КРИМІНАЛЬНИЙ ПРОЦЕС, КРИМІНАЛІСТИКА

УДК 343.98
DOI https://doi.org/10.32837/pyuv.v0i5(34).662

І. О. Коваленко
orcid.org/0000-0001-9522-5971
адвокат,
аспірант кафедри криміналістики та домедичної підготовки
Дніпропетровського державного університету внутрішніх справ

КРИМІНАЛІСТИЧНИЙ АНАЛІЗ ШАХРАЙСТВА У СФЕРІ БАНКІВСЬКИХ ЕЛЕКТРОННИХ ПЛАТЕЖІВ

Постановка проблеми. Сьогодні шахрайство в сфері банківських електронних платежів є однією з головних проблем не тільки України, але і всього світу. За його допомогою кожного року викрадаються десятки мільярдів гривень у їх власників, та, на жаль, кількість постраждалих кожного дня тільки збільшується. Це своєю чергою стало можливим у зв'язку з розвитком всесвітньої мережі Інтернет та розвитком банківського сектору. Але, на жаль, правоохоронна система не встигає у своєму розвитку, у порівнянні з розвитком ІТ-технологій, що не скажеш про правопорушників, які займаються вчиненням досліджуваного кримінального правопорушення. Зазначене діяння в більшості випадків кваліфікується за ч. 3 ст. 190 ККУ, яке вчиняється за допомогою електронно-обчислюваної техніки [1]. Це може бути ноутбук, персональний комп'ютер, планшет, смартфон з обов'язковим підключенням до всесвітньої мережі Інтернет. Тому з метою криміналістичного аналізу шахрайства в сфері банківських електронних платежів дослідимо думки окремих вчених щодо цієї проблеми, а також способи його вчинення.

Аналіз останніх досліджень і публікацій. Проблемам розслідування шахрайств у різний час приділялася увага у дослідженнях багатьох відомих вчених, зокрема С.С. Чернявського, О.В. Журавльова, А.Ф. Волобуєва, Н.В. Павлової, В.Ю. Голубовського, А.А. Сандрачука, С.М. Астапкиної, В.М. Єгошина, В.В. Колесникова, О.І. Лученка, О.С. Овчинського, В.І. Отряхина, Р.С. Сатуєва, Г.М. Спіріна, К.В. Суркова, Є.П. Фірсова, В.О. Фінагеєв та інших. Як влучно зазначає В.О. Фінагеєв, незаконний доступ до банківських рахунків технологічно поєднує пов'язані між собою кримінально карані діяння проти власності (ст. 185, 190, 191 Кримінального кодексу (КК) України), у сфері господарської діяльності (ст. 200, 205, 209, 231 КК України), використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж (ст. 361, 361–1, 362 КК України), службової діяльності [2]. Вищезазначеними науковцями ця проблема розглядалася на момент публікації їх досліджень, але на теперішній час вона є не досить актуальною. Адже з кожним днем способи, техніка, обізнаність шахраїв прогресують. Тому в цьому дослідженні ми надамо криміналістичний аналіз актуальним на кінець 2020 року видам шахрайства у сфері банківських електронних платежів.

Мета дослідження. Метою статті є проведення докладного криміналістичного аналізу шахрайства в сфері банківських електронних платежів.

Виклад основного матеріалу. У період пандемії значно зріс обсяг онлайн-платежів в усіх сферах споживчого попиту, крім туризму. Споживачі стали активніше використовувати методи безконтактної та безготівкової оплати. Учасників ринку це змусило більш уважно вивчити платіжні інструменти і почати підключати нові. Епідемія і суворі обмеження за короткий період привели до значних змін на споживчому ринку, спровокувавши зростання довіри споживачів до безготівкової оплати і масовий перехід у електронну комерцію, зростання числа мерчантів (торговців), транзакцій і при цьому кратне зростання числа шахраїв і «сірих схем».

Основними видами шахрайства в Україні в сфері банківських електронних платежів є: фішинг, сніфферінг, вішинг, кардінг. Розглянемо окремі з них.

