МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
Навчально-науковий інститут бізнесу, економіки та менеджменту
Кафедра фінансових технологій і підприємництва

«До захисту допущено»
Завідувачка кафедри, д.е.н., проф.
_____ Лариса ГРИЦЕНКО
(підпис)
«_____»_____ 2023 р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня магістр

зі спеціальності 072 Фінанси, банківська справа та страхування
освітньо-професійної програми «Фінанси»

на тему: «Удосконалення системи протидії кібершахрайству в фінансовому секторі/ Counteraction Cyber Fraud System Improvement in the Financial Sector»

Здобувача групи Ф.м-21 Марінченка Віктора Юрійовича
(шифр групи) (прізвище, ім'я, по батькові)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ Віктор Марінченко
(підпис) (Ім'я та ПРІЗВИЩЕ здобувача)

Керівник к. е. н., доцент Євгенія Мордань _____ _____
(посада, науковий ступінь, вчене звання, Ім'я та ПРІЗВИЩЕ) (підпис)

Суми 2023

ABSTRACT

of the Master's Degree Qualification Thesis on the topic
Counteraction Cyber Fraud System Improvement in the Financial Sector
by Marinchenko Viktor

The main content of the qualification work is laid out on 27 pages, including the used sources from 33 names, which are placed on pages 38-39. The work contains 2 tables and 5 figures.

Relevance of the topic of the qualification work.

The relevance is determined by the growing threats of cybersecurity in the modern financial environment. The rapid technological advancement in the financial sector creates new opportunities for cybercriminals, necessitating constant improvement of countermeasures. This work is crucial for ensuring the stability and security of the financial system, as well as protecting the interests of clients in the virtual environment.

The research focuses on theoretical and practical aspects of enhancing the system to counter cyber fraud in the financial sector. The main emphasis is on the analysis, improvement, and implementation of measures and technologies aimed at preventing and detecting cyber threats in this sector.

The subject of the study is cyber fraud and measures to counter it in the financial sector. The goal of the qualification work is to study the theoretical foundations and develop practical recommendations for an improved system to counter cyber fraud in the financial sector based on the study of international experience.

- achieving the set goal involved solving the following tasks:
- systematize the types, consequences, and methods of countering cyber fraud.
- study the existing system to counter cyber fraud.
- investigate the current state of cyber fraud in the financial sector in conditions of a state of war.

Substantiate proposals for improving the existing protection system and implementing global experience.

Based on the research findings, the following thesis were published: Mordan Y. Yu., Marinchenko V. Yu. Modern Trends in the Development of Financial Cybercrime in Wartime Conditions. Problems and Prospects of the Development of the Financial Credit System of Ukraine: Materials of the International Scientific and Practical Conference, edited by L. L. Grytsenko, I. V. Tyutyunik. – Sumy: Sumy State University, 2023. Pp. 12−15

In the process of researching the cyber fraud, the methods theoretical generalization, statistical method, systematic and comparative analysis, graphical and tabular methods, scientific method were used

The main result of the work consists of the research based on the three sections.

The first one, which defines cybercrime as a criminal activity that utilizes computers, networks, and other technologies to launch attacks on individuals, organizations, and government structures. Primary objectives include theft of confidential information, financial fraud, dissemination of malicious programs, and privacy breaches. Specifically, its types were identified, including phishing, carding, skimming, vishing, malware, smishing, trapping, and DDoS attacks.

The established counteraction methods demonstrate that our state is significantly interested in the development of cyber hygiene. The specially designed EMA project indicates a high level of awareness and, more importantly, the dissemination of knowledge in the field of cyberspace. Alongside the cyber police, several programs have been created to assist not only citizens but also organizations in combating crimes on the digital front.

The second section is based on an analysis of statistical data from the National Bank of Ukraine, which illustrates the losses incurred by banks, merchants, and clients due to the abuse of payment cards during a state of war. Additionally, the research shows the dynamics of the development of cybercrime, based on international experience.

Analyzing the data from the second section, we determined that cybercrimes are particularly active during high-profile events at both the public and state levels. The country should ensure public awareness by publishing regular reports on cybersecurity efforts and providing accessible results and analyses for educational outreach programs aimed at the population.

The work conducted in the third section is dedicated to enhancing protection against cybercrime through the implementation of world`s experience. This is an extremely crucial aspect that demands thorough preparation and study, as cooperation with international partners on cybersecurity trends in Ukraine is exceptionally limited.

The implementation of world`s experience is a key element in improving the protection system. Regular involvement of foreign experts in the Ukrainian cyber environment will have a positive impact on the realities of the defense system, especially if these representatives have practical experience with large-scale attacks. It is also advisable to send domestic experts to global summits with cutting-edge information and fresh updates in the field of cybercrime. This will help prevent mistakes that other organizations may have already made.

Key words: cybercrime, cybersecurity, cyberspace, countermeasures, payment cards.

The year of defense of the qualification work – 2023.

ЗМІСТ

ВСТУП 5
1 ТЕОРЕТИЧНІ ЗАСАДИ КІБЕРШАХРАЙСТВА У ФІНАНСОВИХ УСТАНОВАХ 7
1.1 Сутність, види та наслідки кібершахрайтсва 7
1.2 Система протидії кібершахрайству 14
2 ПРАКТИЧНІ АСПЕКТИ РЕАЛІЗАЦІЇ СИСТЕМИ ПРОТИДІЇ КІБЕРШАХРАЙСТВУ В ФІНАНСОВІЙ СИСТЕМІ В УКРАЇНІ ТА СВІТІ 19
2.1 Аналіз наслідків кібершахрайських дії в умовах воєнного стану 19
2.2 Міжнародний досвід у боротьбі з кібершахрайством 24
3 МЕТОДИ ВДОСКОНАЛЕННЯ СИСТЕМИ ПРОТИДІЇ КІБЕРШАХРАЙСТУ В УКРАЇНІ НА ОСНОВІ ІМПЛЕМЕНТАЦІЇ СВІТОВИХ ПРАКТИК 29
ВИСНОВКИ 32
СПИСОК ВИКОРИСТАННИХ ДЖЕРЕЛ 37

ВСТУП

У сучасному світі, де цифрові технології переплелися зі всіма аспектами нашого життя, фінансовий сектор стає особливою мішенню для кіберзагроз. Перед фінансовими установами постає нагальне завдання зміцнення захисту від кібершахрайства та злочинних атак в цифровому просторі. За останні роки спостерігається значний приріст інцидентів кібершахрайства в фінансовій галузі. Це не лише загрожує фінансовим інститутам, але й підіриває довіру клієнтів та загалом стабільність фінансової системи. Однією з причин такого зростання кіберзагроз є постійний розвиток технологій та винаходження нових методів атак. У зв'язку з цим, важливо постійно вдосконалювати та адаптувати заходи безпеки для захисту фінансових ресурсів та конфіденційної інформації.

Однією з ключових складових сучасної боротьби з кібершахрайством є використання передових технологій. Удосконалення систем штучного інтелекту, аналізу великих даних, технологій блокчейн та кіберзахисту є необхідністю для виявлення та запобігання кібератак. Дослідження цих технологій та їхнє впровадження в практику стануть вагомим внеском у підвищення ефективності системи протидії кібершахрайству.

Важливим аспектом є також міжнародна співпраця та стандартизація в галузі кібербезпеки. Кіберзагрози не мають кордонів, тому спільні зусилля між країнами, міжнародними організаціями та фінансовими установами є обов'язковим елементом успішної боротьби. Розробка та впровадження спільних стандартів інформаційної безпеки дозволить створити єдину фронтальну лінію оборони від кіберзагроз.

Зважаючи на це, кваліфікаційна робота спрямована на вивчення, аналіз та вдосконалення системи протидії кібершахрайству в фінансовому секторі.

Предметом дослідження є теоретичні та практичні аспекти удосконалення системи протидії кібершахрайству в фінансовому секторі. Основний фокус спрямований на аналіз, удосконалення та впровадження заходів і технологій, спрямованих на запобігання та виявлення кіберзагроз в цьому секторі.

Об’єктом дослідження є кібершахрайство та заходи з його протидії у фінансовому секторі.

Метою кваліфікаційної роботи є вивчення теоретичних засад та розробка практичних рекомендацій щодо удосконаленої системи протидії кібершахрайству в фінансовому секторі на основі вивчення міжнародного досвіду.

Досягнення поставленої мети зумовило вирішення наступних завдань:

− систематизувати види, наслідки та методи протидії кібершахрайству;

− вивчити існуючу систему протидії кібершахрайтсву;

− дослідити сучасний стан кібершахрайства в фінансовому секторі в умовах воєнного стану;

− обґрунтувати пропозиції вдосконалення існуючої системи захисту та імплементації світового досвіду.

Для досягнення поставленої мети було використано наступні методи дослідження: теоретичного узагальнення, статистичний метод, системного та порівняльного аналізів, графічний та табличний методи, науковий метод.

За результатами дослідження було опубліковано тези: Мордань Є. Ю., Марінченко В. Ю. Сучасні тенденції розвитку фінансового кібершахрайства в умовах війни. Проблеми та перспективи розвитку фінансово-кредитної системи України: Матеріали Міжнародної науково-практичної конференції / за заг. ред.: Л. Л. Гриценко, І. В. Тютюник. – Суми : Сумський державний університет, 2023. С. 12−15.

