статистику регресії для навчальних, тестових та загальних вибірок, таких як середній квадрат помилки, коефіцієнт стандартного відхилення та коефіцієнти кореляції (рисунок 2.7).

	Regression summary (Support Vector Machine), SVM: Regression type 1 (C=10,000, nu=0,500), K Number of support vectors= 9 (3 bounded)
Regression summary	cyber threat index
Observed mean	44,4309
Predictions mean	26,9566
Observed S.D.	26,0179
Predictions S.D.	4,4127
Sum of squared error	813,9066
Error mean	17,4744
Error S.D.	24,7035
Abs. error mean	23,9811
S.D. ratio	0,9495
Correlation	0,3751

Рисунок 2.7 – Показники точності SVM-моделі визначення детермінант поширенння кіберзагроз

Джерело: розрахунки автора

Таким чином, побудувавши нейронну модель методом опорних векторів на основі даних країн Європейського Союзу встановлено наявність тісних функціональних залежностей між рівнем кіберзагроз та такими чинниками як частка населення, яка користується онлайн банкінгом (0,49), індикатор рівня навичок в Інтернеті (0,42), індикатор онлайн діяльності (0,41).

Таким чином, збільшення частоти та масштабів кібершахрайств у реальному та фінансовому секторах економіки може призвести до несанкціонованого розповсюдження персональної фінансової інформації про клієнтів, отримання значних збитків та репутаційних втрат фінансовими установами і навіть мати системні наслідки для економіки країни, оскільки загрози можуть швидко поширюватися по різних секторах економіки. За цих умов вчасно ідентифікувати ознаки кібершахрайства та швидко прийняти рішення щодо їх нейтралізації.

2.2. Науково-методичний підхід до оцінювання рівня кібервразливості економічних агентів в контексті цифрових трансформацій

Розширення цифрових можливостей та покращення роботи з клієнтами є неминучим вибором для банків та фінансових установ, які прагнуть залишатися конкурентоспроможними та задовольняти потреби клієнтів протягом наступного десятиліття. У той же час це призводить до збільшення кількості атак кіберзлочинців. Insights, компанія з розвідки кіберзагроз, повідомила, що 25% усіх атак зловмисного програмного забезпечення спрямовані на банки та інші компанії, що надають фінансові послуги, що набагато більше, ніж у будь-якій іншій галузі.

Безпечне та ефективне функціонування інфраструктури фінансового ринку має важливе значення для підтримки та сприяння фінансовій стабільності, підвищення довіри населення до фінансових установ. На

сьогодні питання забезпечення інформаційної безпеки суб'єктів фінансового ринку поступово стає пріоритетним вектором діяльності як національного регулятора, так і надавачів фінансових послуг. У березні 2017 року Рада керуючих Європейського центрального банку затвердила «Стратегію кіберстійкості Євросистеми для фінансових установ», метою якої є покращення інформаційної безпеки фінансових установ у Європейському Союзі та посилення співпраці між національними регуляторами, фінансовими установами та контрагентами для протидії кіберзагрозам.

Національний банк України також посилює контроль за виконанням фінансовими установами заходів із забезпечення кіберзахисту та інформаційної безпеки. З прийняттям постанови Правління Національного банку України від 16 січня 2021 року № 4 [42] фінансові установи зобов'язані щорічно проводити самооцінку з оцінювання ризиків власної інформаційної безпеки та подавати дану інформацію до національного регулятора. Дані регуляторні заходи сприятимуть приведенню вітчизняного законодавства у сфері кіберзахисту фінансової системи до міжнародних стандартів та принципів, а саме Банку міжнародних розрахунків "Керівництво з кіберстійкості для інфраструктур фінансового ринку" [97] та Європейського центрального банку "Очікування з оверсайта щодо кіберстійкості інфраструктур фінансового ринку" [78]. Крім цього, починаючи з серпня 2021 року Національний банк України та кіберполіція співпрацюватимуть для посилення ефективності протидії кіберзлочинам у фінансовій сфері.

В умовах швидко зростаючих кіберзагроз та урізноманітнення форм їх здійснення важливою умовою ефективної боротьби з ними є розвиток комунікації, координації та партнерства у сфері кіберзахисту між фінансовими установами та національним регулятором, що передбачає обмін актуальною інформацією про кіберзагрози між банками.

У сучасних умовах фінансові установи деяких країн світу укладають попередню угоду зі своїми клієнтами, де чітко зазначається необхідний спосіб

ідентифікації та аутентифікації клієнта при підтвердженні фінансової транзакції [79].

Ураховуючи масовий перехід користувачів платіжних послуг в онлайн у період карантину, важливим пріоритетом для центрального банку є необхідність максимально убезпечити їх від можливих інцидентів інформаційної безпеки. Однією з найбільш вразливих ланок в забезпеченні інформаційної безпеки фінансової системи є споживачі фінансових послуг, що й обумовило актуальність обраного напрямку дослідження.

Метою запропонованого науково-методичного підходу є оцінювання інтегрального рівня кібервразливості споживачів фінансових послуг, що передбачає реалізацію наступних етапів:

– збір та обробка статистичних даних, що прямо та опосередковано характеризують ступінь обізнаності клієнтів фінансових установ щодо ймовірних кібершахрайств та способів захисту від кіберзагроз при здійсненні фінансових транзакцій;

– визначення пріоритетності змінних, обраних на попередньому етапі;

– обрання синтезуючої функції для визначення узагальнюючого рівня кібервразливості споживачів фінансових послуг.

Початковим етапом розробленого науково-методичного підходу є збір та систематизація індикаторів, що прямо та опосередковано характеризують вразливості споживачів фінансових послуг до кіберзагроз (проінформованість про ознаки підозрілих кібершахрайств, способи кіберзахисту, канали інформування про кібератаки). Джерелом первинних даних слугувало опитування громадян Європейського Союзу щодо їх ставлення до питань кібербезпеки, яке проводилося у 2020 році [88]. Для потреб даного дослідження відібрано 17 індикаторів, які виключно стосуються фінансових транзакцій та захисту персональних даних, а саме: частка населення, які хвилюються безпекою онлайн-платежів (R1); частка населення, які мають хвилювання щодо несанкціонованого використання їх персональних даних

(R2); частка населення, які змінювали протягом останніх 12 місяців пароль до інтернет-банкінгу (R3); частка населення, які зазначають низький рівень інформованості про ризики кіберзлочинності (R16); частка населення, яким відомо хоча б один спосіб повідомлення про кіберзлочин (R17), а також група показників, що відображають превентивні заходи громадян для підвищення їх рівня захисту віртуальному просторі (R4- R15): частка населення, яка зменшила кількість банківських операцій в Інтернеті (R4); частка населення, яка рідше вводить особисту інформацію на веб-сайтах (R5); частка населення, яка змінила налаштування безпеки (наприклад, у браузері, соціальній мережі, пошуковій системі) (R6); частка населення, яка відвідуєте лише ті веб-сайти, які знаєте і яким довіряє (R7); частка населення, яка використовує різні паролі для різних сайтів (R8); частка населення, яка не відкриваєте електронні листи від незнайовим людей (R9); частка населення, яка встановила актуальне антивірусне програмне забезпечення (R10); частка населення, яка скасувала онлайн-покупку через підозри щодо продавця або веб-сайту (R11); частка населення, яка використовує більш складні паролі, ніж раніше (R12); частка населення, яка використовує біометричні функції (наприклад, розпізнавання обличчя, відбиток пальця) (R13); частка населення, яка не підключається до Інтернету через незахищені точки доступу (R14); частка населення, яки не турбує безпека в Інтернеті (R15). Об’єктом дослідження обрано 30 країн Європи. Узагальнена інформація у розрізі 17 індикаторів станом на 2020 рік представлена в таблиці Б.1, додатку Б , а основні результати подано в таблиці 2.5.

За даними опитування громадян Європейського Союзу щодо рівня їх обізнаності та усвідомлення важливості захисту фінансових операцій у віртуальному просторі встановлено наступні факти: близько половини населення Ірландії, Іспанії та Великобританії мають занепокоєння щодо безпечності їх онлайн платежів; у Кіпрі 60% населення мають хвилювання щодо несанкціонованого використання їх персональних даних при здійсненні розрахунків.

Таблиця 2.5 – Інформація щодо обізнаності громадян про кібератаки та способи захисту від них в європейських країнах у 2020 році

Показ-ник	Сер. знач. по ЄС	Топ-3 країн з найвищими показниками			Топ-3 країн з найнижчими показниками		
		1 місце	2 місце	3 місце	1 місце	2 місце	3 місце
R1	41%	Ірландія (52%)	Іспанія (49%)	Великобри-танія (46%)	Польща (24%)	Естонія (25%)	Данія (27%)
R2	46%	Кіпр (60%)	Греція (57%)	Німеччина (57%)	Угорщина (31%)	Словаччина (31%)	Польща (32%)
R3	30%	Латвія (49%)	Великобри-танія (42%)	Австрія (41%)	Румунія (10%)	Угорщина (13%)	Португалія (15%)
R16	22%	Мальта (44%)	Греція (40%)	Австрія (34%)	Румунія (14%)	Іспанія (14%)	Данія (14%)
R17	17%	Швеція (30%)	Австрія (29%)	Нідерланди (25%)	Португалія (5%)	Латвія (7%	Греція (8%)

Джерело: розрахунки автора

У країнах Європейського Союзу у середньому 22% населення зазначають низький рівень їх інформованості про ризики кіберзлочинності, тоді як найбільші значення у таких країнах як Мальта (44%), Греція (40%), Австрія (34%), а найнижчі – Румунія, Іспанія, Данії (14%).

Важливим елементом в протидії кіберзлочинності є вчасне повідомлення про факти порушення у відповідні контролюючі органи. Проте лище 17% європейців знають про хоча б один спосіб повідомлення про кіберзлочин, найвищі показники у Швеції (30%), Австрії (29%), Нідерландах (25%), а найнижчі – Португалія (5%), Латвія (7%), Греці (8%).

Наступним етапом запропонованого методичного підходу є визначення пріоритетності показників кібервразливості споживачів фінансових послуг на основі комбінації методу головних компонент (при визначенні граничних меж значень показників) та лінійного програмування методом узагальненого знижуючого градієнту. Реалізація даного етапу є комплексною, тому виникає необхідність проведення ряду проміжних кроків. Так, для постановки та вирішення задачі лінійного програмування оптимізації вагових коефіцієнтів показників кібервразливості споживачів фінансових послуг при подальшому

обчисленні єдиного інтегрального індексу кіберврзарливості, проводяться наступні проміжні кроки обчислень:

Крок 2.1. Формалізація цільової функції як суми вагових коефіцієнтів змінних змінних $R_1, \dots, R_{17}$ – показників кібервразливості, яка має дорівнювати одиничному значенню:

$$F(w(R_1), \dots, w(R_{17})) = \sum_{i=1}^{17} w(R_i) \to 1 \tag{2.7}$$

де $F(w(R_1), \dots, w(R_{17}))$ – функціональна залежність між ваговими коефіцієнтами $w(R_i)$ змінних $R_1, \dots, R_{17}$ – показників кібервразливості.

Крок 2.2. Формалізація обмежень задачі оптимізації вагових коефіцієнтів показників кібервразливості споживачів фінансових послуг:

- сума вагових коефіцієнтів показників наступного переліку (від 4-го до 15-го включно) не повинна перевищувати рівня 0,5 частки одиниці:

$$\sum_{i=4}^{15} w(R_i) \leq 0.5 \tag{2.8}$$

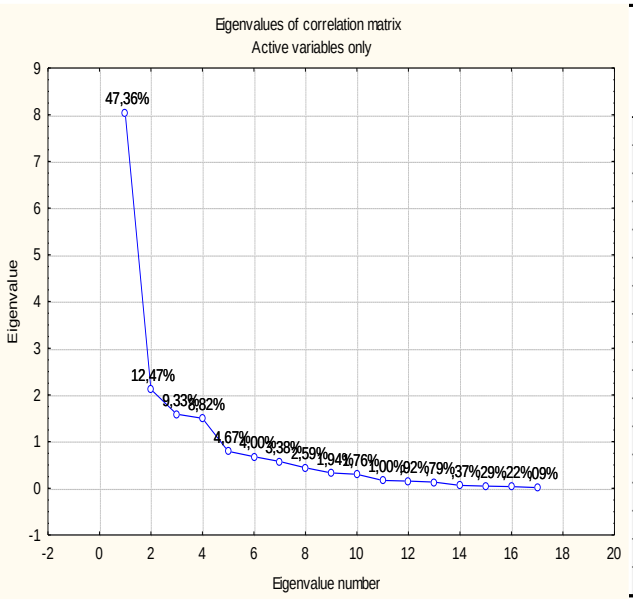
Дана умова введена в економетричну модель, оскільки вищезазначені індикатори (R4- R15) відображають ступінь використання превентивних заходів громадянами для підвищення їх рівня захисту віртуальному просторі.

- значення показників кібервразливості не повинні перевищувати і не повинні бути менше гранично допустимих рівнів:

$$w(R_{i,i=4\div15}) \leq RO_i \tag{2.9}$$
$$w(R_{i,i=1,2,16,17}) \geq RO_i$$

де RO_i – гранично допустимі межі кількісних значень для і-го показника характеристики кібервразливості.

Для встановлення гранично допустимих рівнів показників кібервразливості скористаємось методом головних компонент можливостями програмного пакету Statistica. За своєю сутністю метод полягає у виборі нової ортогональної системи координат у просторі спостережень. Як першу головну компоненту обирають напрям, вздовж якого масив спостережень має найбільшу дисперсію. Кожну наступну компоненту обирають також з умови максимізації частки дисперсії, що залишилася, вздовж неї, доповненої умовою ортогональності всім раніше обраним компонентам. При цьому із зростанням номера компоненти буде зменшуватися пов’язана з нею частка загальної дисперсії. Результати представимо на рисунку 2.8.



Value number	Eigenvalues of correlation matrix, and related statistics Active variables only			
	Eigenvalue	% Total variance	Cumulative Eigenvalue	Cumulative %
1	8,050823	47,35778	8,05082	47,3578
2	2,119587	12,46816	10,17041	59,8259
3	1,586746	9,33380	11,75716	69,1597
4	1,500186	8,82462	13,25734	77,9844
5	0,793672	4,66866	14,05101	82,6530
6	0,679275	3,99573	14,73029	86,6488
7	0,575159	3,38329	15,30545	90,0320
8	0,440670	2,59217	15,74612	92,6242
9	0,330223	1,94249	16,07634	94,5667
10	0,300004	1,76473	16,37634	96,3314
11	0,169155	0,99503	16,54550	97,3265
12	0,155774	0,91631	16,70127	98,2428
13	0,133753	0,78678	16,83503	99,0296
14	0,063031	0,37077	16,89806	99,4003
15	0,048670	0,28629	16,94673	99,6866
16	0,037567	0,22098	16,98429	99,9076
17	0,015708	0,09240	17,00000	100,0000

Рисунок 2.8 – Скріншот фрагмента програми Statistica графіку кам’янистого опису, власних значень кореляційної матриці та пов’язаних статистичних показників

Джерело: розрахунки автора

На основі аналізу рисунку 2.8 можна зробити висновок про доцільність для оцінювання граничних обмежень показників кібервразливості враховувати перші чотири головні компоненти, представлені першими чотирма факторами, на варіацію яких припадає 77,98% загальної варіації, про

що свідчить як графік кам'янистого осипу (лівий фрагмент рисунку 2.8), так і табличні значення власних значень факторів в розрізі показників (правий фрагмент рисунку 2.8). Враховуючи дані рисунку 2.8 та вкладу змінних на основі кореляції показників кібервразливості споживачів фінансових послуг, визначимо обмеження для визначення пріоритетності RO_i на сонові середньої арифметичної зваженої:

$$RO_i = \frac{\sum_{j=1}^{4} F_{ij} \cdot v_j}{\sum_{j=1}^{4} v_j} \quad (2.10)$$

де RO_i – обмеження, що накладається на і-ту змінну - показник кібервразливості;

F_{ij} – значення вкладу і-тої змінної в розрізі j-того фактору (головної компоненти) на основі кореляції;

v_j - % загальної варіації власних значень кореляційної матриці в розрізі j-того фактору (головної компоненти).

Результати обчислень за формулою (2.10) представимо у графі 5 таблиці 2.6.

Таблиця 2.6 – Вклад змінних на основі кореляції, обмеження пріоритетності та ваги показників кібервразливості споживачів фінансових послуг

Показник	Factor1	Factor2	Factor3	Factor4	Обмеження для визначення пріоритетності RO_i	Ваги $w(R_i)$
	47,36	12,47	9,33	8,82		
A	1	2	3	4	5	6
R1	0,0011	0,1829	0,2279	0,0164	0,0590	0,104
R2	0,0030	0,3253	0,0225	0,0812	0,0657	0,111
R3	0,0404	0,0043	0,0582	0,0004	0,0323	0,077
R4	0,0267	0,1753	0,0108	0,0237	0,0483	0,011
R5	0,0772	0,0331	0,0036	0,0446	0,0576	0,021
R6	0,0949	0,0032	0,0189	0,0028	0,0607	0,029
R7	0,0259	0,1418	0,1851	0,0170	0,0625	0,038

Продовження таблиці 2.6

A	1	2	3	4	5	6
R8	0,1127	0,0007	0,0019	0,0059	0,0694	0,045
R9	0,0941	0,0100	0,0619	0,0072	0,0669	0,045
R10	0,0784	0,0040	0,0147	0,0002	0,0500	0,045
R11	0,0468	0,0239	0,1518	0,0246	0,0532	0,049
R12	0,1023	0,0008	0,0103	0,0097	0,0646	0,053
R13	0,1007	0,0264	0,0079	0,0045	0,0668	0,055
R14	0,1009	0,0020	0,0204	0,0005	0,0641	0,055
R15	0,0016	0,0188	0,1293	0,3758	0,0619	0,055
R16	0,0895	0,0064	0,0200	0,0084	0,0587	0,104
R17	0,0039	0,0411	0,0547	0,3770	0,0582	0,103

Джерело: розрахунки автора

Таким чином, враховуючи формули (2.7) – (2.10) постановка задачі оптимізації вагових коефіцієнтів показників кібервразливості споживачів фінансових послуг набуває наступного вигляду:

$$F(w(R_1),\dots,w(R_{17})) = \sum_{i=1}^{17} w(R_i) \to 1$$

$$\begin{cases} \sum_{i=1}^{17} w(R_i) \le 0.5 \\ w(R_{i,i=4\div15}) \le RO_i \\ w(R_{i,i=1,2,16,17}) \ge RO_i \\ w(R_i) \ge 0 \end{cases} \tag{2.11}$$

де $F(w(R_1),\dots,w(R_{17}))$ – функціональна залежність між ваговими коефіцієнтами $w(R_i)$ змінних $R_1,\dots,R_{17}$ – показників кібервразливості.

Вирішення задачі оптимізації вагових коефіцієнтів показників кібервразливості споживачів фінансових послуг як задачі лінійного програмування пропонується провести за допомогою інструментарію «Пошук рішення» MS Excel, зокрема методу узагальненого знижуючого градієнту. Результати проведених розрахунків представимо в графі 6 таблиці 3.3. Таким чином, найбільш впливовим при оцінюванні кібервразливості споживачів

фінансових послуг є показник R2, на частку впливу якого припадає 11,1%. Наступними релевантними показниками виступають R1 та R16, вагові коефіцієнти впливу в розрізі яких сягають 10,4%.

Завершальним етапом є розрахунок інтегрального індексу кібервразливості за основі застосування мультиплікативної згортки Кіні. Враховуючи отримані на попередньому етапі вагові коефіцієнти впливу показників кібервразливості споживачів фінансових послуг, а також характер даних показників як стимуляторів чи дестимуляторів, проведемо їх згортку в єдиний інтегральний індекс кібервразливості за основі застосування мультиплікативної згортки Кіні:

$$ICR_i(R_1, \dots, R_{17}) = \frac{1}{k}\left\{\prod_{i=1\div3,16}[1 + k \cdot w(R_i^+) \cdot R_i^+] \cdot \prod_{i=4\div15,17}[1 + k \cdot w(R_i^-) \cdot (1 - R_i^-)] - 1\right\} \quad (2.12)$$

де $ICR_i(R_1, \dots, R_{17})$ – індекс кібервразливості для і-тої країни (абсолютна оцінка);

k – константа, яка визначає кількість показників кібервразливості;

R_i^+, R_i^- - відповідно, і-ий показник кібервразливості стимулятор та де стимулятор.

Результати проведених обчислень за формулою Кіні (2.12) систематизуємо в табличному вигляді, зокрема графах 1 та 2 таблиці 2.7

Таблиця 2.7 – Абсолютний та відносний рівні кібервразливості економічних агентів на множині відібраних 28 країн Європи

Країна	Абсолютний рівень кібервразливості	Країна	Абсолютний рівень кібервразливості
Бельгія	287378%	Ліхтенштейн	331317%
Болгарія	435179%	Люксембург	214931%
Чехія	349618%	Угорщина	393596%
Данія	125357%	Мальта	192096%
Німеччина	256822%	Нідерланди	120042%
Естонія	172125%	Австрія	208011%
Ірландія	366930%	Польша	309972%
Греція	336109%	Португалія	376243%
Іспанія	526414%	Румунія	491389%
Франція	299869%	Словенія	366733%
Хорватія	447456%	Словачиина	365780%
Італія	519764%	Фінляндія	148774%
Кіпр	394184%	Швеція	117005%
Латвія	361841%	Великобританія	282798%

Джерело: розрахунки автора

Абсолютне значення індексу кібервразливості споживачів фінансових послуг на множині розглянутих країн Європи не дозволяє об’єктивно оцінити та порівняти країни між собою, що призводить до необхідності визначення відносної оцінки кібервразливості споживачів фінансових послуг. Для цього визначимо відносний рівень кібервразливості споживачів фінансових послуг як співвідношення абсолютної оцінки до максимально можливого рівня, який спостерігається на досліджуваній множині значень складових показників. Отже, максимально можливе значення абсолютного індекса кібервразливості обчислимо наступним чином:

$$ICR_{max}(R_1, \dots, R_{17}) = \frac{1}{k}\left\{\prod_{i=1\div 3,16}\left[1 + k \cdot w(\max_{i=1\div 17} R_i) \cdot \max_{i=1\div 17} R_i\right] \cdot \prod_{i=4\div 15,17}\left[1 + k \cdot w(\min_{i=1\div 17} R_i) \cdot (1 - \min_{i=1\div 17} R_i)\right] - 1\right\} \quad (2.13)$$

де $ICR_{max}(R_1, \dots, R_{17})$ – максимально можливе значення абсолютного індекса кібервразливості.

Враховуючи представлені вище формули (2.12) та (2.13), а саме визначивши їх співвідношення, отримаємо шуканий відносний індекс кібервразливості споживачів фінансових послуг:

$$VICR_i(R_1, \dots, R_{17}) = \frac{ICR_i(R_1, \dots, R_{17})}{ICR_{max}(R_1, \dots, R_{17})} \quad (2.14)$$

де $VICR_i(R_1, \dots, R_{17})$ - індекс кібервразливості для і-тої країни (відносна оцінка).

Представимо результати проведених обчислень за допомогою формули (2.14) на рисунку 2.9.

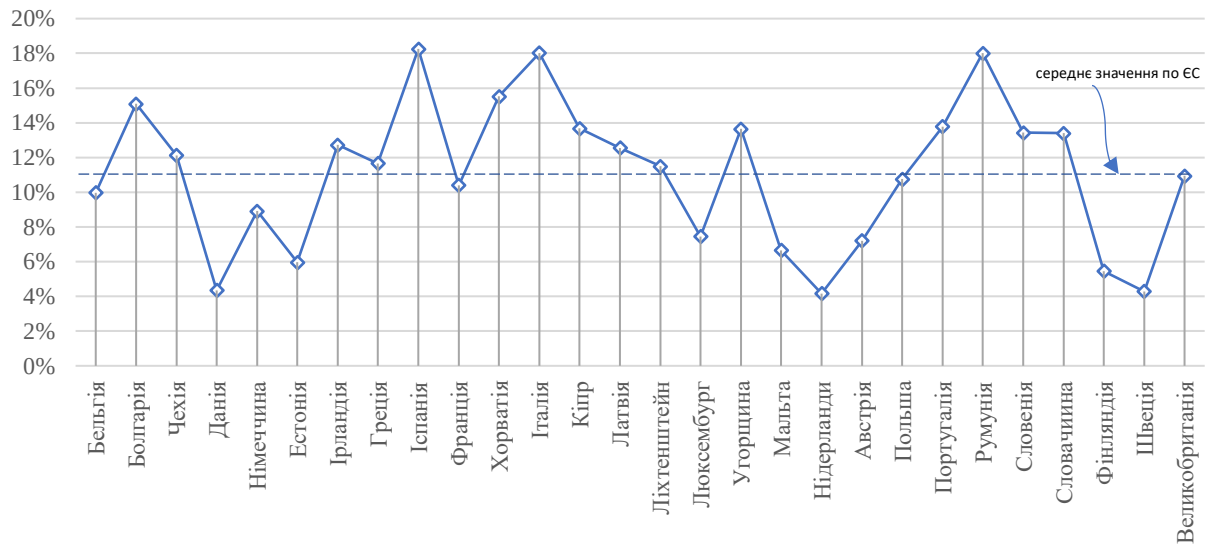


Рисунок 2.9 – Результати оцінювання рівня кібервразливості економічних агентів у країнах Європи станом на 2020 рік

Проведене дослідження засвідчило, що рівень кібервразливості громадян ЄС становить у середньому 11%, що дозволяє стверджувати про усвідомленість населенням європейський країн наявних загроз у віртуальному просторі, способів захисту від кіберзлочинності. Проте рівень кібервразливості споживачів фінансових послуг у розрізі країн ЄС не є однорідним, а саме найменшим ризик стати жертвою кібершахрайства мають громадяни таких країн як Данія, Нідерланди, Швеція. До країн з найвищими

значеннями розрахованого рівня кібервразливості споживачів фінансових послуг (18%) належать: Іспанія, Італія, Румунія.

Таким чином, проведений аналіз рівня кібервразливості споживачів фінансових послуг на прикладі країн ЄС засвідчує ефективність здійснюваних регуляторних та просвітницьких заходів з інформування населення про потенційні загрози у віртуальному просторі та способи захисту від кіберзагроз. Варто зазначити, що для моніторингу рівня кібервразливоті громадян при здійсненні ними фінансових розрахунків необхідно проводити розрахунки на щорічній основі, оскільки відбувається постійна інтелектуалізація методів та способів здійснення кібершахрайств.

2.3. Методичні засади до оцінювання ризику фінансових кібершахрайств

Зростання обсягів електронної комерції, використання системи онлайн-оплати рахунків сприяє збільшенню частки безготівкових розрахунків, що, з одного боку, дозволяє державі більш ефективніше контролювати джерела походження фінансових ресурсів та напрямків їх використання, а іншого – з’являються нові способи здійснення фінансових платіжних шахрайств. Протиправні дії з банківськими платіжними картками становлять підвищену небезпеку для різних верств суспільства та суб’єктів господарювання, оскільки завдають збитків широкому колу осіб, що негативно впливає на рівень довіри до сфери фінансових послуг. Незважаючи на проведення Національним банком України інформаційних кампаній з платіжної безпеки, запровадження внутрішнього моніторингу фінансових транзакцій та перевірки клієнтської бази, все ж таки шахрайства з платіжними картками залишається одним із найбільш поширених протиправних діянь у фінансовій сфері.

Кібершахрайства з платіжною карткою це використання картки іншої особи для здійснення покупок або отримання готівкових авансів без відома чи згоди власника картки у кіберпросторі. Донедавна злочинці були націлені на фізичне викрадення платіжної картки, проте сьогодні все частіше використовуються цифрові засоби для викрадення номера кредитної картки та супровідної особистої інформації для здійснення незаконних операцій. У 2021 році більше 80% банківських шахрайств з використанням платіжної картки в країнах Європейського Союзу здійснено через мережу Інтернет [122].

У 2020 році обсяг збитків від шахрайства з банківськими картками становили 32,4 млрд доларів США, що майже втричі більше порівняно з 2011 роком (9,8 млрд доларів США), при цьому 46% з цих операцій здійснені на території США [94].

Стосовно України, то кількість банківських платіжних карток в обігу динамічно збільшується з кожним роком та станом на І півріччя 2021 року становила 41,3 млн штук, що фактично означає 2 банківські картки у розрахунку на 1 особу економічно активного віку [49]. У 2022 році сума збитків від незаконних дій з платіжними картками становила 481 млн грн, що на 46% більше, ніж у 2021 році. Отже, можемо зазначити, що протидія шахрайством з банківськими картками в Україні є важливим питанням як для національного регулятора, так і фінансової установи та її клієнтів. Тому виникає об’єктивна необхідність удосконалення інструментів та прийомів ідентифікації шахрайських транзакцій, визначення вразливих місць в захисті інформаційної системи фінансової установи, а також запровадження системи попереджувальних заходів для скорочення кількості та частоти здійснення шахрайських платіжних операцій.

У межах даної дисертаційної роботи запропоновано методичний підхід до багатоетапної процедури ідентифікації фінансового шахрайства з платіжними картками з використанням методів нейронного моделювання. На відміну від існуючих підходів, передбачає побудову сукупності нейромережевих моделей та оцінювання їх параметрів, що в кінцевому

підсумку дозволяє знайти оптимальну нейромережеву модель для оцінювання ризику платіжного шахрайства. Для апробації запропонованого наукоко-методичного підходу використано імітовані дані про банківські транзкції банківської установи з загальнодоступного ресурсу Kaggle [37]. Через конфіденційний характер набору даних уся конфіденційна інформація була видалена.

Штучна нейронна мережа побудована за принципом організації та функціонування біологічних нейронних мереж – нервових клітин живого організму Штучна нейронна мережа є системою з’єднаних і взаємопов’язаних між собою простих процесорів (штучних нейронів). Кожен процесор подібної мережі має справу лише з сигналами, які він періодично отримує, та сигналами, які він періодично надсилає іншим процесорам. Нейрони організовані у шари. Кількість шарів для кожної мережі індивідуально і залежить від прикладного завдання, що розв'язується. Технічно нейронні мережі не програмуються, а навчаються. Тобто штучні нейронні мережі спроможні моделювати закономірності у певній інформаційніій базі навіть без відомостей щодо можливих значень результативного показника завдяки своїй здатності до самоорганізації.

Структурно штучний нейрон складається із вхідних сигналів (синапси), суматора (додавання зважених сигналів, які надходять по міжнейронних зв’язках від інших нейронів або зовнішніх вхідних сигналів) та функціонального перетворювача (функція активація). У загальному випадку функція активації є нелінійною, що дозволяє описати нелінійну природу нейронної мережі та ефективно відтворити складні нелінійні функціональні залежності [50].

У межах даного дослідження запропоновано науково-методичний підхід для визначення шахрайських фінансових операцій з використанням платіжних карток, що передбачає поетапне виконання наступних кроків:

Етап 1. Відбір системи інформативних ознак, що несуть у собі достатню для побудови нейромоделі інформацію, та формування статистичної інформації по ним.

Етап 2. Структурний синтез – етап, на якому ідентифікується топологія зв'язків, обираються нейрони, що надалі визначають принцип функціонування мережі та її ефективність для оцінювання ризику фінансових кібершахрайств

Етап 3. Параметричний синтез – етап, на якому відбувається навчання нейромережевої моделі.

Етап 4. Оптимізація побудованої нейромоделі для оцінювання та прогнозування ризику фінансових кібершахрайств.

Для проведення проміжних розрахунків використано статистичний пакет Statistica. Загальний обсяг вибірки становив 549 645 спостереження, при цьому 2141 з них – шахрайські). Аналіз кожної фінансової транзакції буде здійснюватися на основі 8 індикаторів, перелік яких наведено у таблиці 2.8.

