УДК 336.71.078.3 JEL Classification G21, L86

ВПЛИВ КІБЕРШАХРАЙСТВ НА ФІНАНСОВУ СИСТЕМУ НА ПРИКЛАДІ КРАЇН ЄВРОСОЮЗУ[1]

Боженко В. В.,
кандидат економічних наук,доцент, Сумський державний університет,
e-mail: v.bozhenko@uabs.sumdu.edu.ua
https://orcid.org/ 0000-0002-9435-0065
Койбічук В. В.,
кандидат економічних наук, доцент,
Сумський державний університет
e-mail: v.koibichuk@uabs.sumdu.edu.ua
http://orcid.org/ 0000-0002-3540-7922
Габенко М.М.,
студентка,
Сумський державний університет
e-mail: ek81.m_habenko@uabs.sumdu.edu.ua

Експоненційне зростання кількості кібершахрайств у фінансовій сфері та їх інтелектуалізація призводить до масштабних негативних наслідків як фінансового (втрата коштів фінансовими установами та їх клієнтами, банкрутство фінансових установ, недоотримання податкових надходжень до бюджету), так і суспільного характеру (крадіжка персональних даних споживачів фінансових послуг, зниження рівня ділової репутації фінансових установ, втрати довіри населення до фінансового сектору). Кібербезпека посідає перше місце у списку пріоритетів Європейської Комісії: довіра та безпека є основою Стратегії єдиного цифрового ринку, тоді як боротьба з кіберзлочинністю є одним із трьох основних напрямків Європейської програми безпеки. У дослідженні використано методи систематизації, порівняння, структурного аналізу, логічного узагальнення, бібліометричного аналізу (за допомогою VOSviewer 1.6.15) та методи вертикального, горизонтального та трендового аналізу набору даних для оцінки динаміки та тенденцій кіберзлочинності в фінансовій системи крахн Європейського Союзу. Для визначення найбільш релевантних публікацій з цього питання автори провели бібліометричний аналіз наукових робіт, проіндексованих базою даних Scopus з 2015 по 2021 рік. За результатами дослідження встановлено необхідність виокремлення 6 кластерів за результатами наукових досліджень, автори з яких представлені з 34 країн. У статті проаналізовано динаміку та тенденції кіберзлочинності у фінансовому секторі Європейського Союзу. У статті проаналізовано заходи з кібербезпеки, які здійснюються органами державної безпеки, служб фінансового моніторингу, Генерального директорату з інформатики. Авторами статті доведено, що розвиток цифрових технологій призводить до збільшення масштабів кіберзагроз, які вимагають оперативного та своєчасного виявлення, оцінки та розробки відповідних заходів для їх запобігання або мінімізації можливих наслідків. Практична цінність дослідження полягає у використанні напрацювань органами державного регулювання, нагляду та контролю при розробці системи протидії інформаційним ризикам, що загрожують суспільним інтересам.

Ключові слова: *фінансові установи, банки, ризик кібершахрайства, кіберзагроза, кібербезпека.*
DOI: 10.21272/1817-9215.2021.2-6

ВСТУП

З початком пандемії COVID-19, яка призвела до переходу в онлайн-формати та використання цифрових послуг, спостерігається значне зростання кількості кібератак на державні установи, приватні компанії, а також окремих осіб. У 2020 році збитки від кіберзлочинів для світової економіки оцінюється в 5,5 трлн євро, що вдвічі більше порівняно з 2015 роком. При цьому у 2020 році чверть всіх кібератак у світі припадає на учасників ринку фінансових послуг.

Стрімке впровадження інноваційних інформаційних технологій на різних рівня фінансової системи з одного боку сприяють підвищенню конкурентоспроможності країни на світовій арені, а також її інвестиційної привабливості, а з іншого – викликають зростання масштабів транскордонної економічної злочинності, збільшення та розповсюдження різноманітних схем кіберзлочинності, збільшення

[1] *Роботу виконано в межах науково-дослідної теми «Data-Mining для протидії кібершахрайствам та легалізації кримінальних доходів в умовах цифровізації фінансового сектору економіки України» (номер державної реєстрації 0121U100467).*