1 ТЕОРЕТИЧНІ ЗАСАДИ КІБЕРШАХРАЙСТВА У ФІНАНСОВИХ УСТАНОВАХ

1.1 Сутність, види та наслідки кібершахрайтсва

Кібершахрайство – це злочинна діяльність, яка використовує комп'ютери, мережі та інші технології для здійснення атак на індивідів, організації та урядові структури. Основні цілі включають крадіжку конфіденційної інформації, фінансовий обман, розповсюдження шкідливих програм та порушення приватності. Злочинці, що стоять за цією діяльністю, можуть бути індивідами, групами або навіть країнами, мета яких – отримати неправомірний доступ до інформації або завдати шкоду жертвам.

Кібершахрайство визначається високою складністю та ефективністю використання технічних ресурсів для досягнення своїх цілей. Сутність цього явища включає в себе не лише технічні аспекти, а й соціальні та економічні, так як воно може впливати на різні сфери суспільства, включаючи бізнес, політику та особистий простір кожного індивіда.

Багатьма дослідниками вивчалася проблема протидії кіберзлочинності. До числа науковців, які приділяли увагу цьому аспекту, входили О.М. Литвинов, В.В. Голіна, В.І. Трапезніков, В.В. Василевич, А. П. Закалюк, В.О. Туляков, Є.Ю. Мордань, Я. В. Левківська, В.М. Головкін, В.В. Марков та інші. Їх дослідження є цінним внеском у розвиток наукових досліджень. Термін «шахрайство» походить від слова «мошна», що означає сумку, кошель, мішечок із зав'язкою для зберігання грошей. Під вчиненням шахрайства розумілось викрадення такої мошни; обман, шахрайські дії з корисливою метою. Також термін «шахраї» використовується для опису «карманників, тяглець, кишенькових злодіїв; зернщиків, які обкрадали людей на базарах; злодюжок, ошуканців». [3]

Згідно до п. 8 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII, кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про

кримінальну відповідальність (ККУ) та/або яке визнано злочином міжнародними договорами України. До того ж це кримінальні правопорушення, передбачені розділом XVI КК України («Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку»), та зареєстровані кримінальні провадження із кваліфікуючою відміткою в картці про кримінальне правопорушення – «з використанням високих інформаційних технологій і телекомунікаційних мереж». [2]

Доцільно також розглянути як визначається і кіберзахист – це сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем. [2]

Крім того, сутність кібершахрайства визначається його масштабами та глобальним характером. Злочинці можуть операціонувати в будь-якій точці світу, використовуючи анонімність і важкість виявлення в інтернеті. Це ставить перед суспільством великі виклики у забезпеченні адекватного кіберзахисту та ефективного протидії цій загрозі. Отже, сутність кібершахрайства полягає в систематичному використанні цифрових технологій для вчинення злочинних дій, що ставить під загрозу інформаційну безпеку та функціонування сучасного суспільства.

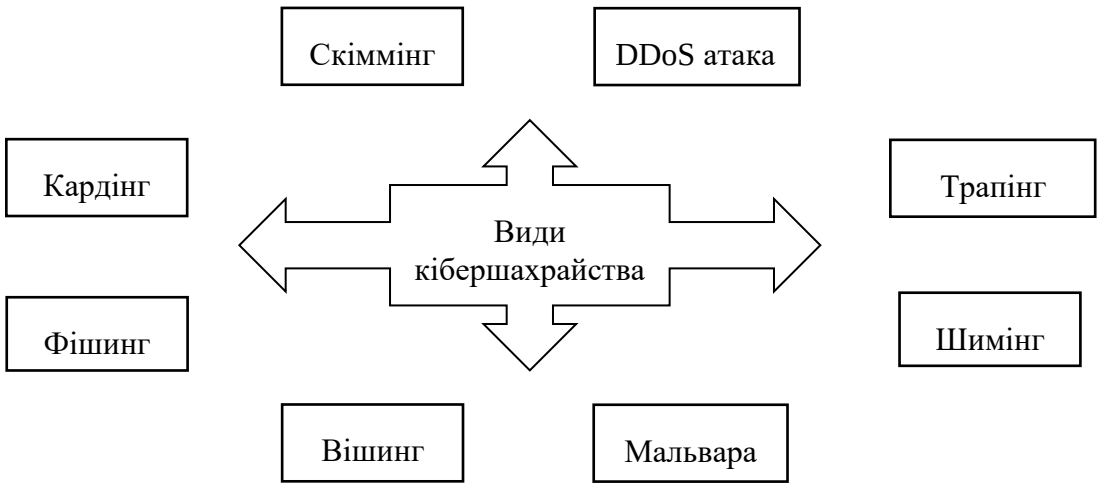

Рисунок 1.1 – Різновид шахрайтсва у кіберпросторі

Розглянемо кожен вид окремо для повного розуміння і подальшого аналізу кіберзлочинів і почнемо з найвідомішого, а саме – Фішинг.

Фішинг (англ. fishing — риболовля), у контексті кібербезпеки, представляє собою методологію кібершахрайства, при якій зловмисники використовують викривальні стратегії з метою отримання конфіденційної інформації від користувачів. Цей вид атаки може виявлятися через електронні листи, що симулюють легітимні комунікації від фінансових установ чи соціальних мереж. [19]

У сценарії «соціального інженерінгу», атаки фішингу можуть включати в себе надсилання електронних повідомлень, де відправник прикидається представником довіреної організації та закликає отримувача виконати певні дії, такі як оновлення паролю чи переходження за посиланням. Іншим поширеним варіантом є створення підроблених веб-сайтів фінансових установ, де злочинці спрямовують потенційних жертв для введення особистих ідентифікаційних даних.

Ці методи ведуть до порушення довіри та використання психологічних прийомів для отримання доступу до конфіденційної інформації, часто внаслідок чого виникають серйозні фінансові збитки та потенційні втрати конфіденційності. Призначення важливе – виявлення і попередження фішингу набуває критичної важливості у контексті сучасних стратегій кіберзахисту.

У світовому контексті, фішингові атаки надзвичайно поширені і призводять до серйозних наслідків. Один із визначних випадків включав фішерську кампанію 2016 року, пов’язану із виборчою кампанією в Сполучених Штатах. Атаки були спрямовані на електронну пошту політиків і членів їхніх команд, і метою було отримати доступ до конфіденційних даних та вплинути на виборчий процес.

Якщо ми розглянемо вітчизняний досвід, то ситуація також вимагає негайного втручання. Починаючи від повномасштабного вторгнення, було введено низку соціальних допомог: від ООН, Червоного Хреста, від нашої держави та багатьох інших організацій, що направлені на благодійну допомогу. Користуючись складним моральним та матеріальним положенням українців, шахраї під видом певної організації надсилали фішингові поссилання на номери телефонів та електронні пошти. Переходячи за посиланням жертва мала ввести дані від

банківського рахунку або зазначити інші платіжні дані (наприклад від рахунку у PayPal) та підтвердити транзакцію через смс або дзвінком.

Ці приклади свідчать про те, як фішинг може використовуватися для цілеспрямованого впливу на політичні та фінансові процеси на глобальному рівні, а також відзначають важливість вдосконалення кіберзахисту для запобігання подібним атакам.

Наступним видом шахрайтсва ми розглянемо DDoS атака. Якщо попередній вид був більше спрямований на необізнаних та вразливих верств населення, то для цього мати надзвичайні навички та професіоналізм як зі сторони нападаючого так і зі сторони захисту.

Дистриб'ювання послуг (DDoS – denial-of-service attack) – це форма кібератаки, що полягає в спробі перевантажити або призвести до непродуктивності комп'ютерні ресурси, сервери чи мережі, збільшуючи обсяг трафіку та створюючи перешкоди для легітимних користувачів. У цьому виді атаки, злочинці, використовуючи різні технічні засоби, спрямовують велику кількість запитань або даних на цільовий об'єкт, перевантажуючи його ресурси та призводячи до відмови в обслуговуванні. [4]

Враховуючи воєнну ситуацію в Україні можна побачити, що майже кожного дня захист нашого простору піддається масивним атакам з боку крани-агресора.

Вранці 12 грудня 2023 року, мережа зв'язку телекомунікаційної компанії «Київстар» стала об'єктом масштабної хакерської атаки, що призвела до серйозного технічного збою. У результаті атаки, яка тривала протягом певного періоду часу, користувачі тимчасово втратили доступ до послуг зв'язку та інтернету. За інформацією, отриманою від представників «Київстар», розслідження і відновлення послуг триває, а точні терміни ще не визначені. Основною метою хакерів було завдання значної економічної та технічної шкоди компанії.

Прес-служба «Київстар» також наголошує, що особисті дані абонентів не були скомпрометовані внаслідок цієї атаки. Компанія вживає всіх необхідних заходів для відновлення послуг та максимально швидкого усунення наслідків інциденту. Причиною успішної атаки стало скомпрометоване облікове запису одного з

працівників компанії. Він також зазначає, що в кожній організації можуть бути особи, які стають об’єктом соціального інжинірингу та наводять ризики безпеки.

Скіммінг є ще одним видом кіберзагрози, зорієнтованим на отримання фінансової вигоди, проте відрізняється від шиммінгу своєю технікою. Цей метод передбачає використання зловмисниками спеціальних пристроїв, так званих «скіммерів», які призначені для незаконного зчитування інформації з магнітних смужок банківських карт. [19]

Скіммери можуть бути розташовані на банкоматах, платіжних терміналах або навіть пристроях для оплати в ресторанах і магазинах. Зловмисники встановлюють їх так, щоб вони були непомітні для потенційних жертв. Зібрані таким чином дані потім використовуються для виготовлення клонів карт або для здійснення онлайн-покупок.