Таблиця 2.8 – Змінні, що використовуються визначення ризиків шахрайства

№	Назва змінної	Пояснення
1	Gender	Стать власника банківської картки (0 – жінка, 1 – чоловік)
2	Birth	Вік власника банківської картки
3	CC_num	Номер банківського рахунку
4	Amt	Сума транзакції, дол США
5	Category	Вид категорій товарів/послуг, які були об'єктом фінансової транзакції. Виділено 16 категорій фінансових транзакцій: 1 – платежі, пов'язані з оплатою у сфері персонального догляду (personal_care); 2 – платежі у сфері охорони здоров'я та спорту (health_fitness); 3 – інші платежі (misc_pos); 4 – платежі, пов'язані з поїдками (travel); 5 – платежі, пов'язані з оплатою дитячих товарів та товарів для домашніх тварин (kids_pets); 6 – оплата товарів (shopping_pos); 7 – оплата харчування (food_dining); 8 – платежі, пов'язані з оплатою речей для дому (home); 9 – платежі щодо оплати палива для транспорту (gas transport); 10 – поатежі у розважальній сфері (entertainment); 11 – оплата товарів (shopping_net); 12 – інші платежі (misc_net); 13 – платежі з оплати продуктів харчування (grocery_net); 14 – платежі з оплати продуктів харчування (grocery_pos)
6	Time	Година проведення операції (від 0 до 23)
7	Week date	День тижня проведення операції (від 1 до 7)
8	Fraud	Чи є операція шахрайською (0 – ні, 1 – так)

Джерело: авторський підхід

Фрагмент вхідної статистичної бази для оцінювання ризику фінансового шахрайства з платіжними картками в таблиці 2.9.

Таблиця 2.9 – Вхідні дані характеристику ризику кібершахрайств (фрагмент)

Week_date	CC_num	Amt	Birth	Time	Gender	Category	Fraud
7	2,29116E+15	2.86	53	12	1	1	0
7	3,57303E+15	29.84	32	12	0	1	0
7	3,59822E+15	41.28	51	12	0	2	0
7	3,59192E+15	60.05	34	12	1	3	0
7	3,52683E+15	3.19	66	12	1	4	0
7	3,04077E+13	19.55	30	12	0	5	0
7	2,13181E+14	133.93	71	12	0	2	0
7	3,58929E+15	10.37	49	12	0	1	0
7	3,59636E+15	4.37	48	12	1	6	0
7	3,5469E+15	66.54	65	12	0	7	0
7	2,24254E+15	7.01	25	12	1	7	0
7	5,71465E+11	42.4	45	12	1	5	0
7	6,59325E+15	2.91	45	12	0	8	0
7	4,9883E+12	7.93	84	12	1	7	0

Джерело: розрахунки автора

Одним із основних індикаторів, які дозволить навчити нейронну мережу, для вчасної ідентифікації ризику шахрайства з банківськими платіжними картками є саме «fraud». Тому проаналізуємо більш детальніше фінансові транзакції, що мають ознаки шахрайства у розрізі виокремлених ознак. На рисунку 2.10 зображено гістограми, які відображають кількість спостережень у відповідному параметрі, за якими зафіксовано факт шахрайства.

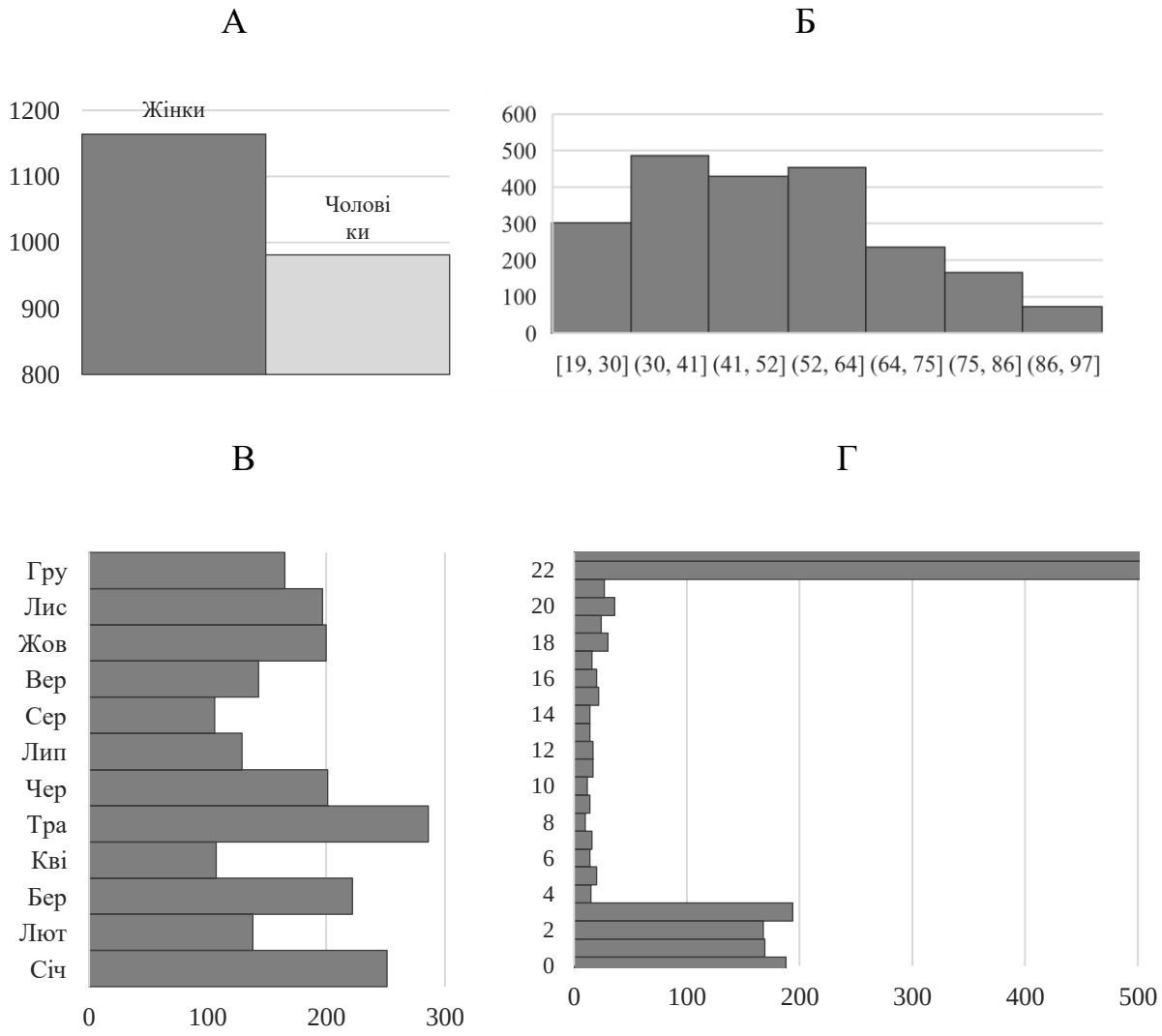


Рисунок 2.10 – Графік розподілу частоти транзакцій у розрізі досліджуваних ознак

Джерело: розрахунки автора

Дані рисунку 2.10а наочно засвідчують, що 54.2% власників банківських карток, за допомогою яких здійснювалися шахрайські транзакції, були жінки. Середній вік держателів банківських карток, які здійснювали шахрайські фінансові транзакції, становив 50 років. Найбільший обсяг незаконних транзакцій реалізується проходить на купівлю продуктів харчування та товарів.

Дані рисунку 2.10в демонструють, що найбільший обсяг шахрайських операцій було проведено у травні (286 операцій), березні (222) та січні (251).

Загалом часова концентрація здійснення шахрайських фінансових операцій є досить рівномірною, проте незначний сплеск фіксується у неділю (17,4% від загального обсягу), тоді як в інші дні тижня: вівторок – 15,4%, четвер – 14,4%, понеділок – 14,1%, п'ятниця – 13,8%, середа й субота – по 12,4%). Половина всіх шахрайських операцій з використанням банківсько картки проведено ввечері (з 22.00 до 23.00 – 550 операцій; з 23.00 до 24.00 – 538 операцій), тоді як вночі (з 24.00 по 03.00) здійснено ще третину шахрайських транзакцій (рис. 2.10б).

Наступним етапом розробленого науково-методичного підходу є структурний синтез, що передбачає побудову нейромережевних моделей залежності ризику шахрайств від ключових факторів його формування з використанням багатошарового персептрону MLP-архітектури з використанням алгоритму BFGS.

Результати побудови нейромережевої моделі залежності ризику кібершахрайств від факторів-складових з використанням багатошарового персептрону MLP-архітектури подано на рисунку 2.11.

Summary of active networks (Spreadsheet1.sta)

Index	Net. name	Training perf.	Test perf.	Training error	Test error	Training algorithm	Error function	Hidden activation	Output activation
1	MLP 7-6-1	0,586371	0,552403	0,005719	0,005844	BFGS 87	SOS	Exponential	Exponential
2	MLP 7-10-1	0,696928	0,672589	0,004477	0,004599	BFGS 270	SOS	Tanh	Tanh
3	MLP 7-5-1	0,598916	0,553488	0,005571	0,005827	BFGS 138	SOS	Tanh	Exponential
4	MLP 7-5-1	0,593724	0,561086	0,005640	0,005757	BFGS 341	SOS	Exponential	Exponential
5	MLP 7-8-1	0,661969	0,630111	0,004894	0,005059	BFGS 338	SOS	Logistic	Tanh

Рисунок 2.11 – Результати побудови нейромережевих моделей залежності ризику кібершахрайств від факторів-складових

Джерело: розрахунки автора

Детальний аналіз даних рисунку 2.11 дозволяє стверджувати, що спектр побудованих нейронних мереж у вигляді багатошарового персептрону MLP. Дві із п'яти представлених нейромережевих моделей (друга модель з архітектурою MLP 7-10-1, п'ята модель з архітектурою MLP 7-8-1) мають найвищий рівень ефективності, а саме на рівні не менше 0,6620 частки одиниці. Водночас три з п'яти нейромережевих моделей мають

продуктивність на рівні від 0,5864 до 0,5989 частки одиниці. Достовірність 5 побудованих моделей нейронних мереж підтверджується також показником помилки в межах навчальної, контрольної та тестової вибірки, яка приймає близькі до нульового рівня значення.

Для проведення більш ґрунтовного аналізу якості побудованих нейромережевих моделей розглянемо статистики передбачених значень ризику кібершахрайств та факторів-складових (рисунок 2.12).

	Data statistics (Spreadsheet1.sta)							
Samples	cc_num Input	amt Input	birth Input	time Input	gender2 Input	category2 Input	Week_date Input	is_fraud Target
Minimum (Train)	6,041621E+10	1,10	16,00000	0,00000	0,000000	1,00000	1,000000	0,000000
Maximum (Train)	4,992346E+18	12882,78	97,00000	23,00000	1,000000	16,00000	7,000000	1,000000
Mean (Train)	4,230247E+17	90,21	48,56405	13,29044	0,402803	7,89833	3,782472	0,017684
Standard deviation (Train)	1,319230E+18	171,91	17,71603	6,74014	0,490466	4,52254	2,187183	0,131803
Minimum (Test)	6,041621E+10	1,10	16,00000	0,00000	0,000000	1,00000	1,000000	0,000000
Maximum (Test)	4,992346E+18	13149,15	97,00000	23,00000	1,000000	16,00000	7,000000	1,000000
Mean (Test)	4,505042E+17	91,78	48,48803	13,26787	0,406515	7,89982	3,817848	0,017053
Standard deviation (Test)	1,356057E+18	198,21	17,66966	6,74779	0,491202	4,52689	2,205872	0,129473
Minimum (Overall)	6,041621E+10	1,10	16,00000	0,00000	0,000000	1,00000	1,000000	0,000000
Maximum (Overall)	4,992346E+18	13149,15	97,00000	23,00000	1,000000	16,00000	7,000000	1,000000
Mean (Overall)	4,285208E+17	90,52	48,54884	13,28593	0,403545	7,89863	3,789548	0,017558
Standard deviation (Overall)	1,326712E+18	177,48	17,70666	6,74162	0,490612	4,52338	2,190962	0,131339

Рисунок 2.12 – Описові статистики значень ризику кібершахрайств та факторів-складових

Джерело: розрахунки автора

Дані рисунку 2.12 надають узагальнену характеристику фінансових транзакцій, у т.ч. шахрайського характеру, що власників рахунків у фінансовій установі. Зокрема, середньостатистична фінансова транзакція проводилася жінкою у віці 48,5 років у середу або четвер з 13.00 до 14.00 для оплати продуктів харчування.

Аналіз статистичних характеристик побудованих нейромережевих моделей, представлених на рисунку 2.13 та в додатку В, свідчить про високу якість моделей (незначну варіацію мінімальних та максимальних рівнів як в межах навчальної, так і контрольної та тестової вибірок) та незначний рівень чутливості моделей до зміни масштабу вхідних даних.

	Network weights (Spreadsheet1.sta)					
Weight ID	**Connections 1.MLP 7-6-1**	Weight values 1.MLP 7-6-1	Connections 2.MLP 7-10-1	Weight values 2.MLP 7-10-1	Connections 3.MLP 7-5-1	Weight values 3.MLP 7-5-1
1	cc_num --> hidden neuron 1	-0,2613	cc_num --> hidden neuron 1	0,0525	cc_num --> hidden neuron 1	-4,0240
2	cc_num --> hidden neuron 2	24,2463	cc_num --> hidden neuron 2	25,3785	cc_num --> hidden neuron 2	-12,6913
3	cc_num --> hidden neuron 3	-0,4269	cc_num --> hidden neuron 3	-1,1746	cc_num --> hidden neuron 3	14,1261
4	cc_num --> hidden neuron 4	-5,9955	cc_num --> hidden neuron 4	-2,1610	cc_num --> hidden neuron 4	35,2826
5	cc_num --> hidden neuron 5	0,3327	cc_num --> hidden neuron 5	-0,3174	cc_num --> hidden neuron 5	27,9063
6	cc_num --> hidden neuron 6	0,4125	cc_num --> hidden neuron 6	-0,4648	amt --> hidden neuron 1	18,7772
7	amt --> hidden neuron 1	-0,4609	cc_num --> hidden neuron 7	-0,0748	amt --> hidden neuron 2	-23,2665
8	amt --> hidden neuron 2	5,8589	cc_num --> hidden neuron 8	-0,0484	amt --> hidden neuron 3	-0,1395
9	amt --> hidden neuron 3	4,8013	cc_num --> hidden neuron 9	-42,5145	amt --> hidden neuron 4	-70,3528
10	amt --> hidden neuron 4	0,4377	cc_num --> hidden neuron 10	0,8976	amt --> hidden neuron 5	0,5410
11	amt --> hidden neuron 5	-7,7284	amt --> hidden neuron 1	1,8963	birth --> hidden neuron 1	-2,6496
12	amt --> hidden neuron 6	-7,3084	amt --> hidden neuron 2	0,2291	birth --> hidden neuron 2	2,0735
13	birth --> hidden neuron 1	7,5904	amt --> hidden neuron 3	0,4390	birth --> hidden neuron 3	0,0485
14	birth --> hidden neuron 2	-0,3647	amt --> hidden neuron 4	0,0998	birth --> hidden neuron 4	-0,2636
15	birth --> hidden neuron 3	-0,5819	amt --> hidden neuron 5	-0,0434	birth --> hidden neuron 5	-0,7097
16	birth --> hidden neuron 4	0,5165	amt --> hidden neuron 6	-42,3234	time --> hidden neuron 1	33,6740
17	birth --> hidden neuron 5	0,1427	amt --> hidden neuron 7	1,2498	time --> hidden neuron 2	9,3340
18	birth --> hidden neuron 6	-6,3185	amt --> hidden neuron 8	2,7336	time --> hidden neuron 3	-16,2636
19	time --> hidden neuron 1	0,1784	amt --> hidden neuron 9	0,3439	time --> hidden neuron 4	-2,9899
20	time --> hidden neuron 2	1,2650	amt --> hidden neuron 10	0,5628	time --> hidden neuron 5	4,8023
21	time --> hidden neuron 3	-0,4903	birth --> hidden neuron 1	0,1272	gender2 --> hidden neuron 1	11,8304
22	time --> hidden neuron 4	-0,3112	birth --> hidden neuron 2	1,4357	gender2 --> hidden neuron 2	-29,0316
23	time --> hidden neuron 5	-24,0762	birth --> hidden neuron 3	9,3003	gender2 --> hidden neuron 3	127,4405
24	time --> hidden neuron 6	0,5436	birth --> hidden neuron 4	-2,6001	gender2 --> hidden neuron 4	-1,6147
25	gender2 --> hidden neuron 1	-6,6268	birth --> hidden neuron 5	6,8840	gender2 --> hidden neuron 5	-0,8162
26	gender2 --> hidden neuron 2	0,6188	birth --> hidden neuron 6	5,1097	category2 --> hidden neuron 1	-0,1927
27	gender2 --> hidden neuron 3	1,1960	birth --> hidden neuron 7	-2,6516	category2 --> hidden neuron 2	-4,1593
28	gender2 --> hidden neuron 4	-0,3847	birth --> hidden neuron 8	0,4990	category2 --> hidden neuron 3	-0,5874
29	gender2 --> hidden neuron 5	-1,2999	birth --> hidden neuron 9	-0,7694	category2 --> hidden neuron 4	7,7014
30	gender2 --> hidden neuron 6	-17,1868	birth --> hidden neuron 10	-62,6995	category2 --> hidden neuron 5	5,7137
31	category2 --> hidden neuron 1	0,5634	time --> hidden neuron 1	0,6689	Week_date --> hidden neuron 1	31,4874
32	category2 --> hidden neuron 2	3,6341	time --> hidden neuron 2	-2,0158	Week_date --> hidden neuron 2	-29,4272
33	category2 --> hidden neuron 3	0,5811	time --> hidden neuron 3	0,3150	Week_date --> hidden neuron 3	7,7142
34	category2 --> hidden neuron 4	-2,0556	time --> hidden neuron 4	7,5426	Week_date --> hidden neuron 4	-13,6799
35	category2 --> hidden neuron 5	0,1679	time --> hidden neuron 5	-0,0640	Week_date --> hidden neuron 5	2,8949
36	category2 --> hidden neuron 6	-0,0228	time --> hidden neuron 6	-0,4629	input bias --> hidden neuron 1	-20,0664
37	Week_date --> hidden neuron 1	0,0009	time --> hidden neuron 7	-6,3181	input bias --> hidden neuron 2	3,6992
38	Week_date --> hidden neuron 2	-0,0002	time --> hidden neuron 8	0,3152	input bias --> hidden neuron 3	24,3658
39	Week_date --> hidden neuron 3	-6,1817	time --> hidden neuron 9	0,0026	input bias --> hidden neuron 4	-8,9063
40	Week_date --> hidden neuron 4	1,2350	time --> hidden neuron 10	0,3332	input bias --> hidden neuron 5	-9,8802
41	Week_date --> hidden neuron 5	0,5424	gender2 --> hidden neuron 1	0,9557	hidden neuron 1 --> is_fraud	0,1254
42	Week_date --> hidden neuron 6	-0,3088	gender2 --> hidden neuron 2	-0,1579	hidden neuron 2 --> is_fraud	-2,3985
43	input bias --> hidden neuron 1	3,3479	gender2 --> hidden neuron 3	-0,0946	hidden neuron 3 --> is_fraud	-4,6354
44	input bias --> hidden neuron 2	-3,3351	gender2 --> hidden neuron 4	23,6766	hidden neuron 4 --> is_fraud	-3,2223
45	input bias --> hidden neuron 3	5,9892	gender2 --> hidden neuron 5	-0,7207	hidden neuron 5 --> is_fraud	-3,4289
46	input bias --> hidden neuron 4	6,6156	gender2 --> hidden neuron 6	-1,0377	hidden bias --> is_fraud	-4,5542
47	input bias --> hidden neuron 5	-2,2966	gender2 --> hidden neuron 7	-0,1759		
48	input bias --> hidden neuron 6	3,7980	gender2 --> hidden neuron 8	-5,2899		
49	hidden neuron 1 --> is_fraud	-2,8213	gender2 --> hidden neuron 9	0,1286		
50	hidden neuron 2 --> is_fraud	-3,2199	gender2 --> hidden neuron 10	0,0173		
51	hidden neuron 3 --> is_fraud	1,1678	category2 --> hidden neuron 1	0,8043		
52	hidden neuron 4 --> is_fraud	-2,8156	category2 --> hidden neuron 2	-0,8911		
53	hidden neuron 5 --> is_fraud	-0,1654	category2 --> hidden neuron 3	-1,7476		
54	hidden neuron 6 --> is_fraud	3,6940	category2 --> hidden neuron 4	-0,2712		
55	hidden bias --> is_fraud	0,0774	category2 --> hidden neuron 5	-0,2949		

Рисунок 2.13 – Фрагмент нейронних мереж з архітектурою MLP 7-6-1 (загальна кількість шарів 7, кількість прихованих шарів 6), MLP 7-10-1 (загальна кількість шарів 7, кількість прихованих шарів 10), MLP 7-5-1 (загальна кількість шарів 7, кількість прихованих шарів 5) ризику кібершахрайств

Джерело: розрахунки автора

Математичну модель другої нейронної мережі з найбільшою продуктивністю з архітектурою MLP 7-10-1 (загальна кількість шарів 7, кількість прихованих шарів 10) ризику кібершахрайств у загальному вигляді

можна представити в наступному вигляді (враховуючи представлені вище ваги прихованих нейронів):

$$
\begin{aligned}
sn_1^{(2)} &= f(v_{11}^{(1)}p_1 + v_{12}^{(1)}p_2 + \cdots + v_{16}^{(1)}p_6 + v_{17}^{(1)}p_7 + s_1^{(1)}) \\
sn_2^{(2)} &= f(v_{21}^{(1)}p_1 + v_{22}^{(1)}p_2 + \cdots + v_{26}^{(1)}p_6 + v_{27}^{(1)}p_7 + s_2^{(1)}) \\
sn_3^{(2)} &= f(v_{31}^{(1)}p_1 + v_{32}^{(1)}p_2 + \cdots + v_{36}^{(1)}p_6 + v_{37}^{(1)}p_7 + s_3^{(1)}) \\
sn_4^{(2)} &= f(v_{41}^{(1)}p_1 + v_{42}^{(1)}p_2 + \cdots + v_{46}^{(1)}p_{16} + v_{47}^{(1)}p_7 + s_4^{(1)}) \\
sn_5^{(2)} &= f(v_{51}^{(1)}p_1 + v_{52}^{(1)}p_2 + \cdots + v_{56}^{(1)}p_6 + v_{57}^{(1)}p_7 + s_5^{(1)}) \\
sn_6^{(2)} &= f(v_{61}^{(1)}p_1 + v_{62}^{(1)}p_2 + \cdots + v_{66}^{(1)}p_6 + v_{67}^{(1)}p_7 + s_6^{(1)}) \\
sn_7^{(2)} &= f(v_{71}^{(1)}p_1 + v_{72}^{(1)}p_2 + \cdots + v_{76}^{(1)}p_6 + v_{77}^{(1)}p_7 + s_7^{(1)}) \\
sn_8^{(2)} &= f(v_{81}^{(1)}p_1 + v_{82}^{(1)}p_2 + \cdots + v_{86}^{(1)}p_6 + v_{87}^{(1)}p_7 + s_8^{(1)}) \\
sn_9^{(2)} &= f(v_{91}^{(1)}p_1 + v_{92}^{(1)}p_2 + \cdots + v_{96}^{(1)}p_6 + v_{97}^{(1)}p_7 + s_9^{(1)}) \\
sn_{10}^{(2)} &= f(v_{101}^{(1)}p_1 + v_{102}^{(1)}p_2 + \cdots + v_{106}^{(1)}p_6 + v_{107}^{(1)}p_7 + s_{10}^{(1)})
\end{aligned}
\tag{2.15}
$$

$$
\begin{aligned}
\tilde{R} = h^{(3)} = f(&v_1^{(2)}sn_1^{(2)} + v_2^{(2)}sn_2^{(2)} + v_3^{(2)}sn_3^{(2)} + v_4^{(2)}sn_4^{(2)} + v_5^{(2)}sn_5^{(2)} \\
&+ v_6^{(2)}sn_6^{(2)} + v_7^{(2)}sn_7^{(2)} + v_8^{(2)}sn_8^{(2)} + v_9^{(2)}sn_9^{(2)} + v_{10}^{(2)}sn_{10}^{(2)} \\
&+ s^{(2)}
\end{aligned}
$$

де f(-) – специфікація функції активації прихованих нейронів, в нашому випадку логістична функція;

$sn_1^{(2)}$ – вихід першого прихованого нейрону в розрізі другого шару нейронної мережі, входи якого є приховані нейрони першого шару $v_{11}^{(1)}p_1, v_{12}^{(1)}p_2, \ldots, v_{16}^{(1)}p_6, v_{17}^{(1)}p_7$ та $s_1^{(1)}$. Інші $sn_1^{(2)}$, $sn_2^{(2)}$, $sn_3^{(2)}$, $sn_4^{(2)}$, $sn_5^{(2)}$, $sn_6^{(2)}$, $sn_7^{(2)}$, $sn_8^{(2)}$, $sn_9^{(2)}$, $sn_{10}^{(2)}$– аналогічно;

$h^{(3)}$ - вихід прихованих нейронів в розрізі третього шару нейронної мережі; входами для даних виходів є зважені виходи прихованих нейронів другого шару нейронної мережі $sn_1^{(2)}$, $sn_2^{(2)}$, $sn_3^{(2)}$, $sn_4^{(2)}$, $sn_5^{(2)}$, $sn_6^{(2)}$, $sn_7^{(2)}, sn_8^{(2)}$, $sn_9^{(2)}, sn_{10}^{(2)}$.

В якості специфікації функції активації виходу нейронної мережі в нашому випадку є функція тангенса:

$$OUT = \tanh(net) \tag{2.16}$$

де OUT – виходи прихованих нейронів нейронної мережі в розрізі третього шару $\mathrm{h}^{(3)}$;

net – сума вхідних сигналів, зважених на відповідні вагові коефіцієнти для другого шаре, наприклад $sn_1^{(2)} = f(v_{11}^{(1)}p_1 + v_{12}^{(1)}p_2 + \cdots + v_{16}^{(1)}p_6 + v_{17}^{(1)}p_7 + s_1^{(1)}$ для $\mathrm{h}_1^{(2)}$.

Переходячи до опису моделі (2.15) на основі реальних даних отримаємо:

$$sn_1^{(2)} = f(0.0525p_1 + 1.8963p_2 + 0.1272p_3 + 0.6689p_4 + 0.9557p_5 + 0.8043p_6 + 0.3169p_7 + 1.2301) \tag{2.17}$$

$$sn_2^{(2)} = f(25.3785p_1 + 0.2291p_2 + 1.4357p_3 - 2.0158p_4 - 0.1579p_5 - 0.8911p_6 + 1.2680p_7 + 0.2855)$$

$$sn_3^{(2)} = f(-1.1746p_1 + 0.4390p_2 + 9.3003p_3 + 0.3150p_4 - 0.0946p_5 - 1.7476p_6 - 0.1926p_7 - 0.0982)$$

$$sn_4^{(2)} = f(-2.1610p_1 + 0.0998p_2 - 2.6001p_3 + 7.5426p_4 + 23.6766p_5 - 0.2712p_{16} + 0.1670p_7 - 12.2102)$$

$$sn_5^{(2)} = f(-0.3174p_1 - 0.0434p_2 + 6.8840p_3 - 0.0640p_4 - 0.7207p_5 - 0.2949p_6 + 111.1298p_7 + 2.9202)$$

$$sn_6^{(2)} = f(-0.4648p_1 - 42.3234p_2 + 5.1097p_3 - 0.4629p_4 - 1.0377p_5 - 0.0408p_6 - 0.1436p_7 - 4{,}8767)$$

$$sn_7^{(2)} = f(-0.0748p_1 + 1.2498p_2 - 2.6516p_3 - 6.3181p_4 - 0.1759p_5 - 0.3754p_6 + 1.7150p_7 + 9{,}3502)$$

$$sn_8^{(2)} = f(-0.0484p_1 + 2.7336p_2 + 0.4990p_3 + 0.3152p_4 - 5.2899p_5 + 7.7285p_6 - 0.0355p_7 + 0{,}0288)$$

$$sn_9^{(2)} = f(-42.5145p_1 + 0.3439p_2 - 0.7694p_3 + 0.0026p_4 + 0.1286p_5 + 0.5150p_6 - 17.9089p_7 + 4{,}5908)$$

$$sn_{10}^{(2)} = f(0.8976p_1 + 0.5628p_2 - 62.6995p_3 + 0.3332p_4 + 0.0173p_5 - 3.0563p_6 - 0.0090p_7 + 18{,}4531)$$

$$\tilde{R} = h^{(3)}$$
$$= f(-0{,}4461sn_1^{(2)} - 2{,}7718sn_2^{(2)} + 2{,}3205sn_3^{(2)} - 0{,}0568sn_4^{(2)} + 0{,}1228sn_5^{(2)} + sn + 6{,}2373sn_6^{(2)} + 14{,}6218sn_7^{(2)} + 1{,}4856sn_8^{(2)} - 2{,}3082sn_9^{(2)} - 2{,}4977sn_{10}^{(2)} - 2{,}3051$$

Заключним етапом розробленого науково-методичного підходу є прогнозування ризику кібершахрайств на основі побудованої нейромережевої моделі для заданого набору факторів. Прогнозні значення факторних ознак представлені у графах cc_num, amt, bith, time, gender2, category2, week_date рисунку 2.14.

	Custom predictions spreadsheet (Spreadsheet1.sta)											
Cases	1.is_fra	2.is_fra	3.is_fra	4.is_fra	5.is_fra	cc_num	amt	birth	time	gender2	category2	Week_date
1	0,961688	0,943209	0,883276	0,983937	0,953800	2,242177E+15	981,220	62,00000	23,00000	1,000000	11,00000	1,000000
2	0,000000	0,752580	0,005126	0,000000	0,428586	2,242177E+15	6,600	62,00000	3,00000	1,000000	16,00000	2,000000
3	0,839559	0,850771	0,750377	0,939077	0,868995	6,390464E+11	835,250	35,00000	23,00000	1,000000	11,00000	4,000000
4	0,363678	0,858755	0,436133	0,599752	0,856521	3,741252E+14	837,530	51,00000	18,00000	1,000000	6,00000	5,000000
5	0,859336	0,768316	0,975571	0,684923	0,754162	1,800400E+14	806,560	64,00000	23,00000	0,000000	12,00000	3,000000
6	0,847441	0,897887	0,825653	0,856722	0,889069	6,390464E+11	1158,640	35,00000	23,00000	1,000000	11,00000	3,000000
7	0,685081	0,903230	0,750069	1,010499	0,954278	4,423489E+15	916,680	64,00000	22,00000	1,000000	6,00000	1,000000
8	0,997502	0,930881	0,897132	1,005839	0,906021	6,011493E+15	991,100	35,00000	22,00000	1,000000	11,00000	1,000000
9	0,000000	0,768728	0,139991	0,000000	0,661648	3,596217E+15	716,960	33,00000	0,00000	0,000000	6,00000	6,000000
10	0,000000	0,676453	0,354723	0,000000	0,545937	3,051820E+13	855,540	46,00000	1,00000	0,000000	6,00000	1,000000

Рисунок 2.14 – Прогнозні значення ризику кібершахрайств

Джерело: розрахунки автора

Графи 1.is_fra, 2.is_fra, 3.is_fra, 4.is_fra, 5.is_fra відповідно відображують розрахункові прогнозні значення ризику кібершахрайств, обчислені за допомогою 5 згенерованих моделей багатошарового перспептрону MLP. Найкращою за показниками ефективності виявлено другу модель, тому і отримані на основі її використання прогнозні значення було обрано для проведення подальшого аналізу. Таким чином, для усіх розглянутих 10 випадків, ризик кібершахрайств коливається в межах від 0,75 до 0,94 частки одиниці.

Отже, запропонований науково-методичний підхід до оцінювання ризику фінансових кібершахрайств може використовуватися для привентивних заходів протидії здійснення незаконних транзакцій за посередництва фінансової установи та підвищити рівень внутрішнього фінансового моніторингу.

Таким чином, до проблеми шахрайства з платіжними картками необхідно підходити комплексно, на рівні держави із застосуванням сучасних методологій аналізу даних та залученням іноземних експертів. Оскільки великі дані стають доступними через фінансових установ, комп'ютерні алгоритми мають важливе значення для виявлення будь-якого шахрайства, та на основі цього розробити комплекс заходів для посиленого перевірки та контролю зі сторони внутрішньобанківського департаменту фінансового моніторингу.

