**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**
**«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ**
**імені ІГОРЯ СІКОРСЬКОГО»**
**НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ**
**Кафедра інформаційної безпеки**

До захисту допущено
Завідувач кафедри

_____ **Дмитро ЛАНДЕ**
(підпис)

«_____»_____2024 р.

# Дипломна робота

**на здобуття ступеня бакалавра**
**за освітньо-професійною програмою «Системи, технології та математичні методи кібербезпеки»**
**спеціальності 125 «Кібербезпека»**

на тему: Сучасні методи та сценарії кібершахрайства.

Виконав (-ла): здобувач вищої освіти **IV** курсу, групи ФБ-03
(шифр групи)

Заболотний Максим Олександрович
(прізвище, ім'я, по батькові) (підпис)

Керівник доцент, к.ф.-м.н Смирнов С. А.
(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові) (підпис)

Рецензент К.ф.-м.н.,, доцент кафедри ММЗІ, Хмельницький М. О.
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище, ім'я, по батькові) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Здобувач вищої освіти _____
(підпис)

Київ – 2024 рок

# АНОТАЦІЯ

Обсяг роботи 61 сторінка, 8 ілюстрації, 27 джерело літератури.

Мета роботи - дослідження та аналіз феномену кібершахрайства через кол-центри, включаючи вплив на потерпілих та засоби протидії такого типу шахрайства.

Об’єкт дослідження – поле активності кол-центрів, включаючи їхню роль в кібершахрайстві та взаємодії зі споживачами.

Суб’єкт дослідження – аналіз специфічних тактик і стратегій, які використовуються незаконними кол-центрами для ведення шахрайської діяльності, з особливою увагою до механізмів рекрутменту та маніпуляції потерпілими.

У роботі використані наступні методи дослідження: критичний аналіз літературних джерел та абстрагування щодо теми роботи, метод аналізу та порівняння використано при здійсненні порівняльного аналізу.

Діяльність, шахрайство, способи та методи, «кол-центр».

# ABSTRACT

The volume of work is 61 pages, 8 illustrations, 27 sources of literature.

The purpose of the work is research and analysis of the phenomenon of cyber fraud through call centers, including the impact on victims and means of countering this type of fraud.

The object of the study is the field of activity of call centers, including their role in cyber fraud and interaction with consumers.

The subject of the research is the analysis of specific tactics and strategies used by illegal call centers to conduct fraudulent activities, with special attention to the mechanisms of recruitment and manipulation of victims.

The following research methods are used in the work: critical analysis of literary sources and abstraction regarding the topic of the work, the method of analysis and comparison is used in the implementation of comparative analysis.

Activities, fraud, methods and methods, "call center"

ЗМІСТ

## Перелік умовних позначень, символів, скорочень і термінів

ККУ - Кримінальний кодекс України.

ФТП - Фінансові трансферні послуги.

МФО - Мікрофінансові організації.

ОВДП - Ощадні відділення державних паперів.

СМС - Служба миттєвих повідомлень.

ПІН - Персональний ідентифікаційний номер.

СІМ - Субсидіарна ідентифікаційна мітка (картка).

HTTPS - Протокол захищеного гіпертекстового передавання.

PIN - Personal Identification Number (Персональний ідентифікаційний номер).

ATM - Automated Teller Machine (Банкомат).

VPN - Virtual Private Network (Віртуальна приватна мережа).

# ВСТУП

Шахрайство, як один із найпоширеніших видів злочинів, вимагає постійної уваги та активної боротьби з боку правоохоронних органів через декілька причин. По-перше, багато випадків шахрайства залишаються непоміченими, оскільки жертви часто не звертаються до поліції. По-друге, в умовах розвитку ринкової економіки, шахраї нерідко прикривають свої дії легальними видами бізнесу, як-от інвестиції чи банківські операції. По-третє, прогрес у сфері інформаційних технологій сприяє появі нових методів шахрайства.

Широке використання кредитних операцій, необхідне для економічного розвитку, також вносить свої корективи в динаміку шахрайської активності. Зміни в системі банківського регулювання та зниження рівня державного контролю часто призводять до збільшення шахрайства, особливо в секторі кол-центрів.

Інтернет-шахрайство має безліч форм, від фішингових атак до шахрайства на аукціонах, і зазвичай має на меті змусити жертву віддати особисту інформацію або кошти за неіснуючі товари чи послуги. Серед них найвідоміші - нігерійські листи, шахрайство з антивірусами, та інші види обману, що стосуються кредитних карток.

Проблема шахрайства вивчається в наукових колах, зокрема кримінальним правом та кримінологією. Значний внесок у розуміння цієї проблематики зробили такі вчені, як Р. А. Запорожець, О. Г. Кальман, та інші. Розробка методів розслідування шахрайства також має теоретичну базу, засновану на дослідженнях в областях кримінального процесу та оперативно-розшукової діяльності, завдяки працям таких науковців, як Г. С. Бідняк та С. В. Головкін.

Відповідно до обраної мети роботи визначено наступні завдання:

- Проаналізовано основні поняття в сучасному шахрайстві;

- Охарактеризовано типи та способи шахрайства;

- Дослідити шахрайство в сфері онлайн-продаж;

- Дослідити Банківське шахрайство в онлайн-банкінгах;

- Провести огляд існуючих підходів та рішень для виявлення шахрайських транзакцій;

- Виконати аналіз використання спеціальних знань під час розслідування шахрайства, пов’язаного з діяльністю шахрайських транзакцій.

Об’єкт дослідження – діяльність кол-центрів.

Предмет роботи – це дослідження незаконної діяльності кол-центрів.

У роботі використані наступні методи дослідження: критичний аналіз літературних джерел та абстрагування щодо теми роботи, метод аналізу та порівняння використано при здійсненні порівняльного аналізу, синтезу та дедукції, узагальнення при формуванні стратегії виходу на ринок.

Інформаційною базою дослідження стали літературні джерела, спеціальні монографічні й періодичні джерела, Інтернет-ресурси, Звіти та огляди міжнародних організацій, Інтернет-сайти, новинні ресурси тощо.

Практичне значення дослідження визначається тим, що отримані результати можуть бути використані студентами, вченими, аспірантами.

Кваліфікаційна робота складається зі вступу, 4-х розділів, висновків, списку використаних джерел з 27 найменувань і додатків. Зміст кваліфікаційної роботи викладено на 61 сторінці друкованого тексту.

# 1 ТЕОРЕТИЧНІ АСПЕКТИ ТЕМИ ДОСЛІДЖЕННЯ

## 1.1 Основні поняття в сучасному шахрайстві

Щодня безліч українців стають жертвами шахрайських дій в Інтернеті, а активність злочинців невпинно зростає.

Офіційні статистичні дані Генеральної прокуратури України свідчать про поступове зменшення кількості зареєстрованих випадків шахрайства та кримінальних проваджень, що стосуються шахрайства, направлених до суду з обвинувальним актом. Наприклад, у 2016 році було зареєстровано 46 019 випадків шахрайства, з яких 6 379 справ було направлено до суду, а 41 412 справ закрито. У 2017 році ці показники становили відповідно 37 014/8 662/46 447, у 2018 році – 33 290/7 019/36 477, у 2019 році – 32 358/6 865/36 630, а у 2020 році – 26 830/7 399/50 942.

Також простежується тенденція до зменшення кількості кредитних спілок в Україні. У 2015 році в Україні було зареєстровано 588 кредитних спілок, у 2016 році – 462, у 2017 році – 378, у 2018 році – 358, у 2019 році – 337, а у 2020 році – 327.

В Україні зараз шахрайство демонструє значний розгір, адаптуючись до змінюваних видів і методів своєї діяльності. Економічні зміни в суспільстві та розвиток ринкових відносин зробили фінансову сферу, включаючи інвестиції, страхування та банківську справу, уразливою до шахрайських атак. Згідно з визначеннями, шахрайство це заволодіння майном або правами на майно через обман чи зловживання довірою. Слово "шахрайство" має іноземні коріння: від польського "szachrajstwo", німецького "schachern", що означає торгівля, і від давньоєврейського "sahar", що означає ремесло мандрівного торговця.

Фінансове шахрайство – це кримінальна діяльність, що передбачає незаконне збагачення шахрая за рахунок збитків жертви. Основні чинники, що сприяють розвитку шахрайства, включають довіру, бажання легкого збагачення, низьку фінансову грамотність, небажання займатися вивченням фінансових

питань, розмаїття фінансових інструментів, збільшення обсягу фінансових транзакцій, та відсутність кордонів в умовах глобалізації. Ці фактори створюють сприятливе середовище для зростання транснаціональної фінансової злочинності. Довірливі інвестори часто опиняються у фінансових пастках, шукаючи зберегти чи збільшити свої кошти.

Шахрайство є результатом впливу економічних, політичних та психологічних чинників, що стимулюють громадян до пошуку простих способів заробітку та реалізації шахрайських схем. В Україні за шахрайство передбачена адміністративна відповідальність у випадку дрібних правопорушень та кримінальна відповідальність за вчинення шахрайства у великому розмірі. Покарання може варіюватися від штрафу у розмірі 30 неоподатковуваних мінімумів доходів громадян (510 грн станом на 1 січня 2019 року) до 12 років позбавлення волі з конфіскацією майна.

З початку 21 століття Інтернет став невід'ємною частиною повсякденного життя, зі зростанням популярності соціальних мереж, онлайн-магазинів та інших цифрових послуг. Ці платформи пропонують більш доступні ціни порівняно з традиційними магазинами, великий вибір товарів, включно з ексклюзивними та тими, що не доступні в звичайній торгівлі, та зручність оплати через електронні платіжні системи.

Однак, інтернет також став ареною для шахрайських дій. Через свою велику відкритість та мінімальний контроль з боку правоохоронних органів, Інтернет приваблює зловмисників, які використовують різні методи обману для заволодіння чужим майном. Шахраї експлуатують людські емоції, такі як бажання допомогти, економити, або отримати щось безкоштовно, для маніпулювання жертвами та уникнення відповідальності завдяки анонімності, яку надає інтернет.

Кількість шахрайських схем в інтернеті щодня зростає, та складно визначити точну кількість таких методів, оскільки злочинці постійно адаптують та удосконалюють свої підходи для введення в оману нічого не підозрюючих користувачів.

Способи протидії фінансовому шахрайству щодо фізичних осіб

Фінансова піраміда

Фінансові піраміди обіцяють високі доходи з мінімальними вкладеннями, але фактично виплати здійснюються за рахунок нових вкладників. Способи протидії:

- Перевірка інформації: Ретельно перевіряйте компанію, в яку плануєте інвестувати. Дізнавайтеся про історію, ліцензії та відгуки.
- Уважність до умов: Ставтеся скептично до обіцянок високих доходів за короткий час без ризику.
- Знання законодавства: Ознайомтеся з законодавством щодо інвестицій та фінансових ринків.
- Консультація з експертами: Перед інвестуванням радьтеся з фінансовими консультантами.

Інтернет-шахрайство

Інтернет-шахраї використовують різні методи для обману, зокрема фішинг, підроблені інтернет-магазини та інші методи. Способи протидії:

- Безпека онлайн-платежів: Використовуйте лише перевірені платіжні системи та сайти.
- Перевірка достовірності: Перевіряйте інформацію про продавця або сайт перед покупкою.
- Захист персональних даних: Не розголошуйте особисті дані на неперевірених сайтах.

Шахрайство з платіжними картками

Це вид шахрайства, де шахраї отримують доступ до вашої платіжної картки та знімають кошти. Способи протидії:

- Не розголошуйте PIN-код: Не повідомляйте PIN-код картки третім особам.
- Безпечне зберігання: Не зберігайте PIN-код разом із карткою.
- SMS-сповіщення: Підключіть SMS-сповіщення про операції за карткою.

- Використання надійних банкоматів: Використовуйте банкомати у перевірених місцях, перевіряйте їх на наявність сторонніх пристроїв.

Мобільне шахрайство

Шахраї використовують мобільні пристрої для отримання доступу до персональних даних. Способи протидії:

- Перевірка інформації: Перевіряйте достовірність інформації, отриманої через SMS або дзвінки.
- Захист телефону: Використовуйте антивірусне програмне забезпечення на мобільному пристрої.
- Блокування SIM-карти: У разі втрати телефону негайно заблокуйте SIM-карту.

