DOI 10.46741/2713-2811-2021-5-114-117
УДК 343.9

Способы мошенничества, совершаемого с использованием средств связи: криминалистический аспект

В. С. ЭКОНОМЮК – аспирант Российского государственного университета правосудия

В статье раскрываются особенности совершения мошенничества с использованием мобильных средств связи, приводится статистика и выявляются причины роста числа преступлений данной категории. Анализируются способы совершения телефонных мошенничеств с описанием технологий их реализации.

Ключевые слова: телефонное мошенничество; организованная преступная группа; способы совершения мошенничества.

12.00.12 – Криминалистика; судебно-экспертная деятельность; оперативно-розыскная деятельность.

Для цитирования: Экономюк В. С. Способы мошенничества, совершаемого с использование средств связи: криминалистический аспект. *Ius publicum et privatum : сетевой научно-практический журнал частного и публичного права,* 2021, № 5 (15), с. 114–117, DOI 10.46741/2713-2811-2021-5-114-117.

Methods of fraud committed with the use of communications: a criminalistic aspect

V. S. ECONOMYUK – Post-Graduate Student of the Russian State University of Justice

The article reveals the features of committing fraud with the use of mobile communications, provides statistics and indicates the reasons for the increase in the number of crimes in this category. Methods of committing telephone frauds with a description of the technologies for their implementation are analyzed.

Key words: phone fraud; organized criminal group; ways of committing fraud.

12.00.12 – Forensics; forensic activity; operational searching.

For citation: Ekonomyuk V. S. Methods of fraud committed with the use of communications: a criminalistic aspect. *Ius publicum et privatum: online scientific and practical journal of private and public law,* 2021, no. 5 (15), pp. 114–117, DOI 10.46741/2713-2811-2021-5-114-117.

Одной из характерных примет современного мира является использование мобильных устройств для передачи информации, количество которой неуклонно растет. С каждым годом развиваются интернет-ресурсы, социальные сети и мессенджеры, привлекая новых пользователей и предоставляя им все больше новой информации. Благодаря современным мобильным устройствам и сервисам сотовой связи стали доступны приложения мобильных банковских систем, через которые можно совершать денежные транзакции и пользоваться услугами банков, не посещая их отделения. Особенно активно граждане стали использовать мобильные приложения для общения и обмена информацией в период пандемии коронавирусной инфекции COVID-19.

Легко представить утро обычного человека, которое начинается с использования мобильного устройства для просмотра социальных сетей и мессенджеров. В течение дня пользователями производится оплата счетов за коммунальные услуги, делаются покупки в продуктовом магазине, осуществляются денежные транзакции с использо-

ванием мобильных банковских приложений. Пользователи также могут получать входящие звонки и уведомления: часть из них от коллег, клиентов, близких и родственников, а часть – навязчивая реклама услуг и сервисов. Чаще всего данная информация не создает финансовых либо моральных проблем, поскольку нежелательный телефонный разговор, касающийся личных денежных средств и их похищения, можно прервать самостоятельно, проигнорировать или отклонить. Однако доверчивым гражданам сделать это сложно по причине отсутствия информационной грамотности, знания нормативно-правовых документов, а также правил использования банковских мобильных приложений и их услуг.

По данным Центрального банка России, объем похищенных средств в первом полугодии 2020 г. на 39 % превышает показатель того же периода 2019 г., когда мошенникам удалось заполучить 2,8 млрд руб.[1] Исходя из этого, телефонное мошенничество можно рассматривать как один из интенсивно развивающихся видов противоправной деятельности.

Определяющим криминалистическим признаком мошенничества служит способ его совершения, который в конечном счете сводится к обману или злоупотреблению доверием обманутого лица, организации и направлен на получение имущественной выгоды[2].