Щодо шимінгу – це видозмінений спосіб перегляду з меншими пристроями, вбудованими в сам приймач карти, вони товщиною з людську волосину, ледь помітні і розміщені всередині картриджа. Таким чином дані кредитної картки можуть бути несвідомо скопійовані.

Шиммінг та скіммінг є серйозними загрозами для фінансової безпеки та вимагають від користувачів та фінансових установ високого рівня уваги та захисту. Для мінімізації ризиків рекомендується регулярно перевіряти виписки по банківських картках, уникаючи введення особистих даних на ненадійних веб-сайтах та використовуючи захист від фішингових атак. [19]

Ще одним видом небезпеки втрачання грошей є кардінг – це шахрайське використання кредитної картки (реквізитів кредитної картки) без згоди власника. Це може бути викрадення або незаконне придбання кредитної картки, копіювання даних картки для подальшої підробки, копіювання даних картки для здійснення покупок через Інтернет без участі власника картки. Незважаючи на це, головна мета зловмисників – заволодіти чужими коштами. Для досягнення цієї мети зловмисники винаходили різні методи отримання необхідної інформації від необачних і довірливих громадян.

«Трапінг» (англ trap – пастка) у контексті шахрайства з платіжними картками є методом обману, за допомогою якого зловмисники намагаються отримати конфіденційну інформацію про платіжні картки від невинних користувачів. Цей вид атаки спрямований на отримання особистих даних, таких як номер картки, термін дії, код безпеки і інші важливі відомості методом встановлення спеціальних пристроїв на банкомат.

Вішинг – це метод шахрайства в інтернеті, при якому зловмисники намагаються отримати конфіденційну інформацію від користувачів, включаючи паролі, номери кредитних карток та інші особисті дані. Зазвичай це маніпуляції за допомогою телефону, спрямовані на отримання особистих даних банківських карток або іншої конфіденційної інформації, зокрема, шахрайське переконання в особистому переказі коштів на картку, належну зловмисникам.

Мальваре (від англійського malware — malicious software) — це загальний термін, що описує будь-яке програмне забезпечення, розроблене з зловмисною метою. Цей вид кіберзагрози включає різноманітні типи шкідливого програмного забезпечення, які можуть завдавати шкоду інформаційним системам, вкрадати конфіденційні дані, відстежувати користувачів та навіть використовувати інфраструктуру для здійснення інших кіберзлочинних дій.

Мальваре може розповсюджуватися через електронну пошту, заражені веб-сайти, компрометовані рекламні мережі та інші шляхи. Зловмисники постійно розвивають нові методи для ухилення від виявлення та проникнення в інформаційні системи.

Щоб захистити себе від Мальваре, рекомендується використовувати антивірусне програмне забезпечення, оновлювати програми та операційні системи, утримувати резервні копії важливих даних та бути обережним при відкритті невідомих посилань чи використанні приладдя з невідомих джерел.

1.2 Система протидії кібершахрайству

Посилаючись на Закон України «Основні засади забезпечення кібербезпеки в Україні»[31], можна визначити суб’єкти національної системи кібербезпеки та їх відповідні завдання. Серед цих суб’єктів виділяють Державну службу спеціального зв'язку та захисту інформації України, Національну поліцію України разом із Міністерством оборони України, розвідувальні органи у співробітництві із Службою безпеки України, Генеральний штаб Збройних Сил України, а також Національний банк України.

Відповідно до затвердженої Стратегії подальший розвиток національної системи кібербезпеки повинен базуватися на засадах виявленнята попередження кіберзлочинів, їх стримуванні та кіберпротистоянні [32]. Важливим є забезпечення кіберстійкості через здатність усіх учасників кібербезпеки своєчасно розпізнавати загрози кібербезпеці, створювати захист, розгортати інструменти для виявлення кібератак, відповідним чином реагувати та швидко відновлювати стабільну роботу під час і після кібератаки.

Однією з основних умов оперативного розкриття злочинів з використанням платіжних інструментів є ефективне взаємодію правоохоронних органів (ПО) та банків. Розмова йде, передусім, про скорочення часу на визначення карткових рахунків, які використовуються зловмисниками для шахрайських цілей, та місць вчинення злочину.

Вирішити цю задачу призначено новий веб-додаток CrimeCheck Online, розроблений Українською міжбанківською Асоціацією членів платіжних систем.

ЕМА спільно з Департаментом кіберполіції НПУ в рамках Національної програми сприяння безпеці електронних платежів та карткових розрахунків Safe Card.

Запитів по UA карткам за листопад 2023 року склав 4 285 грн, автоматичних запитів було 2 636, ручних запитів - 1649, загальна сума склала 63 млн. грн. [7]

НБУ впровадили наступні методи протидії:

– підвищення рівня обізнаності із кіберпростором, щляхом впровадження програми ШахрайГудбай, яка націлена на розвиток захисту громадян від кібершахрайства;

– звернення до хостерів, реєстраторів та організацій, що надають хмарні види послуг. Схема заключається у активному поданні скарг в Legal and Abuse департамент з метою припинити надання послуг клієнтам, що використовують веб-сайти та домени для кіберзлочинів;

– використання Google Save Browsin. Принцип іденинтичний із попереднім, подання скарги (abuse) для припинення роботи сайту. Може використовуватись лише у браузерах Google Chrome, Firefox, Safari та додатку Instagram;

– обмеження фішингових ресурсів на рівні надавачів телекомунікаційних послуг. [8]

Разом із еволюціонуванням шахрайства у кіберпросторі, розвивалися і методи захисту та попередження.

Досліджуючи методи протидії для DDoS атак можна виділити низку основних видів.

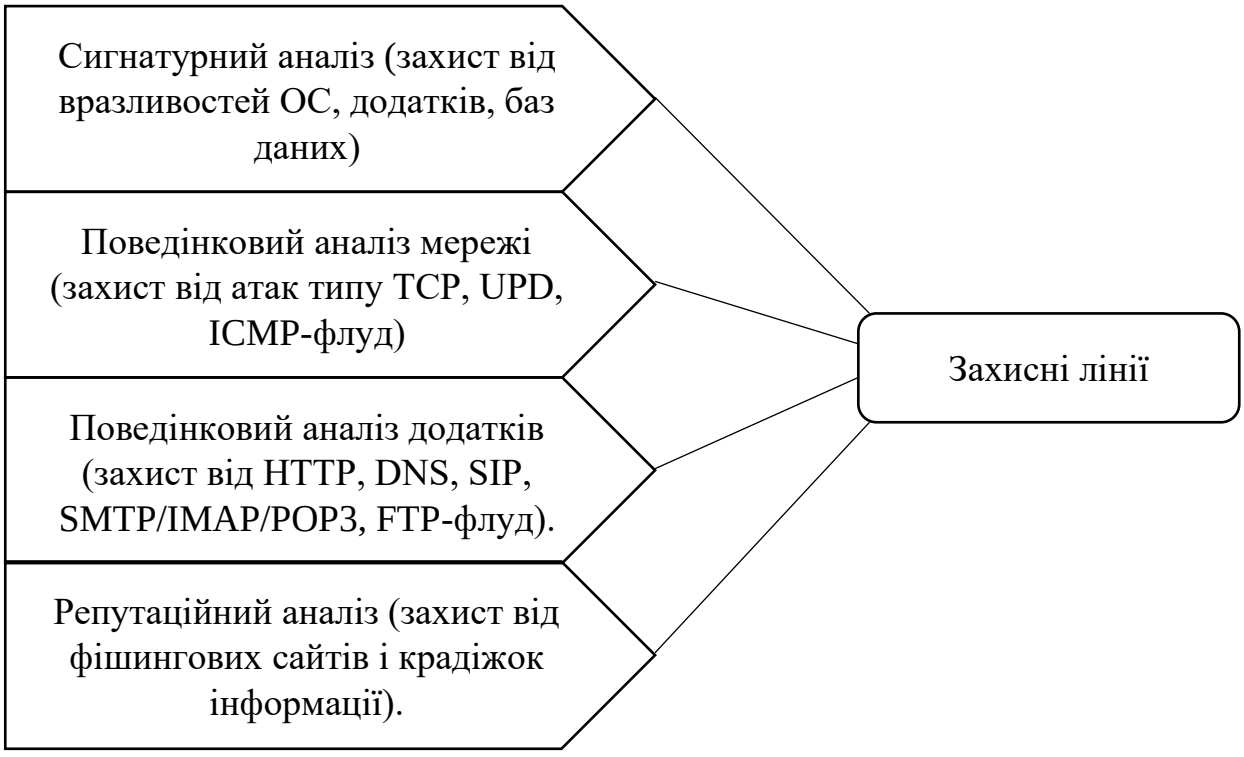

Рисунок 1.2 – Види DDoS захисту

На рисунку 1.2 ми бачимо, які саме методи використовуються при DDoS атаках, розглянемо їх ретельніше.

Сигнатурний аналіз в контексті DDoS – це метод виявлення атак, який базується на визначенні характеристичних сигнатур або відміток, що характеризують конкретні види DDoS атак. [4]

Основна ідея сигнатурного аналізу полягає в тому, щоб визначити вже відомі патерни або особливості в атаках, які вже були ідентифіковані та класифіковані раніше. Такі патерни можуть включати конкретні характеристики пакетів, типи запитів, частоту або обсяг трафіку і т. д.