Висновки до розділу 2

В умовах цифровізації національної економіки вагому роль відіграє вчасна ідентифікації кіберзагроз та здійснення комплексу заходів щодо протидії ним. У роботі запропоновано методику та оцінено узагальнюючий рівень кіберзагроз у розрізі країн Європи, який у 2020 році варіюється від 2,4 ум. од до 74,9 ум.од. та свідчить про нерівномірність здійснення кібератак серед досліджуваних країн. Найбільший рівень кіберзагроз зафіксовано у таких країнах як Іспанія (74,9 ум.од.), Німеччина (63,3 ум.од.), Італія (57,7 ум.од.), а менший рівень загроз у кіберпросторі – в Хорватії (4,3 ум.од.), Польща (2,4 ум.од.) та Словаччина (8,9 ум.од.).

Для визначеня детермінантів поширення кіберзагроз побудовано SVM-моделі машинного навчання двох типів (epsilon-SVM regression та nu-SVM regression) в розрізі чотирьох специфікацій опорних векторів: лінійні, поліноміальні, радіально -базисні функції (RBF) та сигмоподібні на основі дослідження даних вибіркової сукупності країн світу. За результатами емпіричного дослідження причин стрімкого поширення кібершахрайств у фінансовому секторі економіки шляхом використання сигмоїдної nu-SVM regression моделі встановлено, що основними драйверами зростання кібершахрайства є частка населення, яка користується онлайн банкінгом, рівень навичок в Інтернеті, інтенсивність онлайн діяльності.

Ураховуючи масовий перехід користувачів платіжних послуг в онлайн у період карантину, розвитку онлайн розрахунків важливим пріоритетом для державного регулятора є необхідність максимально убезпечити їх від можливих інцидентів інформаційної безпеки. Однією з найбільш вразливих ланок в забезпеченні інформаційної безпеки фінансової системи є споживачі фінансових послуг. У роботі запропоновано методику для оцінювання інтегрального показника кібервразливості споживачів фінансових послуг методом мультиплікативної згортки Кіні 17 нормалізованих індикаторів.

Апробація запропонованого методичного підходу засвідчила, що рівень кібервразливості споживачів фінансових послуг у країнах Європи становить у середньому 11%, що дозволяє стверджувати про усвідомленість населенням європейський країн наявних загроз у віртуальному просторі, способів захисту від кіберзлочинності. Проте рівень кібервразливості споживачів фінансових послуг у розрізі країн ЄС не є однорідним, а саме найменшим ризик стати жертвою кібершахрайства мають громадяни таких країн як Данія, Нідерланди, Швеція. До країн з найвищими значеннями розрахованого рівня кібервразливості споживачів фінансових послуг (18%) належать: Іспанія, Італія, Румунія.

Розроблено науково-методичний підхід до оцінювання та прогнозування ризику кібершахрайств у сфері фінансових послуг на основі базових восьми індикаторів з використанням нейронної мережі: стать власника банківської картки, його вік, номер банківського рахунку, сума транзакції, вид категорій/товару, година проведення операції, день тижня проведення операції та індикатор шахрайства. 54.2% власників банківських карток, за допомогою яких здійснювалися шахрайські транзакції, були жінки. Середній вік держателів банківських карток, які здійснювали шахрайські фінансові транзакції, становив 50 років. Найбільший обсяг незаконних транзакцій реалізується проходить на купівлю продуктів харчування та товарів. Для вчасної ідентифікації ризику шахрайства з банківськими платіжними картками проведено навчання нейронної мережі на основі тестової вибірки.

Основні положення другого розділу дисертаційної роботи опубліковано автором в роботах [13, 24, 25, 30, 31, 32, 104].

РОЗДІЛ 3 ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ УПРАВЛІННЯ КІБЕРРИЗИКАМИ У СУЧАСНИХ УМОВАХ РОЗВИТКУ ЦИФРОВОЇ ЕКОНОМІКИ

3.1. Науково-методичний підхід до ідентифікації сценаріїв раціональної поведінки економічних агентів в умовах цифровізації фінансового сектору економіки України

Дослідивши у попередніх підрозділах дисертаційної роботи такі особливості як оцінювання кібервразливості економічних суб'єктів та ідентифікація значимих детермінантів поширення кіберзагроз, справедливо зауважити, що в подальшому актуальності набуває розробка методичних засад, які виступатимуть основою формування сценаріїв поведінки органів виконавчої влади та, безпосередньо, суб'єктів господарювання в залежності від рівня кіберзагроз фінансовому сектору економіки України, а також під впливом рівня діджиталізації фінансового сектору й технологічного розвитку. Починаючи опис запропонованого науково-методичного підходу доцільно зауважимо декілька базових положень. Перше, дослідження кіберзагроз в умовах цифровізації національної економіки запропоновано прослідковувати через призму фінансового сектору, оскільки цей сектор є основним каналом поширення та подальшої мультиплікації шоків в державі. Крім того, справедливо зазначити, що фінансова система України наразі є однією з найбільш діджиталізованих систем у світі та акумулює не тільки фінансову, але й персональну інформацію більшості громадян держави. Тому кібератаки зазначеної системи, призведуть не тільки до фінансових збитків, а й до втрати приватності українців. Друге, прийнято рішення розглядати стійкість економічних агентів до дії внутрішніх та зовнішніх шоків в умовах цифровізації фінансового сектору економіки України за допомогою ідентифікації взаємозв'язків у трикутнику «діджиталізація фінансового сектору–технологічний розвиток–кіберзагрози».

Обрання вище зазначених трьох складових дослідження раціональної поведінки економічних агентів в умовах цифровізації фінансового сектору національної економіки обумовлено сучасним трендом розвитку цього сектору, а саме тотальним оцифровуванням фінансової інформації з метою активізації бізнес-процесів фінансових корпорацій (віртуального банкінгу, інтернет-страхування, інтернет-трейдингу, тощо). Так, розглядаючи діджиталізацію можливо досягти розуміння про рівень цифрової трансформації фінансового сектору, тобто ступінь проникнення інноваційних технологій до бізнес-процесів банків та інших фінансових посередників. У свою чергу, швидкість та інтенсифікація діджиталізації фінансового сектору, залежить від технологічної розвиненості інформаційної системи України. Рівень забезпеченості суспільства високоякісними та сучасними інформаційно-комунікаційними технологіями є основою розвитку будь-яких діджитал-послуг та діджитал-продуктів. Паралельно з цим, справедливо зазначити, що кіберзагрози виступають, так би мовити, похідними від діджиталізації та технологічного розвитку, оскільки до активної цифровізації усіх сфер життя суспільства кібератак не могло існувати по своїй суті. Таким чином, вершини трикутнику «діджиталізація фінансового сектору–технологічний розвиток–кіберзагрози» є не тільки взаємопов’язаними, але й взаємозалежними. Отже, розглянемо детально кожен з шести етапів розробки та практичної реалізації науково-методичного підходу до побудови сценаріїв поведінки економічних агентів в умовах цифровізації фінансового сектору національної економіки щодо забезпечення їх стійкості до зовнішніх та внутрішніх загроз.

На першому етапі охарактеризуємо окремо кожну зі складових трикутнику «діджиталізація фінансового сектору–технологічний розвиток–кіберзагрози». Так, діджиталізацію фінансового сектору опишемо за допомогою таких показників, як: частка громадян, що користуються онлайн банкінгом; співвідношення безготівкових карткових операцій до загальної кількості трансакцій; частки переказів з картки на картку; кількості

депозитних рахунків на 1000 осіб дорослого населення. Перше, ніж надавати пояснення кожному з показників характеристики діджиталізації фінансового сектору зауважимо, що всі вони відносяться до банківської системи, оскільки для України характерна банкоцентрична модель фінансового ринку. Тобто банки концентрують переважну більшість вільних фінансових ресурсів суб'єктів господарювання й населення (у вигляді депозитів) та в подальшому приймають незалежні управлінські рішення щодо їх інвестування. Обсяги фінансових ресурсів, які перерозподіляються через небанківські фінансові установи майже не впливають на фінансову безпеку України та не мають вирішального значення для розвитку національної економіки. Тобто, саме банки та їх рівень діджиталізації є рушійною силою цифровізації всієї фінансової системи України. Отже, зупиняючись на кожному з показників більш детально, зазначимо, що частка громадян, які користуються онлайн банкінгом відображає рівень залученості населення України до банківських цифрових технологій. Саме попит демонструє наскільки діджитал-послуги та діджитал-продукти банків є корисними, популярними та затребуваними, оскільки тільки якісно розроблені банківські сервіси можуть зацікавити клієнтів й збільшувати їх чисельність з кожним роком. Співвідношення безготівкових карткових операцій до загальної кількості трансакцій відображають трансформацію банківської системи у бік збільшення її діджиталізації, саме переведення операцій у безготівкову форму і є критерієм довіри клієнтів до цифрових послуг банків, їх високу якість та поширеність. Частки переказів з картки на картку, також є показником, що свідчить про становлення діджиталізації банківської системи, оскільки розвинений інтернет-банкінг спрошує цю операцію та робить її максимально зручною для клієнта. Зважаючи на той факт, що саме обсяг депозитних ресурсів для банків є основою їх інвестиційної й операційної діяльності, то фінансові посередники спрямовують значну частину власних зусиль для покращення депозитних продуктів, що в сучасних умовах неможливо без їх активної діджиталізації. Виходячи з цього, визначальним чинником для опису рівня діджиталізації

фінансової системи є показник кількість депозитних рахунків на 1000 осіб дорослого населення.

Технологічний розвиток, запропоновано визначати за допомогою таких показників, як середня швидкість завантаження; кількість захищених інтернет-серверів; активні абоненти мобільного широкосмугового зв'язку на 100 жителів; особи з базовими навичками інформаційно-комунікаційних технологій (ІКТ). Отже, зупиняючись на характеристики кожного з них зауважимо, що середня швидкість завантаження, на нашу думку, є базовий показник технологічного розвитку, його динаміка демонструє рівень інноваційного прогресу та забезпечує подальший стимул розвитку нових фінансових продуктів. Саме швидкість завантаження створила умови для формування необанків. Кількість захищених інтернет-серверів, є показником, який також характеризує рівень технологічного розвитку й прогресу в ньому. Саме рівень кіберзахисту забезпечує впевненість в успіху будь-якого продукту або послуги в інтернет просторі, в іншому випадку фінансовий посередник отримає значні збитки, а клієнти будуть ошукані. Активні абоненти мобільного широкосмугового зв'язку на 100 жителів, це критерій, який демонструє використання преваг технологічного розвитку населенням України. Увесь спектр фінансових цифрових продуктів наразі знаходиться в смартфоні, і саме якісний мобільний широкосмуговий зв'язок створює можливості для зростаючого попиту на фінансові діджитал продукти та послуги. Розглядаючи останній чинник цього напрямку, зазначимо, що яким би не був технологічний розвиток країни, якщо в державі низька цифрова грамотність населення, подальшого інноваційного розвитку не буду. Виходячи з цього, показник особи з базовими навичками ІКТ є вкрай важливим для формування сучасного цифрового суспільства в Україні та подальшого поступального становлення національної цифрової економіки.

Переходячи до аналізу ризику кіберзагроз, відмітимо, що цей напрямок описаний за допомогою таких показників, як шахрайства та кібернетичні загрози, а також суми збитків від незаконних дій з платіжними картками.

Перший показник є якісним й характеризує відношення менеджменту вітчизняних фінансових посередників до ризиків, які загрожують національному фінансовому сектору, тобто він явно відображує очікування суб'єктів ринку фінансових послуг до потенційних загроз кібер атак серед усіх наявних ризиків діяльності компанії. Визначення цього показника відбувається на основі опитування топ-менеджерів провідних банків та небанківських фінансових установ України (у 2023 р. в опитуванні взяли участь керівники 22 банків, 10 страхових компаній та 3 інвестиційних компаній) [38]. Показник суми збитків від незаконних дій з платіжними картками є кількісним та описує втрати клієнтів банків від кіберзагроз найбільш поширеному та найпопулярнішому банківському продукту серед населення України.

З метою повноцінного розуміння вхідного масиву даних реалізації науково-методичного підходу до побудови сценаріїв поведінки економічних агентів в умовах цифровізації фінансового сектору національної економіки щодо забезпечення їх стійкості до зовнішніх та внутрішніх загроз, згрупуємо показники у таблицю 3.1 та проведемо їх експрес-аналіз.

Отже, проводячи аналіз показників характеристики діджиталізація фінансового сектору, зауважимо, що усі чотири релевантні чинники протягом 2019-222 рр. мали тенденцію до зростання. Так, найбільший темп приросту прослідковується для кількості депозитних рахунків на 1000 осіб дорослого населення і складав 29,1%. Перевищення 20% значення темпу приросту за чотири роки характерно й для частки переказів з картки на картку (26,9%) та співвідношення безготівкових карткових операцій до загальної кількості трансакцій (23,4%). Частка громадян, що користуються онлайн банкінгом за 2019-2022 рр. зросла тільки на 8,3%, проте на разі в Україні вона становить 62,3%, що є доволі високим значенням зважаючи на частку людей похилого віку серед клієнтів банків.

Таблиця 3.1 – Вхідні статистичні дані характеристики діджиталізації фінансового сектору, технологічного розвитку та ризику кіберзагроз за 2019–2022 рр.

Умовні позначення показників	Назва групи	Показник	Рік			
			2019	2020	2021	2022
DFS1	Діджиталізація фінансового сектору	Частка переказів з картки на картку, %	42,0	42,8	43,6	53,3
DFS2		Частка громадян, що користуються онлайн банкінгом,%	57,5	60,8	60,6	62,3
DFS3		Співвідношення безготівкових карткових операцій до загальної кількості трансакцій, %	54,8	57,5	61,4	67,6
DFS4		Кількість депозитних рахунків на 1000 осіб дорослого населення	3191,5	3360,3	3853,1	4120,0
TR1	Технологічний розвиток	Середня швидкість завантаження, Мбіт/с	7,7	15,1	25,3	47,7
TR2		Кількість захищених інтернет-серверів (на 1 мільйон осіб)	7,9	9,0	9,3	9,7
TR3		Активні абоненти мобільного широкосмугового зв'язку на 100 жителів	77,3	85,3	80,1	82,9
TR4		Особи з базовими навичками ІКТ (%)	23,9	31,9	35,8	37,8
RC1	Ризик кіберзагроз	Шахрайство та кібернетичні загрози, %*	35,0	27,0	35,0	40,0
RC2		Сума збитків від незаконних дій з платіжними картками, млн грн	149,0	190,0	330,0	481,0

Примітка: * – рівень ризику, що існує у фінансовому секторі України через дію шахрайств та кібернетичних загроз (один з двадцяти одного фактору які були проаналізовані)

Джерело: Національний банк України [49], Cable [66], Світовий банк [81]

Найбільше зростання протягом останнього періоду (2022-2021 рр.) відбувалось в межах частки переказів з картки на картку, так цей показник за рік зріс більше ніж на 22,2% (минулі роки середній темп приросту склав 1,9%). Усе вище зазначене, свідчить про те, що фінансовий сектор України активно діджиталізується з акцентом на удосконалення вже існуючих цифрових банківських послуг та продуктів, які можна реалізувати через смартфон.

Переходячи до показників характеристики технологічного розвитку зауважимо, що вони зростали ще швидше, ніж показники діджиталізації фінансового сектору. Так, темп приросту середньої швидкості завантаження протягом 2019-2022 рр. складав 519,5%, а відповідний показник осіб з базовими навичками ІКТ 58,2%. Більше ніж 20% темп приросту протягом досліджуваного періоду був характерний і для кількісті захищених інтернет-серверів (на 1 мільйон осіб), а саме 22,2%. Показник, який мав не тільки найнижчий темп приросту протягом 2019-2022 рр. (7,2%), але й зменшився у 2021 р. на 5,2% порівняно до 2020 р. є активні абоненти мобільного широкосмугового зв'язку на 100 жителів. У той же час, цей показник протягом останніх трьох років дослідження складав не менше 80% від загальної чисельності абонентів мобільного зв’язку, що є доволі високим значенням. Вище наведені тенденції цілком зрозумілі, оскільки технічний прогрес повинен випереджати процеси цифровізації і щорічне значення темпів приросту середньої швидкості завантаження даних на рівні 84,1% тому підтвердження. Збільшення швидкості завантаження неможливе без розвитку технологій як самої передачі, так і відправлення й отримання даних. Тільки за таких умов, діджитал послуги та продукти у фінансовому секторі будуть безперервно розвиватись на базі нових технологій, а не змінювати форму використовуючи вже існуючу основу створення та розповсюдження.

Досліджуючи останню групу показників характеристики ризику кіберзагроз, зазначимо, що як і рівень оцінювання топ-менеджерами України ризиків, що існує у фінансовому секторі через дію шахрайств та кібернетичних загроз, так і безпосередній обсяг збитків від незаконних дій з платіжними

картками неодмінно зростав протягом 2019-2022 рр. І якщо перший показник коливався протягом досліджуваного періоду в проміжку 27-40% (середній темп просту 7%), то другий зріс за чотири роки на 222,8% (середній темп приросту 49%). Це свідчить як про розуміння фахівців фінансового сектору про існування кібер ризику, так і про його руйнівну роль для стійкості фінансової системи.

Визначивши особливості розвитку показників характеристики вхідного масиву даних перейдемо до другого етапу досліджуваної методики, який полягає у приведенні обраних релевантних показників до співставного вигляду. Виходячи з того, що отримана вибірка дослідження побудови сценаріїв поведінки економічних агентів в умовах цифровізації фінансового сектору національної економіки щодо забезпечення їх стійкості до зовнішніх та внутрішніх загроз сформована з показників стимуляторів та дестимуляторів, необхідності набуває застосування двох підходів до нормалізації. Для стимуляторів запропоновано проводити адаптивну природню нормалізацію, а для дестимуляторів адаптивну нормалізацію Севіджа з урахуванням коригування на середнє квадратичне відхилення, що дозволить привести розглянуту множину показників до співставного вигляду. Отже, проведемо дослідження механізму формалізації наведених методів нормалізації, а саме математичні співвідношення (3.1) та (3.2), які дозволяють обчислити нормалізовані значення показників ідентифікації критичних зон в поведінці економічних агентів в умовах цифровізації фінансового сектору економіки України.

Нормалізація показників за допомогою формули Севіджа для дестимуляторів:

$$n_{igj} = \frac{\max\limits_{j} a_{igj} + SD(a_{igj}) - a_{igj}}{\max\limits_{j} a_{igj} - \min\limits_{j} a_{igj} + 2 \cdot SD(a_{igj})} \quad (3.1)$$

де n_{igj} – нормалізоване значення i-го показника g-тої групи в розрізі j-го року;

a_{igj} – фактичне значення i-го показника g-тої групи в розрізі j-го року;

$\max_j a_{igj}$ – максимальне значення i-го показника g-тої групи в межах розглянутого часового діапазону;

$SD(a_{igj})$ – середнє квадратичне відхилення;

$\min_j a_{igj}$ – мінімальне значення i-го показника g-тої групи в межах розглянутого часового діапазону.

Нормалізація показників за допомогою формули природньої нормалізації для стимуляторів:

$$n_{igj} = \frac{a_{igj} - \min_j a_{igj} + SD(a_{igj})}{\max_j a_{igj} - \min_j a_{igj} + 2 \cdot SD(a_{igj})} \quad (3.2)$$

Обчислені за допомогою застосування формул (3.1) та (3.2) нормалізовані значення показників діджиталізації фінансового сектору, технологічного розвитку та ризику кіберзагроз за період з 2019 р. по 2022 р. згрупуємо в таблицю 3.2.

Виходячи з того факту, що розглянуті показники в межах кожної групи мають різну силу впливу на потенційний результату, то на третьому етапі реалізації запропонованої методики, актуальності набуває ідентифікація їх пріоритетність. Справедливо зазначити, що доцільність реалізації даного етапу обумовлена врахуванням різного рівня значимості кожного релевантного фактору для отримання кінцевого результату. Визначення пріоритетності розглянутих показників діджиталізації фінансового сектору, технологічного розвитку та ризику кіберзагроз запропоновано здійснити за допомогою методу головних компонент, а саме побудови графіку кам’янистого осипу та врахуванні власних значень кореляційної матриці.

Таблиця 3.2 – Нормалізовані значення показників діджиталізації фінансового сектору, технологічного розвитку та ризику кіберзагроз за 2019-2022 рр.

Умовні позначення показників	Рік			
	2019	2020	2021	2022
DFS1	0,2418	0,2783	0,3149	0,7582
DFS2	0,2282	0,5997	0,5816	0,7718
DFS3	0,2321	0,3468	0,5064	0,7679
DFS4	0,2404	0,3348	0,6104	0,7596
TR1	0,2326	0,3312	0,4670	0,7674
TR2	0,2653	0,2654	0,7148	0,7347
TR3	0,2319	0,7681	0,4210	0,6074
TR4	0,2346	0,5401	0,6890	0,7654
RC1	0,4369	0,7736	0,4369	0,2264
RC2	0,7623	0,6975	0,4763	0,2377

Джерело: розрахунки автора

Отже, формалізацію пріоритетності показників в розрізі кожної із груп дослідження доцільно проводити за допомогою ідентифікації вагових коефіцієнтів w_{ig} (для i-го показника в межах g-тої групи) змінних n_{igj} – показників діджиталізації фінансового сектору, технологічного розвитку та ризику кіберзагроз, яка має дорівнювати одиничному значенню (3.3):

$$F\left(w(n_{1gj}), \dots, w(n_{ngj})\right) = F\left(w_{1g}, \dots, w_{ng}\right) = \sum_{i=1}^{n} w_{ig} \to 1 \qquad (3.3)$$

де $F\left(w(n_{1gj}), \dots, w(n_{ngj})\right) = F\left(w_{1g}, \dots, w_{ng}\right)$ – функціональна залежність між ваговими коефіцієнтами w_{ig} змінних n_{igj};

n_{igj} – нормалізоване значення i-го показника g-тої групи в розрізі j-го року;

w_{ig} – ваговий коефіцієнт i-го показника в межах g-тої групи.

Для встановлення пріоритетності груп показників діджиталізації фінансового сектору, технологічного розвитку та ризику кіберзагроз скористаємось можливостями програмного пакету Statistica, зокрема методом головних компонент (команда Statistica/Multivariate Explanatory Techniques/Principal Components and Classification Analysis). Результати представимо на рисунках 3.1 – 3.6.

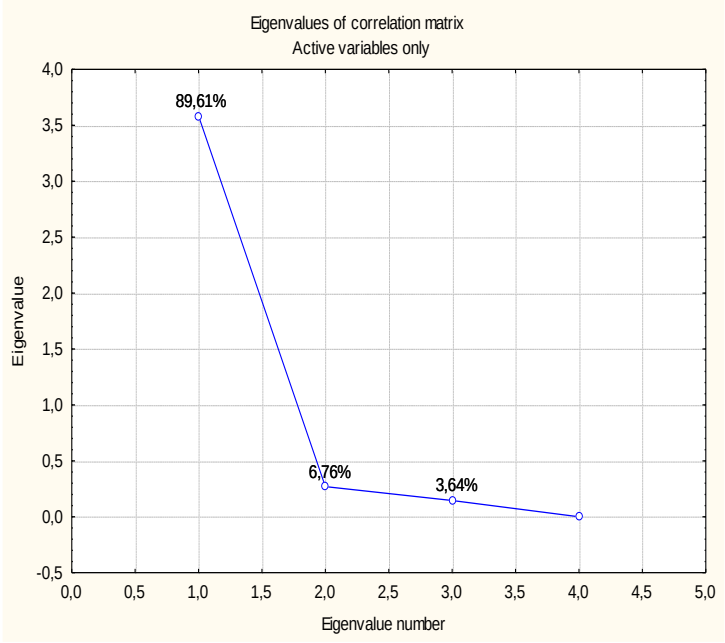


Рисунок 3.1 – Фрагмент програми Statistica графіку кам’янистого опису в розрізі першої групи показників діджиталізації фінансового сектору

Джерело: розрахунки автора

	Eigenvalues of correlation matrix, and related statis Active variables only			
Value number	Eigenvalue	% Total variance	Cumulative Eigenvalue	Cumulative %
1	3,584242	89,60605	3,584242	89,606
2	0,270334	6,75835	3,854576	96,364
3	0,145424	3,63560	4,000000	100,000

Рисунок 3.2 – Фрагмент програми Statistica таблиці власних значень кореляційної матриці та пов’язаних статистичних показників в розрізі першої групи діджиталізації фінансового сектору

Джерело: розрахунки автора

На основі аналізу рисунків 3.1 та 3.2 для першої групи показників діджиталізації фінансового сектору можна зробити висновок про доцільність оцінювання пріоритетності зазначених показників враховувати лише першу головну компоненту, представлену першим фактором, оскільки на його варіацію припадає 89,61% загальної варіації, про це свідчить як графік кам'янистого осипу (рисунок 3.1), так і табличні значення власних значень факторів в розрізі показників (рисунок 3.2).

Безпосередньо, рівень впливу кожного з показників групи діджиталізації фінансового сектору формалізуємо за допомогою рисунку 3.3.

	Variable contributions, based on correlations (Spreadsh		
Variable	Factor 1	Factor 2	Factor 3
DFS1	0,237677	0,403146	0,269043
DFS2	0,227876	0,582377	0,177411
DFS3	0,276856	0,014228	0,026364
DFS4	0,257591	0,000249	0,527182

Рисунок 3.3 – Фрагмент програми Statistica таблиці вкладу змінних на основі кореляції в розрізі першої групи діджиталізації фінансового сектору

Джерело: розрахунки автора

Таким чином, на основі рисунку 3.3 можна стверджувати, що найбільш впливовим виступає показник *DFS3* – співвідношення безготівкових карткових операцій до загальної кількості трансакцій. Другим за пріоритетністю є показник *DFS4* – кількість депозитних рахунків на 1000 осіб дорослого населення. У свою чергу, майже однаковий рівень важливості мають *DFS1* – частка переказів з картки на картку та *DFS2* – частка громадян, що користуються онлайн банкінгом.

Переходячи до аналізу пріоритетності показників технологічного розвитку, зауважимо, що на основі результатів розрахунків зображених на рисунках 3.4 та 3.5 можна стверджувати, що з метою оцінювання пріоритетності показників досліджуваної групи доцільно враховувати перші дві головні компоненти, представлену першим і другим факторами. Це обумовлено тим, що на їх варіацію припадає 71,89% загальної варіації.

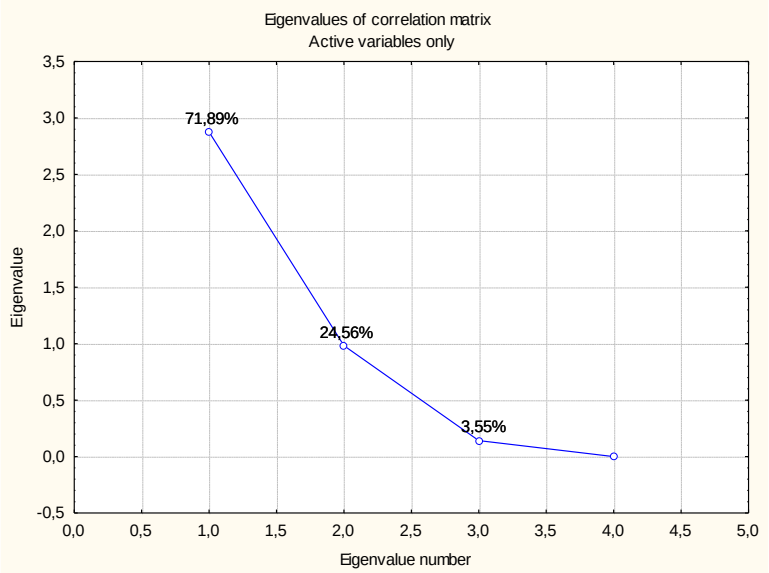


Рисунок 3.4 – Фрагмент програми Statistica графіку кам’янистого опису в розрізі другої групи показників технологічного розвитку

Джерело: розрахунки автора

Value number	Eigenvalues of correlation matrix, and related statis Active variables only			
	Eigenvalue	% Total variance	Cumulative Eigenvalue	Cumulative %
1	2,875579	71,88948	2,875579	71,889
2	0,982549	24,56374	3,858129	96,453
3	0,141871	3,54679	4,000000	100,000

Рисунок 3.5 – Фрагмент програми Statistica таблиці власних значень кореляційної матриці та пов’язаних статистичних показників в розрізі другої групи технологічного розвитку

Джерело: розрахунки автора

Зупиняючись на визначенні рівня впливу кожного з показників групи технологічного розвитку (рисунку 3.6) зауважимо, що найсуттєвіший вплив здійснюють показники TR4 – особи з базовими навичками ІКТ та TR1 – середня швидкість завантаження. Відносно менший вплив, проте теж суттєвий здійснює показник TR2 – кількість захищених інтернет-серверів, найменшу пріоритетність має показник TR3 – активні абоненти мобільного широкосмугового зв'язку на 100 жителів.

Variable	Variable contributions, based on correlations (Spreadsh		
	Factor 1	Factor 2	Factor 3
TR1	0,309498	0,016552	0,660806
TR2	0,267801	0,217430	0,114759
TR3	0,088924	0,757493	0,000123
TR4	0,333776	0,008525	0,224312

Рисунок 3.6 – Фрагмент програми Statistica таблиці вкладу змінних на основі кореляції в розрізі другої групи технологічного розвитку

Джерело: розрахунки автора

Виходячи з того, що у випадку з групою технологічного розвитку визначені дві головні компоненти для ідентифікації пріоритетності, то актуальності набуває проведення наступних перетворень. Враховуючи дані наведені на рисунку 3.5 та 3.6 визначимо вагові коефіцієнти показників w_{ig} на основі середньої арифметичної зваженої:

$$w_{ig} = \frac{\sum_{j=1}^{2} F_{ij} \cdot v_j}{\sum_{j=1}^{2} v_j} \tag{3.4}$$

де w_{ig} – ваговий коефіцієнт i-го показника в межах g-тої групи;

F_{ij} – значення вкладу i-тої змінної в розрізі j-того фактору (головної компоненти) на основі кореляції;

v_j – відсоток загальної варіації власних значень кореляційної матриці в розрізі j-того фактору (головної компоненти).

Результати обчислень за формулою (3.4) представимо в таблиці 3.3.

Таблиця 3.3 – Вклад змінних на основі кореляції, обмеження пріоритетності та ваги показників другої групи технологічного розвитку

Факторні навантаження	71,88948	24,56374	Вагові коефіцієнти
Змінні/Фактори	Фактор 1	Фактор 2	
RT1	0,309498	0,016552	0,235
RT2	0,267801	0,217430	0,255
RT3	0,088924	0,757493	0,259
RT4	0,333776	0,008525	0,251

Джерело: розрахунки автора

Отже, пріоритетність показників: RT1, RT2, RT3 та RT4, відповідно дорівнює 0,235 од., 0,255 од., 0,259 од., 0,251 од.

Розглядаючи останню групу показників характеристики ризику кіберзагрози, зазначимо, що на основі рисунків 3.7 (графік кам'янистого осипу) та 3.8 (табличні значення власних значень факторів в розрізі показників) можна зробити висновок про доцільність оцінювання пріоритетності показників враховувати лише першу головну компоненту, представлену першим фактором (варіація дорівнює 85,99% загальної варіації).

