DOI: https://doi.org/10.32782/2524-0072/2023-50-82

УДК 343.53:[336(477)(047.31)

КІБЕРЗАГРОЗИ ФІНАНСОВОГО СЕКТОРА В УМОВАХ ВІЙНИ

CYBER THREATS OF THE FINANCIAL SECTOR IN THE CONDITIONS OF WAR

Гончаренко Ірина Георгіївна
доктор наук з державного управління, професор,
Черкаський державний технологічний університет
ORCID: https://orcid.org/0000-0002-6056-943X

Honcharenko Iryna
Cherkasy State Technological University

У глобальному секторі кібербезпеки дві основні сфери, які постійно зазнають нападів – фінансова та державна. Триваюча цифрова трансформація фінансового сектору та посилення залежності від хмарних технологій після пандемії спричинили експоненціальне зростання площі атак у цьому секторі, піддаючи організації зростанню кіберзагроз. Атаки включають крадіжку конфіденційних даних клієнтів, шахрайство, фішинг, розповсюдження шкідливих програм, атаки на мережеву інфраструктуру та багато іншого. У статті досліджено сучасний стан виявлення кіберзлочинів у фінансовому секторі та втрати від кібератак на бізнес та громадян. Поточні економічні потрясіння також призвели до збільшення кількості зловмисників, які прагнуть викрасти конфіденційну інформацію та продати її на чорному ринку або вчинити шахрайство та отримати доступ до коштів облікового запису. Разом з тим, необхідним є створення кібербезпечного середовища, дотримання кибергігієни. Детекція та реагування на кібератаки: за допомогою системи моніторингу, виявлення та відстеження вразливостей, погроз та вимагань від користувачів стосовно зміни паролів. Необхідним є застосування передових технологій у межах захисту мереж, шифрування даних та ідентифікації користувачів, яких можна включити в систему вторинної ідентифікації особливо в умовах війни як триває в Україні.

Ключові слова: кіберзагрози, кібератаки, фінансовий сектор, фішинг, держава, шахрайство.

Within the global sector of cyber security, the two major areas that are constantly under attack are financial and governmental. The financial sector's ongoing digital transformation and the post-pandemic increase in cloud reliance have caused the sector's attack surface to grow exponentially, exposing organizations to increased cyber threats. Attacks include theft of sensitive customer data, fraud, phishing, malware distribution, attacks on network infrastructure, and more. The article examines the current state of cybercrime detection in the financial sector and losses from cyber attacks on businesses and citizens. The current economic turmoil has also led to a rise in malicious actors looking to steal sensitive information and sell it on the dark market, or to commit fraud and gain access to an account's funds. And because financial services organizations work with large amounts of information about clients, partners and employees, such sensitive data makes them ideal targets for cybercriminals. Effective security comes down to three key elements. Processes, people and technology. Processes must run seamlessly alongside the organisation. Security experts must have the capability to detect, react and understand the context of a risk. And the technology must be superior, to keep up with cyber threats. The spread of cybercrime is facilitated by such factors as: hyperdemand for various types of information services in developed countries of the world; processes of globalization of the world economy; the development of modern information technologies, especially Internet resources, which provide an almost uncontrolled process of forming temptations. At the same time, it is necessary to create a cyber-safe environment and observe cyber hygiene. Detection and response to cyberattacks: with the help of a monitoring system, detection and tracking of vulnerabilities, threats and requests from users to change passwords. It is necessary to use advanced technologies within the limits of network protection, data encryption and user identification, which can be included in the secondary identification system, especially in the conditions of the war that is ongoing in Ukraine.

Keywords: cyber threats, cyber attacks, financial sector, phishing, state, fraud.

Постановка проблеми. Світова фінансова система переживає безпрецедентну цифрову трансформацію. Розвиток сучасних технологій, трансформація систем обміну даними сприяє не лише легкості та швидкості виконання розрахункових операцій, але й підвищує рівень шахрайських дій. Інтенсивне використання Інтернету та різноманітних додатків призводить до зростання шахрайства нового покоління – кіберзлочинів.

