

Роман Олександрович НЕСТЕРЕНКО*(Харківський національний університет внутрішніх справ, м. Харків)*

ОГЛЯД ШАХРАЙСЬКИХ СХЕМ З БАНКІВСЬКИМИ КАРТАМИ

У статті підкреслено, що вироблення криміналістичних рекомендацій стосовно виявлення, документування та досудового розслідування шахрайств з банківськими картами, а також щодо організаційно-тактичного забезпечення проведення процесуальних дій з метою збирання належної, достовірної, допустимої та належної доказової бази вбачається неможливим без попереднього з'ясування та огляду найбільш поширених і характерних для окресленої сфери суспільних відносин шахрайських схем. Здійснено аналіз наукових підходів до систематизації способів учинення шахрайств, у тому числі з банківськими картами, та аналітико-довідкової інформації про найбільш поширені шахрайські схеми в Україні. З'ясовано, що шахрайства з банківськими картами вчиняються переважно з використанням інформаційних технологій, що значно спрощує досягнення злочинного задуму, адже мінімізує особистісні контакти особи злочинця зі своїми жертвами, розширює «географію» та «сфери» протиправної діяльності, залишає менше «традиційних» слідів кримінальних правопорушень, ускладнює процес виявлення, документування та досудового розслідування всіх епізодів кримінальної протиправної діяльності тощо. Доведено, що цілком логічним і виправданим убачається виокремлення двох груп кіберзлочинів проти власності, до структури яких входять і шахрайства з банківськими картами, залежно від способів їх учинення: кіберзлочини проти власності, що вчиняють шляхом психологічного впливу на людину, та кіберзлочини проти власності, що вчиняють шляхом впливу на обладнання. Наголошено, що все частіше зустрічається поєднання обидвох способів у механізмі вчинення шахрайств з банківськими картами, з огляду на що запропоновано додатково виокремлювати змішані кіберзлочини проти власності, які вчиняються водночас за допомогою соціальної інженерії та впливу на обладнання.

Ключові слова: криміналістична методика, криміналістична характеристика, шахрайство, банківські карти, способи вчинення, шахрайські схеми, механізм учинення шахрайства.

Постановка проблеми. Вироблення криміналістичних рекомендацій стосовно виявлення, документування та досудового розслідування шахрайств з банківськими картами, а також щодо організаційно-тактичного забезпечення проведення процесуальних дій з метою збирання належної, достовірної, допустимої та належної доказової бази вбачається неможливим без попереднього з'ясування та огляду найбільш поширених і характерних

для окресленої сфери суспільних відносин шахрайських схем. З огляду на що актуальним і нагальним є питання про визначення розповсюджених шахрайських схем з банківськими картками.

Питання про схеми вчинення шахрайських дій, у тому числі з банківськими картками, а також кримінально-правову, кримінологічну та криміналістичну характеристики різних видів шахрайств, висвітлюють в своїх наукових працях багато вчених, наприклад, С. Афанасенко, В. Березняк, С. Бугера, М. Думчиков, А. Жилін, О. Заріцька, І. Ігнатова, І. Коваленко, А. Огієвич, Т. Охрімчук, В. Пивоваров, К. Попов, А. Романова, С. Самойлов, К. Терещенко, П. Харламов та інші. Проте чимало питань залишаються не вирішеними чи дослідженими фрагментарно.

Отже, метою представленого наукового дослідження є здійснення аналізу наукових підходів до систематизації способів учинення шахрайств, у тому числі з банківськими картками, та аналітико-довідкової інформації про найбільш поширені шахрайські схеми в Україні.

Виклад основного матеріалу. За даними Національного банку України «переважна більшість випадків шахрайства – це ситуації, в яких клієнти банківських установ передавали свої особисті дані третім особам, таким чином надавши їм інформацію для доступу до своїх рахунків». При цьому найбільша кількість зафіксованих шахрайств з банківськими картками вчиняється через мережу Інтернет і становить 83 % від загальної кількості. «Решта 17 % – злочинні дії, вчинені за допомогою фізичних пристроїв (торговельна мережа, банкомати, термінали самообслуговування)»¹. Більше за все, 53 % суми всіх збитків, завданих шахрайствами з банківськими картками, в 2022 році припало на соціальну інженерію, а в 2023 році вказаний показник зріс до 80 %².

