Ученые записки Крымского федерального университета имени В. И. Вернадского
Юридические науки. – 2024. – Т. 10 (76). № 1. – С. 260–265.

УДК 343.9

К ВОПРОСУ О НЕКОТОРЫХ СПОСОБАХ СОВЕРШЕНИЯ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА

Бадиков Д. А. Елисеева К. А.

В статье раскрывается вопрос об отдельных способах совершения мошенничества с использованием электронных средств платежа, а также механизм их воздействия на потерпевшего. Важно отметить, что что на современном этапе развития современного российского гражданского общества, качественного совершенствования науки и техники в рамках бурного роста электронных технологий, используемых в различных областях нашей жизни, появляются и негативные процессы и элементы, которые фактически вредят жизнедеятельности граждан нашей страны. В целях раскрытия и расследования рассматриваемого вида преступлений целесообразно использовать соответствующий набор специальных знаний, которым может обладать как само лицо, производящее производство по уголовному делу, так и соответствующего рода специалист.

Ключевые слова: электронные средства платежа, скимминг, фишинг, кардинг, вишинг.

Простота осуществления денежных обменов, более безопасный и быстрый доступ к денежным ресурсам среди различных других компонентов значительно продвинули систему онлайн-платежей по сравнению с системой, основанной на наличной валюте, однако в ней возникает множество проблем. Транзакции становятся все более значимыми для экономики в целом, их оперативный перевод осуществляется с минимальными затратами, что позволяет мошенникам постоянно совершенствовать способы осуществления преступной деятельности. Как указывается в юридической литературе на современном этапе отмечается рост количества мошенничеств в рассматриваемой сфере [1].

С развитием технологий, преступники улучшают и методы совершения хищения, модернизируют технику, применяемую для скимминга, шиминга, фишшинга. Для более точного понимания механизма совершения подобного рода мошенничеств необходимо подробнее рассмотреть данные способы [2].

Классический фишинг предполагает отправку электронных писем большому количеству людей со ссылками на веб-страницу, выдающую себя за банк. Затем веб-страница запрашивает учетные данные для входа в систему или данные кредитной карты. Доступ к банковским онлайн-счетам приводит к хищению средств, а кредитные карты монетизируются.

SMS-фишинг предполагает отправку потерпевшим текстового сообщения, выдающего себя за финансовое учреждение. Сообщение может содержать ссылку на классическую фишинговую страницу или содержать номер телефона. В любом случае обращаются к жертве, и конечным результатом становится мошенничество.

Множество видов фишинга широко распространено в социальных сетях, в которых преступники используют платформы для поиска потенциальных жертв. Данный процесс может включать в себя создание имен учетных записей, похожих на имена финансового учреждения, выдачу себя за руководителей банка или отправку сообщений под видом иных сотрудников финансовых учреждений. Затем с жертвами связываются и посредством социальной инженерии совершается мошенничество.

Во всех этих вариантах фишинга используются технические методы для установления контакта с жертвами. В данном случае важно понимать цепочку мошеннических атак от первоначального контакта до окончания перевода средств. На каждом этапе атаки собираются цифровые доказательства, и проводятся расследования для определения лиц, причастных к этому [3].

Существуют также некоторые преступления, связанные с финансовыми технологиями, которые не всегда совершаются через Интернет, но все же имеют технологический аспект. Автоматические кассовые аппараты (банкоматы) часто используются для хищения магнитных карт. Этот процесс выражается в скимминге, который относится к электронному устройству, размещенному над гнездом для вставки карты, считывающем магнитную полосу. Отдельная (неофициальная) камера установлена с видом на клавиатуру для перехвата PIN-кода. PIN-код и информация о карте собираются преступниками (физически или с помощью беспроводного удаленного доступа), а затем используются для мошенничества. Само электронное устройство, размещаемое внутри гнезда для вставки карты, позволяющее перехватывать данные карты, и помещающенное между чипом карты и считывателем чипов, называется шимминг. Кроме того, в банкоматах установлен обычный компьютер, контролирующий выдачу наличных. Некоторые атаки включают в себя компрометацию этого компьютера (через USB или другими способами), что приводит к «джекпоттингу», в результате которого автомат выдает большие суммы наличных.

