УДК 343.721

Матвеева Валерия Олеговна,
магистрант, 2 курс,
направление подготовки «Юриспруденция»
Институт государства и права
ФГАОУ ВО «Тюменский государственный университет»
625003 г. Тюмень, ул. Володарского, 6

СПОСОБЫ СОВЕРШЕНИЯ ДИСТАНЦИОННОГО МОШЕННИЧЕСТВА

Аннотация. *Статья посвящена исследованию основных способов совершения дистанционного мошенничества. Обобщены и систематизированы подходы к определению способов совершения дистанционного мошенничества. Предложенные в процессе исследования способы совершения дистанционного мошенничества позволяют повысить эффективность борьбы с данным видом преступлений.*

Ключевые слова: *дистанционное мошенничество, незаконные операции, фишинг, кража, обман.*

WAYS TO COMMIT REMOTE FRAUD

Annotation. *The article is devoted to the study of the main ways of committing remote fraud. Generalized and systematized approaches to determining the methods of committing remote fraud. The methods of committing remote fraud proposed in the course of the study make it possible to increase the effectiveness of the fight against this type of crime.*

Keywords: *remote fraud, illegal operations, phishing, theft, fraud.*

Как показывает анализ следственной и судебной практики, для мошенничеств, совершенных путем незаконных операций дистанционным способом с использованием ЭВТ, более характерна такая форма совершения, как завладение денежными средствами.

В России под признаки мошенничества, совершенного дистанционным способом с использованием информационно-телекоммуникационных технологий, подпадают три состава преступления из Уголовного кодекса РФ: ст. 159 «Мошенничество», ст. 159.3 «Мошенничество с использованием электронных средств платежа» и ст. 159.6 «Мошенничество в сфере компьютерной информации» [1]. Так, в 2020 г. состояние преступности данной категории имело следующие числовые значения: ст. 159 УК РФ - 210 493, динамика роста по отношению к 2019 г. на 75,5%, к 2018 г. - на 132,2%, ст. 159.3 УК РФ - 25 820, динамика роста по отношению к 2019 г. на 60,2%, к 2018 г. - на 508,7%, ст. 159.6 УК РФ - 970, динамика роста по отношению к 2019 г. на 10,8%, однако по отношению к 2018 г. наблюдается отрицательная динамика на 21,5% [2].

Остановимся на наиболее распространенных в России способах совершения дистанционного мошенничества.

1. Фишинг (англ. Phishing) – один из методов мошенничества с использованием социальной инженерии, заключающийся в том, что злоумышленники, имитируя деятельность реально существующих компаний или банков-эмитентов, используя неголосовые средства коммуникации, под разными предлогами выманивают у владельцев платежных карт реквизиты и другую конфиденциальную информацию. Разновидностями фишинга являются: фишинговые сайты; фишинговые электронные письма; фишинговые SMS-сообщения.

2. Кража персональных данных пользователя кредитной карты и данных о самой кредитной карте. В дальнейшем это позволяет преступникам осуществлять манипуляции с банковским счетом, например, производить

заказ товаров в Интернете под чужим именем и оплачивать их, используя чужую кредитную карту или списание средств с чужого счета.

3. Создание интернет-аукционов путем предоставления недостоверных данных и предложения по продаже несуществующих товаров. Обычно преступники регистрируются на вебсайтах интернет-аукционов. При этом мошенники используют анкетные данные близких или посторонних лиц. После чего на сайте под своим доменным именем размещают лот, в который загружают фото товара с максимальной стоимостью и начальной ставкой, где участники интернет-аукциона, потенциальные жертвы, дистанционно ставят ставки на сайте указанного товара. По завершении торгов мошенник связывается с жертвой на сайте интернет-аукциона, однако часто общение может осуществляться путем переписки по электронной почте или мобильной связи. После договоренности в цене мошенник предоставляет жертве реквизиты банковского счета для оплаты товара и услуг пересылки, однако, в конечном итоге, после перечисления средств жертва товара не получает. Мошенник, с целью сокрытия процесса преступных действий и саморазоблачения, может использовать банковские карты других лиц и в дальнейшем обналичивает их путем снятия средств через банкомат. Более опытные преступники, с целью сокрытия своего места нахождения, постоянно меняют IP-адреса, что создает трудности в установлении места нахождения мошенника.

4. Получение данных о банковской карте потерпевшего и последующее перечисление средств с нее. Для этого преступники на сайтах интернет-торговли подыскивают жертв [3]. Обнаружив информацию потенциальной жертвы о продаже товаров, мошенники устанавливают с ней контакт, заверив, что намерены приобрести товар и им нужны данные карты, куда произвести оплату. Затем мошенник звонит жертве и, представившись работником банка, сообщает информацию о невозможности перечисления средств на карту потерпевшей и что для зачисления денежных средств ей необходимо

сообщить конфиденциальные данные банковской карты (анкетные данные жертвы, защитный код карты и кодовое слово), или подойти к терминалу банкомата и выполнить необходимые операции для якобы зачисления средств. Во время разговора по телефону с жертвой мошенник диктует соответствующие комбинации, которые последняя выполняет и путем обмана и незаконных операций с использованием электронно-вычислительной техники получает денежные средства. В дальнейшем мошенник, используя электронные платежные системы сети Интернет, перечисляет денежные средства с карточного счета потерпевшей на свой банковский счет или счет третьих лиц, которым даже не известно, что с их банковскими карточками проводятся преступные операции. Для того чтобы жертва сразу не узнала, что в отношении нее совершено мошенничество, преступники присылают на мобильный номер последней SMS-сообщение о зачислении средств на банковскую карту.