Хоча сигнатурний аналіз є ефективним для виявлення вже відомих атак, він може бути обмежений у випадках нових атак або таких, що використовують методи, що не входять в існуючі сигнатури. Тому часто використовують комбінацію різних методів виявлення, включаючи аномалійний аналіз та евристичні методи, для більш повного захисту від DDoS атак.

Метод захисту «Поведінковий аналіз мережі» є ефективним засобом виявлення та захисту від атак, таких як TCP, UDP, ICMP-флуд, оскільки він ставить за мету аналіз поведінки мережі та виявлення аномалій, що можуть свідчити про потенційні атаки. Основна ідея полягає в тому, щоб визначити незвичайні та аномальні активності у мережі, які можуть свідчити про DDoS атаки або інші шкідливі дії.

Переваги цього методу включають здатність виявляти атаки, які можуть виявитися новими чи невідомими, а також зменшення кількості ложнопозитивних тривог. Однак важливо пам’ятати, що поведінковий аналіз мережі повинен використовуватися як частина комплексного підходу до безпеки, оскільки немає універсального методу, який гарантує абсолютну безпеку.

Метод захисту від DDoS атак, використовуючи «Поведінковий аналіз додатків,» є ефективним підходом до виявлення та відвернення атак, спрямованих на різні служби, такі як HTTP, DNS, SIP, SMTP/IMAP/POP3, FTP. Цей метод базується на аналізі звичайної поведінки додатків та виявленні аномалій, що можуть бути індикаторами DDoS атак. [4]

Використання поведінкового аналізу додатків для захисту від DDoS атак може значно підвищити ефективність оборони, адже він дозволяє виявляти не тільки обсягові атаки, але й витончені та цілеспрямовані атаки на конкретні служби.

Репутаційний аналіз також відіграє свою роль в захисті від DDoS атак, фішингових сайтів та крадіжок інформації, надаючи ефективний механізм виявлення та управління загрозами. [4]

Використання репутаційного аналізу дозволяє ідентифікувати та відвертати атаки на етапі їхнього походження, скорочуючи вплив DDoS атак, фішингу та крадіжок інформації на комп'ютерні системи та користувачів.

Члени української міжбанківської асоціації членів платіжних систем пропонують використовувати наступні сервіси Anti Fraud HUB для попередження та розслідування шахрайств в платіжній та кредитній сферах.

1) Fraud Payments Tracker – сервіс відслідковування та блокування несанкціонованих переказів.

За результатом на 30 листопада 2023 року 17 банками відправлено 1882 алертів (попереджень) на загальну суму 18 010 735,81 грн. Кількість алертів зросла на 21% в порівнянні з попереднім періодом (жовтень). Середній час опрацювання алерта з моменту його створення банком-відправником склав 10 хвилин, 1 500 грн. - повернуто потерпілому клієнту, 41 832 грн. – доступно для повернення клієнтам Монобанк та ПУМБ. [7]

Згідно таблиці 1.1, 76 % всіх алертів складає шахрайство з використанням методів соціальної інженерії.

Таблиця 1.1 – Статистика даних сервісу Fraud Payments Tracker, [складено за даними 7]

Тип шахрайства	Алерти	Транзакції	млн грн
Соціальна інженерія	1426	1940	13 355 571,56
Ненадання товару/послуги	246	483	1 643 974,50
Несанкціонований платіж	210	333	3 011 189, 75
Усього	**1882**	**2760**	**18 010 735,81**

2) Наступним сервісом є Сервіс “БД Інциденти” – база підтверджених випадків шахрайства за листопад 2023 року:

– 1 011 випадків шахрайства було зареєстровано 11 організаціями;

– 18 332 перевірок було попереджено, що дозволило 29 організаціям викрити шахрайство. [7]

3) Сервіс «Mobile Check» представляє собою універсальний інструмент верифікації (3 в 1), який забезпечує заміну sim-карток для номерів мереж Vodafone, lifecell та Kyivstar. Даний сервіс володіє API та web-інтерфейсами, дозволяючи враховувати заміни фізичних sim-карток на e-sim і навпаки.

4) Кіберполіція та українські банки впровадили новий веб-додаток, який прискорює розслідування платіжних злочинів. CrimeCheck Online допомагає поліцейським швидше визначати місця вчинення злочинів, а банкам - блокувати рахунки шахраїв.

Слід відзначити, що сучасні банківські установи разом із страховими компаніями пропонують своїм клієнтам можливість укладення страхових угод щодо майна власників платіжних карток. Розглянемо дану послугу на прикладі АТ "УКРСИББАНК" [33]. Банк, у межах інтегрованої послуги "All Inclusive", разом із ПрАТ "Страхова компанія "Кардіф", надає можливість страхового захисту не тільки для платіжної картки, а й охоплює ризики, пов'язані з втратою гаманця чи сумки, а також офіційних документів на ім'я власника. Серед ризиків, що покриваються програмою, та відповідних сум покриття можна виділити: шахрайські операції, обманливі дії (вішинг), крадіжка гаманця чи сумки, втрата документів. Вартість такого страхування за програмою визначається відповідно до обраного рівня інтегрованої пропозиції.[33]

Договір страхування представляє собою ефективний інструмент для зниження ризиків і гарантування компенсації клієнтам у випадку фінансових втрат, що можуть виникнути внаслідок дій шахраїв. Згідно договору покриваються наступні списання клієнтських коштів з картки або рахунку:

- операції без присутності картки;
- незаконне отримання коштів з картки;

- фішинг;
- кеш трепінг;
- скімінг та білий пластик;
- фармінг;
- шахрайство під впливом обману.[33]

Методи як внутрішнього, так і зовнішнього шахрайства стають чимдалі досконалішими. Для банків зростає потреба забезпечити операційну ефективність і результативність цифрових систем і засобів контролю ризиків шахрайства, а також підвищити кваліфікацію персоналу щодо прогнозування, запобігання та виявлення шахрайських дій.

Підсумовуючи вищесказане, ми можемо заключити, що усі методи мають використовуватися одночасно для повної готовності від потенційних шахрайських атак. Кожен з них доповнює недоліки попереднього, що не дає змоги скористатися навіть малим шансом для проникнення або спробою «покласти» систему, тож не варто використовувати лише один метод протидії, адже нові види атак розроблюються чи не кожного дня.

2 ПРАКТИЧНІ АСПЕКТИ РЕАЛІЗАЦІЇ СИСТЕМИ ПРОТИДІЇ КІБЕРШАХРАЙСТВУ В ФІНАНСОВІЙ СИСТЕМІ В УКРАЇНІ ТА СВІТІ

2.1 Аналіз наслідків кібершахрайських дії в умовах воєнного стану

В умовах розвитку технологічного прогресу все більше нових інформаційних технологій інтегрується у фінансову сферу. Неможливо уявити зараз фінансову структуру, що не використовує додатки, сайти та електронні бази даних у своїй роботі. Діджиталізація значно полегшує управління будь-якого суб'єкта господарювання, починаючи від занесення клієнтів до власного реєстру та закінчуючи внутрішніми додатками для розрахунку бухгалтерського обліку. Проте, кожен новий крок у розвитку діджиталізації бізнесу потребую удосконалення захисту від кібершахрайства. Саме захист персональних даних – це те що гарантує нам кожна фінансова установа, в якій ми залишаємо особисті дані. З кожним роком кількість випадків про витік даних та розголошення особистої інформації самими клієнтами поступово збільшується, тому системи захисту з протидії кібершахрайству є невід'ємною частиною сучасного бізнесу.

У рамках роботи доцільним є аналіз сучасних тенденцій розвитку кібершахрайста у фінансовому секторі України, його наслідків для суспільства та вивчення існуючих заходів щодо протидії кібершахрайству в умовах воєнного стану.

Згідно опитування від Нацбанку та платформи відкритих даних Опендатабот [13], близько 11 % громадян України із понад 112,9 тисячі опитаних потрапили у пастку кіберзлодіїв від початку повномасштабного вторгнення. Найчастіше жертвами інформаційних злочинів стають люди віком 18-24 роки та люди у віці 65+.

Під час дослідження було встановлено, що найчастіше українців ошукували на покупці/продажі товарів – 52,74 % (рис. 1). З початку воєнних дій шахраї активно використовують такий метод шахрайства як фішинг – це спроба отримати конфіденційну інформацію, шляхом обману людей, здебільшого через електронну пошту чи фальшиві веб-сайти. За даними опитування саме фішингові атаки зайняли друге місце за популярністю – 18,57 % (рис. 1). Шахраї створюють десятки сайтів, які

обіцяють грошові виплати від держави, міжнародних чи благодійних організацій для тих, хто опинився в складній фінансовій ситуації на фоні воєнних дій. Вони розсилають масові повідомлення через SMS та месенджери, і обіцяють соціальні виплати від різних благодійних організацій та програм, таких як єПідтримка, допомога від ЄС, ООН, Червоного Хреста. У цих повідомленнях шахраї закликають перейти за посиланням, ввести особисті дані, такі як мобільний номер телефону, пін-код, пароль до інтернет-банкінгу та смс-код від банку. Також вони створюють фейкові веб-сайти, що схожі на офіційні ресурси державних установ, банків, благодійних фондів та міжнародних організацій. Люди, відкриваючи посилання, потрапляють на схожий з оригіналом сайт, де вводять свої особисті дані, які потім автоматично потрапляють у руки шахраїв. Отримуючи таку інформацію шахраї мають доступ до банківських рахунків жертви і в подальшому знімають кошти з рахунку або оформлюють он-лайн кредити. У 2022 році в Україні було виявлено 4500 фішингових ресурсів [14], що є значним зростанням порівняно з 2021 роком, а фейкова соціальна допомога для постраждалих від війни, створена за допомогою різних фішингових методів, стала основним видом шахрайства.