Зокрема, фішинг – один з видів інтернет-шахрайства, метою якого є отримання доступу до конфіденційних даних користувачів – логінів, паролів, даних особових рахунків і банківських карт [3]. Здебільшого використовується метод проведення масових розсилок від імені популярних компаній або організацій, які містять посилання на помилкові сайти, які зовні важко відрізнити від справжніх. Зовні здається, що фішингові повідомлення приходять від імені популярних організацій або компаній (як LiqPay, Skrill, UPS, урядові організації або банківські установи), однак насправді вони є підробленими.

У листах зловмисники ввічливо попросять оновити або підтвердити вірність персональної інформації, нерідко згадують будь-які проблеми з даними. Потім користувача перенаправляють на підроблений сайт, який дуже важко відрізнити від справжнього, де користувача просять ввести облікові дані. Якщо зловмисники отримають необхідну інформацію, це може призвести до крадіжки персональних даних або коштів [4, с. 57]. Часто трапляється так, що шахраї при цьому отримують інформацію про клієнтів банку від недобросовісних банківських співробітників, що може ввести жертву обману в ще більший обман. Крім цього, розсилка може проводитися не від імені банку, а від імені сервісу онлайн-платежів (наприклад, LiqPay), а також соціальних мереж (Instagram, Facebook) [5, с. 118]. До відомих схем фішингу відносять і підроблені лотереї або конкурси, нібито проведені якоюсь великою корпорацією, а також псевдо-антивіруси [6, с. 51]. Розрізняють такий вид фішингу, як смішинг (англ. SmiShing), – шахрайство за допомогою SMS-повідомлень. У цьому разі посилання на підроблений сайт відправляється через SMS, або шахраї просять надіслати їм необхідну інформацію про банківську карту у відповідному повідомленні. Також існує такий спосіб шахрайства, схожий на фішинг, як фарминг (англ. Farming, від слова “farm” – «ферма»). Він виражається в перенаправленні клієнта на помилкову адресу за допомогою шкідливої програми. Жертва обману вводить в пошуковий рядок адресу сайту свого банку, але ця програма відправляє його на підроблений шахрайський сайт [7, с. 25].

Так, наприклад, у Російській Федерації під виглядом отримання грошової компенсації «в зв’язку з COVID-2019» або за підписку на популярний у період пандемії сервіс онлайн-конференцій Zoom користувачів заманюють на шахрайські сайти, де викрадають гроші і дані банківських карт. При цьому листи відправляються не з шахрайського домену, а від офіційного сервісу. Вся справа в тому, що під час реєстрації Zoom пропонує користувачеві заповнити профіль – вказати «Ім’я» і «Прізвище», надаючи можливість вставити до 64 символів в кожне поле. Шахраї використовують цю можливість, вставляючи фразу: «Вам належить виплата компенсації у зв’язку з COVID-19» і вказують посилання на шахрайський сайт. Сама розсилка шахрайських повідомлень також відбувається з використанням можливості сервісу. Після реєстрації Zoom пропонує новому клієнтові запросити до десяти нових користувачів, вказавши їх електронну поштову адресу. Шахраї вводять адреси потенційних жертв, на які приходить офіційне повідомлення від імені команди сервісу відеоконференцій, але вмістом, яке згенерували інтернет-шахраї. Після того як жертва переходить на шахрайські сайти, їй пропонують ввести 4 або 6 останніх цифр номера її банківської карти. Шахраї розраховують «компенсацію» для користувача: від 30 000 до 250 000 російських рублів. Але для того, щоб отримати ці гроші, жертва повинна була сплатити невелику суму «за юридичну допомогу в заповненні анкети» – близько 1 000 російських рублів. В результаті користувачі вводять дані кредитної картки (номер, ім’я власника, термін дії, CVV-код) на шахрайському ресурсі і, як наслідок, втрачають і гроші, і дані банківської картки.