Найпоширеніші способи фінансового шахрайства

Крадіжка персональних даних

Шахраї використовують різні методи для отримання доступу до персональних даних, які можуть бути використані для крадіжки грошей. Методи протидії:

1. Фізичні методи крадіжки персональних даних

- Крадіжка картки: Завжди тримайте картку при собі і не залишайте без нагляду.
- Скімінг: Перевіряйте банкомати на наявність сторонніх пристроїв.
- Шимінг: Уважно перевіряйте пристрої для зчитування карток перед використанням.

2. Крадіжки персональних даних в онлайн

- Фармінг: Перевіряйте правильність URL перед введенням особистих даних.
- Хакерство: Використовуйте складні паролі та двофакторну аутентифікацію.

3. Соціальні методи крадіжки персональних даних

- Фішинг: Не відкривайте підозрілі посилання та не вводьте особисті дані на неперевірених сайтах.

- Вішинг: Не надавайте особисті дані під час телефонних дзвінків від невідомих осіб.
- SMS-фішинг: Не переходьте за посиланнями в підозрілих SMS.

Фінансове шахрайство є поширеним явищем, проте дотримання простих правил безпеки, обізнаність та скептицизм можуть значно знизити ризики стати жертвою шахраїв. Завжди перевіряйте інформацію, дотримуйтеся правил безпеки та консультуйтеся з експертами у разі сумнівів.

Для характеристики шахрайства важливе значення має суб'єктивна сторона вчинення злочину. Це Внутрішня, психічна діяльність особи, яка відображає її свідоме ставлення та волю до суспільно небезпечного діяння, включає ставлення до самого діяння та його наслідків. Вина при вчиненні шахрайства характеризується прямим умислом, що складається з двох елементів: інтелектуального та вольового. Інтелектуальний момент включає усвідомлення суспільно небезпечного характеру діяння та передбачення його наслідків. Вольовий момент характеризується бажанням настання суспільно небезпечних наслідків, які передбачає винна особа.

За І. О. Сухорадою, найпоширенішим способом шахрайства з фінансовими ресурсами є надання завідомо неправдивої інформації. Це може включати передачу уповноваженим підрозділам банку або державним органам документів, що містять неправдиву інформацію про фінансово-господарську діяльність.

Відповідальність за шахрайство

Шахрайство, тобто заволодіння чужим майном або набуття права на майно шляхом обману чи зловживання довірою, тягне за собою кримінальну відповідальність. Основні санкції включають:

- Штраф, громадські чи виправні роботи, пробаційний нагляд або обмеження волі до 3 років.
- За шахрайство, вчинене повторно, за попередньою змовою групою осіб, або яке завдало значної шкоди потерпілому: обмеження волі до 5 років або позбавлення волі до 3 років.

- За шахрайство в умовах воєнного чи надзвичайного стану, що завдало значної шкоди потерпілому: штраф або позбавлення волі від 3 до 5 років.
- За шахрайство у великих розмірах або з використанням електронно-обчислювальної техніки: позбавлення волі від 3 до 8 років.
- За шахрайство в особливо великих розмірах або організованою групою: позбавлення волі від 5 до 12 років з конфіскацією майна.

Таким чином, санкції за шахрайство є досить суворими, але притягнення зловмисників до відповідальності може бути складним процесом.

## 1.2 Типи та способи шахрайства

Сьогодні неможливо уявити наші повсякденні ритми без Інтернету, який глибоко інтегрувався у всі аспекти життя. Він дозволяє замовляти їжу, купувати товари, сплачувати рахунки та навіть працювати з дому. Проте, з поширенням цифрових технологій, зросла і кількість інтернет-шахрайств.

Шахрайство у мережі охоплює велике розмаїття дій: від фінансових махінацій до крадіжки особистих даних. Відповідно до статті 190 Кримінального кодексу України, шахрайство визначається як заволодіння чужим майном або набуття права на майно через обман або зловживання довірою. Якщо такі дії здійснені з використанням електронних засобів або великих розмірів, вони караються від трьох до восьми років позбавлення волі.

Один з типів інтернет-шахрайства, фішинг, спрямований на викрадення персональних даних. Шахраї створюють підроблені запити на дані, які виглядають достовірно, і направляють жертв на фальшиві сайти, що імітують законні інтернет-платформи. На таких сторінках вас можуть попросити ввести особисту інформацію або банківські дані. Жертви, які вводять свої дані на таких сайтах, часто стикаються з втратою грошей та зловживанням своєї ідентичності.

Тому надзвичайно важливо завжди перевіряти легітимність веб-сторінки перед введенням будь-яких конфіденційних даних і використовувати заходи

безпеки, такі як надійні паролі та двофакторну аутентифікацію, щоб захистити свою особисту інформацію від шахраїв.

Фальшиві рекламації у соціальних мережах про отримання соціальних виплат від імені ПРООН та інших глобальних організацій є яскравим прикладом інтернет-шахрайства. Шахраї запрошують перейти за посиланням і ввести дані для доступу до онлайн-банківських сервісів, використовуючи їх для викрадення коштів. Такі дії призводять користувачів на підроблені вебсайти, які імітують інтерфейси українських банків, де вони розкривають свою конфіденційну інформацію.

Найефективніший спосіб уникнути фішингових атак — уникати переходу за сумнівними посиланнями в електронних листах, текстових повідомленнях або на соціальних мережах, особливо якщо вас просять ввести конфіденційну інформацію. Переконайтеся, що ви перебуваєте на легітимному сайті перед введенням особистих даних і негайно заблокуйте свою банківську картку, якщо помилково ввели дані на підозрілій сторінці.

Інші різновиди онлайн-шахрайства включають крадіжку особистих даних з метою використання їх для незаконних фінансових операцій, таких як відкриття банківських рахунків, оформлення кредитів або замовлення товарів без відома жертви. Зазвичай жертви дізнаються про це після того, як шахраї вже вчинили покупки або інші дії за їх ім'ям.

Для захисту від крадіжки особистих даних необхідно користуватися складними паролями, активувати двофакторну автентифікацію там, де це можливо, і ніколи не ділитися конфіденційною інформацією по телефону або через інтернет без перевірки. Також рекомендується встановити ліміти на онлайн-транзакції та активувати сповіщення про фінансові операції.

Новітні шахрайські схеми можуть включати дистанційну заміну SIM-карток для доступу до фінансових номерів і незаконного вилучення коштів. Шахраї часто використовують переконливі дзвінки для маніпуляції жертвами, спонукаючи їх до зміни налаштувань або відновлення SIM-карток, що може призвести до фінансових втрат.

З розвитком інтернет-технологій часто люди стають жертвами інтернет-шахраїв. Анонімність та вигадливість шахраїв, а також довірливість користувачів підживлюють цей "бізнес". Представляємо вашій увазі 5 найпоширеніших видів інтернет-шахрайства:

1. Шахрайства, пов'язані з покупками через мережу Інтернет

Однією з найпоширеніших схем шахрайства є продаж товарів за дуже низькими цінами. Продавець, зазвичай, вимагає передоплату, відмовляючись від оплати при отриманні. Оплативши товар, покупець часто залишається ні з чим. Рекомендація: Вносіть передоплату лише перевіреним продавцям, з іншими оплачуйте товар після отримання.

2. Шахрайства, пов'язані з продажами через мережу Інтернет

При продажу товарів через інтернет, шахраї можуть намагатися отримати дані вашої платіжної картки під приводом оплати товару. Це дозволяє їм знімати гроші з вашого рахунку. Рекомендація: Для оплати на вашу картку достатньо знати лише номер з 16 цифр. Ніколи не повідомляйте строк дії картки та CVV код. Не надавайте жодних даних з СМС повідомлень, які надходять на вашу картку, та не виконуйте операції в банкоматі на вимогу незнайомців.

3. Віруси-шифрувальники та інше шкідливе програмне забезпечення

Розповсюдження комп'ютерних вірусів, зокрема вірусів-шифрувальників, є серйозною проблемою. Після зараження такі віруси шифрують файли, і відновити їх неможливо навіть за допомогою антивірусу. Найчастіше вони розповсюджуються через електронну пошту. Рекомендація: Використовуйте надійне антивірусне програмне забезпечення, не відкривайте електронні листи та посилання від невідомих відправників, зберігайте копії важливих даних на різних носіях (флеш-накопичувачах, інтернет-сховищах тощо).

4. Фішинг

Фішинг полягає у спробах шахраїв отримати особисту інформацію через підроблені сайти або повідомлення. Шахраї створюють фальшиві вебсторінки, схожі на офіційні, і запрошують користувачів ввести свої дані. Рекомендація: Не натискайте на підозрілі посилання, перевіряйте адреси сайтів, на яких вводите

конфіденційну інформацію, використовуйте надійні паролі та двофакторну аутентифікацію.

5. Шахрайства з SIM-картками

Шахраї можуть отримати доступ до вашого телефонного номера через віддалену заміну SIM-картки, що дозволяє їм отримати доступ до ваших банківських рахунків. Вони телефонують від імені організації і просять вас перетелефонувати, після чого замовляють відновлення SIM-картки, використовуючи для ідентифікації ваш останній дзвінок. Рекомендація: Будьте обережні з запитами на зміну SIM-картки, перевіряйте достовірність інформації від оператора та регулярно перевіряйте стан своїх фінансових рахунків.

6. Інтернет-жебрацтво

В Інтернеті можуть з'являтися оголошення від благодійних організацій, притулків, батьків з проханням про матеріальну допомогу на лікування хворих дітей. Шахраї вигадують історії про хвороби, використовуючи фотографії чужих дітей, або створюють фальшиві оголошення, що копіюють справжні благодійні організації, змінюючи лише реквізити для перерахування грошей. Рекомендація: Перед тим, як зробити пожертву, зв'яжіться з організацією безпосередньо, перевірте реквізити або відвідайте її особисто, щоб переконатися в достовірності розміщеної інформації.

7. Виграш цінного призу

У соціальних мережах поширені підроблені лотереї з привабливими призами. Ви можете отримати повідомлення про те, що виграли приз, але щоб його отримати, необхідно сплатити за доставку, мито або комісію. Сума, яку просять оплатити, зазвичай мала, але після оплати приз так і не буде вам надіслано. Рекомендація: будьте скептичні до таких повідомлень і утримайтесь від будь-яких платежів, поки не переконаєтеся в правдивості інформації.

Інтернет-шахрайство виступає у багатьох формах. Знання про розповсюджені схеми допоможе уникнути пасток та захистити ваші фінанси і особисті дані.

Існує багато шахрайських схем в інтернеті, які дозволяють зловмисникам видурювати гроші у наївних користувачів. Розглянемо деякі з найбільш поширених прикладів і розкриємо, як саме діють шахраї.

Шахрайство при онлайн-покупках товарів. Цей тип шахрайства тісно пов’язаний із бажанням людей купити якісний товар за ціною, нижчою за ринкову. Це часто трапляється в групах та на інтернет-платформах, таких як «барахолка», «куплю-продам», сайт OLX та подібних.

На прикладі студента Євгена, якому знадобився ноутбук для навчання та роботи, ілюструється ризик таких угод. У Євгена було 9000 грн, що не вистачало для покупки нового якісного комп'ютера в магазині, тому він вирішив шукати ноутбук на OLX і знайшов пропозицію від Олега за 8500 грн.

Євген спочатку був насторожений через низьку ціну, але Олег запевнив його, пояснивши, що ноутбук користувався його дочкою всього пару місяців, після чого вона захотіла модель покращену. Олег вирішив продати ноутбук за символічну ціну, щоб він не залишався без використання. Євген був переконаний і згодився на повну передоплату, яку Олег виправдав великою кількістю бажаючих. Одразу після того, як Євген переказав гроші, Олег заблокував його номер, а його сторінка на OLX зникла.

8. Фіктивні інтернет-магазини. Ще один вид шахрайства пов’язаний з підробленими інтернет-магазинами. Вони можуть виглядати дуже переконливо, з великим асортиментом товарів. Але насправді більшість позицій немає в наявності. Такі шахраї встановлюють ціни трохи нижчі за ринкові, але не настільки, щоб викликати підозри у покупців.

Коли довірлива людина оформлює замовлення, з нею зв’язується шахрай, який під будь-яким приводом просить зробити повну або часткову передоплату. Після отримання грошей шахрай зникає, залишаючи покупця без товару.

