ГРОШІ, ФІНАНСИ І КРЕДИТ

УДК 336.71.078.3

Боженко В.В., к.е.н., доцент
Bozhenko V., PhD, Associate Professor
https://orcid.org/0000-0002-9435-0065
Кушнерьов О.С., аспірант
Kushneryov O., PhD student
https://orcid.org/0000-0001-8253-5698
Кільдей А.Д., студентка
Kildei A., student

ДЕТЕРМІНАНТИ ПОШИРЕННЯ КІБЕРЗЛОЧИННОСТІ У СФЕРІ ФІНАНСОВИХ ПОСЛУГ

Сумський державний університет

З початком світової пандемії, яка спровокувала інтенсивну цифрову трансформацію бізнесу, спостерігається значне збільшення кількості кібератак на державні установи, приватні компанії, а також окремих осіб. Мета статті полягає у визначенні причин стрімкого поширення кібершахрайств у фінансовому секторі економіки та особливостей їх здійснення. Систематизація літературних джерел та підходів до дослідження фінансових кібершахрайств засвідчила, що зростання кількості кібератак у сфері фінансових послуг є результатом стрімкого використання інноваційних цифрових технологій у діяльності фінансових установ, появою фінтех компаній, а також збільшенням попиту на цифрові фінансові продукти із-за пандемії COVID-19. Визначено основних ініціаторів кібератак та особливостей здійснення їх протиправних діянь у фінансовому секторі. У результаті дослідження встановлено, що найбільш поширеними формами здійснення кібератак у фінансовому секторі є програма–вимагач, атака ланцюга поставок, прихований майнінг, а також програмне забезпечення для відволікання уваги служб безпеки фінансових установ від справжнього епіцентру кібератаки. У роботі проаналізовано найбільші світові кіберзлочинні угруповання, які здійснюють атаки на фінансові установи. Обґрунтовано, що для побудови ефективної системи 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. Перспективами подальших досліджень у даному напрямі є побудова економіко-математичної моделі для визначення детермінант поширення кібератак на прикладі країн Європейського Союзу.

Ключові слова: кібершахрайства, фінансовий сектор, банки, цифровізація

DETERMINANTS OF SPREADING CYBERTHREATS IN FINANCIAL SECTOR

Sumy State University

With the onset of the global pandemic, which has provoked the digital transformation of business, there has been a significant increase in the number of cyberattacks on government agencies, private companies, and individuals. The purpose of the article is to determine the reasons for the rapid spread of cyber fraud in the financial sector of the economy and the peculiarities of their implementation. Systematization of literature sources and approaches to the study of financial cyber fraud has shown that the growing number of cyber attacks in the field of financial services is the result of rapid use of innovative digital technologies in financial institutions, the emergence of fintech companies and increasing demand for digital financial products due to the COVID-19 pandemic. The main initiators of cyberattacks and features of their illegal actions in the financial sector are identified. The study found that the most common forms of cyberattacks in the financial sector are ransomware, supply chain attacks, cryptojacking, and destractive attack. The paper analyzes the world's largest cybercrime groups that carry out attacks on financial institutions. It is substantiated that in order to build an effective system

to combat cyber threats and ensure the stability of the financial system, it is advisable to take a set of measures aimed at monitoring the information security of financial institutions, combining efforts of national regulators and heads of financial institutions to inform about real and potential competencies in the field of information security by improving the skills of employees of financial institutions and the national regulator. Prospects for further research in this area are to build an economic and mathematical model to determine the determinants of spreading the cyberattacks using data of the European Union countries.

Key words: cyber fraud, financial sector, banks, digitalization

Постановка проблеми у загальному вигляді і її зв'язок з важливими науковими та практичними завданнями. 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 фінансових відносин відкриває як нові можливості для підвищення ефективності фінансових установ 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 фінансового сектору та враховуючи кроссекторальність фінансових відносин виступає загрозою для національної безпеки держави.

Аналіз останніх досліджень, у яких започатковано вирішення проблеми. Проведенням наукових досліджень окремих аспектів щодо аналізу кіберзагроз, їх ступеня поширення та впливу на національну безпеку займаються такі вітчизняні вчені як В.Ліпкан [1], А. Тарасюк [2], Н.Нагайчук [3], Г.М.Яровенко [4] та інші. На сьогодні протидія кіберзагрозам є однією із головних тем для обговорення на міжнародних економічних форумах і конференціях, дана проблематика широко висвітлена у працях зарубіжних вчених. У роботі [5] проведений грунтовний бібліометричний аналіз наукових публікацій, присвячених питання кібербезпеки. Зокрема, виявлено, що протягом 2015-2021 року в наукометричній базі Scopus опубліковано 77 публікацій з даної проблематики, що дозволило виділити 6 тематичних кластерів. Науковцями [6**Error! Reference source not found.**] оцінено вплив потенційних загроз та ризиків, спричинених стрімким зростанням інформаційних технологій, на стабільність функціонування фінансової системи. Проведений регресійний аналіз засвідчив, що за умови підвищення рівня системного ризику в країні відбувається зменшення позитивного ефекту від впровадження цифрових технологій на фінансову стабільність.