Кіберзлочинність охоплює різноманітні сфери життя людей та будь-хто може стати його жертвою. Одним із найбільш розповсюджених видів кіберзлочину є шахрайство у фінансовій сфері. Навіть під час повномасштабної війни в Україні фінансове шахрайство не зникло, а навпаки суттєве збільшилось. Ураховуючи сучасні реалії, шахраї швидко пристосовують та адаптуються до потреб людей. Так 2022 року найпоширенішим видом була фейкова соціальна допомога від державних чи міжнародних організацій постраждалим від війни українцям. НБУ виявив близько 4500 фішингових ресурсів, для порівняння – у 2021 році ця цифра була меншою майже у три рази. Значно зросли й шахрайські дії з платіжними картками. Сума збитків від незаконних дій з платіжними картками за минулий рік становила 481 млн грн, що на 46% більше, ніж у довоєнному 2021 році [1].

Фінансове шахрайство є одним із проявів гібридної війни, а кіберзагрози фінансового сектора охоплюють різноманітні перешкоди та ризики, пов'язані з уразливістю фінансових інституцій до кібератак.

Аналіз останніх досліджень і публікацій. Відповідно до норм вітчизняного законодавства, «кіберзлочин – суспільно небезпечне винне діяння, кримінальна відповідальність за яке передбачено законодавством, вчинене в кіберпросторі за допомогою електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, яке полягає в протиправному, несанкціонованому створенні, зберіганні, обробці, підробці, блокуванні, знищенні об'єктів інформаційної інфраструктури» [2]. Разом з тим, діяльність кіберзлочинців кваліфікується за статтею 200 Кримінального кодексу України – незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їхнього виготовлення [3] та ч. 3 190 Кримінального кодексу України «Шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки», ст. 231 Кримінального кодексу України «Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю» [3].

Основною проблемою зростання фінансових злочинів у 2022 році, на думку експертів, є зростання обсягу транзакцій через цифрові канали, адже все більше людей використовують електронні методи оплати рахунків, купівлі товарів і послуг [4]. Варто зазначити, що значне зростання кібершахрайства розпочалось через пандемію COVID-19, яка спровокувала фінансову доступність, а військові дії на території нашої держави спровокували їхнє подальше прискорення.

Від кібератак страждають, як пересічні громадяни, так і фінансові установи, такі як банки, які стали основним об'єктом через важливість їхньої інформації та потенційного доступу до значної кількості грошей.

З метою боротьби з кіберзлочинами та його наслідками в Україні створено Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України. Сьогодні, спільно з Національним банком України, запущено проєкт із протидії кібершахрайству у фінансовому секторі [5]. Основною метою якого є посилення захисту громадян від кіберзлочинців, які суттєво активізували діяльність у період воєнного стану в Україні.

Згідно з дослідженням IBM Security's Cost of a Data Breach 2020, середній розмір фінансових втрат, спричинених кібератаками на фінансові установи, належить до найвищих у порівнянні з іншими галузями. Середня загальна вартість порушення даних в банках в США становить $7,13 млн, що на 15% більше, ніж загальна вартість в усіх інших галузях [6]. Попри прямі фінансові втрати, кіберзагрози призводять до витрати на відновлення комп'ютерних систем, репутаційних збитків, санкцій від регуляторів тощо.

Україна – друга серед найбільш атакованих країн світу після США. У 2022-му кількість кібератак зросла у 3,5 раза порівняно з 2021-м. На фінансовий сектор України припадає 5% усіх кібератак. Підрозділ CERT-UA зареєстрував у 2,8 раза більше кіберінцидентів, ніж у довоєнному році. Кількість загроз, геолокація яких асоційована з РФ, зросла на 26%. Кожна 10-та атака була спрямована на фінансовий сектор або розробників відповідного програмного забезпечення. Так, з опрацьованих 2194 кіберінциденти: 120 стосувались

фінансового сектора [7]. Найбільше випадків шахрайства у 2022 році відбулося у мережі Інтернет – 86% від загальної кількості випадків, у той час, як інші 14% – через фізичні пристрої (торговельні мережі, банкомати, пристрої самообслуговування) [1].

Фінансові установи впроваджують нові технології, такі як хмарні обчислення, штучний інтелект і цифрові послуги. Більшість фінансових організацій все частіше використовують хмарне програмне забезпечення для покращення можливостей обробки інформації, виявлення шахрайства та фінансової аналітики. Тим часом пандемія COVID-19 прискорила перехід галузевої IT-інфраструктури (цифрову трансформацію) фінансових установ і появу віртуальних банків і фінансових послуг [8].

