Березовская Анастасия Васильевна
магистрант
Филиал ФГБОУ ВО «Ростовский государственный
экономический университет» в г. Кисловодске
г. Кисловодск, Ставропольский край

АНАЛИЗ ОТЕЧЕСТВЕННОГО ОПЫТА БОРЬБЫ С ДИСТАНЦИОННЫМИ МОШЕННИЧЕСТВАМИ: УГОЛОВНО-ПРАВОВЫЕ И КРИМИНОЛОГИЧЕСКИЕ АСПЕКТЫ

Аннотация*: в статье проводится анализ положений отечественной правовой доктрины и законодательных актов по дискуссионным вопросам противодействия мошенничествам, совершенным с использованием технологий дистанционного синхронного взаимодействия. Исследуются мнения отечественных исследователей и практикующих специалистов в области правовых и криминологических наук, представлен теоретический анализ по заявленной теме исследования, а также актуальные проблемы теоретического и прикладного характеров и пути их разрешения в обозримой перспективе.*

Ключевые слова*: криминология, преступление, мошенничество, предупреждение преступлений, профилактика преступлений, общественно опасные последствия.*

Значимость информации в современном обществе бесспорна. Очевидно, что ранее существующие способы ее сохранения и передачи не соответствуют эволюционным цивилизационным процессам [1; 2]. Устные и письменные варианты утратили свою актуальность, приоритет перешел к технологическому восприятию, построенному на аудио и визуальном ряде. К сожалению, понимание этих моментов характерно и для криминальной среды, которая способна быстро адаптироваться к происходящим изменениям в указанной сфере. В сложившихся реалиях во главу угла стала борьба с дистанционными мошенничествами [3].

Общее определение этого вида хищения в уголовном законе, которое сформировалось в советский период, не отвечает произошедшим социально-экономическим переменам в нашей стране. Законодатель, понимая это, наполнил

указанное понятие новыми признаками, сделав выбор в пользу выделения отдельных видов мошенничества, взяв за основу предметную область посягательства [4; 5]. Такой подход сложился на основании Федерального Закона от 29.11.2012 г. №207-ФЗ и сопровождался появлением ряда составов, а именно статей 159.1–159.6 УК РФ.

Для дистанционного мошенничества характерно использование злоумышленником компьютерной и телефонной сети с целью убедить потерпевшего передать аферисту свое имущество или денежные средства. В данном случае используется удаленный способ, поскольку мошенник находится на значительном расстоянии от своей жертвы. Своеобразие ситуации в том, что в непосредственный контакт они не вступают. Преступник использует доверчивость пострадавшего, вербально он манипулирует значимыми для него ценностями, воздействуя на его подсознание, с намерением через введение его в заблуждение завладеть принадлежащей ему собственностью [6].

Алгоритм мошенничества здесь заключается в том, что жертва сама сообщает аферисту необходимые сведения. В результате злоумышленнику открывается доступ к счету мобильного телефона или к реквизитам банковской карты, а затем происходит хищение денег. Нередко пострадавшие сами производят перечисление средств, поддаваясь направленному обману. В этом принципиальное отличие дистанционного мошенничества от классического, где предметом посягательства может быть любое имущество, а не только финансы [7; 8].

В теории уголовного права принято выделять три разряда дистанционного мошенничества. Первый подвид – это махинации, для совершения которых применяются средства сотовой связи и сети Интернет. Криминальные элементы придумали множество способов для получения информации о банковской карте, счете, они даже создают иллюзию оказания содействия пострадавшему в перечислении денег, предоставляя ему реквизиты счетов; осуществляя разблокировку карт; предлагая к приобретению товары на Интернет-площадках. Однако они не ставят своей задачей: передать покупателю какой-либо товар или виртуальный продукт. Таким образом, просто находится предлог для обращения к

потенциальной жертве. Личность его предварительно изучается, чтобы выявить свойства, которые можно использовать для внушения [9]. Например, пенсионеру предлагают получить компенсацию за ранее приобретенные лекарства или бесплатное медицинское обследование; молодой матери товары для новорожденного с существенными скидками.

Вторую группу образуют мошенничества, для совершения которых используются средства сотовой связи, сопряженные с непосредственным контактом злоумышленника с жертвой. Достаточно распространена версия сообщения о родственнике, с которым случилась неприятность (авария, помещение в стационар, задержание полицией, возбуждение уголовного дела).

Третий разряд дистанционных мошенничеств составляют посягательства, где аферист прибегает к интернет-ресурсам. Наиболее часто используются «зеркальные» сайты, которые имеют значительное сходство с оригинальными, имеющими отношение к известным брендам [10; 11]. В этом же ряду взлом страниц пользователей и рассылка от их имени фейковых сообщений с просьбой о перечислении каких-либо сумм.