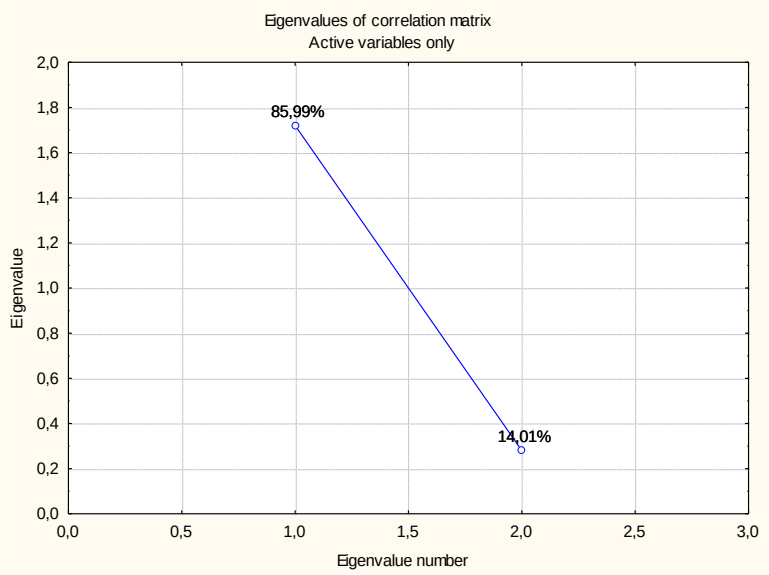


Рисунок 3.7 – Фрагмент програми Statistica графіку кам'янистого опису в розрізі третьої групи ризику кіберзагроз

Джерело: розрахунки автора

Value number	Eigenvalues of correlation matrix, and related statis Active variables only			
	Eigenvalue	% Total variance	Cumulative Eigenvalue	Cumulative %
1	1,719829	85,99144	1,719829	85,991
2	0,280171	14,00856	2,000000	100,000

Рисунок 3.8 – Фрагмент програми Statistica таблиці власних значень кореляційної матриці та пов'язаних статистичних показників в розрізі третьої групи ризику кіберзагроз

Джерело: розрахунки автора

На основі рисунку 3.9., у свою чергу, можна зазначити, що обидва розглянуті показники, а саме й шахрайство та кібернетичні загрози, а також сума збитків від незаконних дій з платіжними картками мають однакову пріоритетність – 0,5 частки одиниці.

	Variable contributions, based on correlations (Spreadsh	
Variable	Factor 1	Factor 2
RC1	0,500000	0,500000
RC2	0,500000	0,500000

Рисунок 3.9 – Фрагмент програми Statistica таблиці вкладу змінних на основі кореляції в розрізі третьої групи ризику кіберзагроз

Джерело: розрахунки автора

Таким чином, узагальнити отримані розрахунки рівня пріоритетності показників характеристики діджиталізація фінансового сектору, технологічного розвитку та кіберзагроз можна за допомогою таблиці 3.4.

Таблиця 3.4 – Рівень пріоритетності показників характеристики діджиталізація фінансового сектору, технологічного розвитку та кіберзагроз

Умовні позначення показників	DFS1	DFS2	DFS3	DFS4	TR1	TR2	TR3	TR4	RC1	RC2
Питома вага	0,238	0,228	0,277	0,258	0,235	0,255	0,259	0,251	0,500	0,500

Джерело: розрахунки автора

Проведені на третьому етапі реалізації науково-методичного підходу до побудови раціональних сценаріїв поведінки економічних агентів в умовах цифровізації фінансового сектору національної економіки розрахунки дозволяють знайти інтегральний показник в розрізі кожної групи окремо за допомогою трансформованої згортки Кіні (четвертий етап). Математична формалізація цього етапу має наступний вигляд (формула 3.5).

$$K_{jg} = \frac{1}{G} \cdot \prod_{i} (1 + G \cdot w_{ig} \cdot n_{igj}) \quad (3.5)$$

де K_{jg} – інтегральний показник Кіні в розрізі j-го року в межах g-тої групи показників.

G – загальна кількість показників і розрізі g-тої групи;

n_{igj} – нормалізоване значення i-го показника g-тої групи в розрізі j-го року;

w_{ig} – ваговий коефіцієнт і-го показника в межах g-тої групи.

Провівши відповідні розрахунки на основі рівняння 3.5 практичні результати згрупуємо в таблицю 3.5

Таблиця 3.5 – Динаміка інтегральних показників діджиталізації фінансового сектору, технологічного розвитку та ризику кіберзагроз за 2019-2022 рр.

Інтегральні показники груп	Рік			
	2019	2020	2021	2022
Діджиталізація фінансового сектору (DFS)	0,583	0,910	1,264	2,417
Технологічний розвиток (TR)	0,593	1,154	1,511	2,169
Ризик кіберзагроз (RC)	1,266	1,505	1,061	0,759

Джерело: розрахунки автора

Отже, на основі отриманих розрахунків справедливо зазначити, що протягом 2019-2022 рр. інтегральні показники досліджуваних напрямків змінювались нерівномірно. Так, інтегральний показник діджиталізації фінансового сектору та технологічного розвитку неодмінно зростали з середнім темпом приросту 62,1% та 56,4 %, відповідно. У свою чергу, для діджиталізації фінансового сектору піковий темп приросту прослідковується у 2022 р. порівняно до 2021 р. – 91,2%, а для технологічного розвитку у 2020 р. порівняно до 2019 р. – 94,6%. Зупиняючись, на ризику кіберзагроз перш за все, зауважимо, що абсолютні значення інтегрального показника необхідно трактувати навпаки, чим воно менше тим ризик більший. Це пов’язано з тим, що

в процесі нормалізації релевантні чинники, що його формували (шахрайство та кібернетичні загрози, сума збитків від незаконних дій з платіжними картками), розглядались за своєю суттю, тобто як дестимулятори. У свою чергу, ризику кіберзагроз, це також показник збільшення якого призводить до негативного ефекту. Отже, на основі даних наведених в таблиці 3.5 зауважимо, що починаючи з 2020 р. абсолютне значення інтегрального показника ризику кіберзагроз зменшувався щороку в середньому на 29%. Тобто, можна стверджувати, що інтенсифікація процесу розширення цифрових технологій в національній економіці спричиняє й збільшення кіберзагроз, тому як суб'єкти господарювання, так і державні органи контролю повинні розширювати засоби моніторингу та ліквідації кіберзагроз. Безумовно, компанії повинні постійна удосконалювати власну системи кбіербезпеки, проте конкретний набір інструментів, заважаючи на обмежений обсяг фінансових ресурсів, можна ідентифікувати розрахувавши рівень загрози у конкретний момент часу в залежності від вхідних параметрів.

На наступному (п'ятому) етапі реалізації запропонованого науково-методичного підходу, актуальності набуває визначення якісної характеристики інтегральних показників діджиталізація фінансового сектору, технологічного розвитку та ризику кіберзагроз. Для вирішення поставленої задачі, запропоновано використати підхід на основі стандартного відхилення (формули 3.6):

$$\begin{cases} [min - SD; \frac{2min-3SD+max}{3}) - \text{низький рівень для DFS й TR, високий рівень для RC;} \\ \left[\frac{2min-3SD+max}{3}; \frac{min-3SD+2max}{3}\right] - \text{середній рівень для DFS, TR та RC;} \\ (\frac{min-3SD+2max}{3}; max + SD] - \text{високий рівень для DFS й TR, низький рівень для RC;} \end{cases} \quad (3.6)$$

де min – мінімальне значення показника;

SD – стандартне відхилення;

max – максимальне значення показника.

Використовуючи наведений вище механізм встановимо три проміжки низького, середнього та високого рівня для інтегральних показників діджиталізація фінансового сектору, технологічного розвитку та ризику кіберзагроз. Результати проведених розрахунків згрупуємо в таблицю 3.6.

Таблиця 3.6 – Якісні характеристики інтегральних показників діджиталізація фінансового сектору, технологічного розвитку та ризику кіберзагроз

Показники	низький рівень (червона зона)		середній рівень (жовта зона)		високий рівень (зелена зона)	
	min	max	min	max	min	max
Діджиталізація фінансового сектору (DFS)	-0,217	0,395	0,395	1,007	1,007	3,217
Технологічний розвиток (TR)	-0,092	0,454	0,454	0,999	0,999	2,882
Ризик кіберзагроз (RC)	0,940	1,822	0,691	0,940	0,442	0,691

Джерело: розрахунки автора

Реалізація п’ятого етапу, дозволяє надати отриманим абсолютним значенням інтегральних показників якісну характеристику та визначити чи знаходиться показник в прийнятному стані, чи їх значення критичні для успішного розвитку процесу цифровізації національної економіки.

На завершальному шостому етапі реалізації науково-методичного підходу до побудови сценаріїв поведінки економічних агентів в умовах цифровізації фінансового сектору національної економіки щодо забезпечення їх стійкості до зовнішніх та внутрішніх загроз проведемо графічну інтерпретацію отриманих результатів (рисунок 3.9).

Отримане графічне зображення дає можливість визначити не тільки динаміку ситуації всередині трикутнику «діджиталізація фінансового сектору–технологічний розвиток–кіберзагрози», але й з’ясувати, які практичні дії та інструменти необхідно застосовувати державним органам виконавчої влади та суб’єктам господарювання в конкретний момент часу. Так, за умови знаходження усіх трьох інтегральних показників у зеленій зоні (таблиця 3.6), справедливо стверджувати про стабільну ситуацію у фінансовому секторі

економіки та рівномірний розвиток діджиталізації й технологій. У свою чергу, рівень кібер загроз, за такої ситуації, знаходиться на прийнятному рівні та не заважає безпечній роботі фінансових посередників. За умови потрапляння інтегрального показника технологічного розвитку у червону зону, а двох інших інтегральних показників у жовту та зелену зону, справедливо стверджувати про те, що з часом цифровий розвиток економіки завершиться і буде поступова стагнація. У випадку потрапляння інтегрального показника діджиталізації фінансового сектору у червону зону, а інтегрального показника технологічного розвитку та ризику кіберзагроз у зелену та жовту зони, доцільно говорити про неспроможність економічних агентів використовувати переваги існуючих технологій. У свою чергу, якщо інтегральний показник ризику кіберзагроз потрапляє у червону зону при високому рівні двох інших індикаторів, то можна стверджувати про сигнал до активного застосування як превентивних, так і радикальних заходів по ідентифікації та локалізації кібер ризиків. Якщо тільки один інтегральний показник потрапляє у зелену та жовту зони, а два інших у червоній, то в першу чергу, треба мінімізувати кібер ризики, а по-друге, шукати або інструменти реалізації наявного технологічного потенціалу (якщо інтегральний показник теологічного розвитку знаходиться у червоній зоні), або проводити активну політики по залученню інвестицій у фінтех (якщо інтегральний показник діджиталізації фінансового сектору знаходиться у червоній зоні).

Переходячи до аналізу реально отриманих результатів графічної інтерпретації таргетних індикаторів в системі: діджиталізація фінансового сектору–технологічний розвиток–кіберзагрози в Україні протягом 2019-2022 рр., зауважимо, що жоден з інтегральних показників не потрапив у критичну червону зону. Найбільш сприятливим для цифрового розвитку фінансового сектору національної економіки був 2021 р. коли в трикутнику «діджиталізація фінансового сектору – технологічний розвиток – кіберзагрози» прослідковувалась повна рівновага й збалансованість. 2019 рік був найбільш неприйнятним в розрізі забезпечення діджиталізації фінансового сектора за

допомогою впровадження технологій. Так, інтегральні індекси DFS та TR знаходились у жовтій зоні. У 2020 році ситуація покращилась і в жовтій зоні залишився тільки інтегральний показник діджиталізації. Зазначена динаміка протягом 2019-2021 рр. свідчить про ефективну та системну роботу економічних агентів в сфері цифровізації бізнес-процесів у фінансовому секторі України, а також не тільки зростанню фінтеху в Україні, але й чіткому розумінню необхідності дотримання фінансової безпеки. У 2022 р. ситуація з кібер загрозами значно погіршилась, приводом чого став початок повномасштабного вторгнення росії до України. Потенційним кібератакам були схильні усі сфери життєдіяльності країни, а особливо її фінансовий сектору.

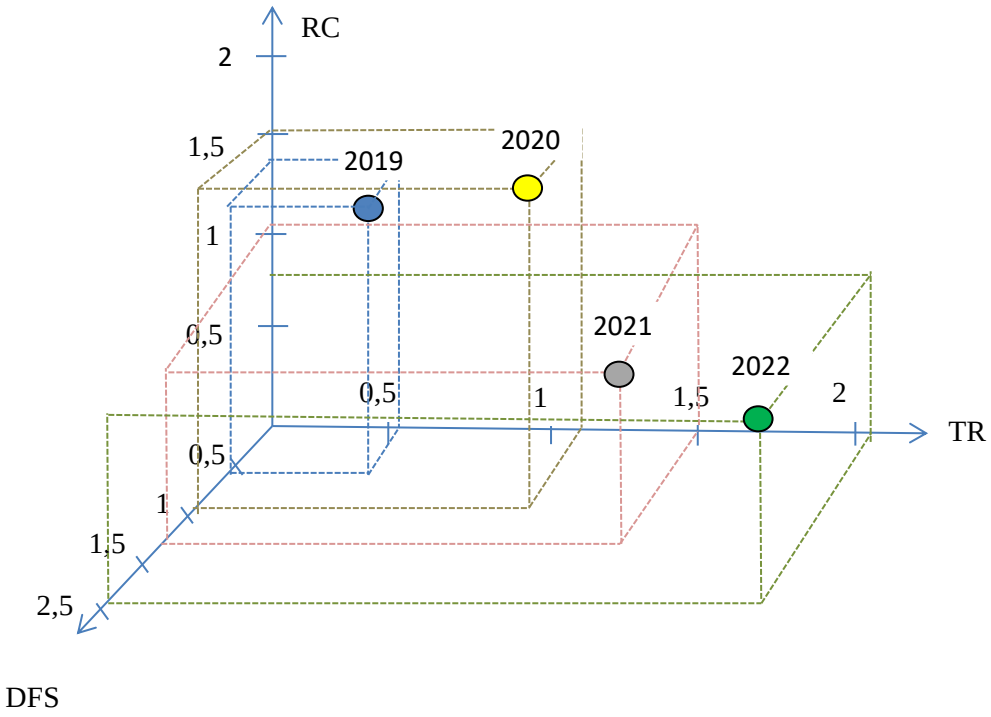


Рисунок 3.10 – Графічна інтерпретація таргетних індикаторів в системі: діджиталізація фінансового сектору–технологічний розвиток–кіберзагроз в Україні протягом 2019-2022 рр.

Джерело: розрахунки автора

У той же час, справедливо зауважити, що навіть не зважаючи на війну в Україні, фінансовий сектор залишається прогресивним вектором розвитку

національної економіки та продовжує надавати якісні послуги українцям. Враховуючи зростання кібер ризиків, фінансовій системі вдалось їх досить успішно локалізувати та тримати високий рівень безпеки обслуговування власних клієнтів. Паралельно з цим, держава повинна продовжувати політику безперервного забезпечення цифрової безпеки як фінансової системи країни, так і громадян України. Системний характер повинні носити реформи пов'язані з удосконалення нормативного забезпечення регулювання ІТ та фінтех секторів національної економіки.

3.2. Оцінювання впливу фінансових та кібернетичних злочинів на рівень довіри до фінансового сектору

Довіра споживачів фінансових послуг є ключовим компонентом стабільного функціонування фінансових установ в контексті постійно зростаючих викликів, спричинених збільшенням частоти та обсягів шахрайства із платіжними картками, несанкціонованого доступу до персональних даних клієнтів, незаконного списання коштів із банківських рахунків тощо.

Довіра споживачів до фінансових установ формується як рівні держави (контроль з боку національного фінансового регулятора за виконанням фінансовими установами заходів із забезпечення кіберзахисту та інформаційної безпеки, проведення просвітницьких заходів щодо підвищення рівня фінансової грамотності та цифрової гігієни) та на рівні фінансової установи (проведення внутрішнього аудиту кібербезпеки фінансової установи, постійний моніторинг інформаційного середовища платіжної інфраструктури, інформування клієнтів про найбільш поширені способи вчинення кібершахрайств у сфері фінансових послуг). Виходячи з цього, збереження та зміцнення довіри споживачів до фінансового сектору є комплексним

пріоритетним завданням як національного фінансового регулятора, так і фінансових установ. Оскільки зниження довіри громадянина до фінансової установи супроводжується відтоком коштів з депозитних рахунків, збільшення обсягу зняття готівки, закриттям банківських рахунків тощо. Дані процеси неодмінно матимуть вплив на показниках функціонування фінансових установ – зниження ліквідності банків, скорочення ресурсів банків для корпоративного та роздрібного кредитування, а також для вкладання коштів в інвестиційні проєкти.

Довіру до фінансових установ у контексті кібернетичних загроз доцільно розглядати з двох точок зору: перша – фінансові установи є ціллю кіберзлочинців, порушення інформаційної безпеки яких може призвести до фінансових збитків, порушення цілісності, доступності та конфіденційності даних як фінансової установи, так і її клієнтів, а також репутаційних ризиків; друга – клієнти фінансової установи є ціллю кіберзлочинців, у результаті чого відбувається крадіжка коштів, збір персональних даних про клієнта.

У межах даного дослідження висунуто робочу гіпотезу – зростання обсягів фінансових кібершахрайства в країні призводить до зменшення довіри населення до фінансових установ.

У межах дослідження запропоновано науково-методичний підхід до оцінювання дискретного лагового впливу фінансових кібершахрайств на рівень довіри клієнтів до фінансових установ. Для врахування часової затримки при кількісному вимірюванні взаємозв’язків між економічними процесами використано поліноміальну модель розподіленого лагу Алмона.

В умовах дефіциту офіційної статистичної інформації щодо обсягу кібершахрайств у сфері фінансових послуг у розрізі окремої країни, а також збільшення кількості цифрових слідів в інтернет просторі для дослідження запропоновано обрати дані про запити користувачів у пошуковій мережі Google. Google Trends є одним з найпоширеніших в емпіричній економічній літературі інструментів для генерації первинного масиву даних. Популярність пошукових запитів, про які повідомляє Google, часто розглядається як

непрямий метод вимірювання уваги до певної події чи теми [69]. Google Trends став важливим аналітичним інструментом для дослідників у галузі медицини [64, 70, 137, 127, 159] та соціальних наук [99, 135].

Дані у звітах Google Trends в основному є валідними. Значення певного атрибута коливається у межах від 0 до 100. Однак існують певні ситуації, в яких значення атрибута набуває нецілого значення, зокрема "<1". Це означає, що пошук певного атрибута в аналізований період часу мав достатній обсяг, щоб відобразитися у звіті Google Trends, але менше, ніж 1/100 частина від періоду з найвищою популярністю [69].

Дослідницька вибірка охоплює період з січня 2005 року по серпень 2023 року, загалом 104 щомісячні спостереження. Об'єктом для дослідження обрано Україну, Німеччину, США та Польщу. Для потреб даного дослідження сформовано 2 групи пошукових запитів, які відображають рівень зацікавленість користувачів відповідним питанням:

1 група – пошукові запити, що відображають віктимізацію споживачів фінансових послуг (кіберполіція (X1), шахрайство (X2), заблокувати картку (X3), повернення помилково перерахованих коштів (X4), інформаційна безпека (X5)). Зауважимо, що всі пошукові запити акумулювалися у сфері «фінансів»;

2 група – пошукові запити, що характеризують довіру до фінансової установи (кредитний ліміт (Y1), змінити банк (Y2), закриття рахунку (Y3), інтернет ліміт (Y4), рейтинг банків (Y5)). До пошукових запитів також було застосовано фільтр «фінанси».

Запропонований науково-методичний підхід до оцінювання впливу фінансових кібершахрайств на рівень довіри клієнтів до фінансових установ запропоновано реалізовувати на основі поетапного виконання таких завдань:

1. Акумулювання первинних даних у межах визначених пошукових запитів у розрізі аналізованих країн з о використанням інструментів пошукової системи Google Trends.

2. Нормалізацію показників за допомогою методу MPI (Mazziotta Pareto Index).

3. Визначення інтегральних показників, що характеризують рівень віктимізації споживачів фінансових послуг та рівень довіри на фінансових установ за допомогою функції Berger and Casella.

4. Ідентифікація величини лагових затримок між інтегральними показниками за допомогою автокореляційних функцій та корелограм.

5. Оцінювання впливу фінансових кібершахрайств на рівень довіри клієнтів до фінансових установ шляхом побудови поліноміальних моделей розподіленого лагу Алмона.

Перший етап науково-методичного підходу передбачає формування статистичного масиву інформацію щодо результатів пошукових запитів.

Другий етап спрямований на приведення показників вхідної статистичної бази дослідження до співставного вигляду відбувається за допомогою застосування методу MPI (Mazziotta Pareto Index), тобто наступного співвідношення:

$$z_{ijg} = \left[100 + \frac{x_{ijg} - M_{x_{ig}}}{S_{x_{ig}}}\right] / 100 \tag{3.7}$$

де z_{ijg} – нормалізоване значення і-го показника в розрізі j-го періоду для g-ої країни;

x_{ijg} - фактичне значення і-го показника в розрізі j-го періоду для g-ої країни;

$M_{x_{ig}}$ – математичне сподівання і-го показника для g-ої країни за розглянутий часовий інтервал;

$S_{x_{ig}}$ – середнє квадратичне відхилення і-го показника для g-ої країни за розглянутий часовий інтервал.

У таблиці 3.7 наведено нормалізовані значення показників.

Таблиця 3.7 – Фрагмент нормалізованих значень показників на прикладі України

Період	X1	X2	X3	X4	X5	Y1	Y2	Y3	Y4	Y5
2015-01	0,869	0,963	0,833	0,841	0,920	0,865	0,921	0,887	1,167	1,113
2015-02	0,880	0,951	0,895	0,841	0,960	0,844	0,921	1,231	0,868	1,341
2015-03	0,869	0,835	0,929	1,195	1,017	0,833	1,098	1,049	0,868	1,363
2015-04	0,869	0,967	0,923	1,075	0,989	0,807	0,921	1,034	0,868	1,124
2015-05	0,869	0,955	0,985	0,981	1,028	0,913	1,028	1,024	0,868	1,163
2015-06	0,869	0,930	0,833	0,841	1,023	0,838	0,921	1,008	0,868	1,141
2015-07	0,869	1,033	1,025	1,244	0,920	0,870	0,921	0,897	0,983	1,335
2015-08	0,869	1,079	1,036	0,841	0,898	0,944	1,093	0,963	1,110	1,124
2015-09	0,869	1,029	0,934	0,981	0,926	0,849	0,921	0,953	0,978	1,141
2015-10	1,145	1,038	1,076	0,841	0,977	0,838	0,921	0,938	1,079	1,058
…	…	…	….	…	…	…	…	…	…	…
2022-11	1,180	1,054	1,013	1,030	1,125	1,199	1,177	0,993	1,180	0,886
2022-12	1,203	0,992	1,036	0,941	1,040	1,140	1,387	1,145	0,996	1,069
2023-01	1,188	1,095	1,053	1,055	0,971	1,252	1,130	1,049	0,934	1,097
2023-02	1,258	1,058	1,087	1,021	1,023	1,162	1,056	1,064	1,009	0,991
2023-03	1,196	1,091	1,183	0,991	1,062	1,225	1,154	1,029	1,079	1,086
2023-04	1,153	1,203	1,070	0,941	1,079	1,183	1,093	1,018	1,013	1,069
2023-05	1,215	1,223	1,398	0,906	1,244	1,199	1,186	1,029	1,018	1,080
2023-06	1,211	1,182	1,285	0,951	1,000	1,294	1,014	1,130	1,013	0,958
2023-07	1,149	1,153	1,364	0,991	0,920	1,220	1,098	1,211	1,062	1,019
2023-08	1,129	1,153	0,833	0,841	0,903	1,337	1,121	1,084	0,868	1,008

Джерело: розрахунки автора

Метою третього етапу є визначення двох інтегральних показників (рівень віктимізації споживачів фінансових послуг (IX), рівень довіри до фінансових послуг (IY)) шляхом застосування трансформації Box-Cox до нормалізованих даних і подальшої згортки за допомогою функції Berger and Casella:

– трансформація Box-Cox:

$$h_1 = x - 1 \tag{3.8}$$

– середня арифметична Berger and Casella:

$$F(\mu_{jg}) = \frac{1}{m}\sum_{i=1}^{m}(z_{ijg} - \mu_{jg})^2 \tag{3.9}$$

$$\mu_{jg} = h_1^{-1}(\frac{1}{m}\sum_{i=1}^{m} h_1\ (z_{ijg})\ \ )$$

де $F(\mu_{jg})$ – інтегральний показник Berger and Casella в розрізі j-го періоду для g-ої країн.

Результати розрахунку інтегральних показників рівня віктимізації споживачів фінансових послуг (FX) та рівня довіри до фінансових послуг (FY) для України наведено на рисунку 3.11.

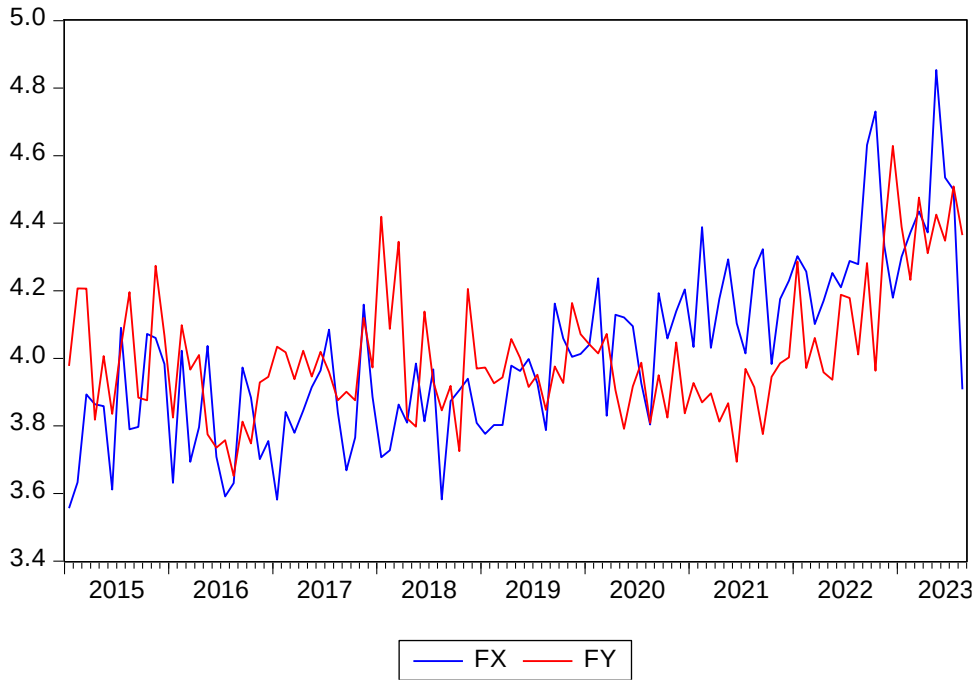


Рисунок 3.11 – Рівень віктимізації споживачів фінансових послуг (FX) та рівень довіри до фінансових послуг (FY) в Україні

Джерело: розрахунки автора

Наступним кроком даного етапу виступає приведення інтегрального показника до проміжку значень від нуля до одиниці за допомогою наступної формули:

$$I_{jg} = \frac{F(\mu_{jg})}{\max\limits_{j} F(\mu_{jg}) + S_j(F(\mu_{jg}))} \tag{3.10}$$

де I_{jg} – інтегральний показник Berger and Casella в розрізі j-го періоду для g-ої країн, приведений до проміжку значень від нуля до одиниці;

$\max\limits_{j} F(\mu_{jg})$ – максимальне значення показника Berger and Casella для g-ої країни за весь розглянутий часовий інтервал;

$S_j(F(\mu_{jg}))$ – середнє квадратичне відхилення показника Berger and Casella для g-ої країни за весь розглянутий часовий інтервал.

Результати приведення значень інтегральних показників, які коливаються від 0 до 1 ум.од., наведено на рисунку 3.12 -3.15.

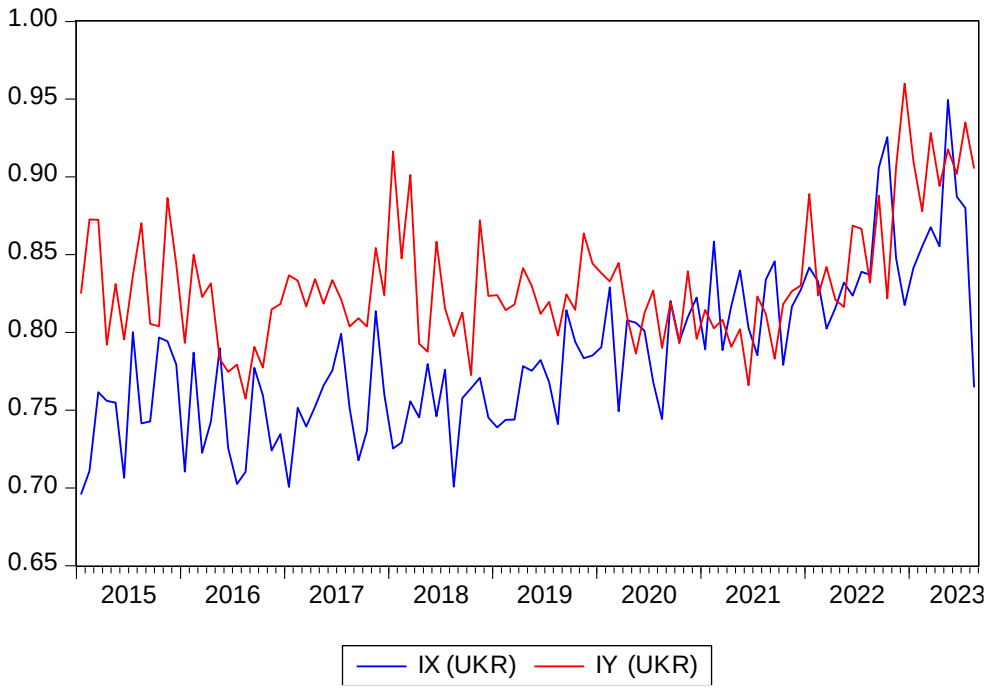


Рисунок 3.12 – Рівень віктимізації споживачів фінансових послуг (IX) та рівень довіри до фінансових послуг (IY) в Україні

Джерело: розрахунки автора

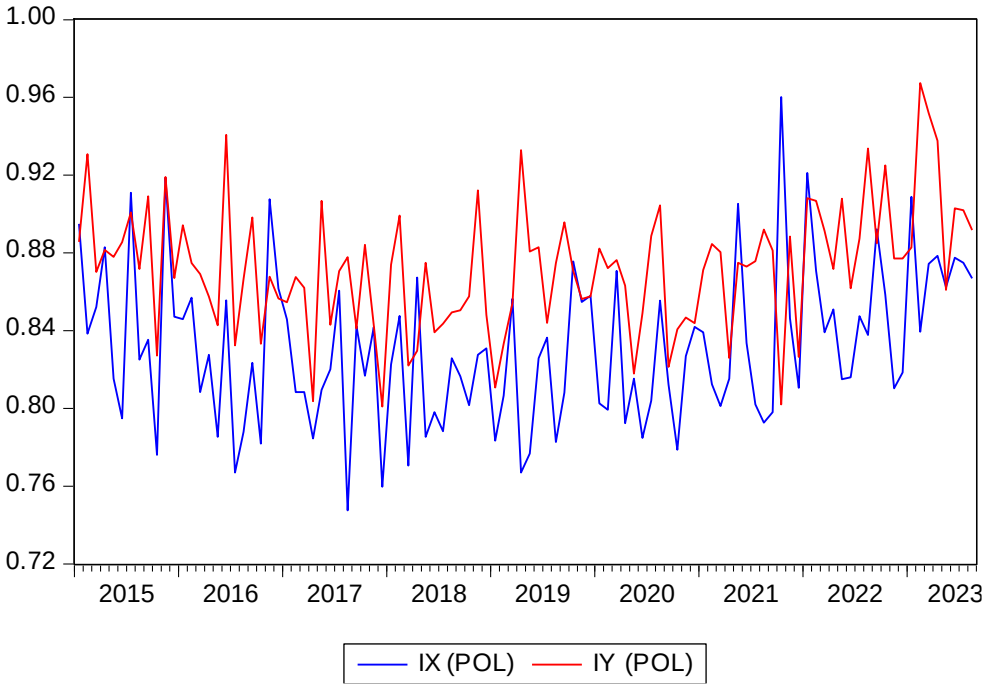


Рисунок 3.13 – Рівень віктимізації споживачів фінансових послуг (IX) та рівень довіри до фінансових послуг (IY) в Польщі