У обох випадках злочинці демонструють високий рівень маніпуляцій та знання психології, що дозволяє їм переконати жертву здійснити передоплату. Найкращий спосіб уникнути таких шахраїв - ніколи не робити передоплату продавцям, з якими ви ще не мали справ. Завжди скасовуйте замовлення, якщо

продавець наполягає на передоплаті. Порядні продавці завжди пропонують можливість оплати після отримання товару.

9. Шахрайство з пропозицією інтернет-заробітку та допомога у погашенні боргу МФО

Вразливі групи та шахрайські схеми

Люди, які гостро потребують швидкого додаткового заробітку, часто стають жертвами шахраїв. Це можуть бути пенсіонери, старші школярі, студенти, мами в декреті та безробітні. Вони шукають легкі способи заробітку, які не вимагають багато часу та зусиль, такі як розміщення відгуків, рекламних посилань, або набір тексту. Шахраї активно користуються їх вразливістю.

Приклад шахрайства

Дарина, молода мама з дворічною дитиною, вирішила знайти додатковий заробіток. Її увагу привернула пропозиція від Карини, яка представилася як молода мама, що успішно поєднує декрет із добре оплачуваною роботою. Карина виглядала доволі переконливо завдяки своєму Інстаграму, де демонструвала розкішне життя. Вона запропонувала Дарині роботу з просування косметичних продуктів, але для цього потрібно було спершу оплатити навчання, вартість якого складала 800 грн. Дарина, сподіваючись на легкий заробіток, перевела гроші, після чого Карина зникла, заблокувавши Дарину.

Як працюють шахраї

Шахраї, що пропонують роботу в інтернеті, масово розсилають свої "вигідні пропозиції" людям, яких вони вважають найбільш наївними та вразливими. Хоча від цього виду шахрайства страждає менше людей, ніж від шахрайства у сфері інтернет-торгівлі, кількість жертв все одно залишається значною.

Запобіжні заходи

Щоб уникнути подібних ситуацій, слід бути обережним і:

1. Не платити за можливість працювати. Якщо вас просять заплатити за навчання або будь-які інші послуги, це сигнал, що перед вами шахраї.

2. Перевіряти інформацію про роботодавця. Відгуки, реальні контакти та наявність у публічному просторі можуть допомогти перевірити, чи є пропозиція справжньою.
3. Не довіряти блискучим профілям у соцмережах. Вони можуть бути створені для обману.

Пам'ятайте, що реальні роботодавці не вимагатимуть передоплати за можливість працювати, і завжди перевіряйте інформацію перед тим, як робити будь-які фінансові дії.

9. Шахрайство через віруси-шифрувальники і сайти-фальшивки

Віруси-шифрувальники

Розповсюдження комп'ютерних вірусів залишається серйозною загрозою. Найбільш небезпечними є віруси-шифрувальники, які після зараження пристрою шифрують всі дані на ньому. Щоб повернути доступ до інформації, зловмисники вимагають викуп. Щоб уникнути такої ситуації, важливо використовувати ліцензійне програмне забезпечення та не економити на антивірусах.

Сайти-фальшивки. Інший поширений спосіб шахрайства – створення підроблених сайтів, які виглядають як справжні, щоб викрасти персональні дані користувачів, такі як логіни та паролі. Найчастіше шахраї розсилають масові повідомлення від імені банків або відомих брендів, пропонуючи перейти за посиланням, яке майже не відрізняється від справжнього. Перейшовши за таким посиланням, користувач ризикує втратити доступ до своїх фінансових ресурсів.

10. Шахрайство з ботами для знайомств

З початком пандемії кількість шахрайських схем у додатках для знайомств значно зросла. Обмеження на пересування стали зручним виправданням для шахраїв, щоб пояснити, чому вони не можуть зустрітися з жертвами в реальному житті.

Боти також використовуються для обману користувачів додатків для знайомств. Вони можуть виконувати декілька функцій, спрямованих на виманювання грошей або персональних даних:

1. Розсилка спаму: Боти можуть надсилати масові повідомлення, що містять шкідливі посилання або рекламу фальшивих товарів та послуг.

2. Фальшиві профілі: Боти створюють профілі, які імітують реальних користувачів, залучаючи жертв до спілкування. Після встановлення контакту бот може перенаправляти користувача на платні сервіси або спробувати отримати особисту інформацію.

3. Платні підписки: Деякі боти можуть змусити користувача підписатися на платні сервіси, обіцяючи ексклюзивний контент або доступ до «преміум» функцій. У результаті користувач втрачає гроші, отримуючи натомість нікчемний або навіть шкідливий контент.

Романтичні шахрайства

Одним із найбільш поширених видів шахрайства у додатках для знайомств є романтичні шахрайства. Зловмисники створюють фальшиві профілі, щоб завоювати довіру та симпатію жертви, а потім починають вимагати гроші на різні нагальні потреби. З початком повномасштабної війни в Україні шахраї адаптували свої схеми, використовуючи воєнні обставини як виправдання для вимагання грошей.

Схема шахрайства

Основна схема романтичного шахрайства полягає в тому, щоб змусити жертву повірити у серйозність стосунків з перспективою шлюбу. Потім шахрай використовує цю ілюзію для виманювання грошей або особистої інформації, яка допоможе йому отримати доступ до фінансів жертви. Шахраї можуть бути як реальними людьми зі справжніми фотографіями та відеоспілкуванням, так і ботами, що використовують чужі зображення і вигадують причини для уникнення особистих зустрічей.

Червоні прапорці

Основний сигнал для настороженості — розмова про гроші. Ніколи не переказуйте гроші своїм романтичним знайомим, навіть якщо сума здається незначною. Це може бути способом викликати довіру, щоб згодом вимагати більші суми. Шахраї можуть спочатку позичати невеликі суми і швидко їх

повертати, а потім просити значніші кошти, які вони обіцяють повернути, але цього не станеться.

Також небезпечно погоджуватися на отримання грошей від незнайомців. Це може викликати почуття зобов'язаності, і коли шахрай опиниться у скрутному становищі, ви відчуєте моральний тиск допомогти. Крім того, для переказу грошей шахрай може запитувати банківську інформацію, що створює додаткову загрозу для вашого рахунку.

Шахрайство з використанням ботів

Боти в додатках для знайомств також становлять небезпеку. Вони можуть виконувати різні функції для обману користувачів:

1. Розсилка спаму: Боти можуть надсилати масові повідомлення з шкідливими посиланнями або рекламуючи фальшиві товари та послуги.

2. Фальшиві профілі: Боти створюють профілі, що імітують реальних користувачів, залучаючи жертв до спілкування, а потім перенаправляють їх на платні сервіси або намагаються отримати особисту інформацію.

3. Платні підписки: Боти можуть змусити користувача підписатися на платні сервіси, обіцяючи ексклюзивний контент або доступ до «преміум» функцій.

Як уникнути шахрайства

1. Будьте уважні до нових знайомств: Якщо хтось занадто швидко стає близьким або починає просити гроші, це має викликати підозру.

2. Не переходьте за підозрілими посиланнями: Не клікайте на посилання, надіслані новими знайомими, особливо якщо вони ведуть на зовнішні сайти.

3. Перевіряйте фотографії та профілі: Використовуйте пошук за зображеннями, щоб перевірити, чи не використовувалися фотографії в інших місцях.

4. Завжди зберігайте пильність: Якщо щось здається підозрілим, краще перестрахуватися і не продовжувати спілкування.

Шахрайства у додатках для знайомств можуть бути дуже складними і вишуканими. Зловмисники використовують психологічні прийоми, щоб викликати довіру та маніпулювати емоціями жертв.

Висновки до розділу 1

Треба розуміти критичну важливість розуміння сучасних методів шахрайства та необхідності адаптації інструментів для їх виявлення та протидії. Шахрайство, яке постійно еволюціонує завдяки технологічному прогресу, вимагає від професіоналів у галузі кібербезпеки не лише вдосконалення засобів захисту, але й глибокого розуміння типів і методів шахрайської діяльності. Це має не тільки фінансові наслідки для жертв, але й суттєвий вплив на суспільну довіру до цифрових економічних систем, що підкреслює важливість ефективної протидії кіберзлочинності.

# 2 ДОСЛІДЖЕННЯ ОНЛАЙН-СПОСОБІВ ШАХРАЙСТВА

## 2.1 Шахрайство в сфері онлайн-продаж

У сучасні часи інтернет став есенційним інструментом для ведення бізнесу, що базується на принципах мережевої економіки. Ця мережа забезпечує виконання всіх бізнес-потреб, включно з продажем і покупкою товарів. Інтернет дозволяє користувачам проводити необхідні транзакції, як для особистих, так і для бізнес потреб, та купувати різноманітні товари. Інтеграція нових комунікаційних технологій у комерційну діяльність і повсякденне життя призвела до появи таких нових економічних понять, як «електронна комерція» та «електронна торгівля», які розглядаються сьогодні з різних перспектив: економічної, соціальної та правової.

Електронна комерція включає в себе відносини, спрямовані на здобуття прибутку, які виникають у процесі здійснення дистанційних правочинів. Ці правочини стосуються набуття, зміни чи припинення цивільних прав та обов'язків за допомогою інформаційно-телекомунікаційних систем, що веде до виникнення майнових прав та обов'язків у учасників цих відносин.

Електронна торгівля представляє собою господарську діяльність, зосереджену на електронній купівлі-продажу та дистанційній реалізації товарів, що відбувається за допомогою електронних транзакцій та використання інформаційно-телекомунікаційних систем. Три країни – Великобританія, Німеччина та Франція – забезпечують 81,5% всіх онлайн-продажів у Європі, демонструючи стійке зростання цього показника.

Інтернет-мережа України включає понад 20 мільйонів користувачів, що підкреслює її значний вплив на ринок. Електронна комерція в Україні почала розвиватися з 2000 року, ініційована платіжними системами та банками, а згодом на ринок увійшли платіжні шлюзи. Ці посередники сприяли розвитку вітчизняної електронної комерції, залучаючи нові інтернет-магазини та послуги, такі як оплата за мобільний зв'язок, телебачення, інтернет та навіть дитячі садки.

На сучасному етапі інтернет перетворився на потужний інструмент ведення бізнесу, заснованого на принципах мережевої економіки. Ця мережа задовольняє всі потреби бізнесу, включаючи реалізацію та придбання товарів. Завдяки інтернету людина може здійснювати необхідні розрахункові операції як для побутових, так і для комерційних потреб, а також купувати різноманітні товари. Використання новітніх комунікацій та технологій у комерційній діяльності та повсякденному житті призвело до виникнення таких нових економічних понять, як «електронна комерція» та «електронна торгівля». Ці терміни розглядаються сьогодні з різних позицій – економічних, соціальних та правових.

Електронна комерція охоплює ділові взаємодії, націлені на прибуток, які відбуваються при укладенні угод на отримання, зміну чи припинення майнових прав і обов'язків за допомогою дистанційних засобів з використанням інформаційно-комунікаційних технологій, створюючи таким чином майнові права та обов'язки для її учасників. Електронна торгівля становить господарську діяльність, яка полягає в купівлі-продажу товарів за допомогою інтернету, де транзакції виконуються дистанційно через електронні системи.

Взаємодія між суб'єктами електронного бізнесу відбувається між чотирма основними групами:

Клієнти – споживачі товарів або послуг.

Бізнес-організації – підприємства, що здійснюють свою діяльність за допомогою інформаційних мереж.

Фінансові установи – організації, які надають послуги, пов'язані з фінансовими потоками, такі як банки.

Уряд регулює ведення електронного бізнесу, встановлюючи правила та здійснюючи загальний нагляд за цією діяльністю.

Ось деякі поширені види шахрайства в інтернеті під час покупки товарів або послуг:

1. Фейкові оголошення: Продавець вимагає передоплату за товар, а після отримання грошей зникає, не відправляючи товар.

2. Шахрайство з картковими рахунками: Шахраї просять переказати кошти на картковий рахунок і в ході цього отримують доступ до персональних даних клієнта, що дозволяє їм зняти кошти.

3. Фальшиві інтернет-магазини: Шахраї створюють онлайн-магазини або імітації вже існуючих сайтів, продають неіснуючі товари за передоплату і зникають після отримання грошей.

4. Завищена вартість доставки: Продавці завищують вартість доставки, іноді перевищуючи вартість самого товару, а товар, який відправляють, може бути низької якості або пошкоджений, без можливості повернення.