Як інформує Департамент кіберполіції Національної поліції України, найпопулярнішими шахрайськими схемами в Україні є недоставлення псевдопродавцями інтернет-замовлень, фішинг та «дзвінки з банку». Начальник відділу протидії різновидам онлайн-шахрайств на першому місці називає таку підкатегорію як «недоставлення замовлень, зроблених через інтернет. Це стосується купівлі-продажу товарів в інтернеті, розміщення оголошення про надання певних послуг, і при цьому отримується часткова або повна передплата. На другому місці – фішинг. Це кваліфіковане

¹ Ігнатова І. Шахрайство з банківськими картками: НБУ вразив статистику про жертв зловмисників. *ТСН. Гроші*. URL: <https://tsn.ua/groshi/shahraystvo-z-bankivskimi-kartkami-nbu-vraziv-statistikoyu-pro-zhertv-zlovmisnikiv-2548954.html>; Причиною більшості шахрайських випадків з платіжними картками стало розголошення даних їхніми користувачами. *Національний банк України*. URL: <https://bank.gov.ua/ua/news/all/prichinoyu-bilshosti-shahrayskih-vipadkiv-z-platijnimi-kartkami-stalo-rozgoloshennya-danih-yihnimi-koristuvachami>.

² Ігнатова І. Шахрайство з банківськими картками: НБУ вразив статистику про жертв зловмисників. *ТСН. Гроші*. URL: <https://tsn.ua/groshi/shahraystvo-z-bankivskimi-kartkami-nbu-vraziv-statistikoyu-pro-zhertv-zlovmisnikiv-2548954.html>; Причиною більшості шахрайських випадків з платіжними картками стало розголошення даних їхніми користувачами. *Національний банк України*. URL: <https://bank.gov.ua/ua/news/all/prichinoyu-bilshosti-shahrayskih-vipadkiv-z-platijnimi-kartkami-stalo-rozgoloshennya-danih-yihnimi-koristuvachami>; Машлаковська Т. «ШахрайГудбай»: як не стати жертвою афери з банківськими картками. *Суспільне Новини*. URL: <https://suspilne.media/516317-sahrajgudbaj-ak-ne-stati-zertvou-aferi-z-bankivskimi-kartkami/>

шахрайство, де за допомогою методів соціальної інженерії та програмних засобів робляться посилання, які схожі на оригінальні сайти. Третє місце на сьогодні займають дзвінки «з банку»¹.

У рамках проєкту «Шахрай Гудбай» було виявлено поширені схеми шахрайства в Україні. Зокрема, такими є:

– злам акаунтів у соціальних мережах. Шахраї зламують облікові записи в соціальних мережах та месенджерах (фейсбук, інстаграм, телеграм). Для цього поширюють фішингові посилання, наприклад, під виглядом пропозицій взяти участь у голосуванні, конкурсі, пропозицій роботи в інтернеті тощо. Перейшовши за посиланнями, громадяни вводять логіни та паролі від своїх акаунтів у соціальних мережах/месенджерах, які автоматично стають відомі шахраям. Далі шахраї від імені власника акаунта розсилають підписникам однакові повідомлення такого змісту: «Привіт! Позич, будь ласка, гроші до завтра! Дуже треба!». Суму шахраї зазначають різну, вказують номери своїх карток і в такий спосіб привласнюють кошти осіб, які погоджуються їх позичити²;

– СМС від шахраїв від імені банку (спуфінг³). Шахраї надсилають смс-повідомлення від імені банку про те, що з рахунка громадянина намагаються переказати кошти. Якщо переказ особа не здійснювала, потрібно зателефонувати «псевдобанку» за номером, зазначеним в смс, або перейти за посиланням. Якщо особа переходить за посиланням, то потрапляє на шахрайський сайт, де під виглядом блокування шахрайської трансакції й автоматичного повернення грошей пропонується ввести: номер телефону; пароль до інтернет-банкінгу; всі реквізити карти; смс-код (код підтвердження проведення операції). Якщо особа телефонує за зазначеним у смс номером телефону, шахрай веде жертву на цей самий шахрайський сайт, де схиляє ввести вищезазначені дані⁴;