Джерело: розрахунки автора

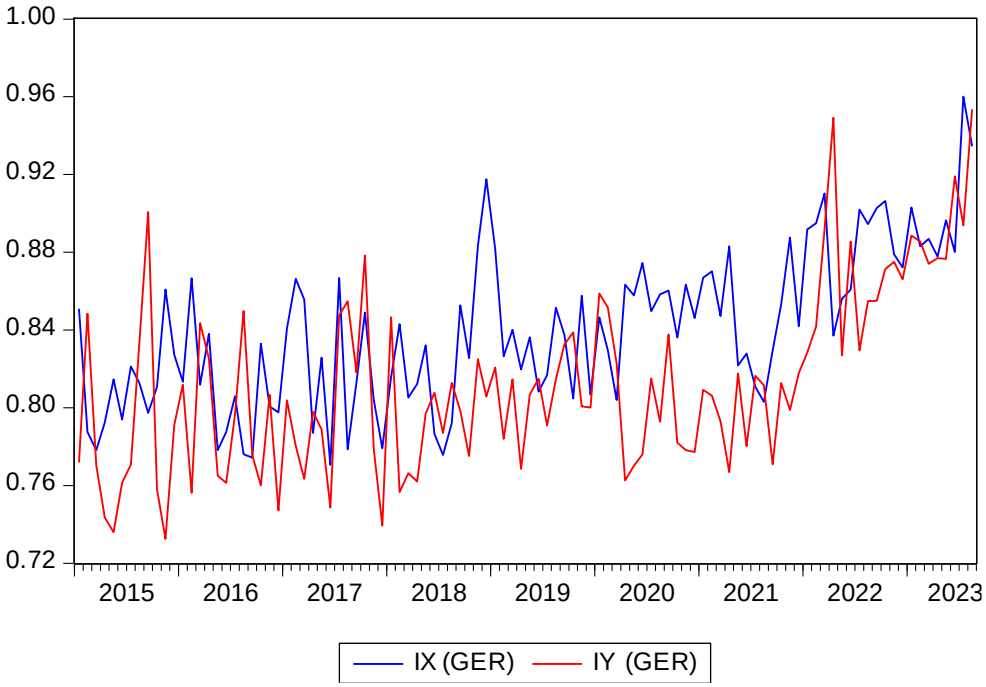


Рисунок 3.14 – Рівень віктимізації споживачів фінансових послуг (IX) та рівень довіри до фінансових послуг (IY) в Німеччині

Джерело: розрахунки автора

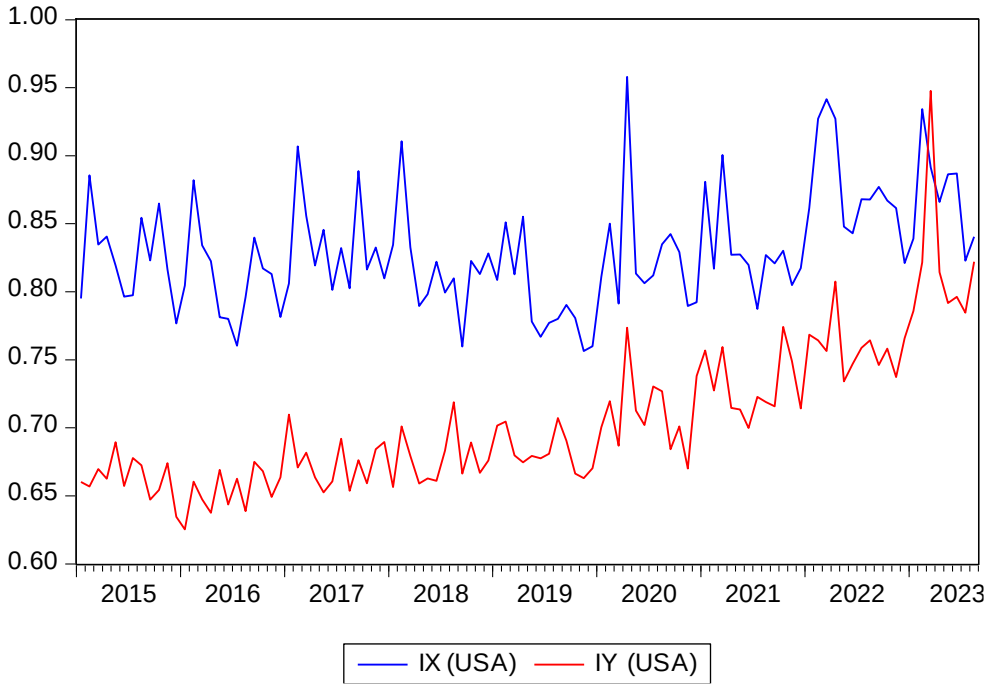


Рисунок 3.15 – Рівень віктимізації споживачів фінансових послуг (IX) та рівень довіри до фінансових послуг (IY) в США

Джерело: розрахунки автора

Дані рисунків 3.12-3.15 демонструють, що середній рівень віктимізації споживачів фінансових послуг серед аналізованих країн становить 0,821 ум.од., при цьому найвище середньомісячне значення цього інтегрального показника зафіксовано для Німеччини (0,840 ум.од.), тоді як найнижче – для України (0,784 ум.од.). Стосовно другого інтегрального показника, то у середньомісячне значення показника рівня довіри населення до фінансових інститутів становить 0,805 ум.од (тоді як найвище значення з поміж чотирьох країн має Польща (0,872 ум.од), а найнижче – США (0,704 ум.од.)).

Для візуалізації сезонних коливань значень двох інтегральних показників у розрізі чотирьох країн побудовано графіки сезонності (рис. 3.16). Аналіз сезонних коливань рівня віктимізації споживачів фінансових послуг дозволяє сформувати наступні висновки: у травні відбувається у середньому збільшення масштабів фінансових кібершахрайств в Україні, тоді як найменший обсяг кібершахрайств у середньому фіксується у серпні; найбільше середнє значення рівня віктимізації споживачів фінансових послуг

у США зафіксовано у лютому, а найменше – у грудні; у Польщі та Німеччині розподіл фінансових кібершахрайств по місяцям є майже рівномірним.

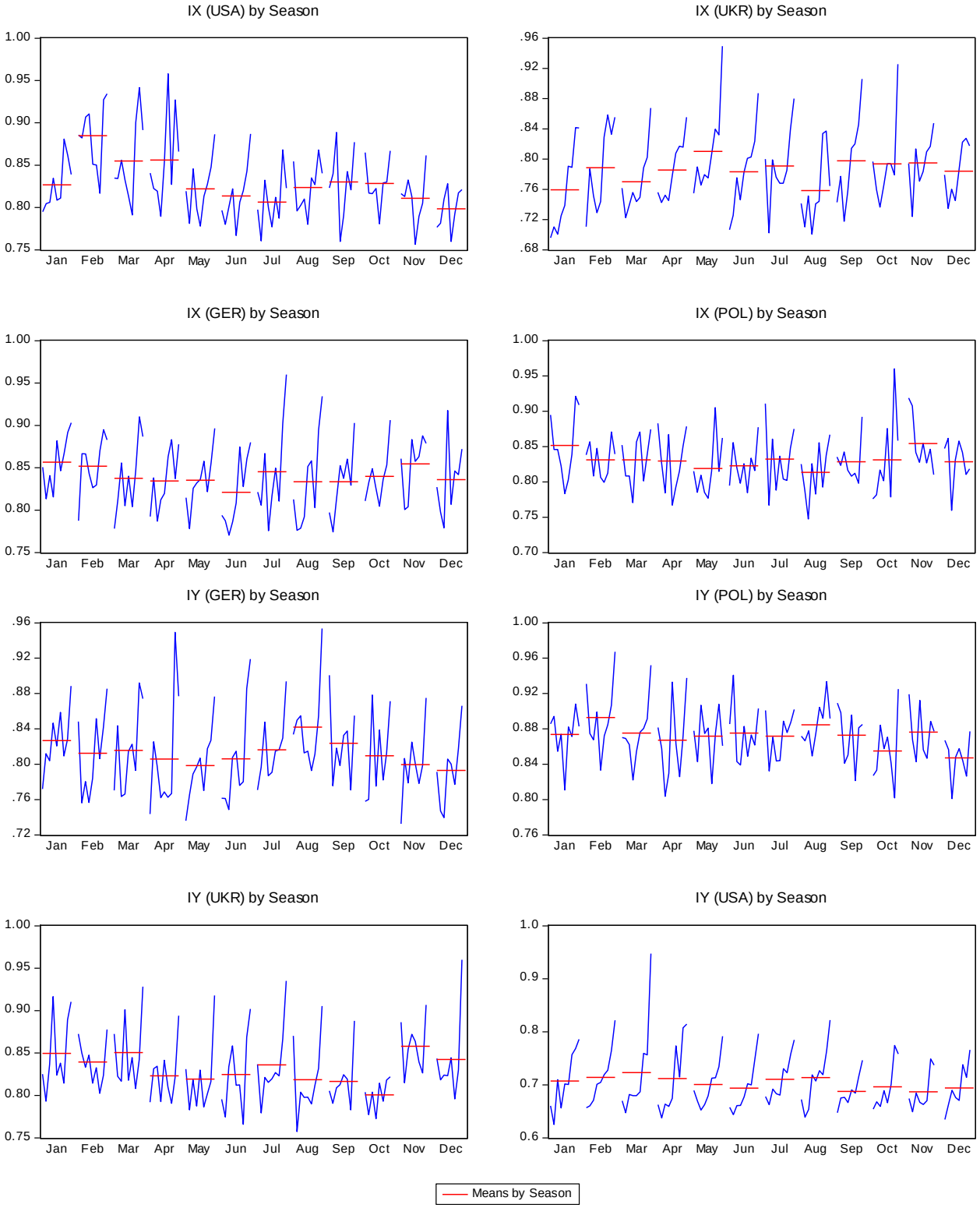


Рисунок 3.16 – Сезонність в динаміці рівня віктимізації споживачів фінансових послуг (IX) та довіри до фінансових послуг (IY)

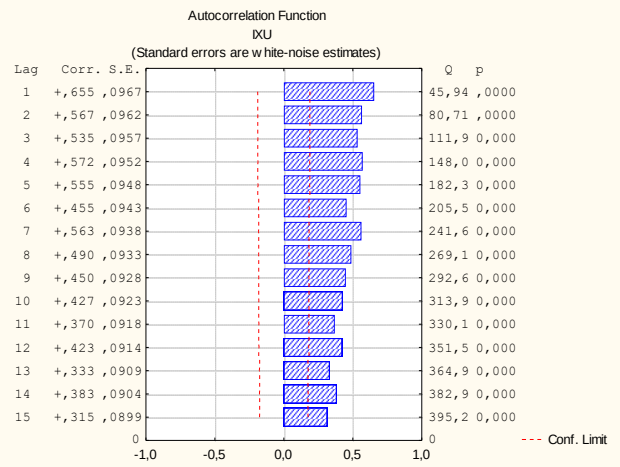
Джерело: розрахунки автора

Сезонна візуалізація інтегрального показника довіри до фінансових установ дозволяє стверджувати, що зниження цього показника в Україні щорічно в середньому відбувається в жовтні, тоді як збільшення – у січні, березні та листопаді. Середньомісячні значення рівня довіри до фінансових установ в США, Польщі та Німеччині є майже рівномірними.

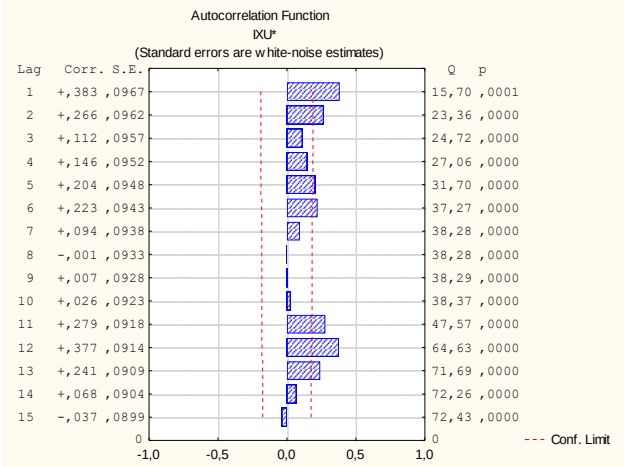
Наступним етапом запропонованого науково-методтчного підходу є ідентифікація величини лагових затримок в розрізі розглянутих країн за допомогою автокореляційних функцій та корелограм. Проведення автокореляційного аналізу здійснено з використанням програми Statistica. Результати побудови корелограми, що відображає залежність рівня довіри до фінансового сектору від кібершахрайств з урахуванням часового лагу подано на рисунку 3.17.

Аналіз рисунку 3.17 дозволяє констатувати варіацію значень автокореляційної функції різних рівнів часового ряду в залежності від часового лагу та статистичну значущість для першого рівня. Так, в розрізі значень автокореляційної функції для України спостерігається тенденція зменшення з першого до третього рівня зі стрибкоподібним збільшенням значення автокореляційної функції четвертого рівня і подальшим поверненням до тенденції зменшення для 6 та 11 рівнів. Але найбільшим за абсолютним значення виступає коефіцієнт автокореляції 1 рівня. Даний факт свідчить про доцільність врахування лагових затримок впливу кібершахрайств на довіру до фінансового сектору для України на рівні 1 місяця. Аналіз автокореляційних функцій для інших країн дозволяє ідентифікувати наступні лагові затримки впливу кібершахрайств на рівень довіри до фінансових установ: США – 1 місяць, Німеччина – 1 місяць, Польща – 3 місяці.

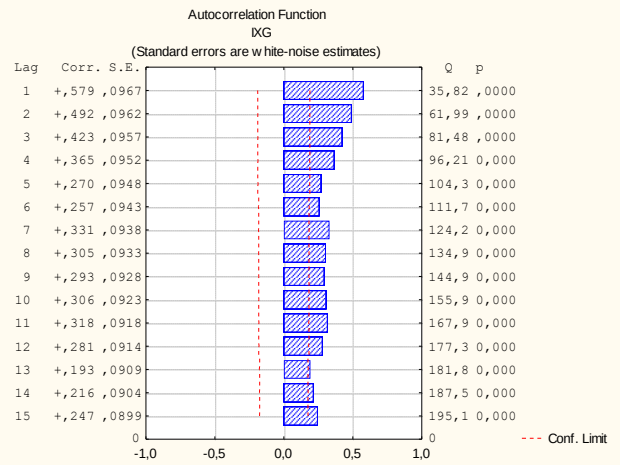
Україна



США



Німеччина



Польща

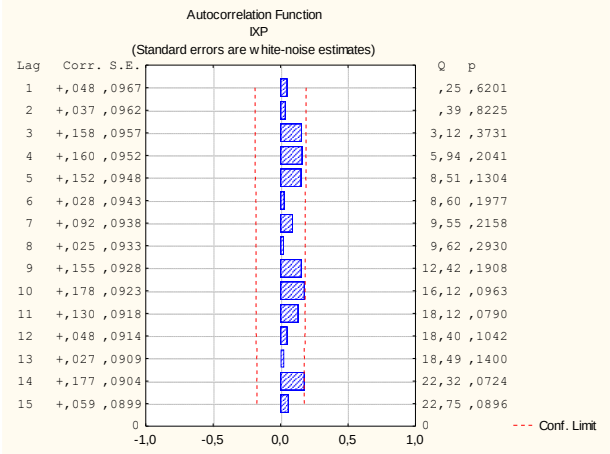


Рисунок 3.17 – Корелограма залежності рівня довіри до фінансового сектору від кібершахрайств з урахуванням часового лагу

Джерело: розрахунки автора

Завершальним етапом науково-методичного підходу є оцінювання впливу фінансових кібершахрайств на рівень довіри до фінансового сектору шляхом побудови поліноміальної моделі розподіленого лагу Алмона. Даний інструментарій дозволяє побудувати регресійну модель з урахуванням лагових затримок значень одного часового ряду на основі іншого. Загальний вигляд моделі розподіленого лагу має форму наступного співвідношення (формула 3.11).

$$y_t = b_0 \cdot x_t + b_1 \cdot x_{t-1} + b_2 \cdot x_{t-2} + \cdots + b_k \cdot x_{t-k} \quad (3.11)$$

де y_t – залежна змінна в момент часу t;

x_t – незалежна змінна в момент часу t;

x_{t-k} – незалежна змінна з лаговою затримкою $t - k$;

b_k – коефіцієнти лінійного регресійного рівняння.

У випадках наявної сильної кореляційної залежності в масиві незалежних змінних, тобто виявленому факті мультиколінеарності, для оцінювання параметрів лінійного регресійного рівняння b_k застосовується поліноміальний підхід Алмона, який формалізовано наступним чином:

$$b_k = a_0 + a_1 \cdot i + a_2 \cdot i^2 + \cdots + a_q \cdot i^q, q < k \quad (3.12)$$

де a_q – поліноміальні коефіцієнти регресійної моделі.

Результати розрахунку параменрів для поліноміальної моделі розподіленого лагу Алмона подано представлено у вигляді рисунків 3.18-3.21.

	Polyn. Distr. Lags; Regression Coefficients (Spreadsheet1.sta) Indep: IXU Dep: IYU Lag: 1 R= ,9984 R-square= ,9967 N: 103			
Lag	Regressn Coeff.	Standard Error	t(101)	p
0	0,548337985337	0,115608076446	4,743076800460	0,000006931906
1	0,508894863063	0,115699253535	4,398428231096	0,000027054545

Рисунок 3.18 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу фінансових кібершахрайств на рівень довіри до фінансових установ в розрізі України

Джерело: розрахунки автора

Аналіз p-рівня дозволяє стверджувати про статистичну значущість в розрізі впливу фінансових кібершахрайств на довіру до фінансових установ лагу на рівні 0 і 1, оскільки відповідне значення ймовірності не перевищує 0,05. Відповідно, стандартна похибка без лагової затримки і з лагом 1 місяць є

низькою, критерій Стьюдента статистичної значущості відповідного регресійного коефіцєнту моделі розподіленого лагу Алмона є прийнятним і перевищує критично допустимий рівень. Отже, на основі даних графи «Regressn Coeff» таблиці 3 закономірність впливу кібершахрайств на довіру до фінансових установ може бути формалізована у вигляді наступної моделі:

$$FYUKR(t) = 0.5483 \cdot FX(t) + 0.5089 \cdot FX(t-1) \qquad (3.13)$$

де $FYUKR(t)$ – інтегральний показник рівня довіри до фінансових установ в момент часу t в розрізі України;

$FX(t)$ – значення показника рівня кібершахрайств в момент часу t.

Проведемо аналогічний аналіз та формалізацію поліноміальної моделі розподіленого лагу Алмона для інших країн.

	Polyn. Distr. Lags; Regression Coefficients (Spreadsheet1.sta) Indep: IXU* Dep: IYU* Lag: 1 R= ,9982 R-square= ,9964 N: 103			
Lag	Regressn Coeff.	Standard Error	t(101)	p
0	0,549529342780	0,090986010039	6,039712506814	0,000000025897
1	0,298514370955	0,091033351491	3,279175885150	0,001428845732

Рисунок 3.19– Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу фінансових кібершахрайств на рівень довіри до фінансових установ в розрізі США

Джерело: розрахунки автора

Дані рисунку 3.19 наочно демонструють, що вплив віктимізації споживачів фінансових послуг на зміну довіри до фінансових установ є значимим на лагу на рівні 0 та 1, оскільки відповідне значення ймовірності не перевищує 0,05. Пропонується обрати в якості лагової затримки впливу 1 місяць. Формалізація взаємозв'язку між цими інтегральними показниками для США подана у вигляді наступної моделі (формула 3.14).

$$FYUSA(t) = 0.5495 \cdot FX(t) + 0.2985 \cdot FX(t-1) \qquad (3.14)$$

де $FYUSA(t)$ – інтегральний показник рівня довіри до фінансових установ в момент часу t в розрізі США;

$FX(t)$ – значення показника рівня кібершахрайств в момент часу t.

	Polyn. Distr. Lags; Regression Coefficients (Spreadsheet1.sta) Indep: IXG Dep: IYG Lag: 1 R= ,9989 R-square= ,9978 N: 103			
Lag	Regressn Coeff.	Standard Error	t(101)	p
0	0,324363476346	0,107634491762	3,013564434941	0,003264195518
1	0,643940781514	0,107745050943	5,976523059569	0,000000034503

Рисунок 3.20 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу фінансових кібершахрайств на рівень довіри до фінансових установ в розрізі Німеччини

Джерело: розрахунки автора

Зв'язок між рівнем віктимізації споживачів фінансових послуг та довірою до фінансового сектору є статистично значимим у розрізі лагів 0 та 1 (значення ймовірності не перевищує 0,05). Пропонується обрати в якості лагової затримки впливу 1 місяць.

На основі значень параметрів поліноміальної моделі розподіленого лагу Алмона закономірність впливу кібершахрайств на рівень довіри до фінансових установ для Німеччини може бут формалізована у вигляді наступної моделі:

$$FYGER(t) = 0.3244 \cdot FX(t) + 0.6439 \cdot FX(t-1) \qquad (3.15)$$

де $FYGER(t)$ – інтегральний показник рівня довіри до фінансових установ в момент часу t в розрізі Німеччини;

$FX(t)$ – значення показника рівня кібершахрайств в момент часу t.

	Polyn. Distr. Lags; Regression Coefficients (Spreadsheet1.sta) Indep: IXP Dep: IYP Lag: 3 R= ,9994 R-square= ,9987 N: 101			
Lag	Regressn Coeff.	Standard Error	t(97)	p
0	0,325996465911	0,073869871502	4,413118085671	0,000026435555
1	0,270132884401	0,070417759071	3,836147130541	0,000222415008
2	0,207192575115	0,070310119259	2,946838624353	0,004020702073
3	0,246740354321	0,073474570549	3,358173480669	0,001122236184

Рисунок 3.21 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу фінансових кібершахрайств на рівень довіри до фінансових установ в розрізі Польщі

Джерело: розрахунки автора

Критерій Стьюдента та його p-значимість вказує на наявність статистично значимого впливу кібершахрайств на зміну довіри до фінансових установ на всіх лагах (0, 1, 2, 3). Пропонується обрати лагову затримку в обсязі 3 місяці. Модель з розподіленим лагом має наступний вигляд:

$$FYPOL(t) = 0.3600 \cdot FX(t) + 0.2701 \cdot FX(t-1) + 0.2072 \cdot FX(t-2) + 0.2467 \cdot FX(t-3) \quad (3.16)$$

де $FYPOL(t)$ – інтегральний показник рівня довіри до фінансових установ в момент часу t в розрізі Польщі;

$FX(t)$ – значення показника рівня кібершахрайств в момент часу t.

Побудовані модель з розподіленим лагом (формули 3.13-3.16) мають високі показники якості, а саме коефіцієнт детермінації становить 0,99, а також порівняння залишкової дисперсії з дисперсією середнього арифметичного на основі значення критерію Фішера також вказує на адекватність побудованої моделі (p-value < 0,05).

Підсумовуючи, за результатами проведеного емпіричного дослідження встановлено, що висунуту гіпотезу доцільно прийняти, оскільки між віктимізацією споживачів фінансових послуг та довірою до фінансових

установ у розрізі різних країн існує статистично значимий зв’язок з лаговою затримкою в основному в 1 місяць. Емпіричні розрахунки наочно демонструють посилення інформаційних заходів для споживачів фінансових послуг для підвищення рівня їх обізнаності у сфері особистої кібербезпекиз особливим акцентом на найбільш вразливу верству населення.

3.3. Удосконалення політики управління кіберризиками в умовах цифровізації економіки в Україні

Фіналізуючи дослідження присвячене детермінантам поширення та локалізації кіберзагроз в умовах цифровізації економіки України, актуальності набуває аналіз існуючої ситуації в державі щодо політики управління кіберризиками та потенційного місця, запропонованих в роботі науково-методичних підходів, у цій системі або напрямків по її удосконаленню. Отже, справедливо зауважити, що починаючи з 2014 р. політика державних органів влади щодо протидії кіберризикам значно розширилась на перетворилась на ключовий елемент забезпечення національної безпеки. Вторгнення росії на територію України та анексія Криму у 2014 р., а також повномасштабна війна розпочата у 2022 р. призвели до перегляду усіх складових національної безпеки України та переоцінки значення інформаційного простору в державі. Так, активні зміни відбулись не тільки в законодавчому та виконавчому полі забезпечення кібербезпеки в Україні, але й у свідомості пересічних громадян з привод кіберзагроз, а також інтенсифікації співпраці з міжнародними організаціями й окремими державами з приводу обміну досвіду щодо боротьби з кіберризиками.

Зупиняючись на базових аспектах законодавчої складової системи кібербезпеки України зауважимо, що її формують Закони України, Укази Президента, накази Адміністрації Держспецзв’язк, постанови Кабінету

Міністрів України. Так, найбільш значимими, є Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII, він охоплює базові засади національних інтересів держави у інформаційному просторі та регламентує цілі, задачі і принципи системи кібербезпеки в Україні.

В цілому ж певні елементи законодавчої складової системи кібербезпеки України на рівні Законів України почали зароджуватись з набуттям незалежності нашої держави. Так, першим Законом України, який дотичний до кібербезпеки був Закон України «Про інформацію» від 2 жовтня 1992 року № 2657-XII, в якому паралельно з основними положення про види інформації, основні принципи інформаційних відносин, гарантії права на інформацію були прописані положення про охорону права на інформацію, а також встановлена відповідальність за порушення законодавства про інформацію.

Значний вплив на розвиток законодавчої складової системи кібербезпеки України також мали наступні Закони України.

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 року № 80/94-ВР, важливий закон з точки зору формалізації об'єкту захисту, суб'єктів відносин, забезпечення захисту інформації, а також повноваження державних органів у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах.

Закон України «Про телекомунікації» від 18 листопада 2003 року № 1280-IV, в розрізі кібербезпеки положення цього закону визначають механізм захисту прав споживачів телекомунікаційних послуг, а також процедуру контролю за ринком телекомунікацій.

Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23 лютого 2006 року № 3475-IV, акумулює усі функціональні положення щодо ефективної роботи центрального органу виконавчої влади, який повинен забезпечувати реалізацію державної політики

з приводу організації спеціального зв'язку усіх критично важливих підприємств та організацій України, а також захисту інформації.

Закон України «Про захист персональних даних» від 1 червня 2010 року № 2297-VI, базовий нормативний акт спрямований на захист прав громадян України. Так, цей закон встановлює основні засади щодо загальних й особливих вимог до обробки персональних даних, регламентує процес збирання, накопичення, зберігання та поширення персональних даних, а також особливості забезпечення їх захисту.

Закон України «Про національну безпеку України» від 21 червня 2018 № 2469-VIII, є найбільш комплексним нормативним актом, який поряд з основними засадами державної політики гарантування громадянам України захисту від загроз будь якого роду (у тому числі і кіберзагроз), визначає систему командування, контролю та координації операцій сил безпеки і сил оборони в державі.

Переходячи до указів Президента України, зазначимо, що їх переважна більшість стосуються рішень Ради національної безпеки і оборони. Це цілком зрозуміло зважаючи на військову агресію з боку росії. Так, указ Президента України Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» №47/2017, визначає ключові елементів системи протидії критичному інформаційному впливу росії в умовах війни.

Указ Президента України Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» від 26 серпня 2021 року № 447/2021. Цей законодавчий акт паралельно з узагальненням глобального контексту кібербезпеки та надбань минулої стратегії (затвердженої 15 березня 2016 р.), визначає виклики й кіберзагрози у кіберпросторі, засади розбудови системи кібербезпеки, стратегічні цілі та завдання забезпечення кібербезпеки в Україні, напрями зовнішньополітичної діяльності України у сфері кібербезпеки, а також узагальнений механізми реалізації стратегії протидії кіберзагрозам.

Указів Президента України «Про Національний координаційний центр кібербезпеки» від 7 червня 2016 року № 242/2016 створює передумови організації ефективної за своїм функціональним призначенням інституції, яка б здійснювала не тільки координацію та контролю за діяльністю суб'єктів, які забезпечують кібербезпеку, але й проводила активну аналітичну роботу щодо стану кіберзахисту, стану виконання вимог законодавства щодо кіберзахисту, даних про кіберінциденти та інше.

Вагомим блоком законодавчої складової системи кібербезпеки України є накази Адміністрації Держспецзв'язку, в назві яких безпосередньо й визначається основне завдання їх ратифікації. Наказ Адміністрації Держспецзв'язку від 10.06.2008 № 94, яким затверджено «Порядок координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», наказ зареєстровано в Міністерстві юстиції України 07.07.2008 за № 603/15294.

Наказ Адміністрації Держспецзв'язку від 02.12.2014 № 660, яким затверджено «Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», наказ зареєстровано в Міністерстві юстиції України 28.01.2015 за № 90/26535.

Наказ Адміністрації Держспецзв'язку від 15.01.2016 № 20, яким затверджено «Порядок сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті», наказ зареєстровано в Міністерстві юстиції України 05.02.2016 за № 196/28326.

Найбільш численна група нормативно-правових актів, що стосуються кібербезпеки охоплює постанови Кабінету Міністрів України. Так, постанова Кабінету Міністрів України від 16.11.2002 № 1772, якою затверджено

«Порядок взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах», визначає основні напрямки роботи та сферу відповідальності адміністрації Держспецзв'язку в напрямку її взаємодії з іншими державними органами виконавчої влади з питань захисту державних інформаційних ресурсів.

Постанова Кабінету Міністрів України від 29.03.2006 № 373, якою затверджено «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах». Цей законодавчий акт визначає об’єкт, предмет, методи, вимоги та організаційні засади захисту державних інформаційних ресурсів.

Постанова Кабінету Міністрів України від 11.04.2012 № 295, якою затверджено «Правила надання та отримання телекомунікаційних послуг»; пункт 36 підпункти 1-7,13-15, пункт 54 підпункти 5-6. Цей законодавчий документ спрямований на ідентифікацію прав, зобов’язань та відповідальності споживачів й провайдерів телекомунікаційних послуг.

Наступні чотири постанови Кабінету Міністрів України, стосуються об’єктів критичної інфраструктури, крім того, ці законодавчі акти взаємопов’язані між собою, так одні з них визначають особливості віднесення суб’єктів господарювання до переліку об’єктів критичної інформаційної інфраструктури, а інші вже обов’язкові умови їх кіберзахисту.

Постанова Кабінету Міністрів України від 23 серпня 2016 р. № 563, якою затверджено «Порядок формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави».

Постанова Кабінету Міністрів України від 19.06.2019 № 518, «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури».

Постанова Кабінету Міністрів України від 09.10.2020 № 943, «Деякі питання об’єктів критичної інформаційної інфраструктури».

Постанова Кабінету Міністрів України від 09.10.2020 № 1109, «Деякі питання об’єктів критичної інфраструктури» .

Останнім нормативно-правовим актом, що формує законодавчу складову системи кібербезпеки України є – постанова Кабінету Міністрів України від 23.12.2020 № 1295, «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки» . В основу цього документи покладені положення щодо складу й суб'єктів системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, а також механізмів створення та функціонування цієї системи.

Переходячи до виконавчої складової існуючої системи кіберризиками, зазначимо, що наразі її представляють Державна служба спеціального зв'язку та захисту інформації України, яка координує діяльність інших суб'єктів забезпечення кібербезпеки і здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти й кібератаки та усунення їх наслідків. Активну участь у забезпеченні політики управління кіберризиками здійснюють урядова Команди реагування на комп'ютерні надзвичайні події України (CERT-UA), державний центр кіберзахисту та Центр реагування на кіберзагрози. Найбільш активну роботу в сфері попередження, виявленні, припинення та розкриття кримінальних правопорушень, які передбачали комп'ютерів й телекомунікаційних мереж здійснює Департамент кіберполіції Національної поліції України та СБУ.

У сучасному цифровому світі, де технології стрімко розвиваються, кібербезпека стає однією з найважливіших сфер для забезпечення стабільності і безпеки як інформаційного, так і фізичного середовища. Удосконалення ресурсного забезпечення (матеріальних, технологічних, трудових, фінансових ресурсів) є необхідним елементом відповіді на постійно зростаючі загрози кібернетичних атак.

Протягом останніх років відбувається стрімке нарощення знань та умінь у сфері кібербезпеки. У межах Європейського Союзу існують численні комплексні програми навчання та /або підвищення кваліфікації працівників, які реалізуються Європейським банківським органом (EBA), Агентством Європейського Союзу з питань кібербезпеки (ENISA) тощо. За рахунок

підтримки міжнародних організацій в Україні проходить навчання з питань кібербезпеки для працівників банківського сектору України (CRDF Global), просвітницькі заходи у рамках програми «Кібербезпека критично важливої інфраструктури України» (USAID).