5. Інтернет-аукціони: Товар продають кільком покупцям одночасно, обіцяючи, що товар отримає той, хто запропонує найвищу ціну, але гроші інших покупців не повертають.

6. Пропозиція передоплати: Клієнтів просять зробити передоплату з обіцянкою приїзду представника для укладання офіційного договору. Після отримання авансу компанія зникає, а договір не передбачає повернення коштів.

Деклінування моральних стандартів і поведінкових норм у суспільстві, на робочому місці та в домашньому житті вважається одним із чинників, що сприяють розповсюдженню корупції та шахрайства. Внаслідок зниження цих стандартів, люди стають менш чутливими до сорому за непристойну поведінку та втрачають почуття вини за свої дії, що може спричинити зростання шахрайських операцій, особливо під час фінансових криз.

Для вдосконалення відносин, які виникають у процесі ведення бізнесу з використанням інтернету, необхідно:

1. **Визначення та законодавче закріплення термінів**:

- «віртуальний простір»;
- «інтернет-суспільство»;
- «інтернет-відносини»;
- «інтернет-злочинність» [2].

2. Актуалізація законодавчих актів, які регулюють інтернет-відносини, що дозволить краще захищати права та інтереси громадян у цифровому просторі.

3. Законодавче уточнення категорій інформаційних прав користувачів на платформах інтернет-магазинів, а також аналіз характеристик і особливостей застосування юридичних положень, які регламентують поведінку користувачів цих платформ в Україні.

4. Встановлення меж державного втручання у суспільні відносини, пов'язані з використанням інтернет-магазинів, для забезпечення балансу між регулюванням та свободою користувачів.

5. Розширення кримінальної відповідальності за злочини, вчинені в інтернет-магазинах, щоб забезпечити адекватну відповідальність за протиправні дії у віртуальному просторі.

6. Посилення відповідальності адміністраторів баз даних та інших осіб, які забезпечують експлуатацію комп'ютерних інформаційних систем, для запобігання витокам даних та зловживанням.

Ці заходи сприятимуть створенню більш безпечного та регульованого інтернет-середовища, захищатимуть права користувачів та забезпечать надійність ведення бізнесу в цифровій епосі.

## 2.2 Банківське шахрайство в онлайн-банкінгах

Виявлення шахрайства стає дедалі більшою проблемою в епоху цифрових технологій. З появою різноманітних форм банківських операцій, таких як інтернет-банкінг, мобільний банкінг та телефонний банкінг, ризики пов’язані з шахрайством зросли значно. Шахрайські операції, особливо з використанням банківських карток, можуть серйозно гальмувати розвиток онлайн-бізнесу, оскільки в результаті шахрайства продавець втрачає і товар, і гроші. Простота придбання товарів онлайн, введення даних карти під час оплати створює можливості для зловмисників використовувати чужі карткові дані, отримані через несанкціонований доступ до банкоматів або через незахищені вебсайти.

Після здійснення шахрайської операції, справжній власник картки зазвичай подає заяву до банку для повернення коштів, списаних без його відома. У випадку, коли шахрайство відбувається через інтернет-магазин, банк-емітент

картки, діючи за дорученням власника, може оскаржити транзакцію, і онлайн-магазин буде зобов'язаний компенсувати повну вартість покупки.

Банківські картки сьогодні є ключовим засобом безготівкових розрахунків у сфері грошового обігу. Їх популярність стрімко зростає, оскільки вони дозволяють клієнтам оплачувати товари та послуги без використання готівки. Банківські картки, які є універсальним міжнародним платіжним засобом, полегшують розрахунки в будь-якій валюті, відкритій на банківському рахунку[1]. Вони також сприяють економії часу та витрат на зберігання, переміщення і конвертацію грошей, дозволяючи швидко отримати доступ до коштів з рахунку. Завдяки широкому використанню в торговельно-сервісних мережах та розширенню онлайн-торгівлі, використання банківських карток стало невід'ємною частиною сучасної економіки[2-3].

Шахрайська транзакція – це несанкціоноване списання коштів з дебетової або кредитної картки клієнта, що може статися через втрату, крадіжку, підробку, неприйняття картки або через шахрайські дії, визначені банком[4-7]. Згідно зі статтею 190 Кримінального кодексу України, шахрайство, яке включає заволодіння майном або придбання права на майно за допомогою обману чи зловживання довірою, особливо якщо воно вчинене у великих розмірах або з використанням електронно-обчислювальної техніки, карається позбавленням волі на термін від трьох до восьми років[8].

У 2016 році VISA та MasterCard впровадили в Україні, як і по всьому світу, принцип нульової відповідальності[9]. Ця політика передбачає, що у випадку доведення факту шахрайства, банки зобов'язані відшкодувати збитки потерпілому власнику картки. Ця міра забезпечує споживачам захист від несанкціонованих транзакцій, однак важливо, що клієнти також знають методи шахрайства та активно діють для їх запобігання.

За інформацією Української міжбанківської асоціації членів платіжних систем, середня сума втрат від платіжного шахрайства знизилася у 2017 році до 145 грн., порівняно з 345 грн. у 2016 році[10]. Таке зниження стало можливим завдяки вдосконаленню банківських систем для виявлення шахрайських дій,

встановленню лімітів на онлайн-платежі та забезпеченню додаткової автентифікації клієнтів[11].

Кількість скіммінгових інцидентів, незважаючи на використання зловмисниками нових мініатюрних пристроїв, що ускладнює їх виявлення на банкоматах, зросла з 71 випадку в 2016 році до 113 у 2017 році[10]. Однак, завдяки встановленню захисних пристроїв та інформуванню громадськості в рамках Національної програми SafeCard, кількість випадків кеш-треппінгу знизилася в чотири рази — з 817 випадків у 2016 році до 191 у 2017 році.

Кількість фішингових сайтів, які незаконно збирають банківські дані, зменшилася: у 2017 році було виявлено та закрито 108 таких ресурсів, порівняно з 174 у 2016 році[10]. Однак це не означає, що проблема зменшилася. Замість цього, шахраї почали створювати більш складні та важкі для виявлення сайти[12].

Значно поширилася практика використання фішингових сайтів для миттєвих переказів грошей, де дані користувача під час операції непомітно змінюються на дані шахрая, що дозволяє вкрасти кошти миттєво[13-14]. Це стало особливо актуальним, оскільки раніше шахраї лише збирали реквізити карток з метою подальшого зняття коштів. У 2017 році таких шахрайських сайтів було зафіксовано понад 25%, що вказує на зростання прямого крадіжки коштів.

Крім того, значна кількість фішингових сайтів почала використовувати SSL сертифікати, які раніше вважалися показником надійності сайту. У 2016 році лише 5% шахрайських ресурсів мали захищене https з'єднання, але цей показник значно зріс[10]. Велика частина шахрайських операцій залишається без покарання, оскільки жертви часто не звертаються за допомогою до правоохоронних органів. Наприклад, за одним випадком шахрайства, що залучав 2600 банківських карток, до поліції звернулися лише 36 власників[10].

За 2017 рік кількість телефонних номерів, що внесені до чорного списку міжбанківської системи обміну даними про інциденти платіжного шахрайства

Exchange-online, зросла в п'ять разів, досягнувши 3430 номерів, з яких шахраї дзвонили та надсилали SMS-повідомлення можливим жертвам.

Фішингові сайти зазвичай центруються навколо тем, які легко привертають увагу користувачів[15], таких як:

- P2P-платежі;
- поповнення мобільного рахунку;
- заробіток за участь у опитуваннях;
- заробіток онлайн;
- отримання кредитів;
- купівля авіаквитків;
- придбання білетів на концерти.

Науковці розрізняють два основних підходи до виявлення шахрайства: наглядова та безконтрольна класифікація[16-17]. Наглядова класифікація вимагає даних про минулі шахрайські та легітимні транзакції і є ефективною для виявлення відомих типів шахрайства, але не може ідентифікувати нові види. Такі методи, як нейронні мережі та байєсівські алгоритми, часто використовуються у цьому контексті, як і аналіз зміщення тренду.

Безконтрольна класифікація базується лише на даних про законні транзакції і показує високу ефективність у виявленні нових типів шахрайства, а також тих, що значно відрізняються від норми. Нормальний стан визначається порівнянням активності клієнта з його попередніми транзакціями або діяльністю інших клієнтів.

Основні проблеми у виявленні шахрайських операцій з банківськими картами включають велику кількість транзакційних даних, де більшість змінних є несуттєвими, і лише малий відсоток операцій (0.1%) становить шахрайство. Шахраї постійно адаптують свої стратегії та технології, що затримує навчання систем. Найважливішим заходом протидії є інформування споживачів про те, як вони можуть захистити себе, а також глибоке розуміння різних видів шахрайства, пов'язаних з дебетовими та кредитними картками.

Існує вісім основних видів шахрайства з банківськими картами[18-19], які включають:

- Загублені чи вкрадені картки – у таких випадках важливо негайно звернутися до банку, аби заблокувати рахунок та мінімізувати можливі збитки.

- Поглинання рахунку – випадок, коли власник картки випадково надає особисту інформацію шахраю, який потім звертається до банку, повідомляє про втрату картки та зміну адреси, отримуючи нову картку на ім'я жертви.

- Підроблені карти – коли шахраї клонують картку для здійснення покупок. Хоча у випадку з новітніми безпековими технологіями, як EMV чіпи, частота таких шахрайств знизилася.

- Картка, яка ніколи не отримана – коли нова або замінена картка викрадається поштою і ніколи не дістається до законного власника[20-21].

- Шахрайське застосування – коли особа використовує чужі дані для отримання кредитної картки.

- Множинний відбиток – коли одна транзакція фіксується кілька разів за допомогою застарілих кредитних карт-машин.

- Продавці, які змовилися – торговці, які співпрацюють із шахраями для обману банківських співробітників.

-Шахрайство через електронну пошту або телефонні замовлення** – яке зараз включає електронну комерцію та становить найбільшу частину всіх випадків шахрайства з платіжними картками, майже три чверті від загальної кількості.

Сектор платежів активно розвиває програми перевірки карт та безпеки, щоб запобігти шахрайствам з транзакціями, що відбуваються онлайн або через поштові та телефонні замовлення[22].

Індустрія платежів активно розвиває нові інновації для боротьби з шахрайством, створюючи безпечне середовище для фінансових операцій. Багато з цих досягнень, таких як голограми, панелі підпису, коди підтвердження та EMV чипи, стали стандартами галузі[23]. Однак, цих заходів недостатньо. Освіта споживачів залишається важливою частиною стратегії захисту інформації про рахунок карткового власника та допомагає банкам та торговельним підприємствам уникнути збитків через шахрайські дії[24].

Загальноприйнята думка, що від інтернет-шахрайства з пластиковими картами страждають переважно покупці, власники карт. Проте, інтернет-магазини стикаються не з меншими проблемами[25]. Шахрайські операції несуть загрозу втрати грошей, клієнтів та репутації для самого продавця. Це особливо небезпечно для торговельно-сервісних підприємств (ТСП), які проводять такі операції, адже в разі заяви власника картки про незаконне списання коштів вони зазнають значних фінансових збитків.

Зазвичай шахрайство відбувається наступним чином: через скіммінг, фішинг або інші протиправні дії власник картки ненавмисно передає зловмисникам свої карткові дані, достатні для здійснення покупки онлайн[26]. Зловмисник виконує покупку і отримує товар або послугу. Після виявлення несанкціонованого списання, власник картки звертається в банк, який видал карту, та ініціює розслідування. У разі підтвердження шахрайства кошти повертаються клієнту, а з ТСП вони списуються. Якщо товар вже був отриманий зловмисником, ТСП зазнає потрійного збитку: повертає кошти власнику картки, втрачає товар та може отримати штраф за виконання шахрайської транзакції.

У найгіршому сценарії, торговці можуть зіткнутися з повною забороною приймати онлайн платежі. Для виявлення та протидії шахрайським операціям використовуються системи антифроду. Антифрод — це система, яка в режимі реального часу моніторить кожен платіж, перевіряючи його через десятки, а іноді й сотні фільтрів, щоб виявити будь-які незвичайні або підозрілі активності[26-29]. Завдання системи полягає у перевірці кожної транзакції, ідентифікації підозрілих моментів і вирішенні, чи відхилити платіж, чи підтвердити його[30].