Более продвинутая атака включает в себя компрометацию центральных систем управления, которые осуществляют контроль над сетями банкоматов или терминалов платежных карт. Когда преступники получают доступ к этим центральным системам, они получают возможность распределять наличные деньги и похищать финансовую информацию в более крупных размерах.

В этих примерах происходят манипуляции с оборудованием, либо системы скомпрометированы, что приводит к хищению наличных денег или информации. В данном случае необходим анализ аппаратного обеспечения и скомпрометированного банкомата или терминала платежных карт, чтобы определить, как был получен доступ к системам и информации и как атака была монетизирована [4].

Для достижения этих целей также используются вредоносные программы для онлайн-банкинга, или банковские трояны, осуществляющие заражение компьютеров, приводящее к несанкционированному доступу к банковским счетам для совершения мошеннических действий. Компьютер становится частью преступной сети зараженных технических средств, называемых ботнетом. Когда какой-либо пользователь пытается получить доступ к своему порталу онлайн-банкинга, вредоносная программа становится активной, манипулируя сеансом для подготовки мошеннических платежей. Как только банковский счет будет успешно очищен, вредоносная программа предотвратит дальнейшие входы в систему или будет манипулировать пользовательским интерфейсом, чтобы избежать обнаружения.

Вредоносное ПО для мобильного банкинга включает в себя заражение мобильных телефонов с целью перехвата процессов в существующих платежных приложениях. Наиболее распространенным методом является атака наложением, при которой перехватываются в том числе и нажатия пальцами.

При использовании мобильного банковского приложения вредоносная программа берет под контроль взаимодействие между пользователем и приложениями для

совершения мошеннических платежных операций. Перехват аутентификации на основе SMS также распространен среди мобильных вредоносных программ. В обоих этих случаях фишинг обычно используются для доставки вредоносного ПО пользователю и заражения устройства.

Вишинг или голосовой фишинг (VoIP) предполагает, что преступники связываются с гражданами по телефону и выдают себя за сотрудников банка. Правдоподобие повышается в сочетании с определенными интонациями и акцентами, а также другими тактиками социальной инженерии (процесс манипулирования людьми с целью заставить их действовать определенным образом или выдать конфиденциальную информацию). Функция VoIP позволяет скрывать вызовы или выдавать себя за них. Подмена идентификатора вызывающего абонента часто используется мошенниками для сокрытия своей реальной личности и затрудняет блокировку спам-звонков или принятие юридических мер против мошенников.

Для этого, как отмечалось следствием, мужчина приобрел на одном из интернет-сайтов специальную программу, используемую для обеспечения цифрового голосового общения удаленных абонентов в целях передачи голоса IP-сетью посредством подменного абонентского номера. Телефония, которая раньше была закрытой системой, за последние несколько десятилетий претерпела фундаментальные изменения. Внедрение новых коммуникационных технологий и интеграция телефонии с Интернетом еще больше усложнили ее. Несмотря на это, проблемы безопасности в данной сфере недостаточно хорошо изучены и должным образом не решены. Исполнителями голосового мошенничества могут быть любые участники телефонной системы, такие как операторы, сторонние поставщики услуг, клиенты, сотрудники и любые другие лица, имеющие мотивацию для совершения мошенничества [5].

Большинство атак могут быть выполнены удаленно, и они не требуют серьезного оборудования или высокого уровня технических знаний. Сама телекоммуникационная индустрия включает в себя операторов, регулирующие органы и пользователей. Операторы и поставщики услуг обычно делятся информацией, связанной с мошенничеством, со своими партнерами и различными отраслевыми ассоциациями. Однако подобные данные часто ограничены и имеют закрытый доступ.

Большинство мобильных сетей поддерживают современные протоколы 3G и 4G /LTE, в которых ведутся соединения. Каждое поколение мобильной связи использует ту или иную форму шифрования (по беспроводному каналу) и специальное оборудование для обработки связи и идентификации клиента. Телефоны используют SIM-карту (модуль идентификации абонента), которая принадлежит определенному пользователю сети. SIM-карта содержит криптографический ключ, который присваивается оператором и связан с индивидуальным номером абонента.