Схемы при всех вышеописанных видах схожи, поэтому оперативно-разыскные мероприятия, которые будут проводиться для их выявления, идентичны. Наиболее успешны они при максимально быстром их осуществлении и совместной деятельности с провайдерами и сотовыми операторами. В случае их начала сразу же после получения заявления о совершении хищении, возрастают шансы выявить техническое устройство, используемое посягающим субъектом; определить локацию нахождения мошенника; отследить движение финансов.

Автором изучены конкретные уголовные дела, что позволило сделать вывод, что в целом раскрываемость подобных случаев выросла. Следственный и оперативный аппарат отличает высокий уровень технической подготовки, что дает возможность эффективной работы со средствами сотовой связи и системой Интернет.

В ходе опроса сотрудников оперативных подразделений было установлено, что наибольшую сложность в выявлении выделенных нарушений для них

составляют ситуации работы с подставными и дублированными сайтами, которые незначительно отличаются от подлинных – цифрой, символом. Более простым случаем считается проведение розыскных мероприятий по схеме разблокировок потерпевшими банковских карт, в связи с получением сообщения злоумышленника.

С криминологической точки зрения данную категорию преступлений совершают различные категории субъектов, причем как ранее не имеющие отношения к криминалу, так и судимые. Неоднократно выявляются случаи совершения телефонных мошенничеств лицами, отбывающими наказание в местах лишения свободы [12; 13]. По анализированным уголовным делам было выделена активно применяемая преступная схема, когда осужденный злоумышленник использовал механизм случайного цифрового набора номера, соединение происходило с ранее незнакомыми ему гражданами. Звонки совершались не только на мобильные, но и на стационарные устройства.

Во время разговора аферист сообщал абонентам ложные сведения, сам представлялся родственником или знакомым, действуя по стандартному алгоритму «о попавшем в беду и ждущим финансовой помощи от близких». Как правило, просил перечислить средства на абонентский номер или на платежную карту Киви-кошелек.

В ряде регионов России дистанционные мошенничества стали подвидом этнической преступности, на них специализируется цыганская диаспора. Техническая составляющая в подобных случаях используется для хищения перевозимых дорогостоящих грузов. Раскрываемость здесь требует серьезных экспертных исследований в области информационных процессов. Проблема заключается в отсутствии универсальной методики выявления и расследования подобных нарушений.

Не улучшает ситуацию отсутствие единой базы по систематизации посягательств рассматриваемого вида, что не дает возможности оперативного обмена данными, что особенно важно при дистанционных мошенничествах. Оптимально было бы расширение кластера электронной переписки, что привело бы к

сокращению сроков исполнения запросов правоохранительных органов; нужно использовать обмен аудио, видеофайлами и фотоматериалами между операторами сотовой связи, кредитными организациями, провайдерами платежных систем [14; 15].

Классификационный подход позволил бы выработать критерии для разделения хищений данного вида, что важно в свете постоянного появления новых методов дистанционных посягательств. Мы согласны с предложением ряда авторов, что для борьбы с указанным видом хищений целесообразно создавать отдельные структурные подразделения, с включением в их штат технических специалистов, которые способны к криминалистической обработке объектов и оперативному сопровождению [16]. В этом связи требует корректировки нормативная база, в частности, Федеральный закон от 07.07.2003 г. №126-ФЗ «О связи», в тексте которого должны появиться допустимые мероприятия по приостановлению оказания услуг связи тем абонентам, номера которых используются в противоправных целях. Недопустимо, чтобы соединение путем мобильной коммуникации было доступно, отбывающим наказание в исправительных учреждениях. В этих целях целесообразно применять технические устройства для подавления радиоволн мобильной связи в местах содержания задержанных и осужденных лиц. В том же ряду грамотный подбор сотрудников системы исполнения наказаний, чтобы не допускать проноса телефонов на территорию пенитенциарных учреждений.

Важным средством профилактики может стать введенный запрет по продаже сим-карт на нестационарных площадках. Допустимо введение службы мониторинга криминальной деятельности отмеченного направления, с обобщением полученных данных.

Весьма значимо расширять сотрудничество правоохранительных и кредитных учреждений в ходе выявления подобных нарушений, поскольку банки нередко отказывают в предоставлении информации, ссылаясь на ее закрытый характер [17]. По подавляющему большинству изученных дел по хищениям

данного вида они были выявлены специалистами служб собственной безопасности структур кредитной системы.

Необходимо также наладить совместное взаимодействие оперативных подразделений и операторов мобильной связи, а также администраторов, работающих с «виртуальными деньгами». Указанный сегмент ведет себя достаточно засекречено, ссылаясь на коммерческую тайну. Правоохранители сталкиваются с отказом в предоставлении сведений на направленные запросы, со ссылками на персональные данные абонентов. В подобной ситуации вопрос о блокировке счета откладывается на неопределенный срок. Выходом из сложившегося положения являются конкретно-адресные обращения, а также установление на нормативном уровне обязательности и срочности предоставления сведений по подобным обращениям. В то же время нужно просчитать допустимость такого вмешательства в экономический оборот в условиях рынка, чтобы установить разумный баланс между важностью получения информации и степенью вхождения в область коммерческой тайны.