Система антифроду включає кілька ключових компонентів: автоматичний моніторинг транзакцій з численними параметрами фільтрації, механізми автентифікації власника картки і верифікації карти, а також можливість моніторингу транзакцій вручну для особливо складних випадків. Ці системи розроблені для захисту учасників процесу онлайн-платежів від потенційних шахрайських дій. Схема взаємодії учасників платіжного процесу в інтернеті може бути представлена, як зображено на рисунку 2.1, де суцільні та пунктирні

лінії відображають зв'язки компонентів у режимі реального часу та з часовою затримкою відповідно[26].

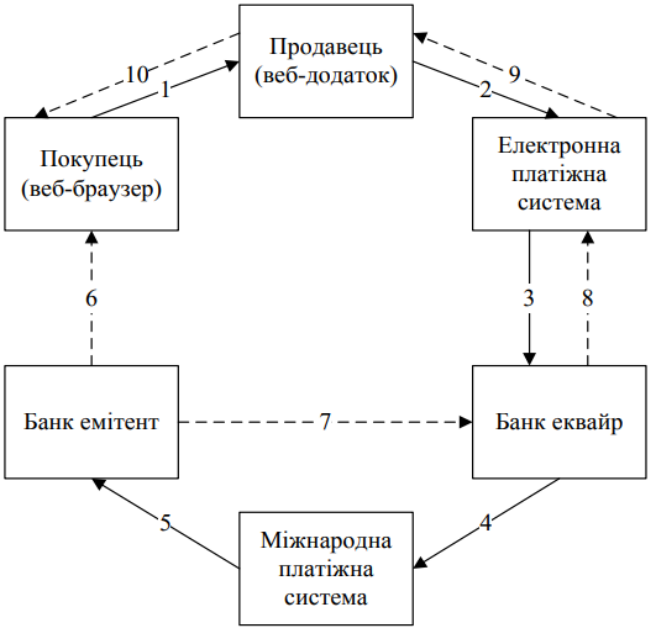



Рисунок 2.1 – Загальний вигляд процесу онлайн-платежів

Залежно від розробника, системи антифроду використовують різноманітні фільтри для ідентифікації шахрайських операцій[28, 31-34]. Ось декілька прикладів:

- Фільтри-валідатори: Наприклад, валідатор реквізитів банківської карти перевіряє номер картки в реальному часі за алгоритмом Луна, щоб засвідчити коректність введеного номеру.

- Географічні фільтри: Ці фільтри аналізують IP-адреси по країнах. Високий рівень скіммінгу та компрометації карток у певних країнах, наприклад у деяких країнах Африки, може зробити платежі з цих регіонів підозрілими.

- Фільтри чорного списку: Карти, що раніше були ідентифіковані як компрометовані або пов'язані з шахрайськими транзакціями, потрапляють в чорний список, і будь-які операції з них автоматично блокуються.

- Фільтри відповідності (збігу) параметрів: Наприклад, відповідність країни IP-адреси платника до країни емітента карти. Невідповідності можуть свідчити про несанкціоноване використання даних карти.

- Фільтри лімітів авторизації: Встановлення максимальних лімітів на суму транзакції або кількість спроб авторизації з однієї IP-адреси або карти допомагає запобігти спробам шахрайства.

Система антифроду виступає як захисний бар'єр, через який має пройти кожна операція. Процес онлайн-платежу, який включає систему антифроду, можна візуалізувати за допомогою схеми, де показано як антифрод система інтегрована в платіжний процес (рисунок 2.2).

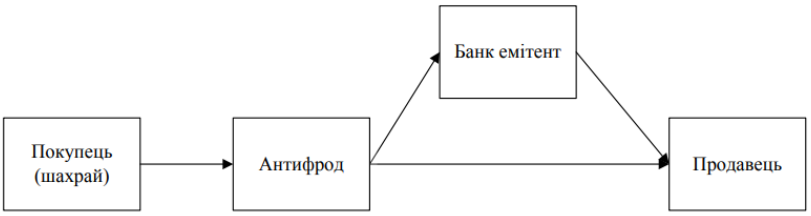



Рисунок 2.2 – Місце антифрод системи в шахрайському процесі онлайн платежу

Коли операція проходить через систему антифроду, дані передаються банку для здійснення переказу коштів до магазину, а також повідомляють продавця про необхідність відправки товару. Якщо платіж не проходить систему, то продавець не отримує замовлення. Системи антифроду можуть включати сотні різних фільтрів, і чим більше бізнес схильний до шахрайських дій, тим більше фільтрів активується, кожен з яких точно налаштований на конкретний інтернет-магазин або онлайн-сервіс[14].

Якщо система антифроду вимкнена або її фільтри неактивні, магазин починає пропускати значно більше шахрайських платежів. Застосування 3-D Secure, де покупець мусить підтвердити платіж одноразовим паролем, що надходить через SMS, може мінімізувати ризики втрат[32]. Однак у випадку великої кількості шахрайських транзакцій, магазин ризикує бути відключеним від платіжної системи, особливо якщо шахрайські транзакції досягають 1-2% від усіх платежів на сайті за певний період, після чого банк-еквайр може заблокувати проведення платежів.

В умовах сучасного ринку важко уявити повне відключення всіх механізмів захисту, адже банки-еквайри та платіжні системи відмовляться співпрацювати з магазином ще на етапі підключення. Активація всіх фільтрів може значно знизити відсоток прийнятих платежів, що може негативно вплинути на деякі бізнеси, як, наприклад, продаж авіаквитків, де обмеження за країнами можуть знизити продажі. Таким чином, максимальна безпека забезпечується за рахунок зниження конверсії в успішні платежі, а розбіжності між країною банку-емітента, сайтом-продавцем та країною проведення онлайн-операції можуть спричинити блокування платежу[14].

Висновки до розділу 2

Описано онлайн-способи шахрайства, зокрема в сферах онлайн-продажів і банківського шахрайства. Розкрито специфіку шахрайства у цих областях та наголошено на потребі розробки цілеспрямованих засобів виявлення та протидії, що враховують особливості кіберпростору. Через зростання числа злочинів, пов’язаних із шахрайством в інтернет-банкінгу та електронною комерцією, виникає необхідність удосконалення законодавчих і технічних інструментів, здатних адекватно реагувати на нові виклики. Розглянуто як методи шахраїв, так і методи їхнього виявлення, акцентуючи на важливості інтеграції новітніх технологій для забезпечення цифрової безпеки споживачів .

# 3 НАПРЯМКИ ВДОСКОНАЛЕННЯ ЗАХИСТУ ВІД СУЧАСНОГО ШАХРАЙСТВА

## 3.1 Огляд існуючих підходів та рішень для виявлення шахрайських транзакцій

Програмні рішення для виявлення шахрайства з кредитними картками розроблені для ідентифікації шахрайських операцій із кредитними та дебетовими картками. Вони використовують машинне навчання та розширену аналітику для аналізу транзакційних даних, виявлення аномалій та шаблонів, які можуть вказувати на шахрайство. Ці інструменти дозволяють фінансовим установам відстежувати транзакції в реальному часі, ідентифікувати підозрілу активність та запобігати здійсненню шахрайських операцій.

Три основні типи систем, які використовуються в цих рішеннях, включають:

Системи на основі правил: Вони працюють на базі заздалегідь встановлених правил для ідентифікації транзакцій, які потенційно можуть бути шахрайськими. Транзакції, які відповідають цим правилам, автоматично відзначаються для додаткової перевірки.

Системи виявлення аномалій: Використовуючи алгоритми машинного навчання, ці системи аналізують історичні дані транзакцій для виявлення відхилень від звичайних моделей, встановлюючи базову лінію нормальної поведінки, з якої будь-яке відхилення вважається підозрілим.

Системи прогнозного моделювання: Використовуючи передову аналітику, ці системи створюють моделі, що дозволяють прогнозувати потенційні шахрайські дії на основі аналізу історичних даних, забезпечуючи сповіщення про можливі шахрайські активності в режимі реального часу.

В 2023 році деякі з найкращих технічних рішень для виявлення шахрайських транзакцій включають Accertify, CybeReady, Cybersource та Ekata. Accertify, розробка American Express, включає комплексні рішення, такі як автентифікація клієнтів і управління поверненням платежів, використовуючи

машинне навчання для аналізу поведінки користувачів і даних пристроїв. CybeReady фокусується на підвищенні безпекової обізнаності через навчальні програми, особливо в таких сферах як фінанси та фармацевтика, зміцнюючи внутрішню культуру безпеки. Cybersource використовує програмне забезпечення Visa Decision Manager для управління платіжним шахрайством, надаючи можливості для використання новітніх платіжних методів з захистом від шахрайства. Ekata пропонує API для підтвердження особи та виявлення шахрайства з глобальним охопленням, що підтримує широкий спектр транзакційних перевірок.

Виявлення шахрайських транзакцій має численні виклики, включаючи необхідність постійного оновлення інструментів для реагування на нові методи шахрайства, проблеми інтеграції з існуючими системами та відповідність нормативним вимогам. Швидкість транзакцій та різноманітність платіжних інструментів також створюють додаткові ризики і можливості для шахраїв, тоді як помилкові спрацювання можуть негативно впливати на досвід користувачів і вартість обслуговування.

## 3.2 Використання спеціальних знань під час розслідування шахрайства, пов’язаного з діяльністю шахрайських транзакцій

Використання спеціальних знань під час розслідування шахрайства, пов’язаного з діяльністю шахрайських транзакцій, є критично важливим для ефективного виявлення, аналізу та попередження фінансових злочинів. Сучасні технології та методи розслідування дозволяють правоохоронним органам, фінансовим установам та приватним детективам значно підвищити ефективність боротьби з шахрайством. Ось деякі ключові аспекти використання спеціальних знань у цій сфері:

1. Фінансовий аналіз та судово-бухгалтерська експертиза

Фінансовий аналіз дозволяє виявити аномальні транзакції та підозрілі фінансові потоки. Судово-бухгалтерська експертиза може допомогти:

- Визначити фальсифікацію бухгалтерських документів.
- Виявити недостовірну звітність та розрахунки.

- Встановити факти приховування доходів та виведення коштів.

2. IT-експертиза та кібербезпека

Сучасне шахрайство часто пов'язане з використанням інформаційних технологій. IT-експерти можуть:

- Відстежити цифрові сліди та встановити джерела шахрайських операцій.
- Аналізувати лог-файли та метадані для виявлення підозрілих дій.
- Розробляти та впроваджувати системи захисту від кібератак.

3. Аналітика великих даних (Big Data) та штучний інтелект (AI)

Використання технологій Big Data та AI допомагає:

- Аналізувати великі обсяги транзакційних даних для виявлення патернів шахрайства.
- Застосовувати машинне навчання для прогнозування майбутніх шахрайських дій.
- Автоматизувати процес моніторингу та аналізу фінансових операцій.

4. Криміналістична психологія

Психологічні методи можуть бути корисними для:

- Встановлення профілів шахраїв та їх мотивів.
- Проведення інтерв'ю та допитів з метою отримання зізнань.
- Аналізу поведінкових патернів, які можуть свідчити про шахрайську діяльність.

5. Правові знання

Розслідування шахрайства вимагає глибоких правових знань для:

- Належного документування доказів для судового переслідування.
- Дотримання законодавства щодо конфіденційності та захисту даних.
- Розуміння нормативно-правових актів, що регулюють фінансову діяльність.

6. Міжнародне співробітництво

Шахрайство часто має транскордонний характер, тому важливо:

- Співпрацювати з міжнародними правоохоронними органами.
- Використовувати інструменти та платформи для обміну інформацією (наприклад, Інтерпол, Європол).
- Розуміти міжнародні стандарти та практики боротьби з фінансовими злочинами.

Приклади застосування спеціальних знань

Case Study 1: Фінансова піраміда

Аналітики фінансових даних виявили підозрілі схеми перерахувань коштів між рахунками, які не мали економічного обґрунтування. ІТ-експерти відстежили IP-адреси та цифрові сліди, що вказували на організаторів піраміди. Психологи допомогли розробити методи допитів, що призвели до зізнань організаторів.