В научном сообществе не сформировано единой точки зрения по вопросу определения понятия «способ совершения преступления». Например, по мнению авторов учебника по криминалистике, важное криминалистическое значение имеет способ совершения преступления, «индивидуальный почерк» преступника, вырабатываемый при многократном повторении аналогичных действий в сходных условиях[3].

Под способом совершения преступления понимается система действий субъекта, направленных на достижение преступной цели и объединенных единым преступным замыслом. В этой системе могут быть выделены действия по подготовке, совершению и сокрытию следов преступления[4].

Отсутствие непосредственного, а также дистанционного зрительного контакта между потенциальным потерпевшим и преступником в случае реализации телефонного мошенничества только способствуют совершению преступления. Мошенник, используя средство мобильной связи, входит в доверие к жертве, чаще всего представляясь сотрудником безопасности одного из популярных банков, например Публичного акционерного общества (далее – ПАО) «Сбербанк», выясняет причину и факт перечисления конкретной суммы денежных средств другому лицу. Упоминание мошенником вымышленного имени сотрудника безопасности именно ПАО «Сбербанк» может ввести в заблуждение, поскольку данный банк имеет целую сеть отделений по всей России, пользуется доверием граждан на протяжении десятилетий. Впрочем, следует отметить, что сейчас набирают большую популярность такие банки, как ПАО «ВТБ» и Акционерное общество «Тинькофф банк»[5]. В ходе разговора мошенник при помощи методов социальной инженерии (уважительного отношения, мягких интонаций, убедительных аргументов и др.) пытается заполучить либо доступ к мобильному приложению банка жертвы (через авторизацию по номеру телефона), либо полные данные банковской карты, включая секретный код (CVV-код).

У потенциального потерпевшего, если он не сталкивался с подобной ситуацией либо не был проинформирован о данных видах противоправных деяний, возникает доверие к представителю отдела безопасности банка, который пытается помочь разобраться в сложившейся ситуации. Чаще всего жертва начинает нервничать, теряет бдительность из-за вероятной возможности потери денежных средств со счета, поэтому сообщает все данные, необходимые злоумышленнику. При упоминании должности сотрудника отдела безопасности снижается уровень критического мышления и появляется надежда на то, что опасность несанкционированного списания денежных средств с банковского счета минует благодаря действиям специалиста.

Преступник, чувствуя свою безнаказанность, защищенность от жертвы дистанционным методом общения, уверенно и тщательно собирает всю интересующую его информацию о денежных средствах.

Однако мошенничество, совершаемое при помощи звонка якобы представителя крупного банка, является далеко не единственным способом обмана граждан. Среди распространенных способов мошенничества можно назвать следующие.

Во-первых, возврат случайно перечисленных денежных средств. В данной ситуации потенциальной жертве приходит СМС-уведомление с номера телефона банка, содержащее информацию о перечислении денежных средств на банковский счет. Де-

нежные средства действительно могут быть зачислены на счет, однако спустя некоторое время потерпевшему поступает телефонный звонок от мошенника с просьбой вернуть денежные средства самостоятельно через приложение банка. Честный гражданин возвращает поступившие денежные средства, затем злоумышленник звонит в банк и просит отозвать платежное поручение на основании письменного заявления об ошибке. Таким образом, с банковского счета денежные средства списываются дважды: по добровольному поручению жертвы без указания назначения платежа и заявлению мошенника. С точки зрения способа совершения преступления необходимо провести анализ действий мошенника. При подготовке к совершению преступления мошенником изучаются данные об открытых банковских счетах жертвы с целью недопущения возможных ошибок и увеличения шансов на обогащение. В момент совершения мошенничества осужденный звонит с извинениями потенциальной жертве, убеждает ее проверить баланс банковского счета и настоятельно просит вернуть денежные средства, избегая информации об обращении в банк с заявлением о возврате. Скрывая следы преступления, мошенник блокирует абонентский номер жертвы и обращается в банк или службу поддержки с заявлением об ошибочном переводе.