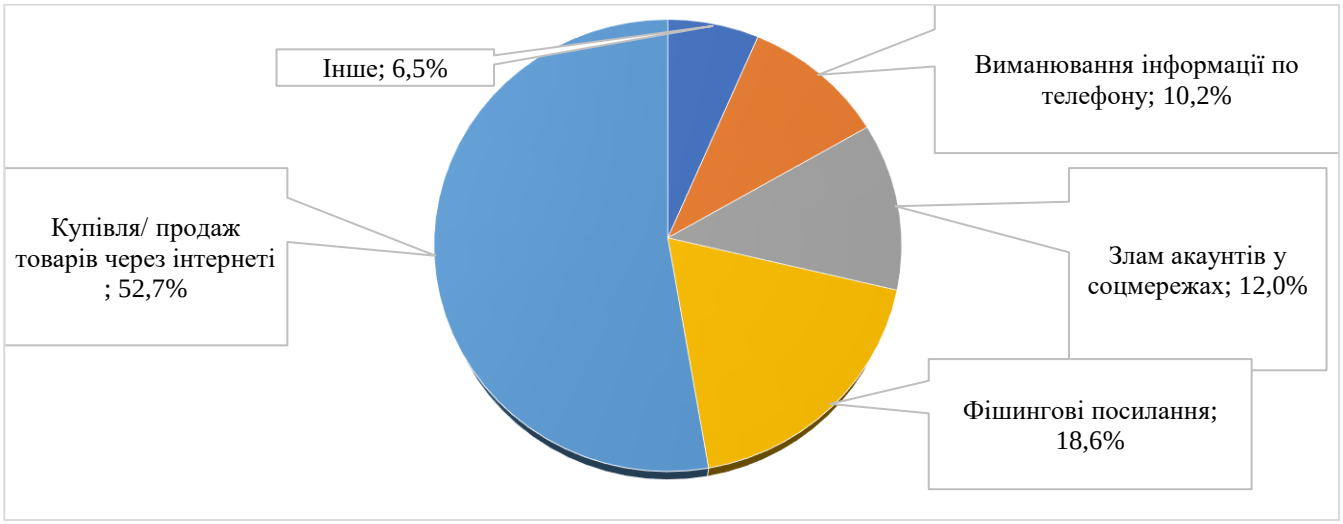

Рисунок 2.1 – Найбільш популярні шахрайські схеми, на які потрапляли громадяни України, за результатами опитування НБУ та Опендатабот [складено за даними **Помилка! Джерело посилання не знайдено.**3]

На рисунку 2.2 зображена кількість фішингових доменів, що були виявлені. Як ми бачимо, починаючи з серпня 2022 року, їхня кількість стрімко зросла з середнього показника 50 і досягнула свого піку у січні 2023 року із цифрою 1618. Це свідчить про те що, через воєнний стан, шахраї почали активно використовувати кіберпростір заради присвоєння коштів громадян.

Рисунок 2.2 – Статистика виявлення фішингових доменів в Україні за 2022-2023 рр.. [складено за даними 8]

За офіційними даними Національного банку України [16] протягом 2022 року сума збитків, завданих банкам, торговцям і клієнтам через зловживання платіжними картками, зросла до 481 млн грн, це на 46 % більше, ніж у 2021 році, а кількість незаконних транзакцій з платіжними картками зросла на 8% та склала 218 тис. Для визначення ступеня шахрайства з платіжними картками важливо порівняти суму збитків із загальною сумою всіх карткових транзакцій. Завдяки співвідношенню цих показників можна точніше визначити ступінь шахрайства. У 2022 році збитки від шахрайства становлять 69 грн на кожен мільйон гривень видаткових операцій з платіжними картками, це трохи більше, ніж у попередньому році, коли сума становила 65 грн.

У 2022 році на кожен 1 млн грн операцій із платіжними картками сума збитків від шахрайських дій здійснених у торгівельних мережах зменшилася з 40 до 16 грн, в

банкоматах – з 29 до 5 грн, проте збитки за шахрайськими операціями в Інтернеті зросли з 114 до 133 грн.

Середня сума однієї незаконної операції за 2022 рік зросла на третину, становлячи близько 2200 грн, порівняно з 1600 грн у 2021 році. Середня вартість однієї операції в торговельній мережі знизилася до 733 грн, в банкоматах – до 2878 грн, а в Інтернеті зросла до 2408 грн залежно від місця проведення шахрайства.

В цілому, лише 14 % випадків шахрайства здійснено з фізичними пристроями (торговельні мережі, банкомати), а 86 % – в Інтернеті. Відповідно, 94 % усіх отриманих збитків від шахрайства припадає на мережу Інтернет, 4 % – на торговельні мережі та 2 % – на банкомати. Таким чином, операції, в яких використовуються фізичні картки, залишаються більш безпечними, оскільки картки підробити складніше, ніж використати їх дані для транзакцій в Інтернеті [16].

Зважаючи, на зростаючу динаміку випадків кібершахрайських дій щодо ошукування громадян досить важливо здійснювати превентивні заходи з їх запобігання.

Виявлення та блокування фішингових ресурсів, які використовуються для виманювання грошей та особистих даних громадян, на рівні реєстраторів, хостерів, надавачів телекомунікаційних послуг, є важливим методом протидії фінансовому кібершахрайству.

Застосування технічних заходів безпеки, таких як шифрування та багатофакторна аутентифікація, є важливою частиною стратегії протидії кібершахрайству. Банки постійно посилюють заходи з кібербезпеки, зокрема, в систему протидій введена «Двохфакторна Аутентифікація», принцип її роботи полягав у наступному, при спробі зняття грошей, клієнту надсилається повідомлення з одноразовим кодом на прив’язаний телефон, який діє протягом обмеженого періоду часу (3-5 хвилин). Проте, через необізнаність люди повідомляли шахраям навіть цей код. Наразі, замість коду у великої кількості сервісів приходить оповіщення, де вказується, що до аккаунта був здійснений вхід з незнайомого девайсу і ви повинні підтвердити, що це саме ви (натискаючи кнопку «Так).

Підвищення рівня кіберосвіти населення є важливою тактикою у боротьбі з кіберзлочинцями. Національний Банк України разом з відділом Кіберполіції організували проєкт присвячений протидії кібершахрайству, який має назву «Шахрай Гудбай» [15]. Головна мета проєкту – поліпшити обізнаність громадян та нагадати їм про основні правила безпеки під час безготівкових розрахунків, особливо в мережі Інтернет [16]. Маючи можливість бути більш інформаційно обізнаними громадяни можуть ідентифікувати потенційно небезпечні ситуації та уникати надання своїх особистих даних шахрайським організаціям.

Отже, регулярний моніторинг і аналіз інтернет-простору дозволяє виявляти нові методи шахрайства та боротися з ними. Щоб запобігати кіберзлочинності, важливо постійно вдосконалювати та оновлювати захисні системи інформаційних технологій, а також співпрацювати з правоохоронними органами та міжнародними партнерами. Для ефективного захисту від нових загроз також важливо постійно адаптувати стратегії протидії до того, як кіберзлочинці змінюють свої методи та тактики.

2.2 Міжнародний досвід у боротьбі з кібершахрайством

Оскільки зловмисники використовують взаємозв’язану природу цифрового світу, необхідність вивчення міжнародного досвіду є важливим пунктом дослідження.

Аналізуючи останні статистичні дані щодо викрадення особистості та шахрайств з використанням кредитних карт у Сполучених Штатах Америки, ми спостерігаємо невтішну картину. Починаючи з 2020 року, вони стали одними з найпоширеніших видів шахрайства. Хоча кількість повідомлень про крадіжки особистості та шахрайства з кредитними картами зменшилась, вони залишаються на рівні, вищому, ніж перед пандемією, протягом перших трьох кварталів 2023 року. [17]

Після подвоєння випадків між 2019 і 2020 роками, звіти про крадіжки особистості продовжили зростати в 2021 році, і близько 1,4 мільйона осіб стали постраждалими. Приблизно 1,1 мільйона повідомлень про крадіжки особистості було зібрано Федеральною торговельною комісією (FTC) в 2022 році, і 805 000 повідомлень було подано до FTC протягом перших трьох кварталів 2023 року.

У 2022 році було зафіксовано 1,108 мільйони випадків крадіжки особистості. З січня по вересень 2023 року було подано 805 000 звітів про крадіжку особистості.

Шахрайство з використанням кредитних карт було найпоширенішим видом крадіжки особистості в 2022 році з 440 666 звітами. Протягом перших трьох кварталів 2023 року було подано 318 087 звітів про шахрайство з використанням кредитних карт. [22, 23].

Шахрайство з використанням документів або зловживання державними документами було найпоширенішим видом крадіжки особистості у 2021 році, але стрімко зменшилося в 2022 році (оскільки грошові винагороди від держави через пандемію COVID-19 були призупинені).

Шахрайство в банківській сфері та шахрайство з використанням кредитних карт були єдиними двома видами крадіжки особистості, що зросли з 2021 по 2022 рік, причому останнє було найпоширенішим видом крадіжки особистості у 2022 році.