Case Study 2: Кібершахрайство з банківськими картками

Використання технологій штучного інтелекту дозволило банку автоматично ідентифікувати нетипові транзакції та блокувати їх у реальному часі. ІТ-експерти провели форензичний аналіз зламаних систем, виявили шкідливе ПЗ та джерело атаки.

Висновок: Використання спеціальних знань є невід'ємною частиною ефективного розслідування фінансових шахрайств. Синергія різних областей експертизи дозволяє забезпечити всебічний підхід до виявлення, аналізу та запобігання шахрайству, підвищуючи таким чином безпеку фінансових операцій та захист інтересів компаній і громадян.

Висновки до розділу 3

У третьому розділі дипломної роботи аналізуються напрямки вдосконалення захисту від сучасного шахрайства, з акцентом на існуючі підходи та рішення для виявлення шахрайських транзакцій та використання спеціальних знань під час розслідування. Підкреслюється необхідність адаптації традиційних методів безпеки до змінних умов цифрового середовища, з огляду на складність і зростаючу кмітливість шахрайських схем. Рекомендується використання інтегрованих технологічних рішень, що поєднують аналіз даних, штучний інтелект та машинне навчання для

проактивного виявлення та запобігання шахрайству, а також залучення міжнародного досвіду та практик для формування ефективнішої відповіді на кіберзагрози .

# 4 НЕЗАКОННА ДІЯЛЬНІСТЬ КОЛ-ЦЕНТРІВ (ДАЛІ - ОФІСІВ)

## 4.1 Передумови появи великої кількості офісів

Впровадження безготівкових форм розрахунків, поширення фінансових установ, поява нових фінансово-кредитних організацій та активне використання сучасних інформаційних технологій у фінансових операціях призвели до зростання шахрайства та інших незаконних дій у сфері фінансових послуг.

В Україні, зокрема, шахрайство та інші незаконні дії у сфері фінансових послуг, здійснювані з використанням інформаційних технологій, набули професійного, системного та організованого характеру. Серед таких дій можна виділити "фінансові піраміди", шахрайські кол-центри та схеми залучення третіх осіб до незаконної діяльності у сфері фінансових послуг.

Масштаби проблеми

Зіткнувшись з незаконними кол-центрами, Тимчасова слідча комісія (ТСК) виявила, що до цих схем часто залучаються неповнолітні. Кол-центри в Дніпрі стали відомими через дзвінки до Росії, виправдовуючи свої дії боротьбою з "москалями". Проте, за словами народного депутата Максима Бужанського, основними жертвами залишаються українці, зокрема внутрішньо переміщені особи, яких шахраї обманюють, у тому числі й через програми державної підтримки. Представники Кіберполіції підтверджують, що кол-центри часто грабують саме українських громадян.

Географія шахрайства

Дніпро та Кам'янське не єдині міста, де розташовані такі кол-центри. Народний депутат Олександр Куницький зазначає, що кількість таких центрів значно зросла під час війни. За даними ТСК, в Україні діє понад 1500 офісів, які спеціалізуються на обмані та зловживанні довірою громадян. Хоча Дніпро називають "столицею телефонного шахрайства", велика кількість таких центрів зосереджена в Києві, Харкові та інших великих містах. Оголошення про роботу в таких організаціях можна знайти в інтернеті.

Незважаючи на масштаби проблеми, правоохоронні органи часто не поспішають припиняти діяльність кол-центрів, оскільки ці структури часто мають підтримку або "кришування". За словами Бужанського, хоча кількість

таких організацій зросла в чотири рази, у судах наразі розглядаються справи лише на 3,6 мільйона гривень, що є незначною сумою у порівнянні з масштабами шахрайства.

Таким чином, питання боротьби з шахрайством у сфері фінансових послуг в Україні залишається актуальним і потребує більш рішучих дій з боку держави та правоохоронних органів.

Коли шахрайські кол-центри тільки почали з'являтися, вони навіть не приховували свою діяльність: знімали офіси в центрі міст і відкрито демонстрували свою діяльність. Окрім правоохоронців, кол-центри також підтримувалися кримінальними авторитетами. Потік грошей був значний, що дозволяло давати хабарі як правоохоронцям, так і кримінальним структурам. З часом кримінальні авторитети почали самостійно відкривати такі організації, займаючись шахрайським бізнесом напряму.

Приклади шахрайських схем

Наприклад, у 2023 році правоохоронні органи викрили масштабну шахрайську схему, замасковану під діяльність інвестиційного проекту. Внаслідок цього було викрадено активи на загальну суму 40 млн доларів у понад тисячу громадян. Шахраї створюють мережу кол-центрів для здійснення шахрайських дій з використанням інформаційних, електронних комунікаційних систем, обманюючи або зловживаючи довірою громадян для отримання персональних даних та реквізитів банківських карток/рахунків, заволодіваючи їхніми коштами.

Масштаби проблеми

За даними Департаменту кіберполіції, з 2021 по 2023 рік надійшло 7300 звернень громадян щодо онлайн-шахрайства, зокрема, шахрайства, що здійснюється кол-центрами. Однак, це лише невелика частина потерпілих, які вирішили повідомити про незаконну діяльність.

Реакція правоохоронних органів. Офіційні джерела часто повідомляють про викриття шахрайської діяльності у сфері фінансових послуг, таких як фінансові піраміди та кол-центри, а також про заходи для їх локалізації та блокування. Проте масштаби збитків та кількість постраждалих залишаються

значними. Така ситуація вимагає посилення боротьби з шахрайськими схемами на всіх рівнях, підвищення ефективності правоохоронних органів та посилення контролю над фінансовими операціями, щоб запобігти подібним злочинам у майбутньому.

Українське суспільство нагально потребує посилення захисту прав людини та впровадження ефективних механізмів для запобігання маніпуляціям і шахрайству. Важливо забезпечити дієву протидію шахрайству та іншим незаконним діям у сфері фінансових послуг, таких як заборона "фінансових пірамід" та шахрайських "кол-центрів", а також активно боротися з їх організацією.

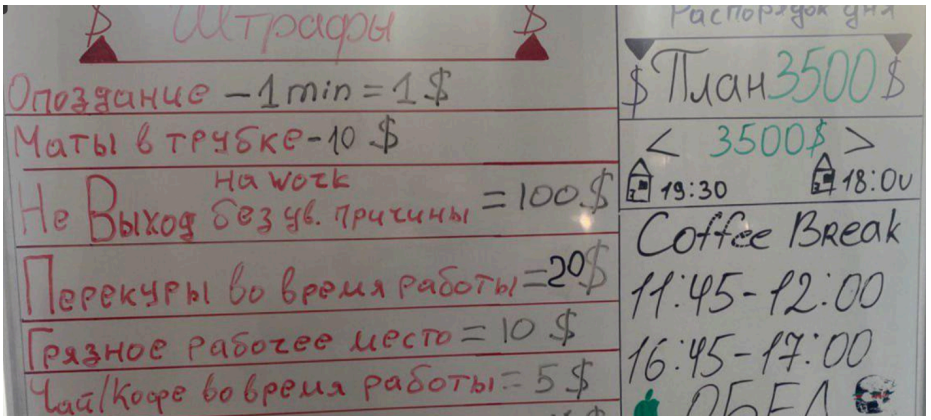



Рисунок 4.1 – Приклади об’яв на дошці задачі в «кол-центрі»

Пропозиція створення Тимчасової слідчої комісії

З метою розслідування незаконної діяльності у сфері фінансових послуг, яка здійснюється з використанням інформаційних, електронних та комунікаційних систем, пропонується створити Тимчасову слідчу комісію Верховної Ради України. Ця комісія буде розслідувати можливі факти шахрайства та інші незаконні дії у фінансовій сфері, використовуючи сучасні інформаційно-комунікаційні технології для виявлення та припинення таких злочинів.

## 4.2 Особливості рекрументу у офіси

В останній час в медіа все частіше згадується збільшена кількість постраждалих громадян від діяльності, що має ознаки "фінансових пірамід", яка

полягає у використанні фінансових інструментів та цивільних прав для створення схеми, обіцяючої значний пасивний дохід в обмін на залучення нових інвесторів. Ця практика також включає залучення та навчання третіх осіб для їх участі в такій незаконній діяльності.

Рекрутинг і навчання

Шахраї часто представляються як відомі та успішні міжнародні форекс брокери або компанії, що працюють у сфері торгівлі акціями та іншими фінансовими інструментами, аби залучити громадян до участі у своїх незаконних схемах. Наприклад, вони активно розміщують оголошення про вакансії на різних платформах, включаючи сайти пошуку роботи та соціальні мережі, та пропонують роботу в сфері інвестицій, використовуючи це як привід для залучення нових жертв.

Якщо ж мова йде про роботу в псевдоінвестиційних компаніях, то оголошення з вакансіями в цій сфері можна побачити всюди: на сайтах з пошуку роботи, у Telegram-каналах, громадському транспорті і просто на електричних стовпах.

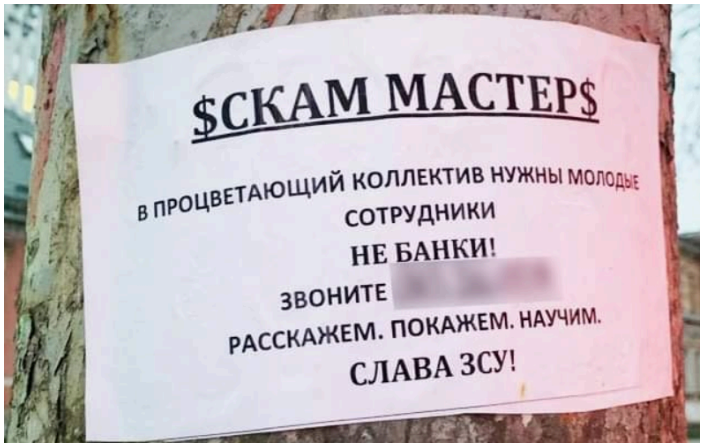



Рисунок 4.2 – Приклад рекрутингу

Ці вакансії приховуються під іншими назвами посад, такими як менеджери з обслуговування клієнтів, спеціалісти з обслуговування vip-клієнтів, адміністратори, менеджери з продажів. Навіть досвід роботи, особливо в фінансовій сфері, не має вирішального значення.

Основними критеріями для успішної співбесіди та отримання роботи є бажання заробляти, енергійність, наполегливість та комунікабельність.

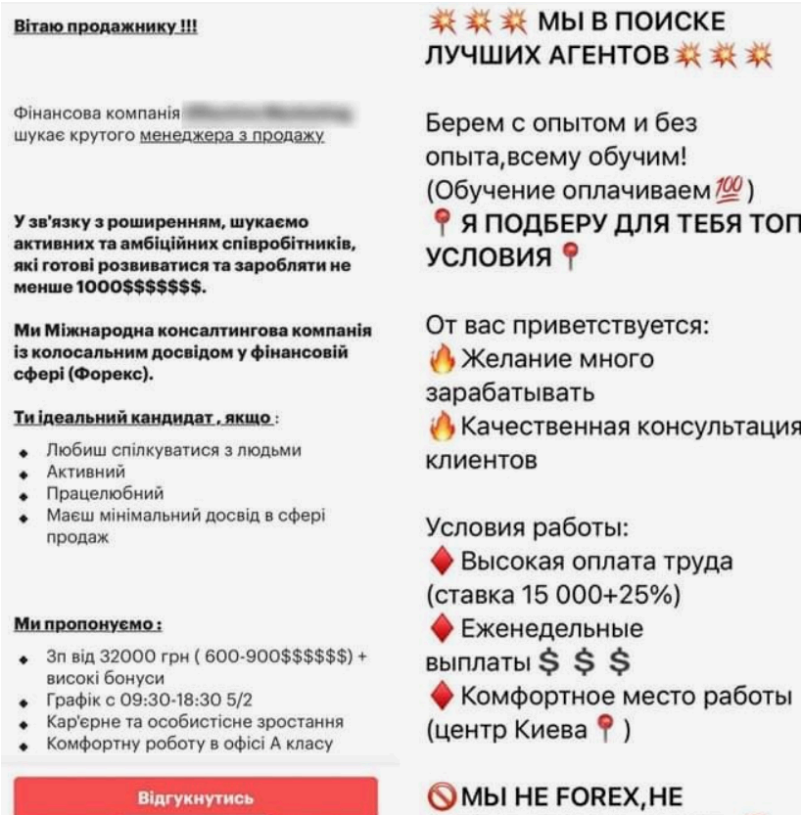



Рисунок 4.3 – Приклад рекрутингу

Після успішного проходження співбесіди з HR-менеджером, кандидат проходить процедуру перевірки, яку здійснює внутрішня служба безпеки компанії. Цей процес передбачає ретельну перевірку документів кандидата, щоб впевнитися в їхній надійності та відсутності будь-яких підозрілих моментів, які могли б вказувати на можливі юридичні або етичні проблеми. Після того, як служба безпеки підтверджує достовірність інформації та відсутність проблем, кандидата запрошують на п'ятиденне навчання.