Важливим елементом забезпечення кіберстійкості національної системи є підвищення рівня кібергігієни громадян країни, що передбачає дотримання правил цифрової безпеки при роботі в мережі Інтернет. Освітні заходи з підвищення рівня обізнаності про кіберзагрози охоплюють широке коло осіб – від учнів молодших класів до осіб пенсійного віку. Яка б нормативна-правова база не було б розроблена та які б ефективні органи протидії кіберзлочинам не функціонували в державі, за умови незнання українцями базових правил поведінки в кіберпросторі неможливо їх захистити від впливу кіберризиків. Тотальна діджиталізація сфер життя в Україні призвела до повноцінного розширення потенційних суб'єктів кібератак до рівня усіх громадян держави.Освітні та просвітницькі заходи в основному реалізуються на рівні країн-учасниць Європейського Союзу (наприклад, Cyberprofilaktyka NASK (Польща), Safer Internet (Німеччина), Internet Segura for Kids (Іспанія) та інші). В Україні також проходять численні освітні заходи у рамках діяльності центр фінансових знань «Талан» при Національному банку України, започатковано освітній проєкт #ШахрайГудбай.

Підвищення кваліфікації у сфері кібербезпеки є важливою складовою стратегії протидії кіберзагрозам і забезпечення стійкості цифрового середовища. Зловмисники постійно модернізують свої методи та інструменти здійснення кібератак, тому фахівці з кібербезпеки повинні вдосконалювати свої навички, щоб вчасно реагувати на нові загрози, виявляти і запобігати атакам. Працівники, які задіяні у сфері кібербезпеки, повинні розуміти міжнародні стандарти та співпрацювати на міжнародному рівні для ефективного боротьби з кіберзагрозами.

Своєчасно й ефективно реагувати на кібератаки, виявляти та усувати передумови до виникнення кіберіндидентів можливе за рахунок розвитку

системи кібербезпеки на національному рівні, що передбачає тематичні кібернавчання та тренінги за участю представників державного та приватного секторів, підтримка науково-дослідних проєктів у сфері кібербезпеки, взаємодію державних органів з приватними особами, освітніми та науковими центрами на принципах партнерства тощо.

У 2014-2018 роках Європейська Комісія профінансувала науково-дослідні гранти та інвестиційні проєкти, які спрямовані на підвищення рівня захисту та стійкості європейських мереж, на суму близько 1,4 мільярда євро [72]. За цей час Європейська Комісія запустила чотири проекти у сфері кібербезщпеки, а саме SPARTA, CONCORDIA, ECHO та CyberSec4Europe. Протягом 2021-2027 років ЄС планує збільшити фінансування в галузі кібербезпеки у розрізі таких програм як Digital Europe, Connecting Europe Facility second generation (CEF2) і Horizon Europe. Зокрема, у межах програми Digital Europe на підвищення рівня кібербезпеки у Європейському Союзі протягом 2021-2027 років буде виділено 1,6 мільярда євро [141].

В Україні виконання масштабних науково-дослідних проєктів у сфері кібербезпеки здійснюється в основному у рамках співпраці з міжнародними організаціями або консорціуму з іноземними навчальними та науковими закладами. Варто відзначити, що починаючи з 2023 року Міністерство освіти й науки України затвердило перелік пріоритетних напрямків при проведенні наукових конкурсів, серед яких є тематика 33 «протидія організованій, транснаціональній та кіберзлочинності органами та підрозділами системи МВС» [43].

Важливе значення для підвищення рівня кіберстійкості є запровадження моделі партнерства між державою та приватним сектором, що дозволяє отримати синергетичний ефект від такої співпраці та підвищити ефективність діяльності у сфері кібербезпеки кожного із учасників. Однією із форм такого партнерства є кластери кібербезпеки, які успішно функціонують як в різних країнах світу (Європейський кластер з безпеки критичної інфраструктури; The Hague Security Delta (Нідерланди); ClujIT (Румунія); GAIA (Іспанія),

Північноєвропейський кластер з кібербезпеки (Фінляндія), Кластер кібербезпеки Бонн e.V. (Німеччина)), так і України (Київ ІТ кластер, Львів ІТ кластер, Харків ІТ кластер та інші).

Зважаючи на активну закордону підтримку України у війні з росією, осторонь не залишається й міжнародна співпраця у сфері боротьби з кіберризиками. Так, обмін інформацією та імплементації кращих практик реалізації політики управління кіберризиками здійснюється з країнами в рамках таких об'єднань, як ОБСЄ, ЄС та НАТО. Міжнародна співпраця у сфері кібербезпеки може приймати різні форми та напрямки для ефективного управління кіберзагрозами, а саме: обмін інформацією та інтелектуальними ресурсами, розробка та впровадження міжнародних стандартів, спільна розробка та проведення тренувань, створення міжнародних центрів кібербезпеки, Захист критичної інфраструктури.

У той же час, справедливо зауважити, що існуюча система кібербезпеки України насичена теоретичними положеннями та напрямками, які необхідно реалізовувати, проте конкретного методичного інструментарію реалізації не наведено. Кожен державний та комерційний орган в системі кібербезпеки повинен самостійно обирати інструментарій реалізації визначених завдань. Виходячи з цього, актуальності набуває групування запропонованих в дисертації науково-методичних підходів у певну взаємопов'язану систему (рисунок 3.22), яка надає можливість сформувати інформаційний базис прийняття управлінських рішень щодо протидії кібер ризикам.

На нашу думку, саме запропоновані у дисертації методологічні засади спроможні забезпечити підвищення ефективності існуючої системи кібербезпеки України на різних ланках її інфраструктури. Так, сім розроблених в дисертації науково-методичних підходів спроможні значно покращити рівень безпечності інформаційного простору в державі та забезпечити адоптацію системи кібербезпеки до своєчасного реагування на динамічні зміни внутрішнього й зовнішнього середовища. Крім того, справедливо зауважити, що для усіх методичних засад прослідковується

можливість адоптації до зміни вхідних параметрів, тобто запропоновані алгоритми розрахунків є універсальними та користувачі інформації можуть розширювати чи скорочувати вхідний масив даних виходячи з нагальної ситуації.

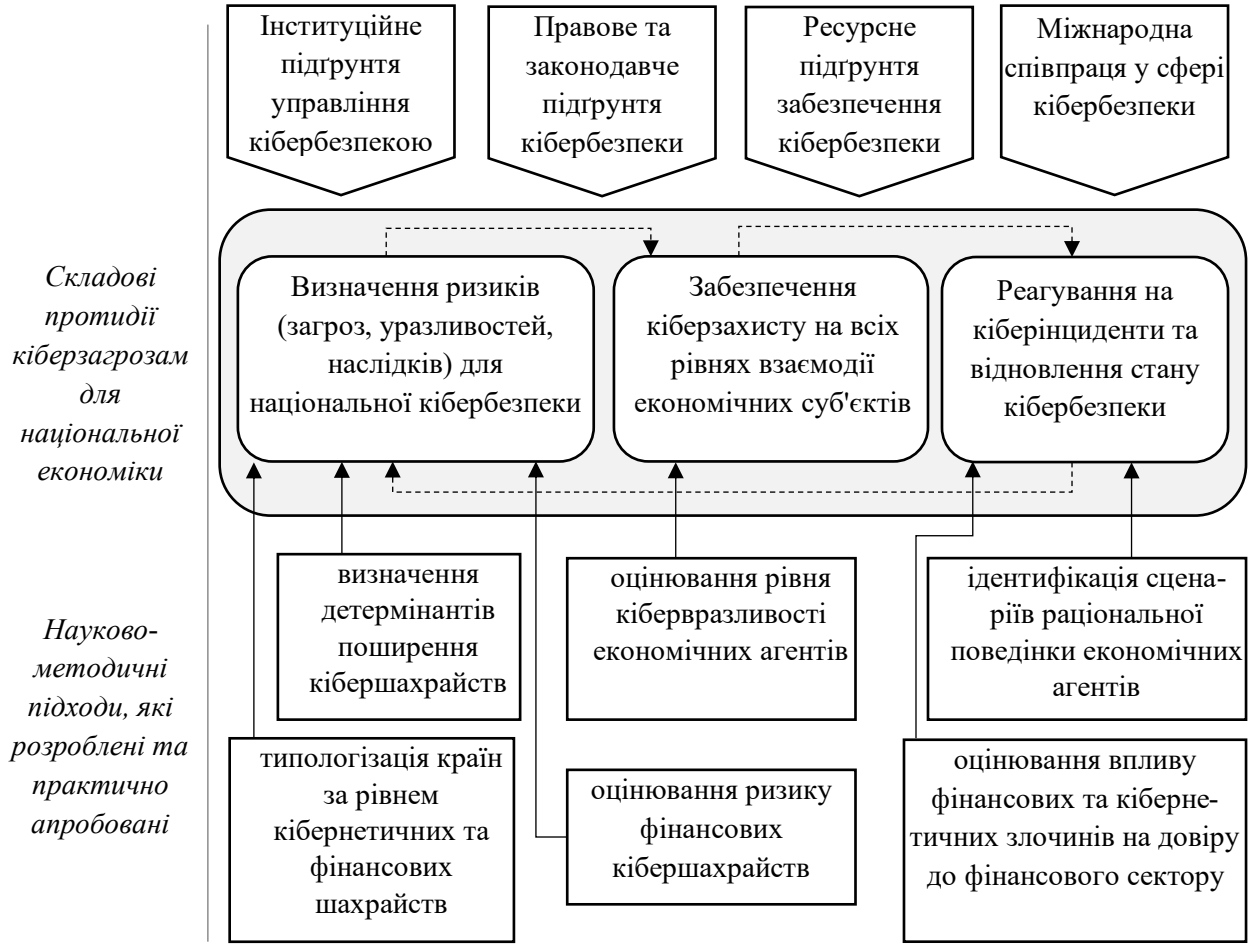


Рисунок 3.22 – Роль запропонованих автором науково-методичних підходів у розрізі складових протидії поширення та локалізації кіберзагроз в умовах цифровізації національної економіки

Джерело: розроблено автором

Для удосконалення національної системи протидії кіберзагрозам проаналізовано європейський досвід у цій сфері. Оскільки європейські державні, приватні та громадські інституції активно проводять інформаційно-просвітницькі та освітні кампанії, спрямовані на підвищення обізнаності щодо персонального та корпоративного захисту в кіберпросторі, а також

здійснюється пошук механізмів для підвищення кіберстійкості економічних суб'єктів.

Визначення ризиків (загроз, уразливостей, наслідків) для національної кібербезпеки.

Частота та складність кібератак у секторі фінансових послуг посилити регулятивний і наглядовий нагляд за кіберризиками. По-перше, переглянуто структуру операційних ризиків фінансових установ та удосконалено внутрішню систему ризик-менеджменту. Різні галузеві нормативні акти Європейського Союзу, а саме Директива про вимоги до капіталу (CRD IV)[67], друга Платіжна Директива (PSD2) [118], друга Директива NIS2 [111], DORA [83] накладають на фінансові установи прямі або непрямі вимоги до управління кіберризиками. У цьому контексті Національним банком України з урахуванням норм законодавства Європейського Союзу внесено зміни до управління ризиками банківських установ, а саме в частині відокремлення в архітектурі операційного ризику ризиків інформаційно-комунікаційних технологій та інформаційної безпеки. Для посилення системи управління інформаційною безпекою банки зобов’язані проводити самооцінку стану кібербезпеки, й подавати звіт з питань самооцінювання на регулятрній основі національному регулятору. У країнах Європейського Союзу дана практика почала функціонувати з 2019 року, тоді як в Україні – з 2021 року. По-друге, запроваджено пруденційні вимоги у сфері інформаційної безпеки для фінансових установ. Зокрема, у Німеччині встановлені мінімальні вимоги до управління безперервністю бізнесу щодо критичних у часі IT-процесів (AT 7.3 MaRisk) [140].

Забезпечення кіберзахисту на всіх рівнях взаємодії економічних суб'єктів.

Європейське та вітчизняне законодавство встановлює основні вимоги та стандарти щодо базових заходів забезпечення інформаційної безпеки, а саме: затверджено технічні стандарти щодо надійної автентифікації до інформаційних систем користувачів; визначено перелік дозволених

криптографічних алгоритмів для захисту інформації; встановлені технічні вимоги для захисту мережі тощо. Для перевірки дотримання законодавчо встановлених вимог до інформаційної безпеки та кіберзахисту фінансових установ національними фінансовими регуляторами країн ЄС і України проводяться виїзні та безвиїзні (аналіз інформації та документів щодо діяльності фінансової установи з питань інформаційної безпеки) заходи контролю.

Важливим елементом захисту від кіберзагроз є проведення аудиту інформаційної безпеки, що дозволяє перевірки відповідність стану інформаційної безпеки визначеним критеріям та показникам безпеки. Для об'єктів критичної інфраструктури дана процедура є обов'язковою, і відповідно до норм законодавства ЄС має проводитися кожні 2 роки, тоді як в Україні – не рідше ніж один раз на два роки.

Реагування на кіберінциденти та відновлення стану кібербезпеки.

Для забезпечення функціонування ефективної системи своєчасного реагування на кіберінциденти має бути розроблений чіткий алгоритм дій суб'єкта який став жертвою кібератаки. Звітування про порушення кібербезпеки є важливою складовою посилення кіберстійкості учасників фінансової системи, оскільки дозволяє ідентифікувати поточні тенденції кіберзагроз та прийняти комплекс заходів для удосконалення системи кібербезпеки з урахуванням виявлених кібервразливостей. У країнах Європейського Союзу правила сповіщення про кіберінциденти запроваджені з 2018 року, тоді як в Україні – з 2023 року. У Директивах ЄС встановлені також чіткі терміни, протягом яких учасники фінансової інфраструктури мають прозвітувати про кіберінциденти: кібератака на безпеку мережевих та інформаційних систем фінансових установ – протягом 72 годин; компрометація персональних даних, конфіденційної інформації – терміново, без зайвої затримки; порушена безпека платіжних послуг – протягом 4 годин; звітування про кіберінциденти системно важливими фінансовими установами

– протягом 2 годин. В Україні не встановлені вимоги щодо термінів звітування про кіберінциденти.

У лютому 2020 року Європол разом із Європейським центральним банком і групою фінансових інфраструктур Європи (центральні банки, клірингові центри, фондові біржі та постачальники платіжних систем) запустили Ініціативу з обміну кіберінформацією та розвідкою (CIISI-EU). Дана ініціатива європейських фінансових інфраструктур дозволяє підвищити рівень кіберстійкості фінансової системи шляхом запобігання, виявлення та реагування на кібератаки, а також обмінюватися інформацією та передовим досвідом між учасниками.

Підсумовуючи, зауважимо, що повністю запобігти кібератакам неможливо, проте фінансові установи та інші суб'єкти господарювання повинні розробити та реалізувати власні стратегії забезпечення кібербезпеки для того, щоб ефективно протистояти кібератакам, адаптуватися до них і швидко відновлюватися, зберігаючи при цьому безперервність роботи фінансової установи.

Справедливо зауважити, що основний вектор подальшого удосконалення політики управління кіберризиками в умовах цифровізації економіки в Україні повинен бути спрямований на: захист об'єктів критичної інфраструктури, моніторинг інтернет контенту, підвищення цифрової грамотності населення за допомогою інтенсивного розвитку методичного забезпечення по своєчасному виявленню, ефективній локалізації та постійному оновленню системи протидії кібер ризикам.

На нашу думку, саме запропоновані у дисертації методологічні засади спроможні забезпечити підвищення ефективності існуючої системи кібербезпеки України на різних ланках її інфраструктури. Так, сім розроблених в дисертації науково-методичних підходів спроможні значно покращити рівень безпечності інформаційного простору в державі та забезпечити адоптацію системи кібербезпеки до своєчасного реагування на динамічні зміни внутрішнього й зовнішнього середовища. Крім того,

справедливо зауважити, що для усіх методичних засад прослідковується можливість адоптації до зміни вхідних параметрів, тобто запропоновані алгоритми розрахунків є універсальними та користувачі інформації можуть розширювати чи скорочувати вхідний масив даних виходячи з нагальної ситуації.

Висновки до розділу 3

Проведений поетапний розрахунок таргетних індикаторів в системі: діджиталізація фінансового сектору–технологічний розвиток–кіберзагрози: 1) за допомогою чотирьох релевантних показників діджиталізації фінансового сектору та технологічного розвитку, а також двох показників характеристики ризику кіберзагроз сформовано інформаційну базу дослідження сценаріїв раціональної поведінки економічних агентів; 2) проведено адаптивну природню нормалізацію показників стимуляторів та адаптивну нормалізацію Севіджа для показників дестимуляторів з урахуванням коригування на середнє квадратичне відхилення; 3) визначено пріоритетність розглянутих трьох груп показників за допомогою методу головних компонент на основі побудови графіку кам'янистого осипу та врахуванні власних значень кореляційної матриці; 4) проведено визначення інтегрального показника в розрізі кожної групи окремо за допомогою трансформованої мультиплікативної згортки Кіні; 5) сформовано три групи якісної інтерпретації кількісних розрахунків інтегральних показників, а саме низький рівень (червона зона), середній рівень (жовта зона), високий рівень (зелена зона); 6) надано графічну інтерпретацію взаємозв'язку ризику кіберзагроз, діджиталізації фінансового сектору та технологічного розвитку.

Практичні результати розрахунків таргетних індикаторів в системі: діджиталізація фінансового сектору–технологічний розвиток–кіберзагрози

засвідчили, що найбільш стійкою ситуація для економічних агентів була у 2021 р., коли в трикутнику «діджиталізація фінансового сектору – технологічний розвиток – кіберзагрози» прослідковувалась повна рівновага й збалансованість. У свою чергу 2019 рік був найбільш ризиковим для економічних агентів, оскільки прослідковувався незадовільний рівень забезпечення діджиталізації фінансового сектора за допомогою впровадження технологій. Виважені рішення економічних агентів у 2019 році щодо діджиталізації призвели до покращення системи протидії внутрішнім та зовнішнім шоками у 2020 р. 2022 р., зважаючи на початок війни та критичне значення кіберзагроз, виявився для економічних агентів найгіршим, сценарії протидії зовнішнім та внутрішнім шокам повинні враховувати як покращення внутрішньої системи протидії ризикам, так і використання зовнішніх інструментів мінімізації втрат завданих ризиками (наприклад страхування).

Одним із ключовим компонентів стабільного функціонування фінансових установ в контексті постійно зростаючих викликів, спричинених збільшенням частоти та обсягів шахрайства із платіжними картками, несанкціонованого доступу до персональних даних клієнтів, незаконного списання коштів із банківських рахунків є довіра споживачів фінансових послуг. Це обумовлює необхідність дослідження наявності статистично значимих зв’язків між довірою до фінансових установ та фінансовими кібершахрайствами та перевірити наявність лагової затримки між даними процесами.

За допомогою дискретного лагового моделювання підтверджено, що між кібервіктимізацією споживачів фінансових послуг та довірою до фінансових установ існує статистично значимий зв’язок з лаговою затримкою, а саме в Німеччині, США, Україна – 1 місяць, Польщі – 3 місяці. Отримані дані засвідчують, що ефект від фінансових кібершахрайств на зміну поведінкових патернів споживачів фінансових послуг присутній та наступає у короткостроковій перспективі. Емпіричні розрахунки наочно демонструють необхідність посилення інформаційних заходів для споживачів фінансових

послуг для підвищення рівня їх обізнаності у сфері особистої кібербезпеки з особливим акцентом на найбільш вразливу верству населення.

Основні положення третього розділу дисертаційної роботи опубліковано автором в роботах [4,14, 15, 30, 33, 103].

ВИСНОВКИ

У дисертації наведено теоретичне узагальнення та запропоновано нове вирішення науково-прикладного завдання розвитку науково-методичних засад дослідження кіберзагроз у контексті динамічної цифровізації фінансових та економічних відносин у країні. За результатами дослідження зроблено наступні висновки.

Науковий інтерес до проблем кіберзагроз та суміжних понять в системі економічних відносин виявив динамічний і стійкий ріст протягом останніх десяти років. Дослідження ґрунтуються на бібліометричному аналізі, здійсненому на основі міжнародної бази даних наукових публікацій Scopus. Протягом 2022 року було опубліковано 690 наукових публікацій, присвячених вивченню кіберзагроз та супутніх аспектів. Результати бібліометричного аналізу вказують на зростаючу важливість теми кіберзагроз у науковому дискурсі. На основі аналізу існуючих підходів до трактування сутності «кіберзагроз» у роботі запропоноване власне визначення цього поняття, а саме як дію наявних та/або потенційно можливих дестабілізуючих факторів та умов навмисного або випадкового порушення безпеки функціонування громадянина, економічних суб’єктів та держави у кіберпросторі. Із-за всеохоплюючого характеру кіберзагроз та їх деструктивного впливу на функціонування не лише суб’єктів господарювання, а також й життєдіяльність громадян країни, то до складу об’єктів кібербезпеки запропоновано також включити інформаційно-комунікаційні засоби фізичних осіб, які використовуються ними для реалізації суспільно та життєво важливих потреб під час використання кіберпростору.

На основі результатів ретроспективного аналізу тенденцій поширення кіберзагроз визначено ключові драйвери стрімкого нарощення загроз та ризиків у кіберпросторі. Упродовж 2005-2020 років найбільша кількість кібератак (41,8% від загального обсягу) була ініційована злочинцями з Китаю,

при цьому 40% з них були направлені на об’єкти критичної інфраструктури у сфері публічного управління та 36% – на об’єкти приватного сектору. Найбільш розповсюдженою формою кібератаки у світі є різні види фішингу, що передбачає викрадення важливої інформації за допомогою електронних листів із застосуванням соціальної інженерії та обману. Щодо України, то у 2022 році офіційно зареєстровано 415 кіберінцидентів, що в 2,8 рази більше порівняно з 2021 роком.

Типологізація країн за рівнем участі їх резидентів у здійсненні фінансових та кібернетичних шахрайств дозволила сформувати список країн, з якими рекомендовано посилити перевірку клієнтів та їх бенефіціарних власників в контексті реалізації превентивних заходів протидії незаконної та сумнівної діяльності. За допомогою кластерного аналізу та дерев класифікації виокремлено 2 групи країн та ідентифіковано тригерні показники та їх значення, на основі яких відбувалося поділ країн на кластери.

Визначення детермінантів поширення кібершахрайств в умовах цифровізації економіки, реалізоване на засадах комплексного поєднання сигмоїдної моделі із застосуванням методів машинного навчання SVM та групового врахування аргументів Івахненка, засвідчило наявність тісних функціональних залежностей між рівнем кіберзагроз та такими чинниками як частка населення, яка користується онлайн банкінгом (0,49), індикатор рівня навичок в Інтернеті (0,42), індикатор онлайн діяльності (0,41).

Результати інтегрального оцінювання рівня кібервразливості економічних агентів дозволили визначити ефективність здійснюваних регуляторних та просвітницьких заходів з інформування населення про потенційні загрози у віртуальному просторі та способи захисту від кіберзагроз. У середньому рівень кібервразливості громадян ЄС становить 11%, вказуючи на те, що населення багатьох європейських країн усвідомлює існуючі загрози в віртуальному просторі та володіє знаннями щодо шляхів захисту від кіберзлочинності. Однак рівень кібервразливості економічних суб’єктів в країнах Європейського Союзу є неоднорідним. Громадяни Данії, Нідерландів

і Швеції мають найнижчий ризик стати жертвою кібершахрайства. З іншого боку, громадяни Іспанії, Італії та Румунії мають найвищий розрахований рівень кібервразливості споживачів фінансових послуг, який складає 18%.

На основі врахування восьми базових індикаторів про користувачів банківських платіжних карток шляхом побудови та навчання нейромережевої моделі розроблено науково-методичний підхід до оцінювання та прогнозування ризику кібершахрайств. За результатами побудови прогностичної моделі встановлено,що 54.2% власників банківських карток, за допомогою яких здійснювалися шахрайські транзакції, були жінки. Середній вік держателів банківських карток, які здійснювали шахрайські фінансові транзакції, становив 50 років. Побудована нейромережева прогностична модель показала високу якість побудованого прогнозу.

Вибір інструментів протидії економічних агентів зовнішнім та внутрішнім шокам національної економіки запропоновано здійснювати з урахуванням активної цифровізації фінансового сектору на основі визначення таргетних індикаторів в системі: діджиталізація фінансового сектору–технологічний розвиток–кіберзагрози. Одержані розрахунки засвідчили, що зважаючи на сталий технологічний розвиток та висхідний тренд діджиталізації фінансового сектору, основні ризики для економічних агентів проявляються в активізації кіберзагроз. У той же час, особливу уваги щодо фінансової і цифрової грамотності повинно приділити населення, оскільки фінансові посередники, не зважаючи на війну продовжують підтримувати високий рівень інформаційної безпеки та швидко адоптуються до новітніх кібер ризиків, а українці залишаються найбільш вразливою ланкою дії нових інформаційних шахрайств.

За результатами оцінювання впливу фінансових шахрайств на рівень довіри споживачів фінансових послуг на засадах дискретного лагового моделювання встановлено, існує статистично значимий зв’язок з лаговою затримкою, а саме в Німеччині, США, Україна – 1 місяць, Польщі – 3 місяці. Отримані дані засвідчують, що ефект від фінансових кібершахрайств на зміну

поведінкових патернів споживачів фінансових послуг присутній та наступає у короткостроковій перспективі.

З метою ефективної протидії кіберзагрозам і забезпечення стійкості фінансової системи доцільно прийняти комплекс заходів, направлених на моніторинг складових інформаційної безпеки фінансових установ, об’єднання зусиль національного регулятора та керівників фінансових установ щодо інформування про реальні та потенційні кібератаки, а також створення якісних компетенцій в сфері інформаційної безпеки шляхом підвищення кваліфікації працівників фінансових установ та національного регулятора.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Боженко В.В., Койбічук В.В., Габенко М.М. Вплив кібершахрайств на фінансову систему на прикладі країн Євросоюзу. *Вісник СумДУ. Серія Економіка*. 2021. № 2. С. 47-52.

2. Боженко В.В., Кушнерьов О. С., Кільдей А.Д. Детермінанти поширення кіберзлочинності у сфері фінансових послуг. *Економічний форум*. 2021. № 4. С. 116-121.

3. Боженко В., Пахненко О., Койбічук В. Досвід ЄС щодо розробки та впровадження національної стратегії кіберстійкості фінансового сектору. *Цифрова економіка та економічна безпека*. 2023. №8 (08). С. 125-129. https://doi.org/10.32782/dees.8-21

4. Бойко А. О., Миненко С. В., Кушнерьов О. С., Хмелик О.С. Створення управлінських інформаційних систем виявлення фінансових операцій, що підлягають під ознаки внутрішнього фінансового моніторингу. *Вісник Сумського державного університету. Серія Економіка*. 2017. № 4. С. 58-66. DOI: https://doi.org/10.21272/1817-9215.2017.4-08

5. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С. В. *Інформаційна та кібербезпека: соціотехнічний аспект*. 2015. URL: https://dut.edu.ua/ua/lib/1/category/1311/view/1209

6. Газізова Ю. Кіберзлочинність в Україні. Ера цифрових технологій – ера нових злочинів. *Юрист&Закон.* 2020. №12. URL: https://uz.ligazakon.ua/ua/magazine_article/EA013606

7. Гарафонова О., Грузіна І., Козирєва О., Маргасова В., Піщенко О., Тарасюк Г. Стратегічні перспективи функціонування українських організацій в умовах євроінтеграції та глобалізації цифрової економіки. *Financial and Credit Activity Problems of Theory and Practice*. 2023. № 1(48). С. 298–311. https://doi.org/10.55643/fcaptp.1.48.2023.3957

8. Демчишак Н., Глутковський М. Розвиток цифрової економіки в Україні: концептуальні основи, пріоритети та роль інновацій. *Інноваційна економіка*. 2020. № 5-6. С. 43-48.

9. Демчишак Н., Радик В. Розвиток цифрової інфраструктури та блокчейн-технологій в Україні. *Інноваційна економіка*. 2020. № 3-4. С. 188-194.

10. Демчишак Н.Б., Шкиря А.С. Управління ризиками у фінансовому секторі України в умовах кіберзагроз і постпандемічного відновлення економіки. *Інноваційна економіка*, 2021. № 3-4. С. 19-27.

11. Дзюбань О. П. Сучасний віртуальний простір: конгеніальність віртуальності й міфи. *Стратегічні пріоритети*. 2017. №3. С. 163-170. URL: https://dspace.nlu.edu.ua/bitstream/123456789/14077/3/St_Dzeban.pdf

12. Діордіца І. В. Поняття та зміст кіберзлочинності. *Глобальна організація союзницького лідерства*. URL: http://goal-int.org/ponyattya-ta-zmist-kiberzlochinnosti

13. Доценко Т. В., Кушнерьов О. С. Використання гравітаційного моделювання при оцінюванні ризику використання банків з метою легалізації доходів, отриманих злочинним шляхом. *Теорія та практика забезпечення розвитку кіберпростору України* : монографія / за ред. О .В. Кузьменко, Г. М. Яровенко. Київ: Інтерсервіс, 2020. С. 110-131.

14. Доценко Т. В., Кушнерьов О. С. Моделювання інтегрального індексу загрози національної економіки за допомогою метода Кернела. *Теорія та практика забезпечення розвитку кіберпростору України:* монографія / за ред. О .В. Кузьменко, Г. М. Яровенко. Київ: Інтерсервіс, 2020. С. 157-172.

15. Доценко Т. В., Миненко С. В., Кушнерьов О. С. Сплайн-моделювання взаємозалежності кібершахрайств, фінансових правопорушень та легалізації кримінальних доходів України // Менеджмент, аудит та фінанси: стан, проблеми та перспективи розвитку : збірник тез наукових робіт учасників Міжнародної науково-практичної конференції для студентів, аспірантів та

молодих учених, м. Київ, 24 квітня 2021 р. Київ: Аналітичний центр «Нова Економіка», 2021. С. 80-85.

16. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія / О. Д. Довгань, І. М. Доронін; НАПрН України, НДІІП. Київ : Видавничий дім «АртЕк», 2017. 107 с.

17. Загуменний О.О. Співвідношень понять «кіберзлочинність» і «компютерні злочини». Процесуальне та техніко-криміналістичне забезпечення досудового розслідування. 2019. URL: https://univd.edu.ua/general/publishing/konf/28_11_2019/pdf/21.pdf

18. Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки 2022. Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. URL: https://nsarchive.gwu.edu/sites/default/files/documents/rr9q9n-glu5j/2023-01-00-SSCIP-Vulnerability-Detection-System-and-Response-to-Cyber-Incidents-and-Cyber-Attacks-%20via-website.pdf

19. Золковер А. О., Кузьменко О. В., Кушнерьов О. С., Койбічук В. В. Бібліометричний аналіз досліджень кіберзлочинності в умовах цифровізації фінансового сектору економіки держави. *Вісник Хмельницького національного університету*. 2019. № 6, Том 2. С. 253-259. DOI: https://doi.org/10.31891/2307-5740-2019-276-6(2)-253-259

20. Козирєва В.П., Гаврилішин А.П. Кіберправопорушення як загроза економічній безпеці України. *Юридичний вісник*. 2020. № 1 (54). С. 148-155.

21. Криклій О.А. Теорія та практика забезпечення кіберстійкості банків. *Ефективна економіка.* 2020. № 10. URL: http://www.economy.nayka.com.ua/?op=1&z=8248

22. Кримінальний кодекс України: Закон від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

23. Криушенко Л. І. До питання класифікації способів шахрайства в банківській сфері. *Вісник Харківського національного університету імені В. Н.*

Каразіна. Право. 2015. С. 261–266. URL: http://nbuv.gov.ua/UJRN/VKhIPR_2015_20_64

24. Кузьменко О. В., Доценко Т. В., Кушнерьов О. С. Оцінювання ризику використання банків з метою легалізації кримінальних доходів на основі гравітаційного моделювання. *Проблеми і перспективи економіки та управління*. 2020. № 1 (21). С. 205-219. DOI: https://doi.org/10.25140/2411-5215-2020-1(21)-205-219.

