Годнюк Ірина
к.е.н., доцент
Подільський спеціальний навчально-реабілітаційний
соціально-економічний коледж
Вольська Ангелія
к.е.н., доцент
Подільський спеціальний навчально-реабілітаційний
соціально-економічний коледж

ФІНАНСОВЕ ШАХРАЙСТВО, ШЛЯХИ ЗАБЕЗПЕЧЕННЯ ЕФЕКТИВНОГО ФУНКЦІОНУВАННЯ КОМЕРЦІЙНИХ БАНКІВ

У 2020 році через карантинні заходи українці все частіше стали обирати безготівкові платежі, розрахунки та покупки онлайн. Завдяки своєї простоти, масовості, доступності технологій, операції з банківськими картками найбільш приваблюють шахраїв. З'явилися й нові сценарії в шахраїв, які під виглядом державних органів обіцяють грошову допомогу через карантин і у такий спосіб виманюють дані платіжних карток.

Фінансове шахрайство – один із найбільш складних видів недобросовісної діяльності, яка набула поширення в банках, що представляє собою систему маніпуляцій у сфері банківського грошового обігу та фінансових маніпуляцій [2].

Складність виявлення фінансового шахрайства полягає в тому, що зацікавленими в його здійсненні можуть бути вищі керівники разом із мажоритарними учасниками комерційного банку. В такій ситуації ошуканими особами є вкладники та інші клієнти комерційного банку. За статистикою, майже 70% злочинів у банківській сфері здійснюються або винятково співробітниками банку, або за їхньої активної участі.

На сьогоднішній день найбільш поширеними видами шахрайських операцій з банківськими картками є соціальна інженерія: скімінг – викрадення інформації з магнітної стрічки картки або ПІН-коду за допомогою спеціальних пристроїв; трапінг – встановлення пасток на шатер банкомату, а також: шахрайство з банкоматами (додаткове обладнання, злом, підрив); фішинг – шахрайство за допомогою Інтернету; вішинг – шахрайство за допомогою мобільного зв'язку; підробка і дублікат платіжних карток; вірусні та хакерські атаки, тощо [4].

За даними Української асоціації міжбанківських платіжних систем в 2019 році, шахраям вдалося "добути" майже 362 млн грн, це в півтора рази більше, ніж в 2018 році. Як і раніше, в топі незаконних методів - соціальна інженерія, коли шахраї обманом підштовхують людей віддати гроші або поділитися конфіденційною інформацією: термін дії платіжних карток, CVV, PIN, паролі тощо (1260 номерів, з яких телефонували шахраї, занесли за рік до чорного списку). Зазвичай жертвами соціальної інженерії стають літні люди (від 55 і старші) – 15%, і середнього віку (35 – 44) – 13% [5].

Почастішали фізичні атаки на банкомати – 77 інцидентів, коли їх підривали, ламали, пиляли тощо, в 2018-му таких випадків було всього 20. Зате стало менше випадків скімінгу, коли на банкомати встановлюють обладнання, яке "краде" дані про картку. А ось примітивний спосіб – клейка стрічка, що перешкоджає видачі готівки в банкоматі, – використовувалася набагато частіше, ніж в 2018 році. Також найяскравіший тренд 2019-го - шахрайські сайти, які обманом схиляють людей витратити гроші на неіснуючі товари або послуги. У ЕМА нарахували більше 300 таких сайтів [5]. Окремо слід зазначити, що попит на шахрайські дії з кредитними картками створив окремий вид злочинної діяльності – торгівлю незаконно отриманими особистими даними їх власників, у т.ч. номерами рахунків за кредитними картками, особистою інформацією власників [3].

На основі проведеного аналізу наслідків кібершахрайств, які відбуваються в сфері використання клієнтами банків платіжних засобів, найбільш вразливим місцем є сам клієнт, який під дією різних методів соціальної інженерії становиться об'єктом шахрайства. Для боротьби з даним способом шахрайства банки не мають досить дієвих інструментів [3].