Во-вторых, мошенничество с использованием «фишинговых» (от англ. fishing – рыбная ловля, выуживание) интернет-ресурсов. Данный вид мошенничества актуален при продаже физическими лицами вещей, бывших в употреблении, на всероссийских торговых площадках, например Авито.ру или Юла.ру и др. Суть преступления заключается в переходе от общения продавца и покупателя на официальных страницах торговых площадок, где установлен порядок торговли и сама площадка является гарантом сделки, к общению в мессенджерах, например Ватсап. Потенциальной жертве присылается ссылка на «фишинговый» интернет-ресурс для оплаты товара, в котором указываются реквизиты платежных карт и сумма[6], однако денежные средства не поступают на счет, а списываются, а потерпевший блокируется преступником, после чего связаться с последним не представляется возможным. В связи с массовостью таких случаев и большим общественным резонансом администрации торговых площадок опубликовали официальный комментарий[7], содержащий в себе признаки отнесения потенциальной сделки к мошеннической. Рассмотрим способ совершения преступления такого рода. Так, при подготовке описанного способа мошенничества преступник отбирает реальные объявления продавцов в ценовом диапазоне 3–5 тыс. руб. Указанная сумма не случайна, поскольку обращение в правоохранительные органы затратно по времени. В процессе совершения преступления жертве задается несколько уточняющих вопросов о состоянии и степени употребления вещи с целью обозначения интереса к покупке, особенно если объявление размещено продолжительное время и цена слегка завышена. Впоследствии продавец убеждает внести оплату якобы на сайте торговой площадки. Уничтожая следы мошенничества, преступники удаляют из поисковой системы данные о сайте и блокируют абонента в мессенджерах.

В-третьих, наиболее опасным и тщательно спланированным считается мошенничество, в котором потенциальной жертве предлагается помочь сотрудникам правоохранительных органов в изобличении преступной группы. Данный способ мошенничества предполагает более тщательную подготовку, а также требует согласованности действий между соучастниками. Внутри группы имеет место четкое распределение ролей вплоть до проговаривания конкретных реплик.

Так, например, гражданке А. позвонил неизвестный и представился сотрудником службы безопасности крупного банка. Заявительница сразу поняла, что ее пытаются обмануть и прекратила разговор с злоумышленниками. После этого мошенники перезвонили потенциальной жертве повторно с подмененного номера дежурной части Управления Министерства внутренних дел России по Ханты-Мансийскому автономному округу – Югре и представились сотрудниками полиции. Они сообщили, что ведут разработку мошенников, которые ей звонили, и попросили следовать инструкциям мошенников, чтобы не сорвать операцию. Жительница согласилась оказать содействие правоохранительным органам, в результате чего преступники получили доступ к личному кабинету потерпевшей и похитили около 150 тыс. руб.[8] В ходе подготовки к совершению преступления мошенники предварительно получают незаконным путем персональную информацию о будущих жертвах, ориентируются в диапазоне дневного времени суток в регионе, куда планируется телефонный звонок. В момент непосредственного совершения преступления

мошенник максимально использует заученные фразы и интонации, характерные для сотрудника банка, задает вопросы, ответы на которые предполагают получение дополнительных сведений.

Таким образом, мошенники используют чувство ответственности и гражданского долга потенциальной жертвы, которая начинает испытывать гордость за проявленные мужество, отвагу, неравнодушие к общественной проблеме телефонного мошенничества, а также понимает свою причастность к снижению числа преступлений. При этом потерпевший не осознает, что совершает точно такие же действия, какие требуется преступникам, например называет CVV-код, и денежные средства списываются с банковского счета.