Наступним видом шахрайства, який ми розглянемо, є сніфферінг (сніффінг, sniffing, від англ. “Sniff”, що означає «Нюхати», «винюхувати») – це спосіб шахрайства, що виражається в перехопленні даних. Спеціальна комп’ютерна програма, яка називається «сніффер» може перехопити дані клієнта (наприклад, реквізити банківської карти або паролі від платіжних акаунтів) в мережі Wi-Fi. Як місце «лову даних» шахраї часто вибирають кафе, вокзали, інші місця з великим скупченням людей. Шахрай приходить в громадське місце, наприклад, ресторан, з ноутбуком, на якому і встановлена програма-сніффер. Він активує точку доступу Wi-Fi, назва якої співзвучна з назвою цього ресторану. І якщо клієнт, не підозрюючи про обман, підключається до цієї точки Wi-Fi, то весь його трафік буде перехоплений і проаналізований сніффером [8, с. 86].

Group-IB – єдина приватна компанія в сфері кібербезпеки, яка брала участь в операції – надала європейським правоохоронним органам інформацію про 90 000 банківських карт, скомпрометованих за допомогою фішингових веб-сайтів, банківських троянів під ПК, Android, а також JS-сніфферів, які зловмисники впроваджують на сайти інтернет-магазинів для перехоплення інформації, яка вводиться користувачем даних, – номерів банківських карт, імен, адрес, логінів, паролів тощо. Весь цей величезний масив розрізненої інформації був ретельно зібраний із закритих джерел хакерських соціальних мереж – кардшопів, форумів, ботнетів, JS-сніфферів, і проаналізований системою для дослідження кіберзагроз та полювання за атакуючими Group-IB Threat Intelligence & Attribution. Щоб запобігти незаконному використанню вкрадених даних, співробітники Європолу в режимі реального часу координували обмін інформацією між правоохоронними органами Італії, Угорщини, Великобританії, банками і платіжними системами. В результаті операції Carding Action 2020 європейським фінансовим установам, за даними Європолу, вдалося запобігти потенційним збиткам на суму близько 40 мільйонів євро.

Надалі дослідимо поняття вішингу (англ. Vishing – від voice phishing). Це вид теле-

фонного шахрайства, що дозволяє красти у клієнтів банків конфіденційну інформацію. Клієнт отримує дзвінок від автоінформатора, який повідомляє, що з картою, наприклад, виробляються шахрайські дії, і дає інструкції – передзвонити за певним номером. Далі, слідуючи інструкціям автовідповідача, клієнт повинен повідомити або ввести на клавіатурі телефону реквізити карти. Іноді зловмисники самі дзвонять жертвам, переконуючи, що є співробітниками банку. У банках стверджують, що в телефонних розмовах з клієнтом ніколи не запитують повний номер карти, тим більше не вимагають повідомляти ПІН-код. Щоб прояснити ситуацію, необхідно передзвонити в банк за номерами телефонів, вказаними на офіційному сайті кредитної організації [9, с. 38]. Так, наприклад, у вересні 2020 р. в м. Мелітополі співробітники Служби безпеки України блокували діяльність колл-центру, учасники якого викрадали кошти з банківських рахунків Сбербанку. Слідство встановило, що злочинну схему організували троє жителів Мелітополя. У центрі міста вони обладнали незаконний колл-центр, де «працювало» 54 оператора. Вони видавали себе за співробітників банку, дзвонили клієнтам і отримували від них інформацію про CVV-коди, номери і пін-коди платіжних карт. Для «роботи» з клієнтами банків з Росії зловмисники використовували маршрутизацію міжнародного телефонного трафіку.

Останнім надамо характеристику кардінгу. Це вид шахрайства, для здійснення якого використовуються банківські картки. Найчастіше операції відбуваються з використанням реквізитів картки, які зазвичай викрадають з серверів магазинів електронної торгівлі, платіжних та розрахункових систем і з персональних комп'ютерів користувачів за допомогою шкідливих програм [10, с. 100]. На цей час шахраї також генерують номера банківських карт і продають викрадені номери і коди банківських карт. Кардінг поділяють на дві групи: реальний кардинг і web-кардинг. Реальний кардинг передбачає створення дублікатів банківських карт, за допомогою яких в подальшому відбувається зняття грошових коштів. Дії шахраїв під час web-кардинг обмежуються мережею інтернет. Шахраї дізнаються номери карт, термін дії, ім'я власника картки, адресу проживання і спеціальний код (CVV / CVV2). Отримавши всю потрібну інформацію, зловмисники або купують товари за рахунок власника певної платіжної картки, або переводять всі грошові кошти з карти на свій рахунок.