Метою статті є визначення причин стрімкого поширення кібершахрайств у фінансовому секторі економіки та особливостей їх здійснення.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Динамічна цифровізація економіки робить банківські та небанківські фінансові установи більш вразливими до кіберзлочинності. 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.

У 2020 році збитки від кіберзлочинів у США оцінюються в 4,2 млн дол США, що вдвічі більше порівняно з 2018 роком (2,7 млн дол США). При цьому впродовж останніх років фінансові послуги були та залишаються основним таргетом для кіберзлочинців. IBM щорічно визначає індекс загроз (X-Force Threat Intelligence Index), який відображає ландшафт кіберзагроз у світі (табл. 1).

Таблиця 1

Рейтинг вразливості сфер діяльності до кіберзлочинів у період з 2018 по 2020 рр.

	2018	2019	2020	Зміна, 2020/2018
Фінансові послуги	1	1	1	-
Виробництво	5	8	2	-3
Енергетика	10	9	3	-7
Роздрібна торгівля	4	2	4	-
Професійні послуги	3	5	5	+2
Адміністративні послуги	7	6	6	-1
Охорона здоров'я	8	10	7	-1
Медіа	6	4	8	+2
Транспорт	2	3	9	+7
Освіта	9	7	10	+1

Джерело: складено авторами на основі даних [8]

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 найбільш вразливими у 2020 році були сфери фінансів, виробництва та енергетики.

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 [7]. З урахуванням зазначених тенденцій, країни ЄС активно вкладають кошти для удосконалення інфраструктури, проведення просвідницьких заходів щодо підвищення рівня цифрової культури серед населення та бізнесу.

Забезпечення безпеки інформаційних технологій фінансових установ та їх баз даних є постійно зростаючим викликом для топ-менеджменту як фінансових 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. З метою протидії кіберзагрозам у фінансовому секторі економіки доцільно проаналізувати найбільш поширені способи здійснення кібератак, інструменти монетизації викрадених даних, а також основних кіберзлочинців та їх мотивів.

Найбільш поширеними формами здійснення кібератак у фінансовому секторі є програма –вимагач (ransomware), атака ланцюга поставок (supply chain attack) прихований майнінг (cryptojacking), а також програми для відволікання уваги служб безпеки від справжнього епіцентру кібератаки (destractive attack) [9].

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 (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) [10].

У переважній більшості випадків кібератаки у фінансовому секторі здійснюються за участю таких суб'єктів як [11]:

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

– злочинці та шахраї, 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 оборони, встановлення геополітичних інтересів, впливу на громадську думку на національному на міжнародному рівнях та інше.

У таблиці 2 представлено найбільші кіберзлочинні угруповання, які атакують фінансові установи в світі.

Таблиця 2

Найбільші кіберзлочинні угруповання, які здійснюють атаки на фінансові установи, у світі [12]

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.
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.

Нині для легалізації доходів, отриманих внаслідок кіберзлочину, в переважній більшості використовується криптовалюта. У 2018 році в Європі за допомогою криптовалют було легалізовано 4 млрд фунтів стерлінгів. Криптовалюта за своєю суттю має низький рівень регулювання і не контролюється центральним органом, і тому фінансові транзакції не можуть бути ретельно відслідковані.

Зростання кількості кібератак у сфері фінансових послуг є результатом стрімкого використання інноваційних цифрових технологій у діяльності фінансових установ, появою фінтех компаній, а також збільшенням попиту на цифрові фінансові продукти із-за пандемії COVID-19. Зокрема, під час пандемії кількість порушень у сфері кібербезпеки серед FinTech компаній в середньому збільшився на 17% [13].

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.

Кіберзлочини 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 [14].

– збільшення кількості пристроїв, підключених до мережі Інтернет;

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

– низький рівень цифрової культури. У 2019 році лише 58% населення в країнах ЄС мають хоча б базові цифрові навички (проти 55% у 2015 році);

– 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% [15];

– використання застарілого та неліцензійного програмного забезпечення;

– збільшення використання Інтернету для оплати товарів/послуг, здійснення фінансових операцій, отримання адміністративної послуги тощо.

Крім вищеперерахованих драйверів зростання кількості кібератак варто виокремити специфічні чинники, які притаманні виключно для сфери фінансових послуг:

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

– 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.

Висновок. 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.

Роботу виконано в межах науково-дослідних тем «Data-Mining для протидії кібершахрайствам та легалізації кримінальних доходів в умовах цифровізації фінансового сектору економіки України» (№ д/р 0121U100467) та «Національна безпека через конвергенцію систем фінансового моніторингу та кібербезпеки: інтелектуальне моделювання механізмів регулювання фінансового ринку» (№ д/р № 0121U10955).

Список бібліографічного опису:

1. Ліпкан В., Діордіца І. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України. *Підприємництво, господарство і право.* 2017. № 5. С. 174-180.
2. Тарасюк А.В. Система суб'єктів забезпечення кібербезпеки в Україні. *Вчені записки ТНУ імені В.І. Вернадського*. Серія: юридичні науки. 2020. № 2. С. 119-124.
3. Нагайчук Н., Третяк Н., Ткаленко О. Страхування в системі управління кібер-ризиками підприємства в умовах цифрової економіки. *Фінансовий простір.* 2019. № 1 (33). С. 97-111.