У результаті цифрової трансформації установи тепер використовують все більше нових програм, пристроїв і компонентів інфраструктури, які збільшують площу атак. Усі ці фактори сприяють зростанню ризиків кібербезпеки для фінансових організацій та їхніх клієнтів. Відтак, підвищення кібербезпеки є вагомою складовою для фінансових установ та громадян для захисту своїх інформаційних ресурсів та даних від кібератак. Адже, за прогнозами аналітиків, кіберзагрози фінансового сектора в умовах війни будуть ще більш серйозними і загрожуватимуть стабільності фінансового сектора в цілому.

Постановка завдання. Основною метою статті є дослідження сучасного стану кіберзагроз у фінансовому секторі, виявлення поносних чинників змін та методів боротьби з ними.

Виклад основного матеріалу дослідження. Кіберзагрози у фінансовій системі постійно зростають, і світова спільнота повинна співпрацювати, щоб захистити її. Ковідна пандемія підвищила попит на онлайн-фінансові послуги та зробила роботу з дому нормою. Все більшої актуальності набирають випадки порушення цілісності фінансових даних, таких як записи, алгоритми та транзакції, адже, наразі доступно небагато технічних рішень для таких атак.

Кіберзагрози фінансового сектора охоплюють безліч різних загроз, які можуть спричинити великі матеріальні збитки та порушити довіру клієнтів до фінансових інституцій. Основні кіберзагрози фінансового сектора представлено в таблиці 1.

Даний перелік є невичерпним, адже поява нових технологій та суспільних викликів стимулюють злочинців до вигадування нових видів шахрайства. Разом з тим, незалежно від складних методів, які зловмисники використовують для проникнення в мережу організації, багато інцидентів безпеки пов'язані з внутрішніми загрозами, створеними теперішніми або нещодавно звільненими співробітниками та ненавмисними помилками персоналу. Згідно з дослідженням, інсайдерські атаки виявити та запобігти їм на 48% важче, ніж зовнішнім кібератакам [9].

Кіберзлочинці використовують війну для масштабування злочинного бізнесу у спосіб оформлення кредитів на зниклих безвісти військовослужбовців та громадян, що виїхали за кордон, викрадаючи їхні SIM-картки і разом з тим отримуючи доступ до їхніх банківських рахунків та оформлюючи онлайн-кредити на їхнє ім'я.

Одним із сучасних видів кіберзлочину є криптозлочини. Все більше фінансових послуг включають крипто-транзакції, і хоча це може бути гарною новиною для крипто-ентузіастів, ці послуги несуть багато ризиків, адже мають внутрішні ризики, оскільки їхні системи не захищені та не перевірені часом.

Кібершахрайство призводе до значних фінансових втрат для жертв, а також підриву довіри до електронних технологій та зменшення участі людей в онлайн-економіці.

За даними дослідження IBM Global Average Data Breach, у 2022 році глобальні втрати даних від кібератак становили 4,4 мільйона доларів, порівняно з 4,2 мільйона у 2021 році та 3,9 мільйона доларів у 2020 році. Середні річні витрати на витік даних найбільше зросли між 2020 і 2021 роками – на сплеск, ймовірно, вплинула пандемія COVID-19 [12].

Оскільки кіберзлочинці розвивають свою тактику та методи, щоб націлитися на найцінніші дані та послуги, фінансові установи повинні покращити свій захист, щоб пом'якшити загрози, що постійно розвиваються. Актуальним стає запровадження стратегії безпеки – структура «Люди, процеси, технології» (PPT). Дана стратегія здатна навчатися на загрозах і адаптувати засоби захисту від них – підхід, орієнтований на загрози. Щоб забезпечити максимальну безпеку у випадку кіберзлочинності, банки та фінансові установи повинні розробити стратегічний план, який буде не лише протистояти початковій кібератаці з мінімальним впливом і втратами, але й забезпечить постійну стійкість проти нових загроз.

Разом з тим, фінансові установи повинні вдосконалювати свої заходи з кібербезпеки, включаючи методи виявлення кіберзагроз.