кількості обсягів нелегально отриманих доходів, що супроводжується вдосконаленням механізмів відмивання кримінальних коштів. З урахуванням посилення геополітичної конкуренції в кіберпросторі та посилення ландшафту кіберзагроз, особливо в умовах пандемії covid-19, питання захисту інформації від кібератак як на рівні фінансової установи, так і держави є постійно актуальною задачею сьогодення та прийдешнього п'ятиліття.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Питання кіберзлочинності та захист майнових та моральних інтересів суб'єктів господарювання років, актуалізувалося протягом останнього десятиліття. Проте кількість публікацій за останні 5 років значно зросла, що підтверджує актуальність зазначеної проблематики та мети дослідження. Бібліометричний аналіз 77 публікацій, що індексуються базою даних Scopus за період з 2015 по квітень 2021 року стосовно кіберзагроз, кіберризиків, інструментів боротьби з кіберзлочинністю у фінансових системах світу, дозволив сформувати 6 кластерів за логікою співіснування в публікаціях 3 та більше ключових слів відповідно до теми дослідження. Кластери сформовано за результатами наукових досліджень авторів з 34 країн світу(10 з них – країни-члени Євросоюзу: Велика Британія, Франція, Італія, Греція, Болгарія, Німеччина, Австрія, Швеція, Бельгія, Мальта), які розглядали співіснування та кореляцію понять кіберзагрози, кіберризики, їх змістовне формування, сфери застосування, інструменти, методи, підходи до протидії кіберзагрозам у фінансових системах (рис. 1). Кількість взаємозв'язків між поняттями складає 456 одиниць.

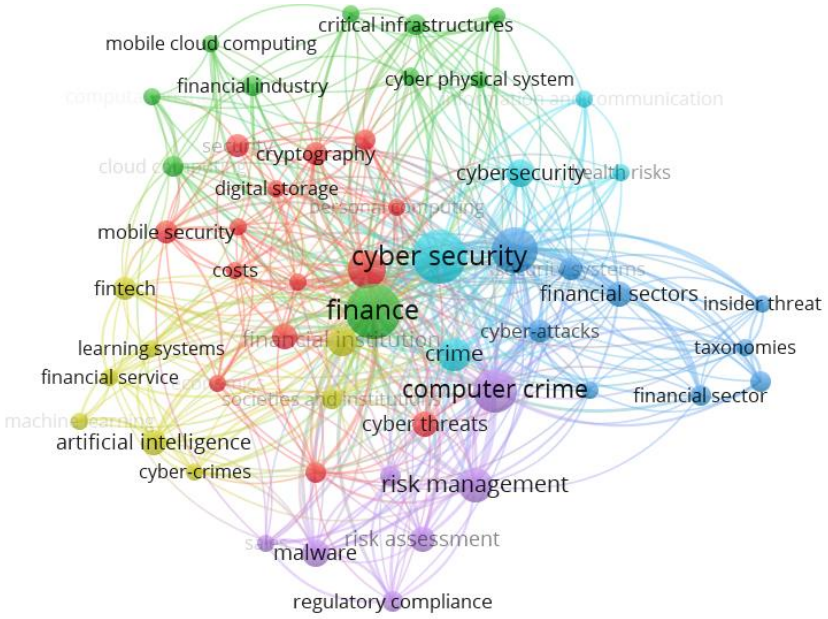

Рисунок 1 – Бібліометричний аналіз наукових публікацій щодо тематики кіберзагроз у фінансовій сфері (побудовано авторами на основі бази даних Scopus та інструментарію програми VOSviewer 1.6.15)

За результатами прогнозу аналітично-консалтингової компанії Juniper Research, що спеціалізується на дослідженні тенденцій розвитку ринку цифрових технологій, втрати бізнес-компаній від кібератак будуть перевищувати 5 млрд $ у 2024 році [1]. Посилення заходів кібербезпеки для фінансових соціально-економічних об'єктів Євросоюзу детально прописується в межах стратегічного плану 2020 – 2024 Генерального директорату з інформатики (DIGIT), який відіграє координаційну роль у розвитку інформаційних технологій та систем інформаційно-комінікаційних

технологій [2]. Основною метою є формування безпечного та сучасного цифрового середовища, здатного забезпечити надійну, економічно вигідну та безпечну інфраструктуру та послуги, в ногу з новими методами роботи та спільної роботи, що узгоджуються із очікуваннями персоналу, громадян, бізнесу та зацікавлених сторін.

ПОСТАНОВКА ЗАВДАННЯ

Метою даного дослідження є проаналізувати впливу кібершахрайств на фінансові системи країн Європейського Союзу.