25. Кузьменко О. В., Доценко Т. В., Кушнерьов О. С. Удосконалення системи фінансового моніторингу: автоматизація процесу верифікації клієнтів банку. *Науковий погляд: економіка та управління*. 2021. № 2. С. 88-95. DOI: https://doi.org/10.32836/2521-666X/2021-72-13

26. Кузьменко О.В., Миненко С.В., Доценко Т.В. Кібершахрайства, фінансові правопорушення та легалізація кримінальних доходів в умовах цифровізації економіки України. *Науковий погляд: економіка та управління*. 2021. №3(72). С. 9-21.

27. Кузьменко О.В., Миненко С.В., Доценко Т.В., Шрамко Е.В. Взаємозалежнысть FinTech інновацій, фінансових, кібернетичних злочинів та легалізації кримінальних доходів за посередництва фінансових установ. *Вісник СумДУ*. 2021. № 1. С. 195-207.

28. Кузьменко О.Ю., Малюк О.В., Чернишова О.О. Кібербезпека бізнесу під час війни. *Економіка та суспільство*. 2022. № 44. URL: https://economyandsociety.in.ua/index.php/journal/article/view/1790/1725

29. Кушнерьов О. С. Тенденції шахрайських операцій на банківському ринку та можливості протидії. *Інноваційна економіка*. 2019. № 3-4. С. 180–188.

30. Кушнерьов О. С., Радько В. В. Організаційні аспекти кібербезпеки платіжних систем у електронній комерційній діяльності. *Priority directions of science and technology development*: збірник тез доповідей V Міжнародної науково-практичної конференції (24-26 січня 2021 р.). С. 1476–1480.

31. Кушнерьов О. С., Яценко В. В. Аналіз тенденцій проведення шахрайських операцій з транзакціями на банківському ринку України. *Проблеми та перспективи розвитку фінансово-кредитної системи України: збірник тез доповідей V Всеукраїнської науково-практичної on-line конференції.* Суми: Сумський державний університет, 2019. С. 156-160.

32. Лєонов С. В., Васильєва Т. А., Кузьменко О. В. Кушнерьов О. С., Скринька Л. О. Проблеми формування інформаційної бази оцінювання ризику легалізації кримінальних доходів в сучасних умовах розвитку фінансової системи України. *Проблеми та перспективи розвитку фінансово-кредитної системи України: збірник тез доповідей V Всеукраїнської науково-практичної on-line конференції*. Суми: Сумський державний університет, 2020. С. 260-265.

33. Лєонов С. В., Кузьменко О. В., Койбічук В. В., Кушнерьов О. С. Розроблення моделі бізнес-процесу автоматизованого моніторингу фінансових операцій банком для протидії легалізації кримінальних доходів. *Вісник Сумського державного університету. Серія Економіка.* 2021. № 1. С. 9−16. DOI: https://doi.org/10.21272/1817-9215.2021.1-1

34. Лєонов С. В., Кузьмено О. В., Кушнерьов О. С., Люльов О. В., Квілінський О. С. Теоретичні основи формування інформаційної бази дослідження ризику використання фінансових установ України з метою легалізації кримінальних доходів. *Вісник Сумського державного університету. Серія Економіка.*. 2020. С. 104-113. DOI: https://doi.org/10.21272/1817-9215.2020.3-11.

35. Лисенко С.М., Харченко В.С., Бобровнікова К.Ю., Щука Р.В. Резильєнтність комп'ютерних систем в умовах кіберзагроз: таксономія та онтологія. *Радіоелектронні і комп'ютерні системи*. 2020. № 1(93). С. 17-28

36. Мельник С.С. Сутність фінансового шахрайства в комерційному банку. *Науковий вісник Ужгородського національного університету*. 2016. № 6, ч. 2. С. 91–95.

37. Набір даних для виявлення шахрайства транзакцій з кредитними картками. Kaggle : веб-сайт. URL: https://www.kaggle.com/kartik2112/fraud-detection?select=fraudTrain.csv

38. Опитування про системні ризики фінансового сектору. Травень 2023 *Національний банк України.* URL: https://bank.gov.ua/ua/news/all/opituvannya-pro-sistemni-riziki-finansovogo-sektoru-traven-2023-roku

39. Островий О.В. Дослідження проблематики забезпечення кібернетичної безпеки в роботах українських науковців: джерельний аналіз. Менеджер. *Вісник Донецького державного університету управління» (серії «Економіка»).* 2018. № 1(78). С. 157-164.

40. Перелік категорій кіберінцидентів. Державна служба спеціального зв'язку та захисту інформації України. URL: https://www.cip.gov.ua/ua/news/perelik-kategorii-kiberincidentiv

41. Платіжні картки в України. Національний банк України. URL: https://bank.gov.ua/ua/news/all/platijni-kartki-v-ukrayini-i-pivrichchya-2021-roku

42. Про затвердження Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг. Постанова НБУ № 4 від 16 січня 2021 року. URL: https://bank.gov.ua/admin_uploads/law/16012021_4.pdf

43. Про затвердження пріоритетної тематики при проведенні конкурсів фундаментальних наукових досліджень, прикладних наукових досліджень та науково-технічних (експерементальних) розробок у 2023 році: наказ Міністерства освіти й науки України № 1104 від 07.09.2023 р. URL: https://mon.gov.ua/storage/app/media/nauka/Konkurs.vidbory.naukovykh.nauk-tekhn.robit.ta.proyektiv/2023/12.09.2023/Nakaz.MON.vid.07.09.2023-1104.pdf

44. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

45. Прудка Л.М. Психологічні особливості шахрайства в мережі інтернет. Південноукраїнський правничий часопис, 2018. №2. С. 30-33. URL: http://dspace.oduvs.edu.ua/bitstream/123456789/1382/1/Прудка_2_2018.pdf

46. Родченко С. С., Живко З. Б. Шахрайство в банківській системі України: способи боротьби із врахуванням зарубіжного досвіду. *Науковий вісник Ужгородського національного університету*. *Міжнародні економічні відносини та світове господарство*. 2020. Вип. 31. С. 103–108

47. Семеног А. Ю. Цифрові технології в умовах формування цифрової економіки. *Наукові записки Національного університету «Острозька академія». Серія Економіка*. 2020. №19(47). С. 20 –28.

48. Семеног А. Ю., Бухтіарова А. Г. Вплив платіжних фінансових технологій на рівень тіньової економіки країни. *Вісник Одеського національного університету І. І. Мечникова. Серія Економіка*. 2020. №4 (83). С. 103-110.

49. Статистика Національного банку України. URL: https://bank.gov.ua/ua/statistic

50. Субботін С. О. Нейронні мережі : теорія та практика: навч. посіб. / С. О. Субботін. – Житомир : Вид. О. О. Євенок, 2020. – 184 с.

51. Цивільний кодекс України від 16.01.2003 № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text

52. Шлапак А. Наглядовий потенціал фінансових установ у протидії кіберзлочинам та інформаційним асиметріям в умовах зростання ролі FINTECH і BIG TECHS на цифровізованих ринках капіталу. *Вісник Хмельницького національного університету*. 2022. № 2(2). С. 273-280. DOI: 10.31891/2307-5740-2022-304-2(2)-43.

53. Штонда Р. М., Паламарчук Н. А., Островський С. М. Соціальні мережі в інтернеті як інструмент загрози національній системі кібербезпеки України. *Актуальні проблеми управління інформаційною безпекою держави*. 2018. Р. 190–192.

54. Akhta S., Sheorey P. A., Bhattacharya S., Ajith K. V. V. Cyber security solutions for businesses in financial services: Challenges, opportunities, and the way Forward. *International Journal of Business Intelligence Research*. 2021. 12(1). URL: https://doi.org/10.4018/IJBIR.20210101.oa5

55. Alhogail A., Alsabih A. Applying machine learning and natural language processing to detect phishing email. *Computers and Security*. 2021. 110. URL: https://doi.org/10.1016/j.cose.2021.102414

56. Allianz Risk Barometer 2023. Allianz. URL: https://www.allianz-trade.com/en_global/news-insights/economic-insights/Allianz-Risk-Barometer-2023.html

57. Al-Tahat S., Moneim O. A. The impact of artificial intelligence on the correct application of cyber governance in Jordanian commercial banks. *International Journal of Scientific and Technology Research*. 2020. 9(3).

58. Andreou P. C., Anyfantaki S. Financial literacy and its influence on internet banking behavior. *European Management Journal*. 2021. 39(5). URL: https://doi.org/10.1016/j.emj.2020.12.001

59. Arcuri M. C., Gai L., Ielasi F., Ventisette E. Cyber attacks on hospitality sector: stock market reaction. *Journal of Hospitality and Tourism Technology*. 2020. 11(2). URL: https://doi.org/10.1108/JHTT-05-2019-0080

60. Bazarbash M. FinTech in Financial Inclusion: Machine Learning Applications in Assessing Credit Risk. *IMF Working Papers*. 2019. 19(109). URL: https://doi.org/10.5089/9781498314428.001https://doi.org/10.17010/ijf/2020/v14i5-7/153326

61. Bauer J. M., Dutton W. H. The New Cybersecurity Agenda: Economic and Social Challenges to a Secure Internet. *SSRN Electronic Journal*. 2015. URL: https://doi.org/10.2139/ssrn.2614545

62. Berdyugin A. A., Revenkov P. V. Cyberattack risk assessment in electronic banking technologies (the case of software implementation). *Finance: Theory and Practice*. 2020. № 24(6). URL: https://doi.org/10.26794/2587-5671-2020-24-6-51-60

63. Bernasco W., Ruiter S., Block R. Do Street Robbery Location Choices Vary Over Time of Day or Day of Week? A Test in Chicago. *Journal of Research in Crime and Delinquency*. 2017. № 54(2). P. 244–275. https://doi.org/10.1177/0022427816680681

64. Borup D., Schütte E. C. M. In Search of a Job: Forecasting Employment Growth Using Google Trends. *Journal of Business and Economic Statistics*. 2022. № 40(1).186–200. https://doi.org/10.1080/07350015.2020.1791133

65. Bukhtiarova A., Semenog A., Razinkova M., Nebaba N., Haber J. A. Assessment of financial monitoring efficiency in the banking system of Ukraine. *Banks and Bank Systems*, 2020. №15(1). P. 98-106.

66. Cable. Global broadband pricing league table 2023. URL: https://www.cable.co.uk/broadband/pricing/worldwide-comparison/

67. Capital Requirements Directive (CRD): Directive EU 2013/36/EU. European Parliament. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013L0036

68. Carlton M., Levy Y., Ramim M. Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills. *Information and Computer Security*. 2019. № 27(1). https://doi.org/10.1108/ICS-11-2016-0088

69. Cebrián E., Domenech J. Is Google Trends a quality data source? *Applied Economics Letters*. 2023. № 30(6). P. 811–815. https://doi.org/10.1080/13504851.2021.2023088

70. Cervellin G., Comelli I., Lippi G. Is Google Trends a reliable tool for digital epidemiology? Insights from different clinical settings. *Journal of Epidemiology and Global Health*. 2017. № 7(3). P. 185–189. https://doi.org/10.1016/j.jegh.2017.06.001

71. Chakrabarty K. C. Fraud in the banking sector – causes, concerns and cures. *Bank for International Settlements*. New Delhi. 2013. URL: https://www.bis.org/review/r130730a.pdf

72. Challenges to effective EU cybersecurity policy. *European Court of Auditors.* Briefing Paper March 2019. URL:

https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_en.pdf

73. Chen D., Wawrzynski P., Lv Z. Cyber security in smart cities: A review of deep learning-based applications and case studies. *Sustainable Cities and Society*. 2021. № 66. https://doi.org/10.1016/j.scs.2020.102655

74. Cloud Computing. *Grand View Research* URL: https://www.grandviewresearch.com/industry-analysis/cloud-computing-industry#

75. Costa M. P. L., Araujo E. Fuzzy financial fraud risk governance system in an information technology environment. *International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies, 3ICT.* 2021. P. 726-732. doi:10.1109/3ICT53449.2021.9581461

76. Craigen D., Diakun-Thibault N., Purse R. Defining Cybersecurity. *Technology Innovation Management Review*. 2014. № 4(10). P. 13–21. https://doi.org/10.22215/timreview/835

77. Crotty J., Daniel E. Cyber threat: its origins and consequence and the use of qualitative and quantitative methods in cyber risk assessment. *Applied Computing and Informatics*. 2022. https://doi.org/10.1108/ACI-07-2022-0178

78. Cyber resilience oversight expectations for financial market infrastructures. 2018. *European Central Bank.* URL: https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf

79. Cyber-resilience: Range of practicesю December 2018. *Basel Committee on Banking Supervision.* URL: https://www.bis.org/bcbs/publ/d454.pdf

80. Data-Mining для протидії кібершахрайствам та легалізації кримінальних доходів в умовах цифровізації фінансового сектору економіки України. Формалізація та оцінка якісних і кількісних параметрів визначення передумов та детермінантів здійснення злочинної діяльності у фінансовому секторі економіки України : звіт про НДР (проміжний) / кер. О. В. Кузьменко. Суми : СумДУ, 2021. 197 с. № 0121U100467

81. Dataset. *World Bank*. URL: https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=UA

82. Digital Economy and Society Index. *European Commission.* URL: https://digital-strategy.ec.europa.eu/en/policies/desi

83. Digital Operational Resilience Act (DORA): Directive EU 2022/2554. *European Parliament*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554&qid=1698394730862

84. Dluhopolskyi O., Pakhnenko O., Lyeonov S., Semenog A., Artyukhova N., Cholewa-Wiktor M., Jastrzębski W. Digital Financial Inclusion: COVID-19 Impacts and Opportunities. Sustainability. 2023. №15(3). https://doi.org/10.3390/su15032383

85. Druhov O., Druhova V., Pakhnenko O. The influence of financial innovations on EU countries banking systems development. *Marketing and Management of Innovations*. 2019. № 3. P. 167–177. https://doi.org/10.21272/mmi.2019.3-13

86. ENISA Threat Landscape 2021. *European Union Agency for Cybersecurity.* URL: https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends.

87. EuRepoc Data. *European Repository of Cyber Incidents.* URL: https://eurepoc.eu/databases

88. Europeans' attitudes towards cyber security. Special Eurobarometer 499. *European Commission.* 2020. URL: https://europa.eu/eurobarometer/surveys/detail/2249

89. Eurostat. Cloud computing - statistics on the use by enterprises. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises

90. Eurostat. Use of Internet of Things in enterprises. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Use_of_Internet_of_Things_in_enterprises#Enterprises_using_IoT

91. Garafonova O., Shestakovska T., Sytnyk N., Marhasova V., Tkalenko N. Financial mechanism for public administration of anti-corruption processes in the context of digitalization of the national economy. *Financial and credit activity: problems of theory and practice*. 2021. № 6 (41). P. 128-137**.**

92. Gaol F. L., Budiansa A. D., Weniko Y. P., Matsuo T. *The digital fraud risk control on the electronic-based companies*. 2022. doi:10.1007/978-981-16-5640-8_56

93. Global Organized Crime Index. URL: https://ocindex.net/report/2023/0-3-contents.html

94. Global Payment Fraud Statistics, Trends & Forecasts. *Merchant Savvy*. URL: https://www.merchantsavvy.co.uk/payment-fraud-statistics/

95. Global Social Network Users 2020. *Emarketer.* URL: https://www.emarketer.com/content/global-social-network-users-2020.

96. González-Manzano L., De Fuentes J. M., Ramos C., Sánchez Á., Quispe F. Identifying Key Relationships between Nation-State Cyberattacks and Geopolitical and Economic Factors: A Model. *Security and Communication Networks*. 2022. https://doi.org/10.1155/2022/5784674

97. Guidance on cyber resilience for financial market infrastructures, CPMI-IOSCO. *Bank for International Settlements*, 2016. URL: https://www.bis.org/cpmi/publ/d146.pdf

98. Haberman C. P., Ratcliffe J. H. Testing for Temporally Differentiated Relationships among Potentially Criminogenic Places and Census Block Street Robbery Counts. *Criminology*. 2015. 53(3). P. 457–483. https://doi.org/10.1111/1745-9125.12076

99. Havranek T., Zeynalov A. Forecasting tourist arrivals: Google Trends meets mixed-frequency data. *Tourism Economics*. 2021. 27(1). P. 129–148. https://doi.org/10.1177/1354816619879584

100. Information technology. Cybersecurity. Overview and concepts ISO/IEC TS 27100:2020. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:ts:27100:ed-1:v1:en

101. Internet Crime Report. *Federal Bureau of Investigation*. URL: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

102. Jouini M., Rabai L. B. A., Aissa A. B. Classification of security threats in information systems. *Procedia Computer Science*. 2014. Vol. 32. P. 489-496. URL: https://doi.org/10.1016/j.procs.2014.05.452

103. Kuzmenko O., Krukhmal O., Koibichuk V., Hrytsenko K., Kushneryov O., Hordiienko V., Pasemko G., Taran O., Smihunova O. Survival Analysis Methods for Assessing the Anti-Money Laundering System Effectiveness. *WSEAS Transactions on Business and Economics*. 2023. 20. P. 1185–1206. DOI: https://doi.org/10.37394/23207.2023.20.106

104. Kuzmenko O.V., Kubálek J., Bozhenko V.V., Kushneryov O.S., Vida I. An approach to managing innovation to protect financial sector against cybercrime Podejście do zarządzania innowacjami w celu ochrony sektora finansowego przed cyberprzestępczością. *Polish Journal of Management Studies*. 2021.№ 24. С. 276-291. DOI: https://doi.org/10.17512/pjms.2021.24.2.17

105. Kuzior A., Vasylieva T., Kuzmenko O., Koibichuk V., Brożek P. Global Digital Convergence: Impact of Cybersecurity, Business Transparency, Economic Transformation, and AML Efficiency. *Journal of Open Innovation: Technology, Market, and Complexity*. 2022. № 8(4). https://doi.org/10.3390/joitmc8040195

106. Li Y., Liu Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports.* 2021. № 7. P. 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

107. Lowry P. B., Zhang J., Wang C., Siponen M. Why do adults engage in cyberbullying on social media? An integration of online disinhibition and deindividuation effects with the social structure and social learning model. *Information Systems Research.* 2016. № 27(4). P. 962–986. https://doi.org/10.1287/isre.2016.0671

108. Motsch W., David A., Sivalingam K., Wagner A., Ruskowski M. Approach for dynamic price-based demand side management in cyber-physical

production systems. *Procedia Manufacturing.* 2020. Vol. 51. P. 1748–1754. URL: https://doi.org/10.1016/j.promfg.2020.10.243

109. Mousa M., Sai A.A., Salhin G. An Exploration for the Motives behind Enhancing Senior Banker's Level of Organizational Resilience: A Holistic Case Study. *Journal of Intercultural Management*. 2017. 9(4). URL: https://doi.org/10.1515/joim-2017-0025

110. Mukhopadhyay A., Chatterjee S., Bagchi K., Kirs P. J., Shukla G. K. Cyber risk assessment and mitigation (CRAM) framework using logit and probit models for cyber insurance. *Information Systems Frontiers.* 2019. Vol. 21(5). P. 997-1018. doi:10.1007/s10796-017-9808-5

111. Network and Information Security Directive (NIS2): Directive EU 2022/2555. *European Parliament*. URL: https://eur-lex.europa.eu/eli/dir/2022/2555

112. Nicholls J., Kuppa A., Le-Khac N. Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. *IEEE Access*. 2021. Vol. 9. P. 163965-163986. doi:10.1109/ACCESS.2021.3134076

113. Nish A., Naumann S., Muir J. Enduring Cyber Threats and Emerging Challenges to the Financial Sector. *Carnegie Endowment for International Peace*. 2020. URL: https://carnegieendowment.org/2020/11/18/enduring-cyber-threats-and-emerging-challenges-to-financial-sector-pub-83239

114. Noor U., Anwar Z., Amjad T., Choo K. K. R. A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise. *Future Generation Computer Systems*. 2019. 96. URL: https://doi.org/10.1016/j.future.2019.02.013

115. Onete C. B., Vargas V. M., Chita S. D. Study on the implications of personal data exposure on the social media platforms. *Transformations in Business and Economics.* 2020. 19(2).

116. Pakhnenko O., Kuan Z. Ethics of Digital Innovation in Public Administration. *Business Ethics and Leadership.* 2023. № 7(1). P. 113-121. http://doi.org/10.21272/bel.7(1).113-121.2023.

117. Pakhnenko O., Rubanov P., Hacar D., Yatsenko V. Digitalization of financial services in European countries: Evaluation and comparative analysis. *Journal of International Studies*. 2021. № 14(2). P. 267–282. https://doi.org/10.14254/2071-8330.2021/14-2/17

118. Payment Services Directive (PSD2): Directive EU 2015/2366. *European Parliament*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366

119. Porcedda M. G., Wall D. S. Modelling the cybercrime cascade effect in data crime. Paper presented at the *Proceedings - 2021 IEEE European Symposium on Security and Privacy Workshops, Euro S and PW*. 2021, P. 161-177. doi:10.1109/EuroSPW54576.2021.00025

120. Prieto Curiel R. Weekly Crime Concentration. *Journal of Quantitative Criminology*. 2023. № 39(1). P. 97-124. URL: https://doi.org/10.1007/s10940-021-09533-6

121. Ransomware Statistics. Trends and Facts for 2023 and Beyond. *Cloudwards*. URL: https://www.cloudwards.net/ransomware-statistics/

122. Report on card fraud in 2020 and 2021. *European Central Bank*. 2021. URL: https://www.ecb.europa.eu/pub/pdf/cardfraud/ecb.cardfraudreport202305~5d832d6515.en.pdf

123. Rodrigues B., Franco M., Parangi G., Stiller B. SEConomy: A Framework for the Economic Assessment of Cybersecurity. *Lecture Notes in Computer Science*. 2019. Vol. 11819 LNCS. P. 154–166. https://doi.org/10.1007/978-3-030-36027-6_13

124. Roshchin I., Pikus R., Zozulia N., Marhasova V., Kaplinskiy V., Volkova N. Knowledge Management Trends in the Digital Economy Age. *Postmodern Openings*. 2022. № 13(3). P. 346-357. https://doi.org/10.18662/po/13.3/493

125. Rubasundram G. A. Fraud risk assessment: A tale of the possible corporate executive fraud and the perceived cyber-security. *International Journal of Recent Technology and Engineering*. 2019. 7(5 Special Issue). P. 164-168.

126. Samoilovych A., Garafonova O., Popelo O., Marhasova V., Lazarenko Yu. World experience and ukrainian realities of digital transformation of regions in the context of the information economy development. *Financial and credit activity: problems of theory and practice*. 2021. № 3(38). P. 316–325. https://doi.org/10.18371/fcaptp.v3i38.237462 .

127. Senecal C., Mahowald M., Lerman L., Lopes-Jimenez F., Lerman A. Increasing utility of Google Trends in monitoring cardiovascular disease. *Digital Health*. 2021. № 7. https://doi.org/10.1177/20552076211033420

128. Shaikh F. A., Siponen M. Organizational Learning from Cybersecurity Performance: Effects on Cybersecurity Investment Decisions. *Information Systems Frontiers*. 2023. https://doi.org/10.1007/s10796-023-10404-7

129. Shkolnyk I., Frolov S., Orlov V., Datsenko V., Kozmenko Y. The impact of financial digitalization on ensuring the economic security of a country at war: New measurement vectors. *Investment Management and Financial Innovations*. 2022. №19 (3). P. 119–138.

130. Shkolnyk I., Kozmenko S., Kozmenko O., Orlov V., Shukairi F., Modeling of the financial system's stability on the example of Ukraine. *Equilibrium. Quarterly Journal of Economics and Economic Policy*. 2021. №16(2). P. 377–411.

131. Shkolnyk I., Kozmenko S., Polach J., Wolanin E. State financial security: Comprehensive analysis of its impact factors. *Journal of International Studies*. 2020. №13(2). P. 291-309.

132. Shitova Yu. Yu., Shitov Yu. A. Contemporary Trends in Economic Cybersecurity. *The World of New Economy*. 2019. № 13(4). P. 22–30. https://doi.org/10.26794/2220-6469-2019-13-4-22-30

133. Significant Cyber Incidents. *Centre for Strategic and International studies.* URL: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

134. Silva C. M. R. D., Feitosa E. L., Garcia V. C. Heuristic-based strategy for phishing prediction: A survey of URL-based approach. *Computers and Security*. 2020. Vol. 88. doi:10.1016/j.cose.2019.101613.

135. Simionescu M., Cifuentes-Faura J. Forecasting National and Regional Youth Unemployment in Spain Using Google Trends. *Social Indicators Research*. 2022. 164(3). P. 1187–1216. https://doi.org/10.1007/s11205-022-02984-9

136. Singh S. K., Jeong Y. S., Park J. H. A deep learning-based IoT-oriented infrastructure for secure smart City. *Sustainable Cities and Society*. 2020. № 60. https://doi.org/10.1016/j.scs.2020.102252

137. Sivesind T. E., Szeto M. D., Kim W., Dellavalle R. P. Google Trends in Dermatology: Scoping Review of the Literature. *JMIR Dermatology*. 2021. https://doi.org/10.2196/27712

138. Srivastava S. K., Das S., Udo G. J., Bagchi K. Determinants of Cybercrime Originating within a Nation: A Cross-country Study. *Journal of Global Information Technology Management*. 2020. №23(2). P. 112–137. https://doi.org/10.1080/1097198X.2020.1752084

139. Sturc B., Gurova T., Zelenková N., Shestak V. Developing a system of indicators for clustering financial cybercrime. *Journal of Applied Security Research*. 2021. doi:10.1080/19361610.2021.2013112.

140. Supervisory Requirements for IT in Financial Institutions (BAIT): EBA/GL/2019/04. *Bundesbank*. URL: https://www.bundesbank.de/resource/blob/598668/a60c043bd815c310f2915408f6544087/mL/2017-10-bait-2021-data.pdf

141. The Digital Europe Programme. *European Commission*. URL: https://digital-strategy.ec.europa.eu/en/activities/digital-programme

142. The Global Covid-19 FinTech Regulatory Rapid Assessment Report. *World Bank Group and the University of Cambridge*. URL: https://www.jbs.cam.ac.uk/wp-content/uploads/2020/10/2020-ccaf-report-fintech-regulatory-rapid-assessment.pdf

143. The Mobile Economy 2020. *GSM Association* URL: https://www.gsma.com/mobileeconomy/wpontent/uploads/2020/03/GSMA_MobileEconomy2020_Global.pdf

144. The Top Threat Actors Targeting Financial Services Organizations. *Insights*. 2018. URL: https://intsights.com/blog/the-top-threat-actors-targeting-financial-services-organizations

145. Tweneboah-Koduah S., Atsu F., Prasad R. Reaction of stock volatility to data breach: An event study. *Journal of Cyber Security and Mobility*. 2020. 9(3). https://doi.org/10.13052/JCSM2245-1439.931

146. Uma M., Padmavathi G. A survey on various cyber attacks and their classification. *International Journal of Network Security.* 2013. *15*(5). P. 390–396.

147. Vasiu I., Vasiu L. Cybersecurity as an Essential Sustainable Economic Development Factor. *European Journal of Sustainable Development*. 2018. № 7(4). https://doi.org/10.14207/ejsd.2018.v7n4p171

148. Von Solms R., Van Niekerk J. From information security to cyber security. *Computers and Security.* 2013. № 38. P. 97–102. URL: https://doi.org/10.1016/j.cose.2013.04.004

149. Waldrop M.M. How to hack the hackers: The human side of cybercrime. *Nature*. 2016. 533. P. 164–167.

150. Wessels M., van den Brink P., Verburgh T., Cadet B., van Ruijven T. Understanding incentives for cybersecurity investments: Development and application of a typology. *Digital Business*. 2021. № 1(2). https://doi.org/10.1016/j.digbus.2021.100014

151. What is a cyberattack? *IBM.* URL: https://www.ibm.com/topics/cyber-attack

152. Which countries have the worst (and best) cybersecurity? *Comparitech*. URL: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/

153. World Robotics Report 2020. International Federation of Robotics. URL: https://ifr.org/downloads/press2018/Presentation_WR_2020.pdf

154. X-Force Threat Intelligence Index 2021. *IBM Security*. URL: https://www.ibm.com/downloads/cas/M1X3B7QG

155. Yang A., Kwon Y. J., Lee S. Y. T. The impact of information sharing legislation on cybersecurity industry. *Industrial Management and Data Systems*. 2020. № 120(9). P. 1777–1794. https://doi.org/10.1108/IMDS-10-2019-0536

156. Yerdon V. A., Lin J., Wohleber R. W., Matthews G., Reinerman-Jones L., Hancock P. A. Eye-Tracking Active Indicators of Insider Threats: Detecting Illicit Activity During Normal Workflow. *IEEE Transactions on Engineering Management*. 2021. URL: https://doi.org/10.1109/TEM.2021.3059240

157. Yevseiev S., Rzayev K., Mammadova T., Samedov F., Romashchenko N. Класифікатор кіберзагроз інформаційних ресурсів автоматизованих банківських систем. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка.* 2018. № 2(2). P. 47–67. URL: https://doi.org/10.28925/2663-4023.2018.2.4767

158. Ying W., Jia S., Du W. Digital enablement of blockchain: Evidence from HNA group. *International Journal of Information Management.* 2018. № 39. P. 1-4. URL: https://doi.org /10.1016/j. ijinfomgt.2017.10.004

159. Zhang H., Wang Y., Zheng Q., Tang K., Fang R., Wang Y., Sun Q. Research Interest and Public Interest in Melanoma: A Bibliometric and Google Trends Analysis. *Frontiers in Oncology*. 2021. *11*. https://doi.org/10.3389/fonc.2021.629687