Таблиця 2.1 – Статистика зареєстрованих випадків шахрайства США 2021-2022, [складено за даними 17,22]

Вид шахрайства	Зареєстровані випадки	Відхилення зареєстрованих інцидентів 2021-2022, у %
З кредитною картою	440,666	13
Банківське шахрайство	156,134	25
Шахрайство з кредитом або арендою	153,578	22
Шахрайство, пов’язане з працевлаштуванням або податками	103,416	7
Шахрайство з телефоном або комунальнами послугами	77,316	13
Шахрайство з державними документами або пільгами	57,912	85
Інші крадіжки особистих даних	326,505	13

Кількість випадків шахрайства в банківській сфері зросла на 25% у 2022 році порівняно з попереднім роком, тоді як шахрайство з використанням кредитних карт зросло на 13%.

Злочинці, які використовують вкрадену інформацію про особу для відкриття нових банківських рахунків на ім’я жертви, зросли на 32% у 2022 році. Згідно з даними FTC, майже 111 000 американців повідомили про шахрайство з відкриттям нового банківського рахунку у 2022 році, порівняно з близько 84 000 у 2021 році. [23]

Щодо шахрайства в банківській сфері, пов’язаного з дебетовими картками, електронними переказами коштів або системою АСН, відзначається зростанням на 12% у 2022 році порівняно з попереднім роком. Шахрайство із використанням існуючого рахунку збільшилося на 22%.

З 2017 по 2019 рік шахрайство з використанням кредитних карт було найпоширенішим видом крадіжки особистості, але воно було випереджене шахрайством з державними документами та фінасовими вигодами в 2020 та 2021 роках (коли шахраї скористалися програмами державних вигід в епоху пандемії).

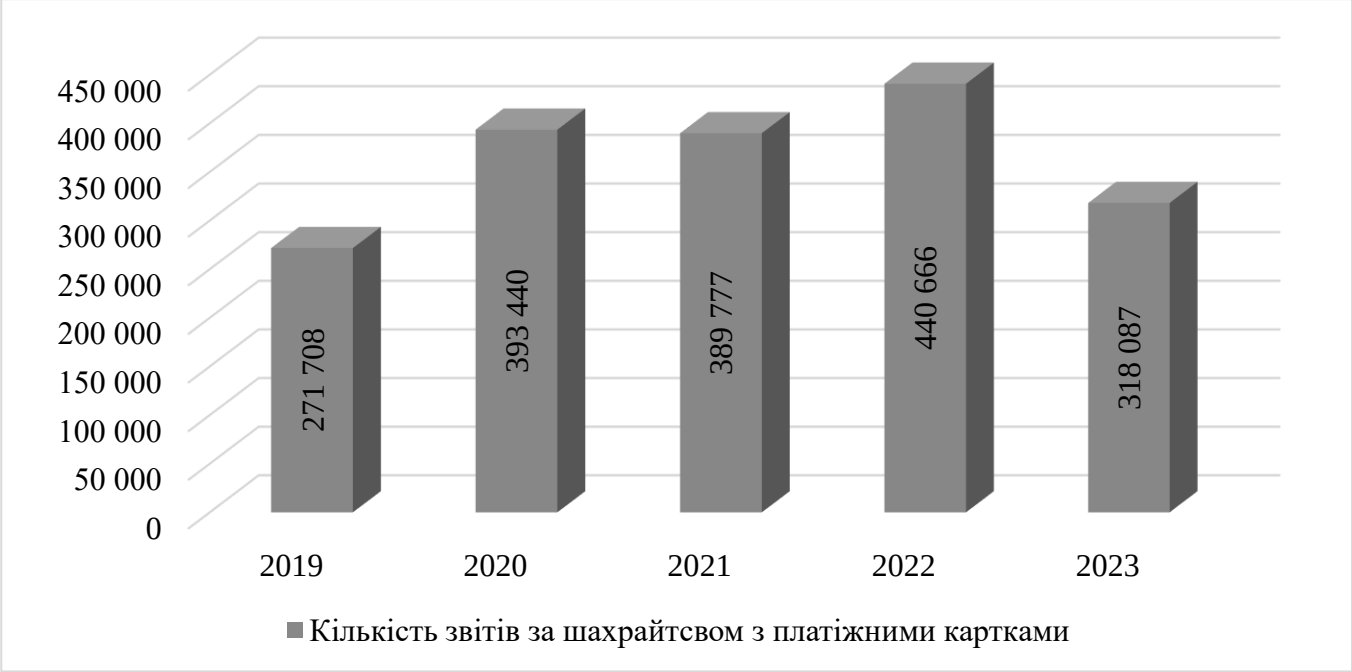

Рисунок 2.3 – Динаміка зареєстрованих звітів за період 2019-2023 рр [складено за даними 17, 21, 22, 23]

Як ми бачимо із малюнку 2.3 шахрайство з використанням кредитних карт систематично зростає, з винятком лише 1% зниження в 2021 році. Це сталося після зростання на 45% з 2019 по 2020 рік і на 72% з 2018 по 2019 рік, і йому передувало зростання на 13% у 2022 році. За даними звітів з трьох кварталів 2023 року, схоже, що шахрайство з використанням кредитних карт відбувається на тому ж рівні, що і у 2022 році. [23]

Існують два типи шахрайства з використанням кредитних карт:

– відкриття нового рахунку: злочинець використовує вашу інформацію для відкриття кредитної карткової угоди на ваше ім’я;

– використання існуючого рахунку: злочинець використовує кредитну картку, яку ви відкрили. Це, як правило, відбувається шляхом крадіжки інформації з кредитної картки.

Якщо ми задумаємось про способи уникнення кредитного карткового шахрайства, ймовірно, перше, що спадає на думку – це запобігання отриманню інформації про нашу картку іншими людьми. Але статистика показує, що набагато ймовірніше те, що хтось відкриє зовсім новий рахунок, використовуючи ваші особисті дані, ніж те, що шахрайство відбудеться через вкрадену кредитну карту.

Чому ж шахраї надають перевагу відкриттю нового рахунку? Є кілька пояснень, які, відіграють свою роль:

– використання існуючого рахунку стало складнішим. Завдяки технології чіпів на кредитних картках процес транзакції став більш безпечним, і злочинцям важче фальшивити кредитні картки;

– витоки даних викрили інформацію для сотень мільйонів людей. Злочинці-крадії особистості можуть використовувати цю інформацію для шахрайства з відкриттям нового рахунку;

– легше вкрасти гроші через шахрайство з відкриттям нового рахунку, оскільки це зовсім новий рахунок, про який споживач не знає. У випадку існуючого рахунку емітент картки або споживач може помітити підозрілу діяльність та блокувати картку в разі захоплення рахунку злочинцями-крадіями особистсті.

Важливо пам’ятати, що ви можете оскаржити операції з кредитною карткою у свого емітента картки, якщо ваша картка чи інформація були вкрадені. Ваш кредитор може допомогти вам видалити шахрайські операції, що може вплинути на ваш кредитний звіт у подальшому.

3 МЕТОДИ ВДОСКОНАЛЕННЯ СИСТЕМИ ПРОТИДІЇ КІБЕРШАХРАЙСТУ В УКРАЇНІ НА ОСНОВІ ІМПЛЕМЕНТАЦІЇ СВІТОВИХ ПРАКТИК

Аналізуючи міжнародні інциденти кібершахрайського походження, постає питання, як саме цей досвід допоможе вдосконалити вітчизняні системи захисту. Тож хто як не самі міжнародні банки зможуть розкрити це питання.

Представники банку USBank виділили перелік практик, які варто ввести в кібергігієну рядового банку або фінансової організації.

Встановлення міцної сиситеми управління.

Адекватний захист конфіденційних даних від кібератак вимагає міцної, інтелектуальної та орієнтованої на ризики програми безпеки, яку підтримують виконавче керівництво та інвестиції. Ця програма повинна включати плани реагування на інциденти, які регулярно перевіряються. Пропонується розглянути стандарт NIST Cybersecurity Framework, який широко використовується в різних галузях. Після впровадження, програму слід часто переглядати та відповідно оновлювати. [27]

Захист ваших комп’ютерів, системи та мережі.

Надійна мережа, система, а також комп’ютерна безпека, є ключовими для захисту конфіденційності та цілісності інформації, яка обробляється, передається та зберігається. На серверах та робочих станціях слід встановлювати антивірусне та антималware-програмне забезпечення. Це програмне забезпечення, а також будь-які програми, завантажені на ваші робочі станції, повинні централізовано керуватися та щоденно оновлюватися. Моніторинг мережі та брандмауера також є важливими для виявлення загроз та запобігання вторгненням. Варто переконатися, що ваша програма безпеки включає регулярні оцінки вразливостей, тестування на проникнення та протоколи патчінгу.

Додатково, організації, які зберігають та передають конфіденційні дані споживачів, відповідальні за безпеку своїх процесів передачі даних. Використання кількох відведених та шифрованих мереж, які активно моніторяться за

використанням пропускної здатності, може допомогти забезпечити безпечне та ефективне завершення передачі файлів.

Впроваджуйте та моніторте засоби контролю доступу.

Керування та моніторинг доступу користувачів до чутливих систем та даних є важливим для забезпечення безпеки оточення. Слід обмежувати доступ лише тим, хто потребує його для основних робочих функцій і встановлювати жорсткі вимоги до паролів, що відповідають стандартам галузі. Зміцнення аутентифікації, необхідної для використання корпоративних електронних адрес, систем та програм на особистих пристроях (тобто мобільних телефонах, планшетах, особистих ноутбуках і т. д.), особливо важливо при впровадженні нових технологій та пристроїв. Постійний моніторинг діяльності користувачів, які мають доступ до чутливих даних, допомагає попереджати будь-які підозрілі або небезпечні дії.