МЕТОДИ ДОСЛІДЖЕННЯ

У процесі дослідження використовувались методи систематизації, порівняння, структурного аналізу, логічного узагальнення, бібліометричного аналізу (з використанням VOSviewer 1.6.15) та методи вертикального, горизонтального, фінансово-трендового аналізу масиву даних для оцінки динаміки та тенденцій розвитку кіберзлочинів у фінансовій системі країн Європейського Союзу.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Нинішня нестабільна ситуація в соціально-економічній та політичній сферах формує сприятливе підґрунтя для поширення різного роду шахрайських схем на теренах цифрової мережі. Лише в офіційній статистичній звітності європейських фірм зазначається, що кількість кібератак у 2020 році в Бельгії складали 49%, в Іспанії – 44%, у Німеччині – 41%, у Новій Зеландії – 37%, у Франції – 34%, у Великій Британії – 30% [3]. Звісно, не всі фінансові установи (банки, фірми, корпорації) бажають розкривати наявність шахрайств, щоб не псувати свою репутацію та імідж. Європейський фонд фінансової стабільності акцентує на необхідності затвердження нових стандартів та наглядових ініціатив щодо кібербезпеки фінансових послуг. Три основні сфери щодо кіберзахисту, на які в першу чергу необхідно звернути увагу: ідентифікація кіберризику, управлінні кіберризиками, стійкість до кіберризиків.

У 2020 році ЄС оголосив про запуск Стратегії кібербезпеки ЄС як ключової складової формування цифрового майбутнього Європи та Плану відновлення Європи, сприяння глобальному та відкритому кіберпростору шляхом посилення співпраці. Європейська Комісія інвестувала понад 63,5 млн. євро в чотири пілотні проекти (CONCORDIA, ECHO, SPARTA, CyberSec4Europe), що виступають основою для створення європейської мережі центрів експертизи з кібербезпеки, спрямованих на удосконалення системи протидії кіберзлочинам у різних сферах суспільного життя.

Органи безпеки все більше зосереджують свою увагу на здатності фінансових соціально-економічних об’єктів (банків, фінансових установ, фірм, організацій, підприємств) об’єктивно оцінювати свою схильність до кібернетичного ризику. Наприклад, виклики, з якими стикаються банки з точки зору узгодженості своєї системи внутрішнього контролю, мають велике значення, особливо з урахуванням зростаючої уваги на внутрішній кіберконтроль між різними підрозділами. Правила звітування про порушення, відповідно до Загального регламенту захисту даних, додають додатковий стимул для банків для посилення їх здатності швидко виявляти кібератаки та порушення даних. Вчасна та зрозуміла управлінська інформація щодо порушень може прискорити пошук вирішення проблеми та завчасно випередити кіберзагрозу [4].

У більшості юрисдикцій здійснюється сильний тиск з боку наглядових органів, щоб уникнути перетворення кіберзагрози на «IT-проблему» та застосувати цілісний підхід щодо мінімізації та реагування на прояви кіберризиків. Однак, залишається невирішеним питання кінцевої відповідальності, кому вона має належати. Деякі фінансові установи дотримуються підходу, який передбачає призначення невиконавчого директора з питань кібербезпеки, який несе відповідальність за безпеку [4].

Стійкість до кіберризиків зумовлена пошуком сучасного та потужного інструментарію для тестування потенційних кіберзагроз окремими фінансовими установами. Наприклад, у Великій Британії в рамках загальногалузевої ініціативи, була запроваджена програма SIMEX 16, що імітувала відключення британських платежів із валовим розрахунком у режимі реального часу. Адже Велика Британія, де сплата побутових послуг (47,6%) та фінансових послуг (27,3%) здійснюється за допомогою мобільного банкінгу, є дуже привабливою площадкою для кібератак [5]. Однак, незважаючи на великі витрати щодо забезпечення кібербезпеки та займаючи високі позиції щодо готовності до кібератак, Банк Англії при моделюванні великої кібератаки проти британської фінансової системи виявився не готовим протистояти їй. Таким чином, тест виявив деякі тривожні результати: найбільша кількість фінансових інститутів не готова до великомасштабної онлайн-атаки на основі ідентифікаційної інформації (identity-based attacks). Навіть невеликі атаки призвели до серйозних порушень безпеки і падіння основних бізнес-процесів [5].