ДОДАТКИ

Додаток А

Таблиця А.1 – Нормалізовані значення показників 1-ої та 2-ї групи

Країни	X1_1	X1_2	X1_3	X1_4	X1_5	X1_6	X1_7	X1_8	X1_9	X2_1	X2_2	X2_3	X2_4
Албанія	0,3	-0,3	0,1	-0,3	0,0	0,3	0,8	0,3	-0,8	0,5	1,0	0,5	-1,0
Білорусь	0,0	0,3	-0,4	-0,8	-0,1	-0,3	-1,0	-0,8	0,0	-0,3	-0,1	1,0	-0,1
Хорватія	0,1	-0,6	0,2	-0,7	-0,3	0,0	0,3	-0,3	0,2	-0,3	0,6	0,3	-0,3
Кіпр	0,1	-0,9	-0,5	-0,5	-0,9	-1,0	-0,1	-0,8	-0,8	-0,4	-0,1	-0,3	0,6
Чехія	-0,1	-0,3	-0,4	0,3	-0,6	-0,2	-0,1	-0,1	0,6	-0,5	-0,1	0,1	-0,3
Данія	-0,3	-0,4	-0,8	-0,8	-0,9	0,0	0,3	-0,5	0,0	0,0	-0,6	-0,9	-0,3
Єгипет	0,0	0,4	-1,0	0,2	-0,4	0,2	-1,0	0,3	0,8	-0,5	0,1	0,7	-0,1
Естонія	-0,7	-0,7	-0,8	-1,0	-0,6	-0,7	-0,5	-0,5	0,6	-0,5	-0,1	-0,9	-0,1
Фінляндія	-0,9	-0,9	-1,0	-1,0	-0,9	-0,5	-0,3	-1,0	-0,2	-0,5	-1,0	-1,0	-0,8
Франція	0,3	0,1	-0,1	0,3	-0,3	0,3	0,6	0,1	0,2	0,3	0,6	-0,6	0,6
Грузія	-1,0	-1,0	-0,2	-0,3	-0,6	-0,5	-1,0	-1,0	-0,4	-0,6	-1,0	-0,6	-0,8
Німеччина	0,4	0,1	-0,8	-0,3	-0,8	-0,2	0,6	-0,5	0,4	0,0	0,6	-0,9	0,5
Греція	0,6	-0,6	-0,7	-0,7	-0,6	0,3	-0,5	-0,5	-1,0	-0,5	0,6	0,6	0,3
Угорщина	0,1	-0,6	-0,2	0,0	-0,5	-0,2	0,1	-0,3	0,2	-1,0	-0,6	0,5	-0,1
Італія	0,3	0,0	-0,5	-0,3	0,0	-0,2	1,0	-0,5	0,0	1,0	-1,0	0,3	0,6
Йорданія	0,0	0,3	-0,2	-0,3	-1,0	-0,5	-0,6	-0,1	0,4	-0,9	0,8	0,3	-0,3
Латвія	-0,6	-0,6	-1,0	-0,8	-0,9	-0,2	0,1	-0,3	0,0	-0,4	-0,8	-0,9	-0,3
Литва	-0,9	-0,9	-1,0	-0,8	-0,9	-0,3	-0,1	-0,8	-0,4	-0,4	-0,6	-0,3	-0,8
Мальта	-0,4	-0,9	-1,0	0,2	-0,1	-0,7	0,1	-0,6	0,2	-0,9	0,8	0,6	-0,1
Молдова	-0,4	-0,1	-0,5	-0,8	-0,6	-0,7	-0,8	-0,6	0,0	-0,3	-0,6	0,5	-0,1
Морокко	0,3	-0,7	-0,4	0,0	-0,6	-0,7	0,5	1,0	0,4	-1,0	0,6	0,5	-0,5
Нідерланди	-0,3	-0,1	-0,4	-0,2	-0,4	-0,3	0,8	-0,3	1,0	-0,1	0,3	-0,7	-0,3
Норвегія	-0,6	-0,6	-0,5	-0,2	-0,5	0,0	-0,1	-0,8	-0,2	-0,1	-0,6	-0,9	-0,5
Польща	-0,3	-0,6	-0,7	-0,7	0,0	-0,3	-0,1	-0,3	0,6	-0,8	0,1	-0,5	-0,6
Португалія	-0,4	-0,4	-0,2	-0,3	-0,6	-0,2	0,1	-0,6	-0,2	-0,1	0,3	-0,2	-0,1
Росія	0,1	-0,3	1,0	1,0	-0,1	0,7	-0,1	-0,5	1,0	-0,1	1,0	0,9	-0,1
Сербія	0,3	0,6	-0,1	-0,2	-0,4	0,7	0,3	-0,1	0,4	0,3	0,8	0,7	0,5
Словенія	0,0	-0,6	-0,7	-0,5	-0,8	-0,3	-0,1	-0,5	0,2	-0,5	-0,3	0,2	-0,1
Іспанія	0,4	-0,4	-0,2	0,2	-0,9	0,5	0,8	0,3	-0,4	0,3	0,6	-0,1	0,8
Швеція	0,0	0,1	-0,7	-0,3	-0,9	-0,3	-0,1	-0,5	0,2	0,1	0,1	-0,7	0,3
Туніс	0,4	-0,1	-0,2	-0,3	-0,1	-1,0	-0,6	-0,5	-0,4	-1,0	-0,6	0,1	-0,8
Туреччина	1,0	1,0	-0,1	-0,5	1,0	1,0	-0,3	-0,5	0,2	0,8	1,0	1,0	-0,1
Україна	0,3	0,7	0,7	-0,2	0,4	0,0	-0,5	-0,5	-0,6	0,3	0,8	0,7	0,3
Великобританія	-0,1	-0,6	-0,5	-0,2	-0,9	-0,2	0,6	-0,6	0,2	-0,3	0,6	-0,6	1,0

Додаток Б

Таблиця Б.1 – Статистична база характеристики детермінант поширення кіберзагроз станом на 2020 рік

Країни	Умовні позначення	I1	I2	I3	I4	I5	I6	I7	I8	I9	I10	I11	I12	I13	I14	I15
Австрія	AUS	1,82	0,02	0	0,2	0,06	2,87	5,51	1,39	0,05	0,15	0,16	0,38	0,62	10,17	22321
Бельгія	BEL	2,85	0,02	0,01	0,2	0,05	4,39	5,85	1,98	0,08	0,2	0,13	0,25	0,28	16,4	49342
Болгарія	BGR	3,5	0,03	0,01	0,5	0,16	4,83	15,43	0,66	0,24	0,56	0,17	0,5	0,38	11,35	301
Хорватія	HRV	2,54	0,02	0,01	0,3	0,08	3,89	7,39	1,04	0,1	0,36	0,13	1,3	0,37	9,15	8418
Данія	DNK	1,33	0	0	0,1	0,02	1,33	2,83	1,42	0,02	0,11	0,07	0,07	0,06	3,26	9208
Фінляндія	FIN	1,06	0,02	0,01	0,3	0,06	2,73	5,77	0,39	0,02	0,36	0,09	0,23	0,01	7,14	1994
Франція	FRA	2,56	0,01	0	0,2	0,08	6,71	6,45	2,53	0,46	0,16	4,03	5,97	1,12	17,9	30485
Німеччина	DEU	1,63	0,02	0,01	0,3	0,06	3,54	4,94	1,8	0,66	0,12	4,67	10,97	7,28	9,68	314459
Греція	GRC	2,75	0,01	0	0,5	0,14	5,39	13,27	1,4	2,52	0,49	0,19	0,21	1,75	16	10677
Угорщина	HUN	3,34	0	0	0,2	0,12	4,33	12,7	1,83	0,3	0,42	0,35	0,83	0,34	15,1	2546
Ірландія	IRL	2,12	0	0,01	0,1	0,04	1,35	3,49	1,63	0,04	0,19	0,33	0,25	0,06	3,42	22331
Італія	ITA	3,26	0,31	0,02	0,5	0,12	4,38	10,74	2,32	1,56	0,22	1,35	1,02	5,45	15,45	578779
Латвія	LVA	3,36	0,02	0	0,3	0,16	7,31	13,95	0,61	0,1	0,73	0,06	0,91	0,3	12,86	78
Нідердланди	NLD	1,66	0,02	0,01	0,2	0,05	1,66	4,24	1,1	0,28	0,19	1,86	4	0,26	4,84	15537
Польща	POL	2,79	0,09	0,01	0,3	0,09	3,69	7,54	1,48	0,61	0,37	0,48	2,05	0,65	12,7	5976
Португалія	PRT	3,38	0,01	0,01	0,9	0,12	5,34	11,5	2,2	0,1	0,44	0,17	0,35	1,88	19,73	2299
Румунія	ROU	5,04	0,02	0,02	0,4	0,04	5,3	14,4	1,32	0,58	0,14	0,29	0,49	0,98	5,76	2812
Словаччина	SVK	3,5	0,03	0,01	0,3	0,11	3,43	8,24	1,24	0,09	0,5	0,04	0,19	0,09	12,94	450
Іспанія	ESP	4,31	0,22	0,01	0,3	0,09	5,92	11,63	2,27	0,7	0,36	0,72	2,66	8,48	13,49	1825476
Швеція	SWE	1,78	0,01	0,01	0,2	0,03	1,435	3,34	1,54	0,28	0,18	0,38	0,19	0,05	3,35	3337
Великобританія	GBR	2,26	0,03	0,01	0,2	0,05	2,71	4,77	1,65	0,89	0,2	1,69	1,04	1,07	9,75	11228

Таблиця Б.2 – Індикатори, що характеризують рівень кібервразливості економічних агентів

Умовні позначення	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13	R14	R15	R16	R17
BE	46%	46%	27%	9%	27%	14%	43%	28%	50%	49%	7%	29%	17%	27%	1%	54%	29%
BG	32%	52%	15%	11%	25%	9%	32%	17%	36%	32%	2%	22%	7%	12%	7%	66%	19%
CZ	36%	37%	27%	7%	26%	6%	31%	23%	43%	34%	5%	24%	7%	19%	2%	54%	24%
DK	27%	39%	25%	2%	41%	19%	34%	41%	59%	58%	9%	27%	25%	31%	6%	19%	14%
D-W	42%	57%	35%	3%	50%	17%	25%	43%	51%	59%	18%	36%	17%	31%	2%	41%	22%
DE	41%	57%	36%	4%	48%	17%	26%	42%	50%	57%	17%	34%	16%	30%	4%	42%	20%
D-E	39%	55%	41%	6%	39%	14%	32%	36%	45%	49%	15%	24%	9%	26%	10%	50%	15%
EE	25%	33%	34%	3%	33%	16%	41%	32%	64%	50%	12%	27%	18%	23%	6%	42%	24%
IE	52%	53%	36%	11%	28%	18%	35%	30%	38%	35%	9%	25%	14%	26%	2%	39%	28%
EL	44%	57%	23%	22%	40%	9%	46%	15%	47%	56%	4%	16%	4%	17%	4%	57%	40%
ES	49%	53%	20%	8%	19%	7%	26%	21%	33%	29%	5%	17%	8%	22%	9%	55%	14%
FR	43%	49%	31%	7%	24%	14%	42%	29%	50%	45%	8%	35%	13%	29%	4%	46%	17%
HR	40%	49%	13%	9%	24%	8%	22%	15%	27%	30%	14%	14%	5%	15%	1%	60%	30%
IT	41%	40%	23%	8%	18%	8%	27%	18%	31%	29%	4%	15%	8%	12%	2%	67%	22%
CY	43%	60%	22%	16%	39%	6%	44%	22%	47%	33%	6%	17%	5%	17%	7%	50%	24%
LV	29%	38%	49%	2%	23%	8%	35%	27%	43%	34%	8%	18%	12%	15%	10%	50%	24%
LT	36%	44%	39%	12%	42%	5%	37%	17%	45%	57%	6%	20%	10%	16%	4%	42%	17%
LU	42%	44%	34%	9%	26%	17%	35%	31%	55%	51%	9%	37%	22%	28%	3%	37%	30%
HU	35%	31%	18%	12%	20%	9%	20%	13%	25%	33%	9%	17%	8%	13%	1%	59%	23%
MT	31%	45%	26%	4%	19%	11%	44%	34%	45%	45%	3%	29%	10%	22%	4%	32%	44%
NL	44%	48%	39%	5%	59%	22%	45%	56%	64%	60%	7%	42%	31%	46%	3%	27%	31%
AT	27%	34%	41%	12%	32%	20%	25%	28%	42%	54%	14%	30%	20%	23%	6%	46%	34%
PL	24%	32%	31%	6%	25%	8%	27%	19%	35%	33%	6%	17%	10%	17%	1%	43%	20%
PT	32%	54%	15%	11%	33%	10%	34%	20%	43%	35%	2%	15%	4%	15%	13%	57%	18%
RO	40%	34%	10%	13%	13%	6%	13%	14%	23%	28%	5%	18%	7%	13%	4%	67%	14%
SI	43%	47%	22%	9%	28%	11%	33%	23%	46%	42%	5%	20%	5%	20%	7%	56%	25%
SK	37%	31%	24%	3%	16%	6%	29%	15%	35%	45%	3%	17%	5%	18%	2%	54%	23%
FI	39%	43%	28%	2%	42%	28%	36%	46%	59%	53%	10%	37%	22%	22%	5%	31%	34%
SE	42%	43%	26%	6%	55%	30%	37%	51%	60%	52%	30%	40%	34%	37%	2%	28%	18%
UK	46%	44%	42%	10%	29%	19%	35%	34%	40%	36%	6%	27%	16%	21%	3%	29%	32%

ДОДАТОК В

Результати побудови нейромережевих моделей для оцінювання ризику фінансового кібершахрайства

Network weights (Spreadsheet1.sta)

Weight ID	Connections 3.MLP 7-5-1	Weight values 3.MLP 7-5-1	Connections 4.MLP 7-5-1	Weight values 4.MLP 7-5-1	Connections 5.MLP 7-8-1	Weight values 5.MLP 7-8-1
1	cc_num --> hidden neuron 1	-4,0240	cc_num --> hidden neuron 1	-1,5944	cc_num --> hidden neuron 1	-0,1076
2	cc_num --> hidden neuron 2	-12,6913	cc_num --> hidden neuron 2	-3,5831	cc_num --> hidden neuron 2	-65,7287
3	cc_num --> hidden neuron 3	14,1261	cc_num --> hidden neuron 3	-7,7976	cc_num --> hidden neuron 3	0,7629
4	cc_num --> hidden neuron 4	35,2826	cc_num --> hidden neuron 4	-1,2634	cc_num --> hidden neuron 4	2,1286
5	cc_num --> hidden neuron 5	27,9063	cc_num --> hidden neuron 5	7,3452	cc_num --> hidden neuron 5	0,2560
6	amt --> hidden neuron 1	18,7772	amt --> hidden neuron 1	-14,5368	cc_num --> hidden neuron 6	1,8959
7	amt --> hidden neuron 2	-23,2665	amt --> hidden neuron 2	-0,8644	cc_num --> hidden neuron 7	0,1180
8	amt --> hidden neuron 3	-0,1395	amt --> hidden neuron 3	4,1276	cc_num --> hidden neuron 8	0,1076
9	amt --> hidden neuron 4	-70,3528	amt --> hidden neuron 4	-19,5980	amt --> hidden neuron 1	-15,0494
10	amt --> hidden neuron 5	0,5410	amt --> hidden neuron 5	-0,8575	amt --> hidden neuron 2	0,7691
11	birth --> hidden neuron 1	-2,6496	birth --> hidden neuron 1	-3,1104	amt --> hidden neuron 3	2,0294
12	birth --> hidden neuron 2	2,0735	birth --> hidden neuron 2	-3,1853	amt --> hidden neuron 4	-6,9032
13	birth --> hidden neuron 3	0,0485	birth --> hidden neuron 3	-1,9019	amt --> hidden neuron 5	-0,2054
14	birth --> hidden neuron 4	-0,2636	birth --> hidden neuron 4	-0,4376	amt --> hidden neuron 6	-0,0154
15	birth --> hidden neuron 5	-0,7097	birth --> hidden neuron 5	1,7453	amt --> hidden neuron 7	0,0077
16	time --> hidden neuron 1	33,6740	time --> hidden neuron 1	2,7679	amt --> hidden neuron 8	40,5452
17	time --> hidden neuron 2	9,3340	time --> hidden neuron 2	-0,7121	birth --> hidden neuron 1	-0,0152
18	time --> hidden neuron 3	-16,2636	time --> hidden neuron 3	-7,1342	birth --> hidden neuron 2	0,5863
19	time --> hidden neuron 4	-2,9899	time --> hidden neuron 4	-2,8074	birth --> hidden neuron 3	-0,1331
20	time --> hidden neuron 5	4,8023	time --> hidden neuron 5	-2,9713	birth --> hidden neuron 4	-1,3970
21	gender2 --> hidden neuron 1	11,8304	gender2 --> hidden neuron 1	-0,3354	birth --> hidden neuron 5	0,0155
22	gender2 --> hidden neuron 2	-29,0316	gender2 --> hidden neuron 2	0,1052	birth --> hidden neuron 6	-0,0485
23	gender2 --> hidden neuron 3	127,4405	gender2 --> hidden neuron 3	-38,4271	birth --> hidden neuron 7	-24,0793
24	gender2 --> hidden neuron 4	-1,6147	gender2 --> hidden neuron 4	0,8018	birth --> hidden neuron 8	0,8223
25	gender2 --> hidden neuron 5	-0,8162	gender2 --> hidden neuron 5	-0,9426	time --> hidden neuron 1	2,2162
26	category2 --> hidden neuron 1	-0,1927	category2 --> hidden neuron 1	0,2355	time --> hidden neuron 2	-2,2427
27	category2 --> hidden neuron 2	-4,1593	category2 --> hidden neuron 2	2,1451	time --> hidden neuron 3	0,5635
28	category2 --> hidden neuron 3	-0,5874	category2 --> hidden neuron 3	-0,0633	time --> hidden neuron 4	0,0390

Network weights (Spreadsheet1.sta)

Weight ID	Connections 3.MLP 7-5-1	Weight values 3.MLP 7-5-1	Connections 4.MLP 7-5-1	Weight values 4.MLP 7-5-1	Connections 5.MLP 7-8-1	Weight values 5.MLP 7-8-1
28	category2 --> hidden neuron 3	-0,5874	category2 --> hidden neuron 3	-0,0633	time --> hidden neuron 4	0,0390
29	category2 --> hidden neuron 4	7,7014	category2 --> hidden neuron 4	-0,2520	time --> hidden neuron 5	0,0030
30	category2 --> hidden neuron 5	5,7137	category2 --> hidden neuron 5	66,6839	time --> hidden neuron 6	1,7963
31	Week_date --> hidden neuron 1	31,4874	Week_date --> hidden neuron 1	-0,9802	time --> hidden neuron 7	-0,2621
32	Week_date --> hidden neuron 2	-29,4272	Week_date --> hidden neuron 2	0,0820	time --> hidden neuron 8	-0,4710
33	Week_date --> hidden neuron 3	7,7142	Week_date --> hidden neuron 3	0,4619	gender2 --> hidden neuron 1	1,4118
34	Week_date --> hidden neuron 4	-13,6799	Week_date --> hidden neuron 4	-0,2642	gender2 --> hidden neuron 2	-0,0290
35	Week_date --> hidden neuron 5	2,8949	Week_date --> hidden neuron 5	0,0382	gender2 --> hidden neuron 3	0,0212
36	input bias --> hidden neuron 1	-20,0664	input bias --> hidden neuron 1	11,1143	gender2 --> hidden neuron 4	-0,1386
37	input bias --> hidden neuron 2	3,6992	input bias --> hidden neuron 2	1,9725	gender2 --> hidden neuron 5	-63,7537
38	input bias --> hidden neuron 3	24,3658	input bias --> hidden neuron 3	9,0650	gender2 --> hidden neuron 6	1,1164
39	input bias --> hidden neuron 4	-8,9063	input bias --> hidden neuron 4	0,2392	gender2 --> hidden neuron 7	3,2812
40	input bias --> hidden neuron 5	-9,8802	input bias --> hidden neuron 5	-7,2556	gender2 --> hidden neuron 8	0,3897
41	hidden neuron 1 --> is_fraud	0,1254	hidden neuron 1 --> is_fraud	-0,0001	category2 --> hidden neuron 1	1,7766
42	hidden neuron 2 --> is_fraud	-2,3985	hidden neuron 2 --> is_fraud	0,8470	category2 --> hidden neuron 2	0,1553
43	hidden neuron 3 --> is_fraud	-4,6354	hidden neuron 3 --> is_fraud	-0,3479	category2 --> hidden neuron 3	0,0709
44	hidden neuron 4 --> is_fraud	-3,2223	hidden neuron 4 --> is_fraud	-2,9155	category2 --> hidden neuron 4	29,7004
45	hidden neuron 5 --> is_fraud	-3,4289	hidden neuron 5 --> is_fraud	-2,0401	category2 --> hidden neuron 5	-0,8916
46	hidden bias --> is_fraud	-4,5542	hidden bias --> is_fraud	0,8388	category2 --> hidden neuron 6	-3,0733
47					category2 --> hidden neuron 7	13,3611
48					category2 --> hidden neuron 8	-0,5454
49					Week_date --> hidden neuron 1	-0,1202
50					Week_date --> hidden neuron 2	0,0484
51					Week_date --> hidden neuron 3	85,4013
52					Week_date --> hidden neuron 4	-0,2817
53					Week_date --> hidden neuron 5	0,0848
54					Week_date --> hidden neuron 6	-0,0995
55					Week_date --> hidden neuron 7	-2,8315

Рисунок В.1 – Фрагмент нейронних мереж з архітектурою MLP 7-5-1 (загальна кількість шарів 7, кількість прихованих шарів 5), MLP 7-8-1 (загальна кількість шарів 7, кількість прихованих шарів 8) ризику кібершахрайств

ДОДАТОК Г

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ

Монографії

1. Доценко Т. В., Кушнерьов О. С. Використання гравітаційного моделювання при оцінюванні ризику використання банків з метою легалізації доходів, отриманих злочинним шляхом. *Теорія та практика забезпечення розвитку кіберпростору України* : монографія / за ред. О .В. Кузьменко, Г. М. Яровенко. Київ: Інтерсервіс, 2020. С. 110-131. (0,4 друк. арк.). *Особистий внесок: в обґрунтуванні необхідності удосконалення методичних підходів до ідентифікації ризику використання фінансових установ в протиправній діяльності (0,2 друк. арк.).*

2. Доценко Т. В., Кушнерьов О. С. Моделювання інтегрального індексу загрози національної економіки за допомогою метода Кернела. *Теорія та практика забезпечення розвитку кіберпростору України:* монографія / за ред. О .В. Кузьменко, Г. М. Яровенко. Київ: Інтерсервіс, 2020. С. 157-172. (0,3 друк. арк.). *Особистий внесок: у визначенні індикаторів для оцінювання рівня загроз для стабільного функціонування національної економіки (0,1 друк. арк.).*

Публікації в наукових фахових виданнях України

3. Золковер А. О., Кузьменко О. В., Кушнерьов О. С., Койбічук В. В. Бібліометричний аналіз досліджень кіберзлочинності в умовах цифровізації фінансового сектору економіки держави. *Вісник Хмельницького національного університету*. 2019. № 6, Том 2. С. 253-259. DOI: https://doi.org/10.31891/2307-5740-2019-276-6(2)-253-259 (0,4 друк. арк.). *Особистий внесок: у проведенні бібліометричного аналізу наукових публікацій, присвячених дослідженню кіберзлочинності в умовах цифровізації економіи (0,2 друк. арк.).*

4. Бойко А. О., Миненко С. В., Кушнерьов О. С., Хмелик О.С. Створення управлінських інформаційних систем виявлення фінансових операцій, що підлягають під ознаки внутрішнього фінансового моніторингу. *Вісник Сумського державного університету. Серія Економіка*. 2017. № 4. С. 58-66. DOI: https://doi.org/10.21272/1817-9215.2017.4-08 (0,38 друк. арк.). *Особистий внесок: у розробці алгоритму для виявлення фінансових транзакцій, що підпадають під ознаки внутрішнього фінансового моніторингу (0,2 друк. арк.).*

5. Боженко В.В., Кушнерьов О.С., Кільдей А.Д. Детермінанти поширення кіберзлочинності у сфері фінансових послуг. *Економічний форум.* 2021. № 4. С. 116-121. DOI: https://doi.org/10.36910/6775-2308-8559-2021-4-16 (0,6 друк. арк.). *Особистий внесок: у визначенні причин стрімкого поширення кібершахрайств у та особливостей їх здійснення (0,4 друк. арк.).*

6. Кузьменко О. В., Доценко Т. В., Кушнерьов О. С. Удосконалення системи фінансового моніторингу: автоматизація процесу верифікації клієнтів банку. *Науковий погляд: економіка та управління*. 2021. № 2. С. 88-95. DOI: https://doi.org/10.32836/2521-666X/2021-72-13 (0,8 друк. арк.). *Особистий внесок: у обґрунтуванні доцільності запровадження автоматизації процесів*

ідентифікації та верифікації клієнтів при проведенні внутрішнього фінансового моніторингу (0,3 друк. арк.).

7. Лєонов С. В., Кузьменко О. В., Койбічук В. В., Кушнерьов О. С. Розроблення моделі бізнес-процесу автоматизованого моніторингу фінансових операцій банком для протидії легалізації кримінальних доходів. *Вісник Сумського державного університету. Серія Економіка.* 2021. № 1. С. 9−16. DOI: https://doi.org/10.21272/1817-9215.2021.1-1 (0,4 друк. арк.). *Особистий внесок: у розробці моделі бізнес-процесу автоматизованої системи внутрішнього моніторингу економічних агентів (0,1 друк. арк.).*

8. Лєонов С. В., Кузьмено О. В., Кушнерьов О. С., Люльов О. В., Квілінський О. С. Теоретичні основи формування інформаційної бази дослідження ризику використання фінансових установ України з метою легалізації кримінальних доходів. *Вісник Сумського державного університету. Серія Економіка.*. 2020. С. 104-113. DOI: https://doi.org/10.21272/1817-9215.2020.3-11 (0,42 друк. арк.). *Особистий внесок: у визначенні індикаторів, які характеризують участь фінансових установ в нелегальних фінансових операціях (0,1 друк. арк.).*

9. Кузьменко О. В., Доценко Т. В., Кушнерьов О. С. Оцінювання ризику використання банків з метою легалізації кримінальних доходів на основі гравітаційного моделювання. *Проблеми і перспективи економіки та управління*. 2020. № 1 (21). С. 205-219. DOI: https://doi.org/10.25140/2411-5215-2020-1(21)-205-219 (0,72 друк. арк.). *Особистий внесок: у систематизації існуючих підходів у науковій літературі до оцінювання ризику шахрайств (0,4 друк. арк.).*

10. Кушнерьов О. С. Тенденції шахрайських операцій на банківському ринку та можливості протидії. *Інноваційна економіка*. 2019. № 3-4. С. 180–188 (0,6 друк. арк.).

Публікації в зарубіжних виданнях

11. Kuzmenko O.V., Kubálek J., Bozhenko V.V., Kushneryov O.S., Vida I. An approach to managing innovation to protect financial sector against cybercrime Podejście do zarządzania innowacjami w celu ochrony sektora finansowego przed cyberprzestępczością. *Polish Journal of Management Studies*. 2021.№ 24. С. 276-291. DOI: https://doi.org/10.17512/pjms.2021.24.2.17 (1,0 друк. арк.). *Особистий внесок: у розробці науково-методичного підходу до визначення детермінаниів поширення кіберзагроз (0,7 друк. арк.).*

12. Kuzmenko O., Krukhmal O., Koibichuk V., Hrytsenko K., Kushneryov O., Hordiienko V., Pasemko G., Taran O., Smihunova O. Survival Analysis Methods for Assessing the Anti-Money Laundering System Effectiveness. *WSEAS Transactions on Business and Economics*. 2023. 20. P. 1185–1206. DOI: https://doi.org/10.37394/23207.2023.20.106 (1,5 друк. арк.). *Особистий внесок: в обґрунтуванні концепції оцінювання ефективності системи протидії легалізації кримінальних доходів (0,8 друк. арк.).*

Тези доповідей на наукових конференціях

13. Доценко Т. В., Миненко С. В., Кушнерьов О. С. Сплайн-моделювання взаємозалежності кібершахрайств, фінансових правопорушень та легалізації кримінальних доходів України // Менеджмент, аудит та фінанси: стан, проблеми та перспективи розвитку : збірник тез наукових робіт учасників Міжнародної науково-практичної конференції для студентів, аспірантів та молодих учених, м. Київ, 24 квітня 2021 р. Київ: Аналітичний центр «Нова Економіка», 2021. С. 80-85. (0,2 друк. арк.). *Особистий внесок: в обґрунтуванні та аналізі індикаторів, що характеризують кібершахрайства (0,1 друк. арк.).*

14. Кушнерьов О. С., Радько В. В. Організаційні аспекти кібербезпеки платіжних систем у електронній комерційній діяльності. *Priority directions of science and technology development*: збірник тез доповідей V Міжнародної науково-практичної конференції (24-26 січня 2021 р.). С. 1476–1480. (0,14 друк. арк.). *Особистий внесок: у визначенні основних принципів забезпечення захисту інформації в електронних платіжних системах (0,07 друк. арк.).*

15. Лєонов С. В., Васильєва Т. А., Кузьменко О. В. Кушнерьов О. С., Скринька Л. О. Проблеми формування інформаційної бази оцінювання ризику легалізації кримінальних доходів в сучасних умовах розвитку фінансової системи України. *Проблеми та перспективи розвитку фінансово-кредитної системи України: збірник тез доповідей V Всеукраїнської науково-практичної on-line конференції*. Суми: Сумський державний університет, 2020. С. 260-265. (0,30 друк. арк.). *Особистий внесок: у визначенні особливостей формування інформаційної бази для оцінювання ризику фінансових шахрайств (0,05 друк. арк.).*

16. Кушнерьов О. С., Яценко В. В. Аналіз тенденцій проведення шахрайських операцій з транзакціями на банківському ринку України. *Проблеми та перспективи розвитку фінансово-кредитної системи України: збірник тез доповідей V Всеукраїнської науково-практичної on-line конференції*. Суми: Сумський державний університет, 2019. С. 156-160. (0,3 друк. арк.). *Особистий внесок: у дослідженні поточних тенденцій шахрайства у банківській сфері (0,15 друк. арк.).*

ДОДАТОК Д

Акти про впровадження

ЗАТВЕРДЖУЮ
проректор з науково-педагогічної роботи
_____ Інна ШКОЛЬНИК
"12" вересня 2022 р.

АКТ
впровадження (використання) результатів дисертаційної роботи у навчальний процес

Дисертаційна робота Кушнерьова Олександра Сергійовича на тему «Детермінанти поширення та локалізації кіберзагроз в умовах цифровізації національної економіки»

яка виконана в період з 01 жовтня 2018 р. по 30 вересня 2022 р.

удосконалено науково-методичне підгрунтя для рейтингування країн за рівнем участі резидентів країни у здійсненні фінансових та кібернетичних шахрайств шляхом поєднанням кластерного аналізу за допомогою ітеративного дивізівного методу k-середніх та побудови дерев класифікації з використанням методу одномірного розгалуження CART.

Здобувач наукового ступеня Кушнерьов Олександр Сергійович

Комісія в складі:

Голова комісії: голова ради з якості інституту/факультету ____доцент_ Олексій ЗАХАРКІН

Члени комісії: гарант освітньої програми _____доцент_____ Ольга КУЗЬМЕНКО

_завідувачка кафедри ЕК___ Віталія КОЙБІЧУК

_____асистент_____ Сергій МИНЕНКО

Встановила, що результати науково-дослідної роботи використовуються в навчальному процесі за освітньою програмою "Економічна кібернетика та бізнес аналітика" освітнього ступеня бакалавр спеціальності 051 Економіка шляхом реалізації наступного: оновлення лекційного матеріалу до теми 8 «Методи дискримінантного та кластерного аналізу даних» з дисципліни «Програмне забезпечення математичного та статистичного аналізу», а також оновлення лекційного матеріалу до теми 9 «Класифікаційний аналіз без навчання» з дисципліни «Прикладна статистика».

"12" вересня 2022 р.

Голова комісії: _____ Олексій ЗАХАРКІН

Члени комісії: _____ Ольга КУЗЬМЕНКО

_____ Віталія КОЙБІЧУК

_____ Сергій МИНЕНКО

Міністерство освіти і науки України
Сумський державний університет

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
Сумського державного університету
_____Анатолій ЧОРНОУС
«13» вересня 2022 р.

АКТ

про впровадження у наукову діяльність результатів дисертаційної роботи
Кушнерьова Олександра Сергійовича
«Детермінанти поширення та локалізації кіберзагроз в умовах цифровізації національної економіки»
на здобуття ступеня доктора філософії
за спеціальністю 051 «Економіка»

Комісія у складі:

Голова – Доцент кафедри економічної кібернетики Навчально-наукового інституту бізнесу, економіки та менеджменту Сумського державного університету, д.е.н., професор, Бойко Антон Олександрович;

Члени комісії:

Завідувачка кафедри економічної кібернетики Навчально-наукового інституту бізнесу, економіки та менеджменту Сумського державного університету, к.е.н., доцент, Койбічук Віталія Василівна

доцент кафедри економічної кібернетики Навчально-наукового інституту бізнесу, економіки та менеджменту Сумського державного університету, к.е.н., доцент Боженко Вікторія Володимирівна;

асистент кафедри економічної кібернетики Навчально-наукового інституту бізнесу, економіки та менеджменту Сумського державного університету, Миненко Сергій Володимирович;

Комісія склала цей акт з приводу розгляду результатів дисертаційної роботи Кушнерьова Олександра Сергійовича «Детермінанти поширення та локалізації кіберзагроз в умовах цифровізації національної економіки».

Висновок: комісія вважає, що результати проведеного Кушнерьовим Олександром Сергійовичем дослідження на тему «Детермінанти поширення та локалізації кіберзагроз в умовах цифровізації національної економіки» отримані на основі ґрунтовного аналізу та вивчення наукового доробку та положень нормативно-правових актів й рекомендацій міжнародних організацій, що визначають основні засади протидії поширення кіберзагроз в національній економіці. Вони мають ґрунтовний та аргументований характер і використовувалися при проведенні наукових досліджень у рамках науково-дослідних робіт «Data-Mining для протидії кібершахрайствам та легалізації кримінальних доходів в умовах цифровізації фінансового сектору економіки України» (номер д/р 0121U100467) та «Моделювання механізмів детінізації та декорумпізації економіки для забезпечення національної безпеки: вплив трансформації фінансових поведінкових патернів» (номер д/р 0122U000783), які виконуються в Навчально-науковому інституту бізнесу, економіки та менеджменту Сумського державного університету.

Голова комісії — Антон БОЙКО

Члени комісії — Віталія КОЙБІЧУК

Вікторія БОЖЕНКО

Сергій МИНЕНКО