В свою очередь, передача голоса по IP (VoIP), которая используется для совершения мошенничеств, появилась как альтернатива традиционной. В настоящее время телефонные сети состоят из различных шлюзов. Однако имеются сервисы, которые работают поверх каналов передачи данных и, как правило, находятся вне контроля операторов. Такие голосовые сервисы (например, Skype, Viber, WhatsApp) привлекают все больше пользователей и рассматриваются операторами как угроза. Прежде всего, это связано с тем, что их трудно идентифицировать, обнаружить и предотвратить [6].

Коммутаторы в главных офисах операторов управляют установлением вызова путем создания канал от телефона вызывающего абонента к телефону вызываемого абонента. Они позволяют осуществлять цифровую передачу данных по беспроводным линиям связи. Манипулирование маршрутизацией вызовов возможно, поскольку операторы имеют полный контроль над вызовами, которые проходят через их сети (либо законно, либо из-за перехвата).

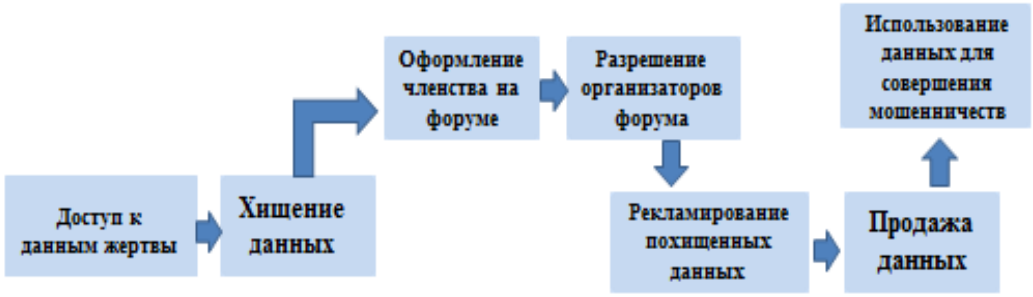
Лицо, совершающее мошеннические действия и выступающее в качестве оператора, может переадресовывать вызов или незаконно отправлять его по сети. В данном случае идентификатор вызывающего абонента (номер телефона мошенника, совершающего звонок) может быть изменен, чтобы подделать источник вызова. Различные онлайн-сервисы и мобильные приложения обеспечивают подмену идентификатора вызывающего абонента через соединения шлюза поставщика услуг.

Подобная ситуация отражена в решении суда Малодербетовского районного суда Республики Калмыкия по делу № 2-36/2020. Согласно информации, отраженной в источнике, у гражданина О. возник преступный умысел на совершение мошеннических действий с использованием информационно-телекоммуникационных сетей. Для его осуществления им была приобретена специальная программа, передающая голосовые данные при звонке посредством IP-сети с подменой индивидуального абонентского номера. После этого он совершил звонок гражданину Н., представляясь сотрудником ПАО «Сбербанк России», отправил ему сообщение на номер телефона, привязанный к дебетовой карте, с кодом подтверждения входа в личный кабинет банка. Гражданин Н., предполагая, что звонок поступает действительно от сотрудника банка, сообщил код из смс-сообщения. В свою очередь, гражданин О. путем обмана получил доступ к личному кабинету клиента и перечислил с расчетного счета гражданина Н. денежные средства в размере 15 587 руб. на свой счет и распорядился ими по своему усмотрению [7].

Преступники умело используют всю доступную информацию и технологии, разбираются в психологии людей, вынуждая жертву раскрывать необходимую информацию для доступа к его персональным личным данным, либо совершать нужные преступнику действия. К сожалению, следует отметить, что широкому распространению дистанционных видов мошенничеств с использованием электронных средств платежа способствует использование банковскими организациями неэффективных средств аутентификации клиентов, что позволяет злоумышленникам использовать карты, оформленные на других лиц [8]. Подобным образом законодатель, учитывая общественную опасность хищения электронных средств платежей, сделал самостоятельными составами преступлений элементы способа подготовки к хищению [9].