Європейський центральний банк досяг значного прогресу у формуванні свого розуміння та спроможності втручатися у кіберзабезпечення. З моменту створення системи управління корпоративним контентом (ECM) у 2014 році, органи влади застосовували найкращі практики в галузі нагляду за IT-ризиками шляхом взаємодії з національними наглядовими органами та старшими спеціалістами з IT-ризиків у банках. Протягом останніх років європейський центральний банк акумулював інформацію, щоб визначити основні патерни здійснення кібератак як на рівні окремої фінансової установи, так і на системному рівні. Дана інформація була використана для розроблення інструментів боротьби з кібершахрайствами. Поза банківським наглядом ЄЦБ переслідує ініціативи щодо кращого розуміння кіберврaзливостей, притаманних фінансовій системі, розробив кіберстратегію, засновану на трьох опорах: кіберготовність фінансової установи, стійкість сектору та залучення стратегічних регуляторів-галузей.

У 2011 р. у Німеччині були прийнято «Стратегію кібербезпеки Німеччини», відповідно до якої Федеральний уряд застосував заходи на основі вже створених структур до відповідних рівнів загроз за такими стратегічними цілям: 1) створення IT-система безпеки; 2) захист інфраструктури потребує більшої надійності IT-систем громадян, а також малих та середніх підприємств; 3) посилення IT-безпеки в публічному управлінні; 4) оптимізація оперативної співпраці всіх державних установ і покращення координації заходів щодо захисту проти IT-випадків було створено Національний центр кіберзахисту; 5) створення Національної ради кібербезпеки, діяльність якої спрямована на виявлення і усунення конструктивних причин криз – важливий превентивний інструмент у кібербезпеці; 6) ефективна боротьба зі злочинністю у кіберпросторі – посилюються можливості правоохоронних органів, Федеральної служби безпеки у сфері IT та економіки в контексті подолання кіберзлочинності; 7) ефективна співпраця у кібербезпеці в Європі та світі. Безпека в глобальному кіберпросторі досягається лише за допомогою сукупності узгоджених засобів та методів на національному і міжнародному рівнях; 8) використання надійних і достовірних інформаційних технологій. Всі ці заходи підтверджують високий ступінь рівня підготовки Німеччині до питання кібербезпеки та якість зусиль боротьби з найновішими технологіями кіберзагроз.

Не можливо не враховувати в умовах сьогодення ризик впливу пандемії COVID-19 на цифрову безпеку. Кіберзлочинці використовують епідемію, щоб зробити свої атаки більш успішними. З лютого 2020 року спостерігається зростання фішингових атак, що використовують вміст COVID-19, включаючи: електронні листи з темою коронавірусу в полі теми; листи, які нібито надіслані від імен лідерів чи установ, таких як Всесвітня організації охорони здоров'я; посилання або веб-додатки, що імітують законні ініціативи. Наприклад, італійські фінансові установи зафіксували зростання кількості фішингових атак у березні 2020 року до 75% (у березні 2019 року ця кількість складала 25%). Одна фішинг-кампанія на тему COVID-19 охопила понад 10% усіх

організацій у країні, що електронною поштою залучає одержувачів до відкриття шкідливого вкладення. У Німеччині з березня 2019 р. по березень 2020 р. фішингові атаки зросли з 21% до 25% [6].

У 2020 році ЄС оголосив про запуск Стратегії кібербезпеки ЄС, як ключового компонента «Формування цифрового майбутнього Європи» та «Плану відновлення Європи», сприяння розвитку глобального та відкритого кіберпростору шляхом посилення співпраці та виділив загалом 64 мільйони євро на фінансування проектів, спрямованих на кращий захист від кібератак.

ВИСНОВКИ

Сучасні фінансові інститути, які пропонують банківські продукти на основі діджитал та мобільних послуг, стикаються дедалі з більшим тиском шкідливих програм, фішингу і шахрайських дій. Глобальна пандемія COVID-19 сприяла пришвидшенню переходу до онлайн-формату великої кількості бізнес-процесів, фінансових послуг та операцій з використанням цифрових послуг. Водночас спостерігається значне збільшення кібератак на державні установи, приватні компанії та приватні особи.

Кібербезпека займає перше місце в списку пріоритетів Європейської Комісії: довіра та безпека є основними в стратегії цифрового єдиного ринку, тоді як боротьба з кіберзлочинністю є одним із трьох стовпів Європейської програми безпеки.

Крім того, результати проведено дослідження дозволяють узагальнити, що для ефективної протидії кіберзагрозам країнам необхідно активно розвивати власні сектори безпеки, кібербезпеки відповідно до викликів сучасності, особливо зважаючи на потенціал використання мережі Інтернет у фінансових цілях, використовувати передові технології ЄС для запобігання, стримування та швидкого реагування на кібератаки та посилення співпраці з іншими країнами для формування глобального безпечного кіберпростору.