Таблиця 1

Топ кіберзагроз фінансового сектора

Фішинг	використання підробленого сайта або направлення шахрайських повідомлень, з метою отримання доступу до конфіденційних даних клієнтів (паролі, номери кредитних карт тощо)
Розповсюдження шкідливих програм	використання шкідливих програм, які можуть пошкодити комп'ютерні системи фінансових інституцій та отримати доступ до конфіденційної інформації
DDoS-атаки	атаки, коли зловмисники здійснюють спробу перенести веб-сайт фінансової установи за допомогою хакерських серверів, щоб перевантажити сервери та зробити сайт недоступним
Розвідка	зловмисники збирають конфіденційну інформацію про фінансову установу та її клієнтів з метою використання цієї інформації для кібератак
Перехоплення інформації	зловмисники використовують шпигунське програмне забезпечення для перехоплення інформації, яка передається через мережу
Скімінг	встановлення пристроїв на банкоматах або терміналах для оплати, які крадуть інформацію, введену користувачем (наприклад, номер кредитної картки, PIN-код тощо)
Кібершпигунство	отримують доступ до конфіденційної інформації про бізнес, фінансові операції, інтелектуальну власність і т.д.
Шахрайство з кредитними картками	зловмисники використовують крадені кредитні картки або отримують конфіденційну інформацію про карти, щоб здійснювати транзакції без дозволу власника карти
Обман Інтернет-аукціонів	зловмисники розміщують підроблені оголошення про продаж товарів на аукціонних сайтах та надають невірну інформацію про товар або не постачається товар після оплати
Програми-вимагачі	тип зловмисного програмного забезпечення, яке перешкоджає або обмежує користувачам доступ до їхньої системи чи даних і загрожує опублікувати або продати викрадені дані, доки жертва не сплатить викуп зловмисникові

Джерело: узагальнено автором за даними [9; 10; 11]

Деякі з найбільш ефективних методів виявлення кіберзагроз у фінансовому секторі включають наступні:

1. Моніторинг мережі – системи моніторингу мережі, щоб відстежувати та аналізувати відправлення та отримання даних. Ці системи можуть виявляти незвичайну активність у мережі, яка може означати, що зловмисники намагаються виконати атаку.

2. Використання аналізу поведінки – використання аналізу поведінки, з метою виявлення незвичайних змін у роботі систем і користувачів. Ці системи можуть виявляти незвичайну активність у проміжку часу та надавати спеціалістам з кібербезпеки сповіщення про підозрілі активності.

3. Управління журналами подій – збір та зберігання журналу подій, щоб мати можливість вивчити що сталось, якщо відбулася атака. Ці журнали містять детальну інформацію про дії користувачів та систем в режимі реального часу, і вони можуть виявити підозрілі дії.

4. Здійснення регулярних тестів на проникнення. Ці тести можуть допомогти виявляти слабкі місця в системі та узгоджувати плани дій на випадок атак.

5. Використання штучного інтелекту.

Але, наразі існує безліч проблем кібербезпеки з якими стикнувся фінансовий сектор. Так, сьогодні в умовах війни та постійного збільшення кіберзлочинів, в країні існує значний дефіцит кадрів у сфері кібербезпеки, наразі кількість належним чином підготовлених фахівців значно менша за попит на них. А мобільні пристрої та додатки, які використовуються для здійснення фінансових операцій, стають мішенню для тих, хто хоче їх використати.

Висновки. Існування кіберзлочинності становить досить серйозну проблему в умовах глобального процвітання інноваційно-технологічних ресурсів. Це впливає абсолютно на всіх, як на окремих фізичних та юридичних осіб, так і на об’єкти критичної інфраструктури й державні органи. Окрім,

відповідної прямої шкоди, кіберзлочинність є величезною перешкодою для цифрової довіри, значною мірою підриваючи переваги кіберпростору.

Поширенню кіберзлочинності сприяють такі чинники, як: гіперпопит на різні види інформаційних послуг у розвинутих країнах світу; процеси глобалізації світової економіки; розвиток сучасних інформаційних технологій, особливо інтернет-ресурсів, що забезпечують майже неконтрольований процес формування спокус.

Тісні фінансові та технологічні взаємозв'язки у фінансовому секторі можуть сприяти швидкому поширенню атак по всій системі, потенційно спричиняючи масові збої та втрату довіри. Кібербезпека є явною загрозою для фінансової стабільності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. З карт зникають гроші: в НБУ розповіли, як шахраї найчастіше ошукують українців. URL: https://www.unian.ua/economics/finance/shahraystvo-z-platizhniki-kartkami-u-nbu-rozpovili-de-ta-yak-oshukuyut-ukrajinciv-12242889.html#:~:text=.

2. Кримінальна відповідальність за кіберзлочини. URL: https://wiki.legalaid.gov.ua/index.php/%.