Деякі махінації в Інтернеті також пов'язані з крадіжкою особистих даних – незаконним отриманням та шахрайським використанням чиїхось особистих даних, зазвичай в економічних цілях. Додамо декілька прикладів із досвіду правоохоронних органів США. Як з'ясувалося в ході одного федерального процесу, відповідачі, як стверджується, взяли імена та ідентифікаційні номери соціального забезпечення офіцерів Збройних Сил США з веб-сайту, а потім використовували понад 100 з цих імен і номерів для отримання кредитних карт в одному з банків штату Делавер через Інтернет. В іншому федеральному процесі відповідачі, як стверджується, взяли особисті дані з сайту федерального органу, а потім використовували ці особисті дані для подачі в режимі онлайн 14 заяв про отримання кредиту для покупки машини в один з банків Флориди.

Висновки. Таким чином, існує безліч способів шахрайства у сфері банківських електронних платежів. Шахраї спритно і досвідчено адаптуються до ходу прогресу, винаходячи нові шахрайські схеми. Основними видами шахрайства в Україні в сфері банківських електронних платежів можна виділити: фішинг, сніфферінг, вішинг, кардінг. Власникам банківських карт, користувачам мережі Інтернет необхідно бути обізнаними про способи шахрайства. Крім того, проявляти грамотність і обережність під час користування онлайн-банкінгом, мобільним зв'язком, послугами в Інтернет-магазинах, уважно заповнювати анкети і форми на різних сайтах.

Література

1. Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI. Офіційний сайт ВР України. URL: http://zakon4.rada.gov.ua/laws/show/4651-17 (дата звернення 15.12.2020).

2. Фінагеєв В.О. Способи вчинення злочинів, пов'язаних із використанням засобів доступу до банківських рахунків. *Науковий вісник Національної академії внутрішніх справ*. 2016. № 1. С. 63–82. URL: http://nbuv.gov.ua/UJRN/Nvknuvs_2016_1_7 (дата звернення 15.12.2020).

3. Методичні рекомендації щодо управління операційним ризиком (у тому числі кіберризиком та безперервністю діяльності) та забезпечення зберігання інформації про клієнтів об'єктами платіжної інфраструктури. URL: https://bank.gov.ua/ua/news/all/metodichni-rekomendatsiyi-schodo-upravlinnya-operatsiynim-rizikom-u-tomu-chisli-kiberrizikom-ta-bezperervnistyu-diyalnosti-ta-zabezpechennya-zberigannya-informatsiyi-pro-kliyentiv-obyektami-platijnoyi-infrastrukturi (дата звернення 15.12.2020).

4. Сазонов М.М. Виды мошенничеств с банковскими картами и совершенствование мер виктимологического предупреждения. *Виктимология:* 2018. № 2 (16). 60 с.

5. Сухова А.Р. О способах незаконного получения средств с банковских карт. *Наука, техника и образование*. 2016. С. 85-86.

6. Изотов Д.С., Быкова Н.Н. Виды мошенничества с банковскими картами. *Вестник НГИЭИ*. 2015. № 3 (46). С. 49–53.

7. Бахтеев Д.В. О некоторых современных способах совершения мошенничества в отношении имущества

физических лиц. *Российское право: Образование. Практика. Наука.* 2016. № 3. С. 24–26.

8. Ягупова Е.А., Палий М.В. Мошенничество с банковскими картами и методы их противодействия в России. *Символ науки.* 2017. № 1. С. 85–88.

9. Табак И.С. Мошенничество с банковскими картами. *Современные инновации.* 2018. № 4 (26). № 1 (19). С. 37–40.

10. Октябрева М.С. Кардинг в Российской практике. *Экономика и управление: анализ тенденций и перспектив развития.* 2014. № 15. С. 99–103.