На нашу думку, для даного випадку шахрайства, доцільно застосовувати сукупність засобів, що базуються на методах інтелектуального аналізу, інформаційних технологій та кримінальному кодексі. Серед шляхів протидії даному виду зловмисної діяльності варто виділити наступні:

Підвищення обізнаності громадян України про ефективні способи захисту власної інформації та правила безпечного використання платіжних карток, електронних платежів і банкоматів. З цього приводу Національний банк запустив Всеукраїнську інформаційну кампанію ШахрайГудбай з протидії платіжному шахрайству. Мета кампанії – навчити українців основним правилам безпеки безготівкових та онлайн-платежів;

Програмний захист – підвищення якості обслуговування власників банківських карт і можливість запобігання і виявлення нових видів шахрайства за допомогою впровадження спеціальної системи надання авторизації (блокування операцій та подвійна (потрійна) ідентифікація клієнта); технічне забезпечення банкоматів, включаючи антискімінгові пристрої, установку антивірусних програм і вдосконалення структури карт, в тому числі випуск «чіпованих» карт за новим стандартом EMV (технологія ЧІП та ПІН), а також різні створення додатків безпеки, зокрема, додаток 3D Secure для операцій онлайн. Запровадження карток цього стандарту суттєво зменшить кількість традиційного шахрайства, пов'язаного з клонуванням карток [1];

Створення інтегрованого банку даних, який буде містити інформацію щодо: способу, методу, виду шахрайства, характерних ознак, характеристик шахрая та його жертви, мобільні телефони, IP-адреси шахраїв, тощо [4];

Жорстке обмеження прав доступу працівників банків до бази даних клієнтів для зменшення шахрайств з боку працівників. Даний підхід потребує створення та модифікацію посадових інструкцій працівників банків та розробку інструкцій та рекомендацій головних банків та Національного банку України;

Вдосконалення системи оперативного отримання та перевірки правоохоронними органами інформації про злочини з платіжними картками, електронними платежами і в банкоматах; вдосконалення взаємодії між банками, патрульною поліцією, кіберполіцією і слідством при розслідуванні та протидії злочинам з платіжними картками, електронними платежами і з банкоматами;

Удосконалення кримінального законодавства України в сфері неправомірного використання засобів платежу та приведення його у відповідність до світових стандартів і поширених видів карткових і платіжних злочинів. Запровадити досвід США щодо правого регулювання боротьби із кіберзлочинністю;

Страховий захист – можливість отримання послуг страхування банківської карти. При цьому необхідно формування резервів, або за рахунок банку, або у вигляді страховки, які дозволять компенсувати втрачені кошти клієнтам [1].

Список використаних джерел

1. Кривошапова С.В., Литвин Е.А. Оценка и способы борьбы с машенничеством с банковскими картами в России – Режим доступу: file:///C:/Users/User/Google% 20Диск/Стаття%20банкывське%20шахрайство/ elibrary 23213322_44664285.pdf

2. Мельник С.С. Сутність фінансового шахрайства в комерційному банку. Науковий вісник Ужгородського національного університету. 2016. № 6 (ч.2). С. 91-95.

3. Олександра Олійничук. Банківські картки як об'єкт шахрайства: стан і протидія явищу – Режим доступу: file:///C:/Users/User/Google%20Диск/Стаття% 20банкывське%20шахрайство/ Олійничук%20О..pdf

4. Яровенко Г.М. Аналіз наслідків кібершахрайств в банківській системі України – Режим доступу: file:///C:/Users/User/Google%20Диск/Стаття%20 банкывське%20шахрайство/116%20 (1).pdf

5. У 2019-му шахраї вкрали з наших карток 362 млн грн. Чотири способи, як вони це зробили – Режим доступу: https://ua-news.liga.net/economics/articles/u-2019-mu-shahrai-vkrali-z-nashih-kartok-362-mln-grn-chotiri-sposobi-yak-voni-tse-zrobili