– шахрайство під виглядом соціальних виплат. Шахраї привласнюють гроші під виглядом надання виплат українцям, які постраждали від війни. Для цього роблять смс-розсилання та розсилання в месенджерах про нарахування соціальних виплат, зокрема «Підтримки, допомоги від ЄС, представників ООН, Червоного Хреста, різних програм благодійних фондів. У розсиланнях шахраї пропонують перейти за посиланням для зарахування коштів просять ввести мобільний номер телефону, пін-код, пароль до інтернет-банкінгу, смс-код від банку. Також зловмисники створюють шахрайські сайти, схожі на справжні сайти державних органів, міжнародних організацій, банків та благодійних фондів. Громадяни переходять за посиланням, бачать сайт, схожий на справжню сторінку відповідної

¹ Кіберполіція назвала три найпопулярніші в Україні шахрайські схеми. *Офіційний сайт кіберполіції України*. URL: <https://cyberpolice.gov.ua/news/kiberpoliczija-nazvala-try-najpopulyarnishi-v-ukrayini-shahrajiski-sxemy-8249/>

² Поширені схеми шахрайства. *#ШахрайГудбай*. URL: <https://promo.bank.gov.ua/stopfraud/>

³ Шахрайство з банківськими картками: 4 способи захисту. *Zen.com*. URL: <https://www.zen.com/uk/blog/personal-finance-uk/fraud-with-payment-cards/>.

⁴ Поширені схеми шахрайства. *#ШахрайГудбай*. URL: <https://promo.bank.gov.ua/stopfraud/>

організації, вводять усі дані, що автоматично стають відомі шахраям¹;

– телефонне шахрайство, коли шахрай телефонує і переконує жертву повідомити особисту, фінансову чи конфіденційну інформацію або переказати гроші².

І. Ігнатова за результатами журналістського розслідування, а також здійснивши аналіз дані Національного банку України, встановила, що «поширеними сценаріями соціальної інженерії, через які зловмисники крадуть гроші з карток, у 2023 році стали:

– розсилання фейкових повідомлень про можливість отримання допомоги від держави, соціальних фондів – клієнти переходять за посиланням та заповнюють відповідну форму, зокрема свої особисті дані, що дають доступ до рахунку;

– виготовлення електронної SIM-карти або фінансового номера телефону клієнта – у людини просять код доступу до застосунку мобільного оператора, а потім за допомогою фінансового номера зловмисники отримують доступ до інтернет-банкінгу для незаконного розпорядження коштами на рахунку (зокрема придбання товарів або отримання миттєвих кредитів);

– дзвінок від нібито представників банку з метою дізнатися реквізити картки для доступу до рахунку, начебто щоб уникнути блокування коштів (CVV/CVC код, одноразові паролі з смс-повідомлень тощо);

– повідомлення у месенджерах та соціальних мережах про легкий та швидкий прибуток – людині пропонують виконати певні «завдання» у соцмережі чи на певному сайті, зробити «вигідний» закуп, що надасть додаткові привабливі бонуси»³.

Своєю чергою, І. Ареф'єва називає 10 найбільш розповсюджених способів шахрайства з платіжними картками:

1) використання схеми «повідомлення про опитування з розіграшем грошових призів від імені великого банку або відомої компанії». Цей спосіб полягає в тому, що «після участі в опитуванні шахраї надсилали людям повідомлення про виграш грошей. Щоб отримати гроші потрібно було лише вказати дані платіжної карти, або інший варіант – сплатити податки за виграш за вказаними реквізитами»⁴;

2) здійснення телефонного дзвінку з метою отримати секретні дані. За вказаної шахрайської схеми особа злочинця телефонує потенційній жертві,

¹ Там само.

² Там само.