3. Кримінальний кодекс України 5 квітня 2001 року № 2341-III Редакція від 28.04.2023. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

4. Financial crime trends to watch out for in 2023. URL: https://fintech.global/2023/01/30/financial-crime-trends-to-watch-out-for-in-2023.

5. Стартував проєкт із протидії кібершахрайству у фінансовому секторі. URL: https://bank.gov.ua/ua/news/all/startuvav-proyekt-iz-protidiyi-kibershahraystvu-u-finansovomu-sektori.

6. Cost of a Data Breach Report 2020. URL: https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf.

7. Броня фінтеху за сотні тисяч доларів. Під час війни кібератаки на фінансовий бізнес почастішали в рази. Як компанії захищаються від нападів. URL: https://forbes.ua/money/bronya-fintekhu-za-sotni-tisyach-dolariv-pid-chas-viyni-kiberataki-na-finansoviy-biznes-pochastishali-v-razi-yak-kompanii-zakhishchayutsya-vid-napadiv-04052023-13434.

8. Suleyman Ozarslan Key Threats and Cyber Risks Facing Financial Services and Banking Firms in 2022. URL: https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022#:~:text=Ransomware%2C%20phishing%2C%20web%20application%2C,financial%20institutions%20face%20in%202023.

9. 2023 Insider Threat Report, *Gurucul*, грудень 2022. URL: https://gurucul.com/2023-insider-threat-report.

10. Edward Kost (2023) The 6 Biggest Cyber Threats for Financial Services in 2023. URL: https://www.upguard.com/blog/biggest-cyber-threats-for-financial-services.

11. Guard Rails (2023)The Top 10 Cybersecurity Threats to Digital Banking and How to Guard Against Them. URL: https://www.guardrails.io/blog/the-top-ten-cyber-security-threats-to-digital-banking-and-how-to-guard-against-them.

12. Global average total cost of a data breach in 2022 growth up to $4.4 mn. URL: https://beinsure.com/news/global-average-data-breach-2022.

REFERENCES:

1. Money disappears from the cards: the NBU told how fraudsters most often cheat Ukrainians. Available at: https://www.unian.ua/economics/finance/shahraystvo-z-platizhniki-kartkami-u-nbu-rozpovili-de-ta-yak-oshukuyut-ukrajinciv-12242889.html#:~:text=.

2. Criminal liability for cybercrimes. Available at: https://wiki.legalaid.gov.ua/index.php/%.

3. Criminal codex of Ukraine. Available at: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

4. Financial crime trends to watch out for in 2023. Retrieved from: https://fintech.global/2023/01/30/financial-crime-trends-to-watch-out-for-in-2023.

5. The project to counter cyberfraud in the financial sector was launched. Available at: https://bank.gov.ua/ua/news/all/startuvav-proyekt-iz-protidiyi-kibershahraystvu-u-finansovomu-sektori.

6. Cost of a Data Breach Report 2020. Available at: https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf.

7. Fintech armor for hundreds of thousands of dollars. During the war, cyber-attacks on financial businesses became more frequent. How companies protect themselves from attacks. Available at: https://forbes.ua/money/bro-

nya-fintekhu-za-sotni-tisyach-dolariv-pid-chas-viyni-kiberataki-na-finansoviy-biznes-pochastishali-v-razi-yak-kompanii-zakhishchayutsya-vid-napadiv-04052023-13434.

8. Suleyman Ozarslan Key Threats and Cyber Risks Facing Financial Services and Banking Firms in 2022. Available at: https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022#:~:text=Ransomware%2C%20phishing%2C%20web%20application%2C,financial%20institutions%20face%20in%202023.

9. 2023 Insider Threat Report, Gurucul, December 2022. Available at: https://gurucul.com/2023-insider-threat-report.

10. Edward Kost (2023) The 6 Biggest Cyber Threats for Financial Services in 2023. Available at: https://www.upguard.com/blog/biggest-cyber-threats-for-financial-services.

11.Guard Rails (2023)The Top 10 Cybersecurity Threats to Digital Banking and How to Guard Against Them. Available at: https://www.guardrails.io/blog/the-top-ten-cyber-security-threats-to-digital-banking-and-how-to-guard-against-them.

12. Global average total cost of a data breach in 2022 growth up to $4.4 mn. Available at: https://beinsure.com/news/global-average-data-breach-2022.