Анотація

Коваленко І. О. **Криміналістичний аналіз шахрайства у сфері банківських електронних платежів.** – Стаття.

У цій статті виконано криміналістичний аналіз шахрайства в сфері банківських електронних платежів. З настанням пандемії COVID-19 людство фактично замінило реальне життя на Інтернет: всі покупки здійснюються в інтернет-магазинах, доставки їжі стали більш актуальними, ніж похід у ресторан, навіть усі освітні процеси у нашій країні, а також у світі, здійснюються за допомогою онлайн-конференцій у різноманітних додатках, таких як Zoom, Skype, Viber тощо. У зв'язку з цим значно збільшилися масштаби шахрайства у сфері банківських електронних платежів, яке в більшості випадків кваліфікується за ч. 3 ст. 190 Кримінального кодексу України. Моніторинг останніх досліджень і публікацій багатьох відомих вчених в сфері електронного шахрайства показав, що з кожним днем способи, техніка, обізнаність шахраїв прогресують, і вкрай важливо володіти актуальною інформацію про способи вчинення досліджуваного правопорушення для викриття такого виду шахрайства. Таким чином, у статті було виділено такі основні види шахрайства у сфері банківських електронних платежів: фішинг, сніфферінг, вішинг, кардінг. Фішинг – один з видів інтернет-шахрайства, метою якого є отримання доступу до конфіденційних даних користувачів за допомогою проведення масових розсилок від імені популярних компаній або організацій, які містять посилання на помилкові сайти, що практично не відрізняються від сайтів справжніх компаній. Сніфферінг – це спосіб шахрайства, що виражається в перехопленні даних з використанням шахрайської Wi-Fi-мережі та спеціальних сніффер-програм. Вішинг – вид телефонного шахрайства, в якому зловмисники вводять в оману людей, виманюючи персональні дані та дані кредитних карток і рахунків, представившись переважно співробітником банківської установи. Кардінг – вид шахрайства, за якого операції відбуваються з використанням реквізитів картки, які зазвичай викрадають з серверів інтернет-магазинів, платіжних та розрахункових систем і з ПК користувачів за допомогою шкідливих програм. У статті наведено декілька прикладів викриття шахрайства у сфері банківських електронних платежів із досвіду українських правоохоронних органів, а також зарубіжних країн.

Ключові слова: шахрайство, фішинг, вішинг, сніфферінг, кардінг.

Summary

Kovalenko I. O. **Forensic analysis of fraud in bank electronic payments.** – Article.

This article performs a forensic analysis of fraud in the field of electronic banking. In time of the COVID-19 pandemic, humanity has virtually replaced real life with the Internet: all purchases are made in online stores, food delivery has become more relevant than going to a restaurant, even all educational processes in our country and in the world are made online -conferencing in various applications, such as Zoom, Skype, Viber, etc. In this regard, the scale of fraud in the field of electronic bank payments has significantly increased, which in most cases qualifies under Part 3 of Art. 190 of the Criminal code of Ukraine. Monitoring of recent research and publications of many well-known scientists in the field of electronic fraud has shown that every day the methods, techniques, awareness of fraudsters are progressing, and it is extremely important to have up-to-date information on how to commit the offense to detect this type of fraud. Thus, the article highlighted the following main types of fraud in the field of electronic bank payments: phishing, sniffing, vishing, carding. Phishing is a type of online fraud that aims to gain access to sensitive user data through mass mailings on behalf of popular companies or organizations that contain links to erroneous sites that are virtually indistinguishable from the sites of real companies. Sniffering is a method of fraud, which is expressed in the interception of data using a fraudulent Wi-Fi network and special sniffer programs. Witching is a type of telephone fraud in which attackers mislead people by extorting personal and credit card and account information, posing primarily as an employee of a banking institution. Carding is a type of fraud in which transactions are made using card details, which are usually stolen from online store servers, payment and payment systems, and from users' PCs using malware. The article presents several examples of exposing fraud in the field of electronic bank payments from the experience of Ukrainian law enforcement agencies, as well as foreign countries.

Key words: fraud, fishing, vishing, sniffering, carding.