Захист фізичного середовища.

Фізична безпека завжди була ключовою складовою для захисту чутливих даних. Важливо, щоб працівники на всіх рівнях організації дотримувались практик, які забезпечують безпеку фізичних середовищ - як у будівлях офісів, так і вдома.

Хоча фізичні заходи безпеки, такі як використання системи карток для запобігання несанкціонованому входу в офіс, є важливими, віддалені працівники також потребують рекомендацій щодо найкращих практик, щоб забезпечити залишання інформації в безпеці в умовах роботи вдома. Використання технологій кібербезпеки, таких як віртуальна приватна мережа (VPN), може допомогти зменшити ризик витоку даних.

Кіберзлочинці постійно розвивають свої можливості, що означає, що для повної безпеки використання VPN вже не може обмежуватися лише ім’ям користувача та паролем. Бажано використовувати багатофакторну аутентифікацію (MFA) для захищеної мережі. Крім того, найміцніші форми MFA не залежать від текстових повідомлень, які можуть бути підроблені, а замість цього працюють з одноразовими кодами, згенерованими від токена чи додатку токена. [27]

Надння підготовки для всієї організації.

Злочинці, які здійснюють кібератаки, завжди шукають нові способи доступу до чутливої інформації, а їх цілі - як і фізичні особи, так і організації. Щоб належним чином захистити свою компанію та співробітників від кіберзагроз, важливо навчати всіх працівників боротьбі з кібератаками. Демонстрація підтримки виконавчого рівня для ініціатив з питань кібербезпеки, таких як навчання з освіти в галузі кібербезпеки, також може допомогти створити безпечне середовище на всіх рівнях вашої організації. [27]

Фішінг – це поширений метод, яким користуються кіберзлочинці для атак на організації, намагаючись отримати доступ до інформації за допомогою шахрайських електронних листів. Проведення вправ щодо фішингу - ефективний спосіб постійно нагадувати працівникам про найкращі практики та перевіряти їхню адекватну реакцію. Можливі наслідки невдачі в таких вправах можуть включати подальше слідкування менеджменту та перевідновлення для забезпечення належної реакції у майбутньому. Висока освіченість працівників щодо того, як виглядає фішинг, є критичною для захисту чутливої інформації компанії.

Управління постачальниками.

Зовнішні постачальники є критично важливою частиною операцій бізнесу, і наявність надійного процесу для їхнього огляду є так само важливою, як і забезпечення безпеки функціонування вашої організації. Під час вибору постачальників запитуйте їхні звіти SOC 2 або SSAE 18 та переконайтеся, що ви орієнтовані на те, як вони захищають інформацію клієнтів. Проведення регулярних оглядів в рамках догляду допомагає впевнитися, що постачальники продовжують відповідати вимогам безпеки, і дозволяє вам слідкувати за будь-якими змінами в послугах або штаті працівників. [27]

Планування щодо відповідної реакції на інциденти.

Проведення регулярних тестів чи вправ з вашого плану реагування на інциденти стає все більш важливим. Оскільки оточення змінюється, це допомагатиме визначити, чи потрібно оновити чи змінити будь-які процедури, забезпечуючи безперебійне функціонування вашого бізнесу навіть у часи невизначеності. Це може

включати встановлення засобів зв’язку та технології для віддалених працівників. Розуміння того, як ситуація вплине на всіх стейкхолдерів, внутрішніх і зовнішніх, допоможе вам оптимізувати ці процеси для задоволення потреб всіх у майбутньому.

Вищезазначені дії також трактували фахівці із «Federal Reserve Bank of Minneapolis», і додатково поділилися декількома важливими порадами, яких потрібно дотримуватись при кібератаці:

– зв’яжіться з критичними постачальниками, включаючи постачальника технічного обслуговування (TSP), постачальника інтернет-послуг та основного обробника;

– зверніться до вищого менеджменту та членів ради директорів, щоб забезпечити їх розуміння ситуації та запросіть ресурси для координації планів реагування на інцидент та відновлення після катастрофи;

– зв’яжіться з постачальником кіберстрахування банку, який може допомогти зі збором інформації на етапі інциденту та часто може порекомендувати компанії для реагування на інциденти, з якими вони раніше співпрацювали;

– забезпечте наявність у працівників готового та однорідного повідомлення для спілкування з клієнтами;

– сповістіть основного регулятора банку та правоохоронні органи та забезпечте дотримання нового Правила звітування про інциденти, пов’язані з комп’ютерами. [25]

Опираючись на іноземний досвід, фінансовим організаціям варто переглянути структуру своєї поведінки під час кіберзагроз, а також імплементувати поради від міжнародних банків до свого робочого простору. Таким чином, фінустанови зможуть розвивати напрям своєї діяльності краще, шидше, а головне – надійніше.

ВИСНОВКИ

У сучасному світі, де інформаційні технології стали неодмінною частиною фінансового сектору, зростає загроза кібершахрайства. Фінансові установи стають метою атак з боку кіберзлочинців, які прагнуть використати різноманітні технічні прийоми для отримання неправомірного доступу до конфіденційної інформації та економічних ресурсів. У контексті постійно зростаючих загроз кібербезпеки важливо удосконалювати системи протидії кібершахрайству в фінансовому секторі.

Дослідження першого розділу визначає кібершахрайство як злочинну діяльність, яка використовує комп’ютери, мережі та інші технології для здійснення атак на індивідів, організації та урядові структури. Основні цілі включають крадіжку конфіденційної інформації, фінансовий обман, розповсюдження шкідливих програм та порушення приватності. Зокрема, було виділено його види: фішинг, кардинг, скімінг, вішинг, мальвара, шимінг, трапінг, DDoS атака.

Сформовані методи протидії показують, що наша держава суттєво зацікавлена в розвитку кібергігієни. Окремо створений проєкт ЕМА показує хороший рівень обізнаності, а що головніше розповсюдження знань в галузі кіберпростору. Разом із кіберполіцією було створено декілька програм, що допомагають не тільки громадянам, а й організаціям боротися із злочинами на цифровому фронті. Використовуючи такі додатки як «Fraud Payments Tracker», «БД Інциденти», «Mobile Check», CrimeCheck Online представникам ЕМА вдалось запобігти шахрайським намірам привласнити кошти. Проте, судячи із представлених статистичних даних, організації не мають наміру стрімко посилювати свою кібербезпеку, адже показник кількості опрацьованих заявок навіть і близько не поруч біля кількості регулярних кібератак. Тож наша рекомендація – це поширити використання вищезазначених додатків шляхом впливу великих державних структур на освітню програму щодо кіберзахисту серед інших організацій.

В основу другого розділу покладено аналіз статистичних даних НБУ, які показують, що збитки завдані банкам, торговцям і клієнтам через зловживання платіжними картками за період 2022 року склала 481 млн грн, що на 46% перевищує показники 2021 року. Середня сума однієї незаконної операції за 2022 рік зросла на третину, становлячи близько 2200 грн, порівняно з 1600 грн у 2021 році. Середня вартість однієї операції в торговельній мережі знизилася до 733 грн, в банкоматах – до 2878 грн. Ситуація видається вкрай катастрофічною і показує, що є доцільним впровадження сформованої програми базових навичок протидії і розпізнання шахрайства у кіберпросторі.

За період воєнного стану в країні значно підвищились випадки шахрайтсва, більше 112,9 тисяч опитаних громадян стали жертвами кіберзлочинів і половину з них займає вид соціальної інженерії, а саме покупка/продаж товарів, відсоток якого склав 52.74%. При масових подіях на державному рівні (війна, криза, тощо) верстви населення стають більш вразливими до злодіїв, які навпаки активно реагують на такі ситуації і розробляють нові план-схеми для привласнення чужих коштів.

В цілому, лише 14 % випадків шахрайства здійснено з фізичними пристроями (торговельні мережі, банкомати), а 86 % – в Інтернеті. Відповідно, 94 % усіх отриманих збитків від шахрайства припадає на мережу Інтернет, 4 % – на торговельні мережі та 2 % – на банкомати. Таким чином, операції, в яких використовуються фізичні картки, залишаються більш безпечними, оскільки картки підробити складніше, ніж використати їх дані для транзакцій в Інтернеті.

Аналізуючи, дані другого розділу ми визначили, що кіберзлочини особливо активні під час гучних подій як на громадському, так і на державному рівні. Країна має забезпечувати чутливість населення, оприлюднюючи регулярні звіти з проведної роботи над кіберзахистом, а також надавати доступні результати та аналіз, з метою освітньої програми населення

Робота, проведена у 3 розділі присвячена удосконаленню захисту від кібершахрайтсва на основі імплементації світового досвіду. Це є надзвичайно важливим аспектом і вимагає ретельної підготовки та вивчення, адже кооперації із міжнародними партнерами щодо тенденцій кіберзахисту в Україні надзвичайно мало.

Регулярне залучення іноземних фахівців до українського кіберсередовища позитивно відобразиться на реаліях системи захисту, особливо якщо ці представники мають реальний досвід з масованими атаками. Також варто відправляти вітчизняних фахівців на всесвітні саміти із передовою інформацією та свіжими новинами в області кібершахрайтсв, це допоможе не допустити помилок, яких вже припускалися інші організації.