³ Ігнатова І. Шахрайство з банківськими картками: НБУ вразив статистикою про жертв зловмисників. *ТСН. Гроші*. URL: <https://tsn.ua/groshi/shahraystvo-z-bankivskimi-kartkami-nbu-vraziliv-statistikoyu-pro-zhertv-zlovmisnikiv-2548954.html>; Причиною більшості шахрайських випадків з платіжними картками стало розголошення даних їхніми користувачами. *Національний банк України*. URL: <https://bank.gov.ua/ua/news/all/prichinoyu-bilshosti-shahrayskih-vipadkiv-z-platijnimi-kartkami-stalo-rozgoloshennya-danih-yihnimi-koristuvachami>.

⁴ Ареф'єва І. Топ 10 видів шахрайства з платіжними картками. *Financer*. URL: <https://financer.com.ua/kartky/statti/vydy-shahraystva/>; Топ-10 шахрайств з платіжними картками. *Черкаський науково-дослідний експертно-криміналістичний центр МВС України*. URL: <https://ndekc.ck.ua/novini/568-top-10-shahraystv-z-platizhnimi-kartkami.html>.

представляється працівником банку та повідомляє про затриману (підозрілу) транзакцію, яку заблокував банк. Шахрай просить назвати персональні дані і цифри з карти для «перевірки», після чого «надсилає» SMS з разовим кодом, який просить повідомити. Насправді шахраї проводять платіж в інтернет-магазині, вказавши дані картки, і їм не вистачає лише разового коду для проведення платежу, який банк надсилає на фінансовий номер¹;

3) «заміна SIM-карти для доступу до онлайн-банкінгу». Шахраї звертаються до оператора зв'язку з повідомленням про втрату SIM-карти та проханням її замінити. Після заміни SIM-карти шахраї отримують доступ до онлайн-банкінгу особи потерпілого. Це дозволяє злочинцеві збільшити кредитний ліміт і зняти готівкові кошти в банкоматі без використання банківської карти. Також така схема дає можливість шахраєві розраховуватися за товари в інтернеті²;

4) повідомлення про грошову допомогу від держави. Приміром, особа злочинця телефонує жертві, представляється працівником Національного банку України, повідомляє її про грошову допомогу, просить вказати номер банківської картки та сплатити податок з доходу 18 %³;

5) фішинг. Указаний спосіб полягає у підробці веб-сторінок та електронних листів⁴. Наведена схема крадіжки карткових даних в інтернеті заснована на масовій розсилці банківським клієнтам спеціальних листів або СМС-повідомлень, що маскуються під повідомлення від банків або відомих компаній, брендів. У таких листах міститься посилання на сайт, що зовні не відрізняється від справжнього, на якому банківському клієнту пропонують ввести логін і пароль для доступу до інтернет-банкінгу⁵;

6) копіювання даних банківської картки, наприклад, шляхом фотографування їх номерів та CVV кодів⁶;

7) використання незахищених мереж WI-FI⁷;

8) «скімінг для крадіжки даних карти». Скімінг – це процес встановлення шахраями спеціального додаткового обладнання на банкомат з метою зчитування і запису даних банківської картки, які в подальшому використовуються для виготовлення копії картки («білого пластику»)⁸. Мова йде про використання спеціальних накладок на картридж для картки

¹ Там само.

² Там само.

³ Там само

⁴ Топ-10 шахрайств з платіжними картками. *Черкаський науково-дослідний експертно-криміналістичний центр МВС України*. URL: <https://ndekc.ck.ua/novini/568-top-10-shahraystv-z-platizhnimi-kartkami.html>.

⁵ Картки, гроші та обман! Найпопулярніші схеми карткових шахраїв, і як від них уберегтися. *Finance.ua*. URL: <https://finance.ua/ua/cards/karti-dengi-obman>.

⁶ Топ-10 шахрайств з платіжними картками. *Черкаський науково-дослідний експертно-криміналістичний центр МВС України*. URL: <https://ndekc.ck.ua/novini/568-top-10-shahraystv-z-platizhnimi-kartkami.html>.

⁷ Там самою

⁸ Картки, гроші та обман! Найпопулярніші схеми карткових шахраїв, і як від них уберегтися. *Finance.ua*. URL: <https://finance.ua/ua/cards/karti-dengi-obman>.