Одним из таких способов является отдельная отрасль мошенничества-«кардинг». В нормативных правовых актах Российской Федерации данное понятие отсутствует. Его сущность заключается в получении материальной выгоды посредством незаконного получения данных держателей карт с помощью банковских инструментов электронных расчетов [10]. Основным способом аккумулирования данной информации являются кардинг-форумы – это места встреч (настройки конвергенции), где происходит обмен учебными пособиями, программным обеспечением и украденной информацией, а также её продажа. Целями кардинг-форумов являются информирование, помощь, обучение и создание возможности предлагать похищенную информацию или ресурсы, предназначенные в основном для совершения различного рода

преступлений. Примерная схема действий участников кардинг-форумов представлена на Рисунке 1. Схема действий участников кардинг-форумов



Его использование начинается с получения доступа к личной информации жертв, для чего необходимо членство на форуме. На данном этапе лицо подготавливает технические средства, устройства и программное обеспечение для обмена данными, затем собирает максимальный объем информации из форума путем покупки незаконно продающихся баз данных. После этих операций происходит непосредственная связь с держателями счетов в различных формах (звонки, сообщения, гиперссылки для перевода денежных средств) [11].

Как справедливо отмечается в специализированной литературе, в зависимости от способа получения информации об электронном денежном счете держателя-собственника кардинговые преступления можно разделить на удаленные бесконтактные удаленные контактные, когда кардер лично пересекается либо с собственником денежных средств, либо с банковскими средствами платежа.

Одной из методик выявления лиц, совершающих кардинговые преступления, может быть, постоянный мониторинг рынков сбыта подобных предметов на Интернет-сервисах, размещающих объявления граждан о различных товарах. Также необходимо усилить контроль со стороны банков за подозрительными транзакциями на счетах, на которые кардеры перечисляют денежные средства, для последующего их обналичивания. Вторым классическим способом вывода денежных средств со счета держателя-собственника на условный счет лица, совершившего мошеннические действия для получения денежных средств, является их вывод со счета держателя-собственника на различные счета кардера с предварительным усложнением цепочки транзакций по счетам с целью скрыть следы совершенного преступления [12].

Подводя итог вышесказанному, следует отметить, что рассмотренные способы совершения действий по обману граждан на основе установления с ними доверительных отношений преступники, как правило, объединяют с иными способами получения интересующей их информации о финансовых возможностях граждан и с последующим заражением их электронных устройств, компьютеров и т.д. соответствующими программами-вирусами, котрые позволяют считывать и копировать информацию, интерессующую преступников, а именно комбинации симвовлов, составляющие пароли и иные сведения, необходимые для для получения доступа и управления финансовыми потоками гражданина.

Список литературы:

1. Бадиков Д.А., Елисеева К.А. Алгоритм действий следователя при расследовании мошенничества с использованием электронных средств платежа // Закон и порядок. 2023. № 4. С. 153-155.
2. Соловьева Е.А. Преступления, совершаемые в платежных системах: монография / Е.А. Соловьева; под ред. Н.А. Лопашенко. Москва: Юрлитинформ. 2021. С. 115-118.
3. Петрякова Л.А. Проблемы квалификации мошенничества в банковской сфере // Сибирский юридический вестник. 2020. № 3 (90). С. 80-84.
4. Клепицкий И.А. Новое экономическое уголовное право: монография. М.: Проспект, 2021. 984 с.
5. Саблина Т.И., Никитенко И.В. Мошенничество с использованием платежных карт: вопросы теории, законодательства и практики его применения // Молодой ученый. 2019. № 48 (182). С. 275-279.
6. Яни П.С. Мошенничество с использованием электронных средств платежа // Законность. 2019. №. 5.
7. Решение № 2-36/2020 2-36/2020 (2-930/2019;)~М-935/2019 2-930/2019 М-935/2019 от 21 февраля 2020 г. по делу № 2-36/2020. URL: https://sudact.ru/regular/doc/tOcpqYekicZJ/.
8. Анненкова Е.А. Преступления в сфере электронных средств платежей как объект криминалистического исследования // Экономическая безопасность и качество. 2020. № 2(39). С. 45-48.
9. Волков А.С., Мозговая Д.А. Криминалистическая классификация в методике расследования подлога документов // Российский следователь. 2018. № 4. С. 8-15.
10. Бадзгарадзе Г.Д. Современные способы совершения преступлений с использованием электронных средств платежа, кардинг // Право. Общество. Государство. 2020. № 4. С. 107-110.
11. Малянова К.П. Актуальные проблемы в деятельности правоохранительных органов при выявлении и раскрытии преступлений с использованием электронных средств платежа // Юристъ-Правоведъ. 2021. № 2(97). С. 148-151.
12. Бадзгарадзе Г.Д. Современные способы совершения преступлений с использованием электронных средств платежа, кардинг // Сборник научных трудов студентов и аспирантов. Том 10. Редколлегия: Д.В. Рыбин (пред.), Е.В. Трофимов (отв. ред.) [и др.]. Санкт-Петербург, 2020. С. 105-109.