4. Yarovenko H. Evaluating the threat to national information security. *Problems and Perspectives in Management*. 2020. Vol. 18, Issue 3. P. 195–210.
5. 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.
6. Risman A., Mulyana B., Silvatika B. A., Sulaeman A. S. The effect of digital finance on financial stability. Management Science Letters. 2021. P. 1979–1984. URL: https://doi.org/10.5267/j.msl.2021.3.012
7. Europeans' attitudes towards cyber security. Special Eurobarometer 499. European Commision. 2020. URL: https://europa.eu/eurobarometer/surveys/detail/2249
8. X-Force Threat Intelligence Index 2021. *IBM Security*. URL: https://www.ibm.com/downloads/cas/M1X3B7QG
9. Cyber Threat Landscape for the Finance Sector. *F-Secure*. 2019. URL: https://www.f-secure.com/content/dam/f-secure/en/business/common/collaterals/f-secure-cyber-threat-landscape-finance-sector.pdf
10. Internet Crime Report. *Federal Bureau of Investigation*. URL: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
11. 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
12. The Top Threat Actors Targeting Financial Services Organizations. *Insights*. 2018. URL: https://intsights.com/blog/the-top-threat-actors-targeting-financial-services-organizations
13. 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
14. The Mobile Economy 2020. GSM Association URL: https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/03/GSMA_MobileEconomy2020_Global.pdf
15. Global Social Network Users 2020. – URL: https://www.emarketer.com/content/global-social-network-users-2020.

References:

1.Lipkan V., Diorditsa I. Natsional'na systema kiberbezpeky yak skladova chastyna systemy zabezpechennya natsional'noyi bezpeky Ukrayiny. Pidpryyemnytstvo, hospodarstvo i pravo, 2017, no. 5, pp. 174-180 [in Ukrainian].
2.Tarasyuk A.V. Systema sub"yektiv zabezpechennya kiberbezpeky v Ukrayini. Vcheni zapysky TNU imeni V.I. Vernads'koho. Seriya: yurydychni nauky, 2020, no 2, pp. 119-124 [in Ukrainian].
3.Nahaychuk N., Tretyak N., Tkalenko O. Strakhuvannya v systemi upravlinnya kiber-ryzykamy pidpryyemstva v umovakh tsyfrovoyi ekonomiky. Finansovyy prostir, 2019, no. 1 (33), pp. 97-111[in Ukrainian].
4.Yarovenko H. Evaluating the threat to national information security. Problems and Perspectives in Management, 2020, Vol. 18, Issue 3, pp. 195–210.
5.Bozhenko V.V., Koybichuk V.V., Habenko M.M. Vplyv kibershakhraystv na finansovu systemu na prykladi krayin Yevrosoyuzu. Visnyk SumDU. Seriya Ekonomika, 2021, no. 2, pp. 47-52 [in Ukrainian].
6.Risman A., Mulyana B., Silvatika B. A., Sulaeman A. S. The effect of digital finance on financial stability. Management Science Letters, 2021, pp. 1979–1984. Available at: https://doi.org/10.5267/j.msl.2021.3.012 [in English].
7.Europeans' attitudes towards cyber security. Special Eurobarometer 499. European Commision. 2020. Available at: https://europa.eu/eurobarometer/surveys/detail/2249
8.X-Force Threat Intelligence Index 2021. IBM Security. Available at: https://www.ibm.com/downloads/cas/M1X3B7QG
9.Cyber Threat Landscape for the Finance Sector. F-Secure. 2019. Available at:: https://www.f-secure.com/content/dam/f-secure/en/business/common/collaterals/f-secure-cyber-threat-landscape-finance-sector.pdf
10. Internet Crime Report. Federal Bureau of Investigation. Available at: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
11. Nish A., Naumann S., Muir J. Enduring Cyber Threats and Emerging Challenges to the Financial Sector. Carnegie Endowment for International Peace. 2020. Available at: https://carnegieendowment.org/2020/11/18/enduring-cyber-threats-and-emerging-challenges-to-financial-sector-pub-83239
12. The Top Threat Actors Targeting Financial Services Organizations. Insights. 2018. Available at: https://intsights.com/blog/the-top-threat-actors-targeting-financial-services-organizations
13. The Global Covid-19 FinTech Regulatory Rapid Assessment Report. World Bank Group and the University of Cambridge. Available at: https://www.jbs.cam.ac.uk/wp-content/uploads/2020/10/2020-ccaf-report-fintech-regulatory-rapid-assessment.pdf
14. The Mobile Economy 2020. GSM Association Available at: https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/03/GSMA_MobileEconomy2020_Global.pdf
15. Global Social Network Users 2020. Available at: https://www.emarketer.com/content/global-social-network-users-2020.

DOI: https://doi.org/10.36910/6775-2308-8559-2021-4-16