та на клавіатуру для введення пін-коду («скімеру»)¹. Скімер зчитує і запам'ятовує інформацію, записану на магнітній смужці. Крім того, шахраї також крадуть і PIN-код картки. Для цього використовуються або спеціальні накладки на клавіатуру, які записують натискання клавіш, або мініатюрні відеокамери, які встановлюються на банкоматі. Шахраї, що спеціалізуються на такому виді крадіжки інформації, називаються «кардерами»²;

9) «несанкціоноване проведення мікроплатежів»³;

10) «платежі на незахищених сайтах»⁴.

Т. Машлаковська, крім вищенаведених схем шахрайств з банківськими картками, виокремлює створення та використання фейкових чат-ботів в Телеграмі, які схожі на банківські. Зокрема, головна експертка Управління зв'язків з громадськістю та фінансової обізнаності департаменту комунікацій Національного банку України зазначає, що в фейкових чат-ботах людині пропонують оформити соціальну виплату і ввести банківські реквізити. При цьому шахрайський чат-бот від банківського складно відрізнити. У банківських є галочка верифікації, і шахраї також почали ставити собі такий голубий стікер, який схожий на цю галочку⁵.

Крім того, зустрічається позиція, згідно з якою до найчастіших схем шахрайства з банківськими картками належать:

– шахрайство з копією телефонної карти. Зловмисники створюють дублікат sim-карти, дочекавшись поки основна картка у вашому смартфоні знаходиться поза зоною досяжності. Саме за допомогою дублікату вони віддалено управляють рахунками, перераховуючи з них гроші⁶;

– соціальна інженерія. Таке шахрайство з платіжними картками не передбачає використання технологій. Воно засноване виключно на зловживанні довірою людей. Зловмисники дізнаються всі дані карти (включно з CVV-номером) за допомогою телефонних дзвінків чи повідомлень⁷. Такий метод соціальної інженерії, який активно використовують шахраї для крадіжки карткових даних безпосередньо у клієнтів, називається «вішинг»⁸;

– банкоматне шахрайство пов'язане з встановленням на банкоматі спеціального обладнання (фізичний скімінг) чи програмного забезпечення

¹ Топ-10 шахрайств з платіжними картками. *Черкаський науково-дослідний експертно-криміналістичний центр МВС України*. URL: <https://ndekc.ck.ua/novini/568-top-10-shahraystv-z-platizhnimi-kartkami.html>.

² Картки, гроші та обман! Найпопулярніші схеми карткових шахраїв, і як від них уберегтися. *Finance.ua*. URL: <https://finance.ua/ua/cards/karti-dengi-obman>.

³ Топ-10 шахрайств з платіжними картками. *Черкаський науково-дослідний експертно-криміналістичний центр МВС України*. URL: <https://ndekc.ck.ua/novini/568-top-10-shahraystv-z-platizhnimi-kartkami.html>.

⁴ Там само.

⁵ Машлаковська Т. «ШахрайГудбай»: як не стати жертвою афери з банківськими картками. *Суспільне Новини*. URL: <https://suspilne.media/516317-sahrajgudbaj-ak-ne-stati-zertvou-afери-z-bankivskimi-kartkami/>.

⁶ Шахрайство з банківськими картками: 4 способи захисту. *Zen.com*. URL: <https://www.zen.com/uk/blog/personal-finance-uk/fraud-with-payment-cards/>

⁷ Там само.

⁸ Картки, гроші та обман! Найпопулярніші схеми карткових шахраїв, і як від них уберегтися. *Finance.ua*. URL: <https://finance.ua/ua/cards/karti-dengi-obman>.

(програмний скімінг та прямий диспенс), що дозволяє зчитати дані з карти або ж блокувати видачу готівки¹.