На курсах зустрічається різноманітна аудиторія до 30 років, які прийшли з різних сфер економіки. Серед них колишні страхові агенти, продавці інтернет-магазинів, пекарі з деокупованих територій, кур'єри піцерій, студенти та арбітражники, що займаються продажем інтернет-трафіку. Це різнобарвне зібрання показує, що компанія відкрита до різних досвідів і бачень, намагаючись знайти унікальні таланти серед широкого спектра кандидатів.

## 4.3 Бізнес-процеси офісів

Співробітники "офісу" займаються виманюванням грошей у росіян, пропонуючи їм заробіток через інвестиції. Схема діє наступним чином:

На першому етапі вони розміщують оголошення на російських вебсайтах та соціальних мережах про можливість заробітку шляхом інвестування у відомі компанії, такі як "Газпром", Socar, Сбєрбанк, "Тинькофф банк". Оголошення ведуть на фальшиві сайти цих компаній, де заманюють заповнити реєстраційну форму із вказанням імені та номера телефону. Особа, яка реєструється, стає новим клієнтом і потрапляє до CRM-системи "офісу", яка фіксує всі контакти та інтеракції з клієнтом.

На другому етапі, продавці комунікують із клієнтами, працюючи над відповідями на їхні заперечення, роблять презентації та намагаються переконати внести стартовий депозит, розмір якого може варіюватися від 50 до 500 доларів.

Третій етап полягає в передачі клієнта більш досвідченому співробітнику, відомому як "клоузер", який має переконати клієнта внести значніші інвестиції. На ділі "клоузер" працює поруч із продавцями і отримує підтримку через навушники.

Клієнти, як правило, вважають, що вони поповнюють свій інвестиційний рахунок через легітимний сайт або додаток, хоча насправді всі транзакції контролюються "офісом". Якщо клієнт передає кошти, робота продавця та "клоузера" завершується.

На четвертому етапі, рет-відділ бере на себе комунікацію, працюючи з клієнтами тривалий час, прикидаючись їхніми фінансовими аналітиками і намагаючись переконати їх у необхідності продати майно або взяти кредит для інвестування. Щоб клієнти не підозрювали шахрайства, їм іноді дозволяють вивести частину коштів, показуючи можливість заробітку значних сум.

Продавці в "офісі" зазвичай працюють стоячи, оскільки це покращує голос і дозволяє зосередитися завдяки гучній музиці. Щодня їм дають контакти десяти осіб, які заповнили форму на сайті, і вони роблять додаткові дзвінки тим, хто раніше відмовився внести депозит. Завдання продавця – переконати близько 250 осіб щомісяця внести стартовий депозит.

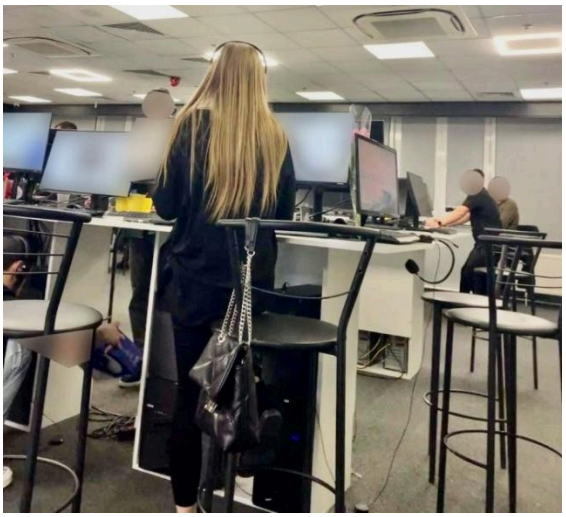


Рисунок 4.4 – Принцип роботи

Оплата праці залежить від бонусів за результати. Наприклад, новий працівник, який протягом місяця залучить п’ять клієнтів, які внесуть стартовий депозит, може заробити між 500 і 600 доларами. Кожен додатковий депозит приносить ще 50-60 доларів. Досвідчені продавці, які залучають десять клієнтів за місяць, можуть заробити від 1,5 до 2 тисяч доларів.

Старші продавці, які демонструють високі результати — приблизно 12 депозитів на місяць протягом двох місяців — можуть зайняти керівні позиції. Наприклад, тимліди, які координують до десяти продавців, заробляють від 2,5 до 3,5 тисяч доларів, залежно від командного результату; клоузери заробляють 2-3 тисячі доларів; а рет-агенти можуть заробляти понад 4 тисячі доларів.

Щодо технічного оснащення, коли "офіс" телефонує клієнту, номер телефону повинен відображатись як російський. Для цього використовують комп'ютери та російські сім-карти. Гроші, які клієнти відправляють, зазвичай потрапляють на рахунки, контрольовані "офісом", такі як криптогаманці або

банківські рахунки в країнах Балтії чи офшорних компаніях на Кіпрі. Після декількох конвертацій кошти потрапляють в Україну у вигляді криптовалюти, де вони обробляються через конвертаційні центри.

## 4.4 Вплив на культуру та збитки

У сучасних умовах воєнного стану в Україні значно активізувались шахрайські операції, особливо у сфері фінансових послуг. Це включає випадки, коли особи шляхом обману передають свої особисті дані або стають жертвами фішингу, що призводить до втрати грошей з їхніх банківських рахунків.

В Україні шахрайство в сфері фінансових послуг часто носить організований характер і включає в себе створення фінансових пірамід та шахрайських кол-центрів, де використовуються сучасні інформаційно-комунікаційні технології для приваблення і навчання нових учасників незаконної діяльності.

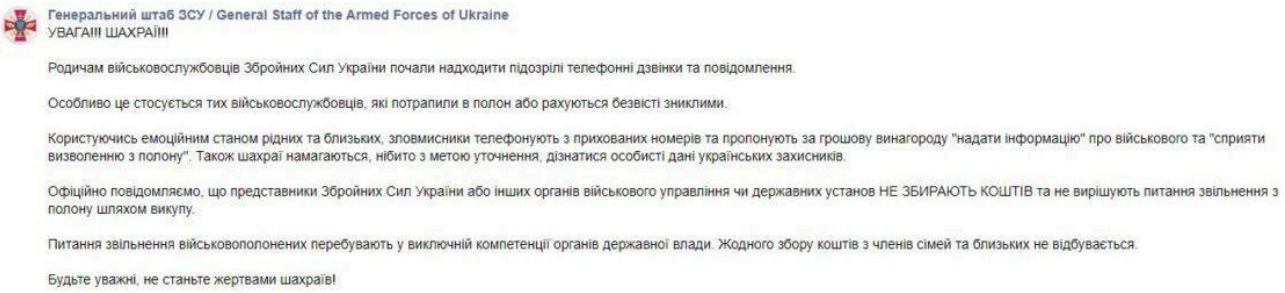
ЗМІ все частіше повідомляють про велику кількість громадян, які стали жертвами фінансових пірамід. Ці схеми базуються на створенні і розвитку системи взаємовідносин між засновниками і інвесторами, де останнім обіцяється значний пасивний дохід. Розмір такого доходу часто залежить від привернення нових інвесторів, що призводить до стійкого росту такої шахрайської діяльності.

Ця процедура включає звернення потерпілої особи до Департаменту кіберполіції Національної поліції України через електронну систему звернень. Тим часом, швидкість відгуку потерпілого до банку та правоохоронних органів, а також їх реакція на крадіжку коштів має критичне значення. Чинний статут 190 "Шахрайство" Кримінального кодексу не дозволяє ефективно запобігати таким злочинам і включає застарілі терміни, як "електронно-обчислювальна техніка", що ускладнює доведення правопорушень правоохоронцями.

Крім того, якщо не доведено обман або зловживання довірою як спосіб отримання майна або прав, це може служити основою для не визнання

винуватості згідно ст. 190 КК України. У відповідь на широко розповсюджену діяльність шахрайських кол-центрів, запропоновано законопроект, який вносить зміни до Кримінального кодексу додавши нову статтю 190-1 "Електронно-комунікаційне шахрайство".

Найбільш цинічною вважається схема, яка використовується проти родичів українських військовослужбовців, зокрема тих, хто вважається полоненими або зниклими безвісти. Використовуючи емоційний стан родичів, зловмисники з невідомих номерів пропонують "надати інформацію" про стан військових і "допомогти в звільненні з полону" за грошову винагороду, а також намагаються витягнути персональні дані для подальшого шахрайства.


Генеральний штаб ЗСУ / General Staff of the Armed Forces of Ukraine
УВАГА!!! ШАХРАЇ!!!

Родичам військовослужбовців Збройних Сил України почали надходити підозрілі телефонні дзвінки та повідомлення.

Особливо це стосується тих військовослужбовців, які потрапили в полон або рахуються безвісті зниклими.

Користуючись емоційним станом рідних та близьких, зловмисники телефонують з прихованих номерів та пропонують за грошову винагороду "надати інформацію" про військового та "сприяти визволенню з полону". Також шахраї намагаються, нібито з метою уточнення, дізнатися особисті дані українських захисників.

Офіційно повідомляємо, що представники Збройних Сил України або інших органів військового управління чи державних установ НЕ ЗБИРАЮТЬ КОШТІВ та не вирішують питання звільнення з полону шляхом викупу.

Питання звільнення військовополонених перебувають у виключній компетенції органів державної влади. Жодного збору коштів з членів сімей та близьких не відбувається.

Будьте уважні, не станьте жертвами шахраїв!

Рисунок 4.5 – Допис з Генерального штабу ЗСУ

Багато родичів морських піхотинців отримували численні повідомлення, що спровокували серйозні занепокоєння навіть у командуванні ВМС. За даними СБУ, вартість пропонованих шахраями "послуг" варіювалась в залежності від емоційного стану родичів. Шахраї вимагали від 10 до 50 тисяч гривень за телефонний дзвінок до полоненого, від 50 до 200 тисяч гривень за його звільнення, а перевезення тіла загиблого коштувало до 10 тисяч гривень.

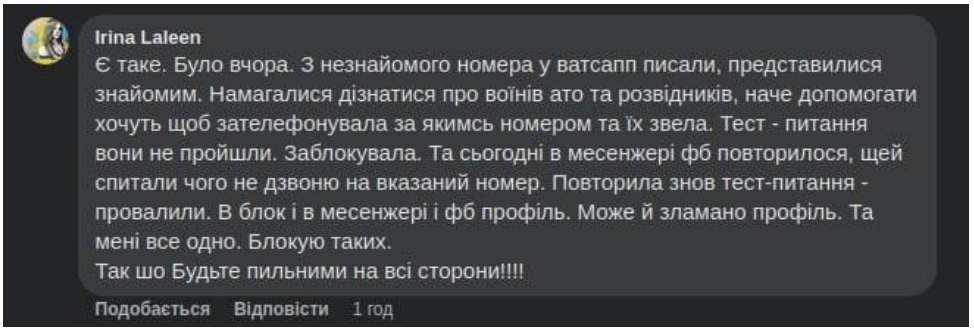

Irina Laleen
Є таке. Було вчора. З незнайомого номера у ватсапп писали, представилися знайомим. Намагалися дізнатися про воїнів ато та розвідників, наче допомогати хочуть щоб зателефонувала за якимсь номером та їх звела. Тест - питання вони не пройшли. Заблокувала. Та сьогодні в месенжері фб повторилося, щей спитали чого не дзвоню на вказаний номер. Повторила знов тест-питання - провалили. В блок і в месенжері і фб профіль. Може й зламано профіль. Та мені все одно. Блокую таких.
Так шо Будьте пильними на всі сторони!!!!
Подобається Відповісти 1 год

Рисунок 4.6 – Допис з мережі Інтернет

**Служба безпеки України** · Подписаться
12 June, 10:00 ·

СБУ заблокувала шахрайську схему «Ваш родич у полоні!»