Следует отдельно остановиться на ситуации, когда мошенник представляется сотрудником правоохранительных органов и внушает жертве, что в отношении нее возбуждено уголовное дело по факту причастности к легализации доходов, полученных преступным путем, либо незаконному предпринимательству. Преступник использует особую интонацию и манеру общения, перечисляет статьи УК РФ, оказывает негативное влияние на моральное и психологическое состояние потенциальной жертвы, которая введена в заблуждение и теряет бдительность, у нее создается впечатление реального разговора с представителями правопорядка, факт общения с которыми для многих граждан является стрессовой ситуацией.

Мошенничество с использованием средств сотовой связи, осуществляемое из учреждений уголовно-исполнительной системы, – явление не новое и достаточно изученное. Однако с течением времени механизм совершения таких преступлений усложняется и принимает изощренный характер, поскольку злоумышленники изобретают и постоянно совершенствуют способы завоевания доверия граждан, также меняются степень технической оснащенности преступников и технологии получения персональных данных клиентов банков.

Для предупреждения, выявления и пресечения рассматриваемых противоправных действий, увеличения числа раскрытых преступлений необходимы новые комплексные меры, которые будут способствовать уменьшению количества устройств, проносимых в исправительные учреждения, информированию граждан, а также выработке технических решений, направленных на усиление безопасности и снижение возможностей осуществления противоправных деяний с использованием мобильных устройств, сотовой связи, мобильных банковских приложений.

ПРИМЕЧАНИЯ

[1] Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств за I и II кварталы 2019/2020 года. URL: https://www.cbr.ru/analytics/ib/review_1q_2q_2020/ (дата обращения: 03.11.2021).
[2] Криминалистика : учеб. для вузов / под ред. Р. С. Белкина. М., 2001. С. 524.
[3] Ищенко Е. П., Топорков А. А. Криминалистика : учеб. 2-е изд. М., 2010. С. 361.
[4] Криминалистика : учеб. для вузов / под ред. Р. С. Белкина. С. 66.
[5] Названы самые популярные банки в России. URL: https://plusworld.ru/daily/banki-i-mfo/nazvany-samye-populyarnye-banki-v-rossii/ (дата обращения: 14.03.2021).
[6] Как меня обманули на 15 000 рублей с «Авито-доставкой». URL: https://journal.tinkoff.ru/avito-delivery-fraud (дата обращения: 04.10.2021).
[7] Как не попасться мошенникам. URL: https://www.avito.ru/dostavka/bezopasnost (дата обращения: 04.10.2021).
[8] В России появился новый вид мошенничества. URL: https://www.audit-it.ru/news/finance/1026286.html (дата обращения: 18.03.2021).

[1] Obzor otchetnosti ob incidentah informacionnoj bezopasnosti pri perevode denezhnyh sredstv za I i II kvartaly 2019/2020 goda. URL: https://www.cbr.ru/analytics/ib/review_1q_2q_2020/ (data obrashcheniya: 03.11.2021).
[2] Kriminalistika : ucheb. dlya vuzov / pod red. R. S. Belkina. M., 2001. S. 524.
[3] Ishchenko E. P., Toporkov A. A. Kriminalistika : ucheb. 2-e izd. M., 2010. S. 361.
[4] Kriminalistika : ucheb. dlya vuzov / pod red. R. S. Belkina. S. 66.
[5] Nazvany samye populyarnye banki v Rossii. URL: https://plusworld.ru/daily/banki-i-mfo/nazvany-samye-populyarnye-banki-v-rossii/ (data obrashcheniya: 14.03.2021).
[6] Kak menya obmanuli na 15 000 rublej s «Avito-dostavkoj». URL: https://journal.tinkoff.ru/avito-delivery-fraud (data obrashcheniya: 04.10.2021).
[7] Kak ne popast'sya moshennikam. URL: https://www.avito.ru/dostavka/bezopasnost (data obrashcheniya: 04.10.2021).
[8] V Rossii poyavilsya novyj vid moshennichestva. URL: https://www.audit-it.ru/news/finance/1026286.html (data obrashcheniya: 18.03.2021).

Статья поступила 18.10.2021