При цьому банкоматне шахрайство може здійснюватися двома способами. Перший – це Cash Trapping, коли власник карти проводить операцію з видачі готівки, а зловмисник блокує її в банкоматі і забирає самостійно, коли власник відходить від пристрою. Другий – Transaction Reversal Fraud (TRF), який полягає в розміщенні спеціального пристрою в шатері банкомату типу «виделки». Тоді проводиться операція зі зняття готівки: зловмисник вводить PIN-код і запит на зняття грошей. Банкомат розміщує гроші перед заслінкою, а шахрай залишає карту в слоті так, щоб вона застрягла. Банкомат сповіщає про помилку і скасовує транзакцію. Гроші залишаються у «виделці», зловмисник силою відкриває заслінку і отримує гроші, а баланс на карті при цьому залишається незмінним².

На велике різноманіття способів учинення шахрайств з банківськими картами вказують В. В. Пивоваров, К. В. Терещенко. Зокрема, науковці називають такі види шахрайств з банківськими картками та банкоматами – «скімінг», «траппінг», «фантом», «шаттер», «шиммінг», «трешинг», «фармінг», «фітинг», що, своєю чергою, вказує на винахідливість особи злочинця та її поінформованість про досягнення в сфері інформаційних технологій³.

Останнім часом усе більшої розповсюдженості отримує такий спосіб шахрайств з банківськими картами як створення фінансових пірамід. Про це йдеться як в офіційних повідомленнях правоохоронних органів, так і на шпальтах медіа. Зокрема, йдеться про зростання кількості «постраждалих громадян від незаконної діяльності, так званих, «фінансових пірамід», що являє собою шахрайство з використанням фінансових інструментів, а так само об'єктів цивільних прав, що мають ознаки фінансових інструментів, яке передбачає створення, функціонування та просування, в тому числі за допомогою засобів масової інформації, схеми взаємовідносин між засновником схеми та її інвесторами, відповідно до якої залученим інвесторам обіцяється отримання значного пасивного доходу та виплата такого доходу залежить від залучення нових інвесторів до функціонування такої схеми». Крім того, у вказаних джерелах указують на існування практики «щодо залучення та навчання третіх осіб з метою їх участі в незаконній діяльності у сфері фінансових послуг та ринків фінансових послуг. Так, шахраї представляються потенційним жертвам, як відомі та успішні міжнародні фореक्स брокери з торгівлі акціями та іншими фінансовими інструментами, в результаті чого, шляхом обману та зловживання довірою, залучають громадян до участі в незаконній діяльності»⁴. Також «для досягнення своїх злочинних цілей шахраї

¹ Шахрайство з банківськими картками: 4 способи захисту. Zen.com. URL: <https://www.zen.com/uk/blog/personal-finance-uk/fraud-with-payment-cards/>

² Там само.

³ Пивоваров В.В., Терещенко К.В. Шахрайство із банківськими картками: окремі питання віктимологічної профілактики. *Карпатський правничий часопис*. 2015. № 10. С. 133.

⁴ У Раді створили ТСК з розслідування можливої неправомірної діяльності, пов'язаної з

створюють мережу «колцентрів», що являє собою інструмент для здійснення шахрайських дій з використанням інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем та електронних комунікаційних мереж, шляхом обману чи зловживання довірою громадян для отримання персональних даних, зокрема, реквізитів банківських карток/рахунків, заволодівають їх коштами»¹.

Окремо варто наголосити, що початок повномасштабного вторгнення РФ на територію України, ведення активних бойових дій на значній території нашої держави, окупація окремих регіонів тощо безпосередньо вплинули не тільки на кількісні, а й якісні показники кримінальної протиправної діяльності загалом та проти власності зокрема. Не минули стороною такі зміни й структуру шахрайств з банківськими картами. Зокрема, поширення отримали наступні шахрайські схеми з банківськими картами: фейкові оголошення про оренду житла, «евакуаційний транспорт громадян», «неправдива реклама продажу військової амуніції», фейкові оголошення для збору коштів на лікування дітей, які нібито постраждали від військової агресії і т. п.²

Способи шахрайств з банківськими картами представлені не тільки комплексом дій, спрямованих на підготовку протиправної діяльності та реалізацію кримінального протиправного умислу, а й на приховування як факту вчинення кримінального правопорушення, так і походження коштів, отриманих злочинним шляхом. Наприклад, М.О. Думчиков, виокремлює такі основні способи легалізації злочинних доходів за допомогою віртуальних активів, як використання:

- сервісів для конвертації віртуальних активів;
- P2P-обміну;
- сайтів азартних ігор;
- міксерів віртуальних активів;
- фіктивних інтернет-сайтів із продажу цифрових товарів³.