На Запоріжжі були викриті зловмисники, які телефонували рідним і близьким воїнів ЗСУ та пропонували свою «допомогу» у нібито визволенні їх з полону.

За це шахраї вимагали окрему плату. Розцінки різнилися і в більшості випадків залежали від емоційного стану родичів.

Серед псевдопослуг, які пропонували шахраї:

- телефонна розмова з полоненим, за яку просили від 10 до 50 тисяч гривень;
- визволення з полону, яке оцінили у суму від 50 до 200 тисяч гривень;
- перевезення тіла загиблого - до 10 тисяч гривень.

Звичайно, що жодну з цих міфічних обіцянок зловмисники не могли виконати. А після отримання грошей, які їм пересилали онлайн, - просто зникали зі зв'язку.

Для правдоподібності своїх слів шахраї моніторили інтернет, де збирали дані про безвісті зниклих або загиблих українських бійців та їхні родини.

Організатором схеми виявився чоловік, який наразі перебуває у тимчасово окупованому Маріуполі. Він нещодавно вийшов з тюрми.

Крім того, у Запоріжжі в нього була спільниця, яка відповідала за фінансову складову та забезпечувала мобільні дзвінки, постійно змінюючи номери та операторів зв'язку.

Її затримали спецпризначенці СБУ.

У ході обшуку у підозрюваної вилучено:

- комп'ютерну техніку з доказами протиправної діяльності;
- велику кількість мобільних телефонів і сім-карток;
- банківські картки для отримання платежів;
- чверть мільйона гривень готівкою.

У межах кримінального провадження встановлюються всі потерпілі особи та вживаються заходи для притягнення до відповідальності інших учасників схеми.

❗ Звертаємо Вашу увагу, що питання звільнення військовополонених перебуває у виключній компетенції органів державної влади!

Якщо ви або ваші знайомі потрапили у ситуацію, коли невідомі вимагають гроші за «визволення» родича з полону, негайно звертайтесь до Об'єднаного центру з пошуку та звільнення полонених:

+38 067 650-83-32
+38 098 087-36-01
або на електронну адресу united.centre.ssu@gmail.com



Рисунок 4.7 – Допис з Служби безпеки України

Визначити точну кількість людей, які втратили свої кошти через ці шахрайські операції, та суму, яку заробили організатори цих схем, є надзвичайно складно. Щоб уявити масштаби: у одному лише великому київському "офісі" працює десять рекрутерів, які щоденно мають завербувати щонайменше шість продавців, що в місяць складає приблизно 1,5 тисячі осіб. Використання терміну "великих" пояснюється франчайзинговою моделлю, де велика компанія керує кількома "офісами", отримуючи відсотки від прибутків менших, яким вона надає доступ до своїх баз даних.

Щомісяця, якщо 250 клієнтів внесуть початковий вклад по 200 доларів, сума доходів тільки від таких операцій становитиме близько 50 тисяч доларів. Однак, основний прибуток забезпечують рет-агенти, оскільки, згідно внутрішньої статистики, близько 40% клієнтів, які здійснили початковий внесок, продовжують вносити значно більші суми, що іноді сягає десятків тисяч доларів.

Приблизно сто людей щомісяця залишають у кожному "офісі" близько 8 тисяч доларів, сумарно до 800 тисяч доларів. А враховуючи, що таких "офісів" в Україні може бути понад тисячу, масштаби діяльності вражають.

Хоча "офіси" забезпечують роботою в умовах високого рівня безробіття — 30% в Україні, більшість заробітків йде не на користь країни, а збагачує тих, хто стоїть на чолі цих схем. Це включає діяльність не тільки проти Росії, а й проти ЄС, несплату податків та забезпечення роботою конвертаційних центрів.

Таке шахрайство є лише одним з багатьох способів, яким зловмисники обманюють людей, поряд з іншими схемами, які включають шахрайство з кредитними картками, допомогу ошуканим, або продаж товарів у рази дорожче їх собівартості. Ця проблема стала частиною української реальності та субкультури, обсяг якої можна було б значно зменшити, залежно від дій держави і її правоохоронних органів.

Висновки до розділу 4

Розглянута незаконна діяльність кол-центрів, зокрема механізми їхнього формування, рекрутменту, бізнес-процесів та впливу на культуру та суспільні збитки. Аналіз підкреслює, що шахрайські кол-центри здатні швидко адаптуватися до контрзаходів, використовуючи новітні технології для уникнення виявлення. Наголошується на необхідності комплексного підходу до боротьби з такими центрами, що включає підвищення обізнаності серед населення, розробку більш ефективних правових рамок та міжнародне співробітництво. Важливим є інтеграція зусиль правоохоронних органів різних країн для боротьби з транснаціональними шахрайськими мережами .

## ВИСНОВКИ

Аналіз практичної діяльності свідчить, що всі перераховані види шахрайства через мережу Інтернет є досить поширеними в Україні. Однак, шахрайство, пов'язане з наданням грошей для допомоги, зазвичай здійснюється через телефонну мережу або мережу Інтернет.

Осередки злочинної організації найчастіше організовані в формі офісів – орендовані приміщення, частіше в бізнес-центрах, розташованих в центральних районах міста, які оснащуються комп’ютерною технікою та спеціальними телефонами. Основна та найбільш важлива інформація про функціонування офісу зберігається на віддаленому серверному обладнанні. Інформація про функціонування подібних офісів наявна по всій території України: в Києві, Львові, Дніпрі, Одесі. Також наявна інформація про функціонування подібних офісів в Польщі, Болгарії та Греції.

Правоохоронні органи України значно розширили перелік відомих інтернет-шахрайств, який тепер включає такі види, як SMS-підтвердження реєстрації, що вимагає переказу коштів; продаж «унікальних» методик для різних видів діяльності; обмани в інтернет-казино; шахрайство з лотерейними виграшами; шахрайства в інтернет-магазинах і на соціальних мережах; різноманітні схеми шахрайства з використанням платіжних систем; обмани на договірних спортивних матчах; автосерфінг; обміни валюти і грошей; шахрайство, пов'язане з розповсюдженням оголошень про роботу в інтернеті; збір страхових внесків під виглядом реальної страхової діяльності; шахрайства з приводу отримання будь-яких виграшів; SMS-шахрайство та шахрайство, пов'язане з оголошеннями про втрату документів.

Отже, аналізуючи практику правоохоронних органів України, можна стверджувати, що в кримінальній сфері України поширені різноманітні види інтернет-шахрайства. Зокрема, наступні види шахрайства є найбільш розповсюдженими:

Збір добровільних внесків і благодійних пожертв, особливо для лікування дітей і підтримки учасників АТО.

Використання електронних торгових платформ, таких як «HIFI FORUM», «OLX» і інших.

Пропозиції товарів за акційними цінами або зі значними знижками.

Пропозиції автомобілів на іноземній реєстрації або на замовлення через «сірі» автосалони за привабливими цінами.

Розповсюдження фішингових та вірусних програм.

Продаж товарів через групи в соціальних мережах.

## ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Самойлов С.В. Розслідування шахрайств, учинених із використанням мережі «Інтернет» : автореф. дис. ... канд. юрид. наук : 12.00.09; Донецьк. юрид. ін-т МВС України. Донецьк, 2013. 18 с.

2. Скачко Є.Ю. Топ-5 новин в сфері шахрайства з платіжними інструментами. 26.05.2017. URL: https://pingvin.pro/gadgets/article-gadget/top-5-novyn-v-sferi-shahrajstva-z-platizhnymy-instrumentamy-13.html.

3. Схеми «Out-of-OLX» шахрайства + інфографіка. Український сайт міжбанківської асоціації членів платіжних систем ЄМА. URL: https://www.ema.com.ua/citizens/cyber-safety-school/shemi-out-of-olx-shahrajstva-infografika.

4. Чернявський С.С. Теоретичні та практичні основи методики розслідування фінансового шахрайства : автореф. дис. ... д-ра юрид. наук : 12.00.09. Нац. акад. внутр. справ. Київ, 2015. 21 с.

5. Закон України «Про електронну комерцію» (із змінами і доповненнями, внесеними Законом України від 23 березня 2017 року N 1977-VII). URL : http://search.ligazakon.ua/l_doc2.nsf/link1/T150675.html. 2. Правопорушення в мережі Інтернет. URL : http://dobrobiblio.ucoz.ru/publ/pravoporushennja_v_merezhi_internet/3-1-0-135

6. Шахрайство в інтернеті і як від нього вберегтися / Антикібер. URL : http://anticyber.com.ua/article_detail.php?id=549.

7. Інтернет-шахраї розробили нову схему обману українців / Internetua. URL : http://internetua.com/nternet-shahra--rozrobili-novu-shemu-obmanu-ukra-nc-v.

8. Правові засади електронної комерції в Україні. URL : http://eworks.com.ua/work/4073_Pravovi_zasadi_elektronnoi_komercii_v Ykraini.

9. Annual report: True Cost of Fraud. 2016. URL: https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2016.pdf.

10. Credit Card & Debit Card Fraud Statistics, 2017. URL: https://wallethub.com/edu/credit-debit-card-fraud-statistics/25725/.

11. Fraud Trends 2016. Latest perspectives on international eCommerce fraud. 2016. 19 p. URL: http://www.worldpay.com/sites/default/files/Fraud-trends2016.PDF

12. Preventing money laundering and bank fraud in the banking industry. URL: https://www.aciworldwide.com/-/media/files/collateral/case-studies/ preventing-money-laundering-and-bank-fraud-in-the-banking-industry-cs-us.pdf.

13. Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності : Матеріали Міжнародної науково-практичної конференції (м. Харків, 12 лист. 2014 р.). Харків, 2014. 200 с.

15. Клочко А. М. Злочини у сфері банківської діяльності. Суми, 2014. № 1(10). С. 68-71.

16. Кримінальний кодекс України URL: http://zakon.rada.gov.ua/laws/ show/2341-14 (дата звернення: 28.05.2024).

17. Кібербезпека в Україні: правові та організаційні питання: Матеріали Всеукраїнської науково-практичної конференції (21 жовтня 2016, м. Одеса). Одеса, 2016. 235 с.

18. Статистика платіжного шахрайства – підсумки 2017 року URL: https://ema.com.ua/cyberfraud-ema-statistics-results-2017/ (дата звернення: 28.05.2024).

19. Постанова НБУ № 95 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» від 28.09.2017. 2017. URL: http://zakon3.rada.gov.ua/laws/ show/v009-5500-17 (дата звернення: 28.05.2024).

20. Луговець В. В. Кібернетичні загрози державному сектору економіки. Моделювання та прогнозування економічних процесів: Матеріали X науково-практичної конференції (м. Київ, 7-9 грудня 2016). Київ, 2016. С. 69-72. URL: http://mses.kpi.ua/konfer/37.pdf (дата звернення: 28.05.2024).

21. Baesens B. Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques: A Guide to Data Science for Fraud Detection. 2015. URL: http://www.dataminingapps.com/wp-content/uploads/2015/08/68614_excerpt1.pdf (last accessed: 28.05.2024).

22. Wrobel-Konior S. Payment Trends in 2017: Fighting Fraud Using Machines. URL: https://www.business2community.com/cybersecurity/ paymenttrends-2017-fighting-fraud-using-machines-01690864 (last accessed: 28.05.2024).

23. Ryan C. Hybrid Risk: The truth behind first party fraud. The official site of the company «Experian». 2015. URL: http://www.experian.com/blogs/insights/ 2015/10/hybrid-risk-the-truth-behind-first-party-fraud/ (last accessed: 28.05.2024).

24. Мельник С. І. Організаційно-правове забезпечення системи економічної безпеки банку, 2011. №1. С. 199–206.

25. Изотов Д.С., Быкова Н.Н. Виды мошенничества с банковскими картами. Вестник НГИЭИ. 2015, № 3 (46). С.81-83.

26. Фінагеєв В. О., Чернявський С. С., Татаров О. Ю. Виявлення та розслідування злочинів, пов’язаних з використанням засобів доступу до банківських рахунків. Київ, 2013. 79 с.

27 Яровенко Г. М. Розробка інформаційної моделі виявлення ознак шахрайств у банках. Економічна наука. 2018.№ 14. С. 23-28. URL: http://www.investplan.com.ua/pdf/14_2018/7.pdf (дата звернення: 28.05.2024).