Badikov D.A., Eliseeva K.A. To the question of some ways of committing fraud using electronic means of payment // Scientific notes of V. I. Vernadsky crimean federal university. Juridical science. – 2024. – T. 10 (76). № 1. – P. 260–265.

The article reveals the issue of individual methods of committing fraud using electronic means of payment, as well as the mechanism of their impact on the victim. It is important to note that at the present stage of the development of modern Russian civil society, the qualitative improvement of science and technology within the framework of the rapid growth of electronic technologies used in various areas of our life, there are also negative processes and elements that actually harm the life of citizens of our country. In order to disclose and investigate the type of crimes under consideration, it is advisable to use an appropriate set of special knowledge, which may be possessed by both the person conducting the proceedings in a criminal case and the appropriate kind of specialist.

Keywords: electronic means of payment, skimming, phishing, carding, phishing..

Spisok literatury:

1. Badikov D.A., Eliseeva K.A. Algoritm dejstvij sledovatelya pri rassledovanii moshennichestva s ispol'zovaniem elektronnyh sredstv platezha // Zakon i poryadok. 2023. № 4. S. 153-155.
2. Solov'eva E.A. Prestupleniya, sovershaemye v platezhnyh sistemah: monografiya / E.A. Solov'eva; pod red. N.A. Lopashenko. Moskva: YUrlitinform. 2021. S. 115-118.
3. Petryakova L.A. Problemy kvalifikacii moshennichestva v bankovskoj sfere // Sibirskij yuridicheskij vestnik. 2020. № 3 (90). S. 80-84.
4. Klepickij I.A. Novoe ekonomicheskoe ugolovnoe pravo: monografiya. M.: Prospekt, 2021. 984 c.
5. Sablina T.I., Nikitenko I.V. Moshennichestvo s ispol'zovaniem platezhnyh kart: voprosy teorii, zakonodatel'stva i praktiki ego primeneniya // Molodoj uchenyj. 2019. № 48 (182). S. 275-279.
6. YAni P.S. Moshennichestvo s ispol'zovaniem elektronnyh sredstv platezha // Zakonnost. 2019. №. 5. S. 25.
7. Reshenie № 2-36/2020 2-36/2020 (2-930/2019;)~M-935/2019 2-930/2019 M-935/2019 ot 21 fevralya 2020 g. po delu № 2-36/2020. URL: https://sudact.ru/regular/doc/tOcpqYekicZJ/.
8. Annenkova E.A. Prestupleniya v sfere elektronnyh sredstv platezhej kak ob"ekt kriminalisticheskogo issledovaniya // Ekonomicheskaya bezopasnost' i kachestvo. 2020. № 2(39). S. 45-48.
9. Volkov A.S., Mozgovaya D.A. Kriminalisticheskaya klassifikaciya v metodike rassledovaniya podloga dokumentov // Rossijskij sledovatel'. 2018. № 4. S. 8-15.
10. Badzgaradze G.D. Sovremennye sposoby sovershheniya prestuplenij s ispol'zovaniem elektronnyh sredstv platezha, karding // Pravo. Obshchestvo. Gosudarstvo. 2020. № 4. S. 107-110.
11. Malyanova K.P. Aktual'nye problemy v deyatel'nosti pravoohranitel'nyh organov pri vyyavlenii i raskrytii prestuplenij s ispol'zovaniem elektronnyh sredstv platezha // YUrist"-Pravoved". 2021. № 2(97). S. 148-151.
12. Badzgaradze G.D. Sovremennye sposoby sovershheniya prestuplenij s ispol'zovaniem elektronnyh sredstv platezha, karding // Sbornik nauchnyh trudov studentov i aspirantov. Tom 10. Redkollegiya: D.V. Rybin (pred.), E.V. Trofimov (otv. red.) [i dr.]. Sankt-Peterburg, 2020. S. 105-109.