Таким чином ми можемо перейняти іноземний досвід і вчитися на чужих помилках. Банк Сполучених Штатів Америки USBank надав перелік практик, що ми можемо відобразити у своїх фінансових структурах. Серед них ми б радили звернути увагу на:

- Встановлення міцної сиситеми управління, що допоможе позбутися ієрархічних проблем з доправленням інформації до відповідного департаменту (представника) без будь-яких бюрократичних або технічних проблем. Тож реагування на інциденти стане в рази ефективнішим;
- Планування щодо відповідної реакції на кібератаки, допоможе скоротити час реагування, а час при таких атаках це – все. Тож проведення регулярних тестів, практикумів, імітацій атак сприятиме розвитку інформаційного захисту організацій.

Досліджучи досвід США із злочинами по викраденню особистості та махінаціям з платіжними картками, ми можемо спостерігати тенденцію зростання, особливо за підзвітні періоди 2022 року, що показує як навіть одна з провідних країн по викристанню сучасних методів кіберзахисту отримує величезні збитки кожного року. Варто окремо виділити вид шахрайства з використанням кредитних карт. А саме «відкриття нового рахунку». Схема є доволі простою і з проаналізованих мною даних не розповсюдженою на території України (за виключенням окремих випадків). Вважаю за доцільне розлянути цей вид злочину ретельніше з боку відповідних служб, щоб попередити майбутні інциденти, таким чином банки можуть не тільки зберегти кошти своїх клієнтів, а й свою репутацію перед ними.

Імплементація світового досвіду є одним з ключових моментів в удосконаленні системи захисту. Регулярне залучення іноземних фахівців до українського кіберсередовища позитивно відобразиться на реаліях системи захисту, особливо якщо ці представники мають реальний освід з масованими атаками. Також варто відправляти вітчизняних фахівців на всесвітні саміти із передовою інформацією та свіжими новинами в області кібершахрайтсв, це допоможе не допустити помилок, яких вже припускалися інші організації.

У світлі сталого розвитку кіберзлочинності важливо акцентувати увагу на створенні та впровадженні міжнародних стандартів безпеки в фінансовому секторі таких як стандарт NIST Cybersecurity Framework. Встановлення загальноприйнятих норм та вимог щодо кіберзахисту сприятиме уніфікації підходів та забезпеченню високого рівня безпеки на глобальному рівні.

СПИСОК ВИКОРИСТАННИХ ДЖЕРЕЛ

1. О.В. Кузьменко, Г. М. Яровенко. Сучасні інструменти боротьби з кібершахрайствами у банках : Монографія. Суми, 2018. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/79743/1/Kuzmenko_%20Kibershakhraistvo_%20paper.pdf

2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII : станом на 17 серп. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 20.11.2023)

3. Діброва Т., Пісенко Д., Сметаніна Н. Кіберзлочинність та кібершахрайство в умовах воєнного стану. Юридичний науковий електронний журнал. 2022. С. 546–549. URL: http://lsej.org.ua/11_2022/132.pdf

4. Захист від DOS/DDoS-атак. System.Network.Technologies. URL: https://www.snt.ua/portfolio/it-resheniya/informacionnaya-bezopasnost/zashchita-ot-dosddos-atak (дата звернення: 24.11.2023).

5. Шахрайство під час війни: топ-4 схеми і нові тенденції. Міністерство Фінансів України. URL: https://minfin.com.ua/ua/2022/03/15/82162508/ (дата звернення: 23.11.2023).

6. Левківська Я. В. Вплив воєнного стану на трансформування та розвиток інтернет-шахрайства в Україні. «Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» : матеріали Міжнар.наук.-практ. конф, м. Одеса. 2022. С. 521–523. URL: http://dspace.onua.edu.ua/handle/11300/19993

7. Звіт української міжбанківської асоціація членів платіжних систем ЄМА. 2023. URL: https://www.ema.com.ua/news/novyny-platizhnoho-rynku-vid-iema-5/

8. Протидія кібершахрайству у фінансовій сфері. Нац. банк України, 2023. 10 с. URL: https://bank.gov.ua/admin_uploads/article/Protydiya_kibershakhraystvu_u_finansoviy_sferi_pr_2023-02-15.pdf?v=6 (дата звернення: 10.11.2023).

9. Боженко В. В., Койбічук В., Габенко М. Вплив кібершахрайств на фінансову систему на прикладі країн Євросоюзу. Вісник СумДУ. 2021. С. 47–52. URL: https://visnyk.fem.sumdu.edu.ua/issues/2_2021/6.pdf.

10. Strategic plan 2020-2024 – Informatics. Directorate-General for Informatics, 2020. 34 с. URL: https://commission.europa.eu/publications/strategic-plan-2020-2024-informatics_en

11. Кравчук Д. Способи злочинного професіоналізму у сфері незаконного використання платіжних карток, пов'язаних із втручанням у роботу банкоматів. Актуальні проблеми вдосконалення чинного законодавства України: Збірник наукових статей. 2016. № 41. С. 59–69. URL: http://lib.pnu.edu.ua:8080/handle/123456789/8843

12. Яровенко Г., Бояджян М. Аналіз наслідків кібершахрайств в банківській системі України. Економіка та суспільство. 2018. № 18. С. 836–843. URL: https://economyandsociety.in.ua/journals/18_ukr/116.pdf

13. Результати опитування від НБУ та Опендатабот. Офіційний вебпортал НБУ. URL: https://bank.gov.ua/ua/news/all/rezultati-opituvannya-vid-nbu-ta-opendatabot-kojen-devyatiy-opitaniy-stavav-jertvoyu-shahrayiv-z-pochatku-voyennogo-stanu

14. Протидія кібершахрайству у фінансовій сфері, лютий 2023 року. Офіційний вебпортал НБУ. URL: https://bank.gov.ua/ua/news/all/startuvav-proyekt-iz-protidiyi-kibershahraystvu-u-finansovomu-sektori

15. Проєкт НБУ та Кіберполіції «Шахрай Гудбай». Офіційний вебпортал НБУ. URL: https://promo.bank.gov.ua/stopfraud/

16. Стартувала інформаційна кампанія #ШахрайГудбай: нагадуємо про важливі правила платіжної безпеки. Офіційний вебпортал НБУ. URL: https://bank.gov.ua/ua/news/all/startuvala-informatsiyna-kampaniya-shahraygudbay-nagaduyemo-pro-vajlivi-pravila-platijnoyi-bezpeki

17. Consumer Sentiel Network. Federal Trade Commission, 2021. URL: https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2021

18. Мельник С. С. Сутність фінансового шахрайства в комерційному банку. Науковий вісник Ужгородського національного університету. 2016. № 6. С.91–95. URL: http://www.visnyk-econom.uzhnu.uz.ua/archive/6_2_2016ua/23.pdf

19. Родченко С. С., Живко З. Б. Фінансове шахрайство у банківській сфері. Науковий вісник Ужгородського національного університету. 2020. № 31. С. 103–108. URL: http://www.visnyk-econom.uzhnu.uz.ua/archive/31_2020ua/19.pdf

20. Боженко В.В., Кушнерьов О.С., & Кільдей А.Д. (2021). Детермінанти поширення кіберзлочинності у сфері фінансових послуг. Економічний форум, 1(4), 116-121. URL: https://doi.org/10.36910/6775-2308-8559-2021-4-16

21. Impressive Cybersecurity Statistics: 2023 Data & Market Analysis. FinancesOnline Research Center, 2023. URL: https://financesonline.com/cybersecurity-statistics/

22. Consumer Sentiel Network 2020. Офіційний вебпортал Federal Trade commission, 2020. URL: https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf

23. Identity Theft Reports. Офіційний вебпортал Federal Trade Commission, 2022. URL: https://www.idtheftcenter.org/post/2022-annual-data-breach-report-reveals-near-record-number-compromises/

24. Despite rising concern, Americans leave themselves vulnerable to cyberattacks. Офіційний вебпортал Nationwide, 2022. URL: https://news.nationwide.com/despite-concern-americans-vulnerable-to-cyberattacks/?utm_source=prpitch

25. Cybersecurity trends and best practices for community banks. Офіційний вебпортал Federal Reserve Bank of Minneapolis. URL: https://www.minneapolisfed.org/article/2022/cybersecurity-trends-and-best-practices-for-community-banks

26. Analysis Finds Synthetic Identity Fraud Growing to Record Levels. Офіційний вебпортал TrunsUnion. URL: https://newsroom.transunion.com/transunion-analysis-finds-synthetic-identity-fraud-growing-to-record-levels/

27. Cybersecurity: protecting client data through industry best practices. Офіційний вебпортал USbank, 2023. URL: https://www.usbank.com/financialiq/improve-your-

operations/minimize-risk/cybersecurity-protecting-client-data-through-industry-best-practices.html

28. Share of European firms reporting a cyber attack 2020, by country. Офіційний вебпортал Statista, 2020. URL : https://www.statista.com/statistics/1006664/european-firms-cyberattack-target-reporting/

29. 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

30. Мордань Є. Ю., Бардакова В. В., Сокол Л. В. (2023) Удосконалення вітчизняної системи протидії кіберзлочинності та кібершахрайству на основі впровадження міжнародного досвіду. Ефективна економіка. № 10. URL: https://www.nayka.com.ua/index.php/ee/article/view/2329/2361

31. Про основні засади забезпечення кібербезпеки України.Офіційний вебпортал парламенту України. URL:https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 22.08.2023)

32. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.21 р. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 22.08.2023

33. Догоговір страхування майна держателя платіжних карток Офіційний вебпортал АТ «УКРСИББАНК». URL: https://ukrsibbank.com/products/personal-bank-services/pip/