Дистанционные мошенничества показывают, что массовая виктимность считается показателем современного состояния преступности и широкого круга ее потенциальных жертв, демонстрирующих высокий уровень доверчивости.

Список литературы

1. Русанов Г.А. Экономические преступления: учебное пособие для вузов / Г.А. Русанов. – М.: Юрайт, 2021. – С. 99.

2. Русанов Г.А. Экономические преступления: учебное пособие для вузов / Г.А. Русанов. – М.: Юрайт, 2021. – С. 201.

3. Яни П.С. Специальные виды мошенничества / П.С. Яни // Законность. – 2015. – №3 (965). – С. 49.

4. Ланг П.П. Правовая деятельность: аксиологические и мировоззренческие основания / П.П. Ланг. – Самара: Стандарт, 2021. – 372 с. – ISBN 978-5-6046361-8-3. – EDN IFVNSI.

5. Ланг П.П. Идеи блага в праве / П.П. Ланг // Вопросы экономики и права. – 2020. – №142. – С. 15–19. – DOI 10.14451/2.142.15. – EDN NVUQPH.

6. Ланг П.П. Аксиологические начала права / П.П. Ланг // Российская юстиция. – 2018. – №8. – С. 2–4. – EDN XUXMCL.

7. Ценность права в условиях цифровой реальности / О.Ю. Рыбаков, М.А. Беляев, Ю.Ю. Ветютнев [и др.]. – М.: Проспект, 2024. – 312 с. – ISBN 978-5-392-40426-1. – EDN VWQLQY.

8. Ланг П.П. Ценность и экзистенция принципов права / П.П. Ланг // Евразийский юридический журнал. – 2021. – №6 (157). – С. 84–87. – DOI 10.46320/2073-4506-2021-6-157-84-87. – EDN MPGGRN.

9. Churakova E.N. E-Money as a Financial Instrument in Globalized Economy: Russian Legislation Experience / E.N. Churakova, P.P. Lang // Economic Systems in the New Era: Stable Systems in an Unstable World / Editors: Svetlana Igorevna Ashmarina, Jakub Horák, Jaromír Vrbka, Petr Šuleř. Cham: Springer Nature, 2021. – P. 815–821. – DOI 10.1007/978-3-030-60929-0_105. – EDN IMNJUX.

10. Ланг П.П. Особенности делопроизводства в юриспруденции: учебник / П.П. Ланг, Ю.В. Руднева, А.В. Фадеев. – М.: Проспект, 2024. – 248 с. – ISBN 978–5-392-40008-9. – EDN FTAGWS.

11. Ланг П.П. Правовая процедура и юридический процесс (теоретико-правовой аспект) / П.П. Ланг // Современные проблемы права и управления: 5-я Международная научная конференция: сборник докладов (Тула, 18–19 сентября 2015 года) / Институт законоведения и управления Всероссийской полицейской ассоциации; гл. ред. И.Б. Богородицкий, отв. ред. Ю.В. Киселевич. – Тула: Папирус, 2015. – С. 80–85. – EDN UGIJCJ.

12. Ланг П.П. Институт несостоятельности (банкротства) самостоятельная процедура юридического процесса / П.П. Ланг // Вопросы экономики и права. – 2013. – №55. – С. 43–47. – EDN QINWAP.

13. Ланг П.П. Состязательность и злоупотребление процессуальным правом в арбитражном процессе: корреляционная связь / П.П. Ланг // Вопросы экономики и права. – 2022. – №169. – С. 14–21. – EDN ZYIKOZ.

14. Ланг П.П. Правовая процедура как элемент юридического процесса / П.П. Ланг // Вопросы экономики и права. – 2013. – №58. – С. 63–66. – EDN QIWLTD.

15. Ланг П.П. Соотношение и взаимодействие права и морали в регулировании общественных отношений / П.П. Ланг // Вопросы российского и международного права. – 2021. – Т. 11. №2А. – С. 172–180. – DOI 10.34670/AR.2021.71.85.023. – EDN ETSFCN.

16. Peculiarities of protecting the rights of participants of financial markets in court / G.E. Ageeva, P.P. Lang, A.V. Loshkarev [et al.] // The Future of the Global Financial System: Downfall or Harmony. Cham, Switzerland: Springer Nature, 2019. P. 545–552. DOI 10.1007/978-3-030-00102-5_57. – EDN YUFZUQ.

17. Право на жизнь, здоровье, собственность: монография / Л.А. Андреева, В.В. Батин, К.В. Дядюн [и др.]. – Новосибирск: НП «СибАК», 2013. – 160 с. – EDN TZNUDT.