5. Обманное завладение денежными средствами посредством создания или использование сайтов благотворительных организаций. При использовании благотворительных сайтов преступники посылают письма от имени благотворительных организаций или людей, нуждающихся в помощи. При этом ссылки могут принадлежать реальным благотворительным фондам, но реквизиты для перечисления средств принадлежат мошенникам. Кроме этого, преступники путем незаконных операций с использованием ЭВТ создают сайты благотворительных организаций, на которых публикуют объявления с просьбой о материальной помощи на лечение больным детям. Также мошенники на указанных сайтах могут размещать вымышленную информацию о болезни, при этом размещают чужие фотографии людей, нуждающихся в финансовой помощи на лечение, или копируют объявления с сайтов благотворительной помощи, принадлежащих реальным людям, изменяя реквизиты для перечисления денег.

6. Завладение имуществом путём создания и обеспечения деятельности интернет-магазина. Это более сложный способ, чем продажа товаров на интернет-аукционе и состоит из нескольких этапов. Сначала мошенники создают в сети Интернет-сайты в виде интернет-магазинов – аналогов интернет-сайтов, действовавших на территории страны, где размещают заведомо ложную информацию в виде объявлений о продаже товаров, которых в наличии никогда не было. Следующим этапом является создание и получение контроля за фиктивными предприятиями, открытие банковских счетов, на которые заказчики/клиенты фиктивных интернет-магазинов в дальнейшем осуществляют предоплату в виде денежного перевода за приобретение заказанного товара за реквизитами принадлежащих им пластиковых карт. При этом названия фиктивных предприятий должны быть похожи на названия фиктивных интернет-магазинов, чтобы вызывать доверие у пользователей. После чего осуществляется оформление договоров с операторами телефонной связи о предоставлении услуг связи и интернет-связи, так называемой SIP-телефонии, телефонные номера которых служат для обратной связи с заказчиками интернет-магазинов [4]. При этом во входящих звонках на телефоны заказчиков фиктивных интернет-магазинов отображаются городские телефонные номера, что вызывает доверие у пользователей. В отдельных случаях создаются «колл-центры», операторы которых общаются с клиентами, имитируя деятельность колл-центров настоящих интернет-магазинов, принимают заказы и предоставляют реквизиты для перечисления денежных средств. Также разрабатывается специальная веб-страница с базой данных для работы организаторов и операторов «колл-центра», с помощью которой преступники принимают и ведут учет заказов [5]. После совершения мошеннических действий телефонные номера обманутых клиентов заносятся в «черный список».

7. Создание и деятельность фиктивных денежных бирж. Деятельность таких бирж обеспечивается деятельностью преступной группы, которая

маскируется за официально зарегистрированными предприятиями. Мошенники предлагают потенциальным клиентам покупать ценные бумаги для получения прибыли. Используя бренды, преступники задействуют различные веб-ресурсы для имитации добросовестной деловой репутации. После чего так называемые «брокеры» создают у потерпевшего ошибочное представление о процессе осуществления торгов на мировых биржах. Для этого они используют уже установленное на компьютер потерпевшего специальное программное обеспечение для проведения торгов, фактически предоставляющее возможность осуществлять удаленный контроль за его компьютером. Такие компании создают воображение у потерпевших о сотрудничестве с легальными и реальными иностранными компаниями, торгующими ценными бумагами. Такими действиями преступники побуждают потерпевшего вносить свои средства на счет мошеннического торгово-сервисного предприятия, преследуя при этом цель – завладеть его средствами под предлогом заключения сделок по купле-продаже ценных бумаг.

Также в 2020 г. приобрели популярность мошеннические схемы, замаскированные под сервисы доставки платформ объявлений [6]. В таком случае преступники размещали объявления о продаже товаров и для обсуждения деталей предлагали перейти в мессенджеры. Туда покупателям посылали фальшивые накладные для оплаты или ссылки на фейковый ресурс, где нужно оформить доставку. Однако, в конце концов, оплата поступала не на платформу объявлений, а на карту мошенника.

Анализ указанных выше и других способов дистанционных мошенничеств, совершенных с использованием ЭВТ, позволяет разделить их по следующим критериям:

1. По периодичности совершения уголовного правонарушения: единовременные (мошенничество совершается с целью обмана одного лица один раз). К примеру, путем имитирования продажи несуществующего товара

через объявление на сайте Авито [7]; длительные (мошенничество совершается с целью обмана неопределенного круга лиц). К примеру, путем создания сайта по продаже услуг (туристических) или товара (медицинских масок) для неопределенного количества лиц.