Висновки. Отже, з вищенаведеного помітно, що шахрайства з банківськими картами вчиняються переважно з використанням інформаційних технологій, що значно спрощує досягнення злочинного задуму, адже мінімізує особистісні контакти особи злочинця зі своїми жертвами, розширює «географію» та «сфери» протиправної діяльності, залишає менше «традиційних» слідів кримінальних правопорушень, ускладнює процес виявлення, документування та досудового розслідування

незаконними фінансовими операціями та шахрайством «колл-центрів». *Судово-юридична газета в Україні*. URL: <https://sud.ua/uk/news/ukraine/271946-v-rade-sozdali-vsk-po-rassledovaniyu-vozmozhnoy-nepravomernoy-deyatelnosti-svyazannoy-s-nezakonnymi-finansovymi-operatsiyami-i-moshennichestvom-koll-tsentrov>.

¹ Там само.

² Огієвич А. О., Романова А. Є. Шахрайство у сфері обігу банківських платіжних карток: кримінально-правовий аспект. *Юридичний науковий електронний журнал*. 2022. № 11. С. 382. DOI: <https://doi.org/10.32782/2524-0374/2022-11/90>

³ Думчиков М. О., Репін Д. А. Легалізація доходів, отриманих злочинним шляхом, за допомогою використання віртуальної валюти (криптовалюти): кримінологічний та кримінально-правовий аспект. *Журнал східноєвропейського права*. 2020. № 82. С. 32–37.

всіх епізодів кримінальної протиправної діяльності тощо. Тому цілком логічним і виправданим убачається виокремлення двох груп кіберзлочинів проти власності, до структури яких входять і шахрайства з банківськими картами, залежно від способів їх учинення: кіберзлочини проти власності, що вчиняють шляхом психологічного впливу на людину (обман, введення в оману, загроза); кіберзлочини проти власності, що вчиняють шляхом «впливу» на обладнання (комп'ютери, смартфони та інше обладнання)¹. Проте, на нашу думку, все частіше зустрічається поєднання обидвох способів у механізмі вчинення шахрайств з банківськими картами, з огляду на що пропонуємо додатково виокремлювати змішані кіберзлочини проти власності, які вчиняються водночас за допомогою соціальної інженерії та впливу на обладнання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ареф'єва І. Топ 10 видів шахрайства з платіжними картками. *Financer*. URL: <https://financer.com.ua/kartky/statti/vydy-shahraystva/>.
2. Думчиков М. О., Репін Д. А. Легалізація доходів, отриманих злочинним шляхом, за допомогою використання віртуальної валюти (криптовалюти): кримінологічний та кримінально-правовий аспект. *Журнал східноєвропейського права*. 2020. № 82. С. 32–37.
3. Ігнатова І. Шахрайство з банківськими картками: НБУ вразив статистикою про жертв зловмисників. *ТСН. Гроші*. URL: <https://tsn.ua/groshi/shahraystvo-z-bankivskimi-kartkami-nbu-vraziv-statistikoyu-pro-zhertv-zlovmisnikiv-2548954.html>.
4. Картки, гроші та обман! Найпопулярніші схеми карткових шахраїв, і як від них уберегтися. *Finance.ua*. URL: <https://finance.ua/ua/cards/karti-dengi-obman>.
5. Кіберполіція назвала три найпопулярніші в Україні шахрайські схеми. *Офіційний сайт кіберполіції України*. URL: <https://cyberpolice.gov.ua/news/kiberpolicziya-nazvala-try-najpopulyarnishi-v-ukrayini-shahrajski-sxemy-8249/>.
6. Машлаковська Т. «ШахрайГудбай»: як не стати жертвою афери з банківськими картками. *Суспільне Новини*. URL: <https://suspilne.media/516317-sahrajgudbaj-ak-ne-stati-zertvou-aferi-z-bankivskimi-kartkami/>.
7. Огієвич А. О., Романова А. Є. Шахрайство у сфері обігу банківських платіжних карток: кримінально-правовий аспект. *Юридичний науковий електронний журнал*. 2022. № 11. С. 380–383. DOI: <https://doi.org/10.32782/2524-0374/2022-11/90>.