SUMMARY

V. Bozhenko, V. Koibichuk, M. Gabenko. **The impact of cyber threats on the financial system on the example of EU countries**

Exponential growth in the number of cyber frauds in the financial sector and their intellectualization leads to large-scale negative consequences of both financial (loss of funds by financial institutions and their customers, the bankruptcy of financial institutions, lack of tax revenues) and public (theft of personal data of consumers of financial services, reduction the level of business reputation of financial institutions, loss of public confidence in the security and reliability of financial transactions). The study used methods of systematization, comparison, structural analysis, logical generalization, bibliometric analysis (using VOSviewer 1.6.15) and methods of vertical, horizontal, financial, and trend analysis of the data set to assess the dynamics and trends of cybercrime in the financial system of the European Union. To determine the most relevant publications on this issue, the authors conducted a bibliometric analysis of scientific papers indexed by the Scopus database from 2015 to 2021. According to the study results, the expediency of separating 6 clusters by the results of scientific research, the authors of which are represented from 34 countries. The article analyzes the dynamics and trends of cybercrime in the financial sector of the European Union. Cybersecurity measures are summarized in terms of state security agencies, financial monitoring services, the Directorate General of Informatics. Cybersecurity features high on the list of the priorities of the European Commission: trust and security are at the core of the Digital Single Market Strategy, while the fight against cybercrime is one of the three pillars of the European Agenda on Security. The authors of the article emphasize that the development of digital technologies leads to an increase in the scale of cyber threats, which require prompt and timely detection, assessment, and development of appropriate measures to prevent them or minimize the possible consequences. The practical value of the study lies in the use of state regulation, supervision, and control in the development of a system of counteraction to information risks that threaten the public interest.

Keywords: *financial institutions, banks, cyber fraud risk, cyber threat, cybersecurity*

СПИСОК ЛІТЕРАТУРИ

1. Business Losses to Cybercrime Data Breaches to Exceed $5 Trillion by 2024. URL: https://www.securitymagazine.com/articles/90806-business-losses-to-cybercrime-data-breaches-to-exceed-5-trillion-by-2024
2. Strategic plan 2020-2024 – Informatics. URL: https://ec.europa.eu/info/publications/strategic-plans-2020-2024-informatics_en

3. Share of European firms reporting a cyber attack 2020, by country: Statista. URL : https://www.statista.com/statistics/1006664/european-firms-cyberattack-target-reporting/
4. Deloitte. Centre for regulatory strategy EMEA : Cyber risk and regulation in Europe A new paradigm for banks. URL: https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu_deloitte-cyber-risk-regulation-europe.pdf
5. Клочко А. М., Єременко А. О. Шахрайство з використанням банківських платіжних карток. *Юридичний науковий електронний журнал*. 2016. № 1. С.85–92. URL: http://www.lsej.org.ua/1_2016/24.pdf
6. OECD Policy Responses to Coronavirus (COVID-19). Dealing with digital security risk during the Coronavirus (COVID-19) crisis. Version 3 April 2020. URL: https://www.oecd.org/coronavirus/policy-responses/dealing-with-digital-security-risk-during-the-coronavirus-covid-19-crisis-c9d3fe8e/

REFERENCES

1. Business Losses to Cybercrime Data Breaches to Exceed $5 Trillion by 2024. Available at https://www.securitymagazine.com/articles/90806-business-losses-to-cybercrime-data-breaches-to-exceed-5-trillion-by-2024
2. Strategic plan 2020-2024 – Informatics. Available at https://ec.europa.eu/info/publications/strategic-plans-2020-2024-informatics_en
3. Share of European firms reporting a cyber attack 2020, by country: Statista. Available at https://www.statista.com/statistics/1006664/european-firms-cyberattack-target-reporting/
4. Deloitte. Centre for regulatory strategy EMEA : Cyber risk and regulation in Europe A new paradigm for banks. Available at https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu_deloitte-cyber-risk-regulation-europe.pdf
5. Клочко А. М., Єременко А. О. (2016). Шахрайство з використанням банківських платіжних карток. *Юридичний науковий електронний журнал*. № 1. С.85–92. Available at http://www.lsej.org.ua/1_2016/24.pdf
6. OECD Policy Responses to Coronavirus (COVID-19). Dealing with digital security risk during the Coronavirus (COVID-19) crisis. Version 3 April 2020. Available at https://www.oecd.org/coronavirus/policy-responses/dealing-with-digital-security-risk-during-the-coronavirus-covid-19-crisis-c9d3fe8e/