2. В зависимости от сферы применения: банковская (завладение конфиденциальными данными клиента банка и последующее перечисление средств с банковских счетов, и получение кредитов); бытовая (получение дорогостоящих вещей по документам своих родственников, по похищенным или найденным документам); страхование (предоставление несуществующих страховых полисов);

3. В зависимости от количества задействованных преступников: совершено одним лицом; группой лиц; организованной группой лиц;

4. В зависимости от предмета посягательства: денежные средства; материальные ценности; информация о личности, аккаунте или банковской карте; право на имущество.

5. От вида ЭВТ, которая использовалась: компьютеры и ноутбуки; телефоны; планшеты; другие виды.

6. В зависимости от информационной поддержки: целенаправленное создание отдельного интернет-сайта; размещение информации на уже существующих интернет-сайтах; путем несанкционированного доступа к ЭВМ потерпевшего;

7. В зависимости от характера «отношений», возникающих между потерпевшим и преступником: данные преступника неизвестны; предварительные данные о лице-преступнике известны; известны предварительные данные только об одном лице, действовавшем в составе группы лиц.

8. В зависимости от места создания и места регистрации IP-адреса ЕОТ: место нахождения установлено (Россия); местонахождение – за границей

(страна и учредительные данные провайдера известны); местонахождение страны не установлено.

9. В зависимости от способов введения в заблуждение или злоупотребления доверием: фальсификация фактов или умышленное сокрытие истины; сокрытие части правды или параллельное представление несуществующих и существующих фактов в качестве истины; уведомление двузначной или не конкретизированной информации; умолчание – полное сокрытие правды; искажение – умышленное сообщение ложной информации

10. По характеру представления сведений: активный (сообщение ложных сведений); пассивный (преднамеренное умалчивание юридически значимой информации).

11. По новизне способа совершения мошенничества: способ обмана (злоупотребление доверием) неизвестен в правоохранительной практике; способ обмана (злоупотребление доверием) встречался ранее в правоохранительной практике.

12. В зависимости от способа подготовки к совершению мошенничества: совершению мошенничества способствовал несанкционированный доступ к ЭВТ; совершение мошенничества осуществлялось с использованием вредоносных программных или технических средств; совершению мошенничества способствовало распространение рекламной или другой продукции о предмете посягательства (оказания услуг).

Подводя итоги, отметим, что проведенный анализ позволил установить следующие виды имущества, на которое может посягать дистанционное мошенничество:

- имущество (движимое, недвижимое);

- право на имущество.

Особенностью предмета мошенничества, совершенного с использованием ЭВТ, является завладение информацией о владельцах

платежных банковских карт и их реквизитах. Способы мошенничеств, совершенных с использованием ЭВТ – это совокупность действий преступника, заключающаяся в определенном порядке, последовательности и конкретном методе деятельности мошенника, направленной на подготовку, совершение и сокрытие конкретного уголовного преступления.

Список литературы:

1. «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ (ред. от 21.11.2022, с изм. от 08.12.2022) // «Собрание законодательства РФ», 17.06.1996, N 25, ст. 2954.
2. Аксенов В.А. Современное состояние и мировые тенденции совершения мошенничества с использованием информационно-телекоммуникационных технологий в период пандемии COVID-19 // Безопасность бизнеса. 2021. N 5. С. 45 - 49.
3. Интернет-мошенничество [Электронный ресурс] URL: https://ria.ru/20220118/internet-moshennichestvo-1768431202.html (Дата обращения 02.11.2022)
4. Шипулин Г. Ф. Способы совершения мошенничества, связанные с использованием мобильной связи // Международный журнал гуманитарных и естественных наук. – 2022. – №. 2-2. – С. 186-189.
5. Бозиев Т.О., Коротков А.В., Сипягина М.Н. Имущественные преступления с использованием IT-технологий: криминологический аспект //Ленинградский юридический журнал. – 2022. – №. 1 (67). – С. 125-138.
6. Орцханова, Т.М. «кибермошенничество» как угроза безопасности: краткий обзор ситуации в условиях пандемии / Т.М. Орцханова, М.Д. Попов // Тамбовские правовые чтения имени Ф.Н. Плевако: Материалы IV международной научно-практической конференции. В двух томах, Тамбов, 22–23 мая 2020 года. – Тамбов: Издательский дом «Державинский», 2020. – С. 332-337.

7. Аскерова, Э.С. Мошенничество в социальных сетях / Э.С. Аскерова, А.В. Гаранин // Научная дискуссия современной молодёжи: актуальные вопросы, достижения и инновации: сборник статей X Международной научно-практической конференции, Пенза, 17 декабря 2019 года. – Пенза: «Наука и Просвещение» (ИП Гуляев Г.Ю.), 2019. – С. 187-190.