¹ Піцик Ю. М. Класифікація кіберзлочинів проти власності. *Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція*. 2017. № 30. Том 2. С. 67.

8. Пивоваров В.В., Терещенко К.В. Шахрайство із банківськими картками: окремі питання віктимологічної профілактики. *Карпатський правничий часопис*. 2015. № 10. С. 132–137.
9. Піцик Ю. М. Класифікація кіберзлочинів проти власності. *Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція*. 2017. № 30. Том 2. С. 65–68.
10. Поширені схеми шахрайства. *#ШахрайГудбай*. URL: <https://promo.bank.gov.ua/stopfraud/>.
11. Причиною більшості шахрайських випадків з платіжними картками стало розголошення даних їхніми користувачами. *Національний банк України*. URL: <https://bank.gov.ua/ua/news/all/prichinoyu-bilshosti-shahrayskih-vipadkiv-z-platijnimi-kartkami-stalo-rozgoleshennya-danih-yihnimi-koristuvachami>.
12. Топ-10 шахрайств з платіжними картками. *Черкаський науково-дослідний експертно-криміналістичний центр МВС України*. URL: <https://ndekc.ck.ua/novini/568-top-10-shahraystv-z-platizhnimi-kartkami.html>.
13. У Раді створили ТСК з розслідування можливої неправомірної діяльності, пов'язаної з незаконними фінансовими операціями та шахрайством «колл-центрів». *Судово-юридична газета в Україні*. URL: <https://sud.ua/uk/news/ukraine/271946-v-rade-sozdali-vsk-po-rassledovaniyu-vozmozhnoy-nepravomernoy-deyatelnosti-svyazannoy-s-nezakonnymi-finansovymi-operatsiyami-i-moshennichestvom-koll-tsentrov>.
14. Шахрайство з банківськими картками: 4 способи захисту. *Zen.com*. URL: <https://www.zen.com/uk/blog/personal-finance-uk/fraud-with-payment-cards/>.

Стаття надійшла до редакції 21.08.2023

Roman OI. NESTERENKO,

Postgraduate Student

(*Kharkiv National University of Internal Affairs, Kharkiv, Ukraine*)

OVERVIEW OF FRAUDULENT SCHEMES WITH BANK CARDS

In this article, it has been emphasized that the development of forensic recommendations regarding the detection, documentation and pre-trial investigation of bank card fraud, as well as regarding the organizational and tactical support for conducting procedural actions in order to collect an appropriate, reliable, admissible and appropriate evidentiary base, is considered impossible without a preliminary clarification and review of the most widespread and characteristic fraudulent schemes for the outlined sphere of public relations. An analysis of scientific approaches to the systematization of methods of committing fraud, including with bank cards, and analytical and reference information on the most widespread fraudulent schemes in Ukraine has been carried out. It has been found that bank card fraud is committed mainly using information technologies, which greatly simplifies the achievement of the criminal

intent, as it minimizes personal contacts of the criminal with his victims, expands the “geography” and “spheres” of illegal activity, leaves fewer “traditional” traces of criminal offenses, complicates the process of detecting, documenting and pre-trial investigation of all episodes of criminal illegal activity, etc. It has been proven that it is quite logical and justified to distinguish two groups of cybercrimes against property, the structure of which also includes bank card fraud, depending on the methods of their commission: cybercrimes against property committed through psychological influence on a person, and cybercrimes against property committed through influence on equipment. It has been emphasized that a combination of both methods is increasingly common in the mechanism of committing fraud with bank cards, in view of which it is proposed to additionally distinguish mixed cybercrimes against property, which are committed simultaneously using social engineering and influencing equipment.

Key words: *forensic methodology, forensic characteristics, fraud, bank cards, methods of commission, fraudulent schemes, mechanism of commission of fraud.*