Ученые записки Крымского федерального университета имени В. И. Вернадского
Юридические науки. – 2024. – Т. 10 (76). № 2. – С. 223–228.

УГОЛОВНО-ПРАВОВЫЕ НАУКИ

УДК 343

К ВОПРОСУ О ПРОБЛЕМНЫХ АСПЕКТАХ РАССЛЕДОВАНИЯ ИНТЕРНЕТ-МОШЕННИЧЕСТВ И МОШЕННИЧЕСТВ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ СОТОВОЙ СВЯЗИ

Бадиков Д. А., Зоз В. А.

В данной статье рассматриваются наиболее актуальные на сегодняшний день проблемы, возникающие в следственной практике в ходе расследования мошенничеств, совершаемых с использованием информационно-телекоммуникационных технологий (ИТКТ). Особое внимание уделяется изучению процедур сбора и формирования доказательственной базы по таким делам с учётом имеющейся в практической деятельности специфики, на основе чего предложены возможные варианты решения имеющихся недостатков. Отмечается, что основной проблемой, возникающей в ходе расследования данного вида преступлений, выступают вызванные нестандартностью (особенностью) среды, в которой они совершаются, пробелы в специальных знаниях сотрудников правоохранительных органов, необходимых как при изъятии электронных носителей информации, так и при производстве иных необходимых следственных действий, имеющих свою специфику.

Ключевые слова: интернет-мошенничество, информационно-телекоммуникационные технологии, особенности расследования, преступная деятельность, обман и злоупотребление доверием, электронные средства платежа, банковские карты.

В настоящее время информационные технологии – неотъемлемая часть нашей жизни, поскольку они пронизывают многие сферы деятельности человека. Этот факт оказал существенное влияние в том числе и на преступную деятельность: по данным различных международных фондов оценки общественного мнения – Россия занимает лидирующие позиции в Европе по темпам роста количества интернет-мошенничеств (обманных действий/злоупотреблений доверием с использованием при этом электронных средств платежа и банковских карт) [1]. Как следствие этого, интернет становится как местом, так и средством совершения преступлений [2].

Объяснением этому становится преобладание безналичных расчётов в отечественной экономической системе, (что существенно облегчает преступникам совершение таких противоправных деяний), а также имеющие место быть сложности в процессе расследования данного вида преступлений, как минимум, возникающие в силу того, что деяния, связанные с использованием информационно-телекоммуникационных технологий, отличаются достаточно высоким уровнем латентности, а правоохранительные органы зачастую оказываются на «шаг позади» преступников в объёме знаний, требующихся для понимания непростых схем совершения интернет-преступлений. При этом необходимо понимать психологический портрет личности преступника, совершающего преступления в сети Интернет, что является одним из основных элементов оперативно-розыскной характеристики. Пол, возраст, образование, место жительства, наличие судимости – это сведения, необходимые для составления характеристики личности преступника, совершающего такие неправомерные действия [3].

Так, по некоторым оценкам специалистов, из общей массы мошеннических действий, осуществляемых с использованием электронных средств платежей, находят своё отражение в статистике лишь около 15% случаев [4]. Необходимо упомянуть о

том, что на сегодняшний день предпринимаются попытки по разрешению имеющихся проблем [5]. Так, осуществляются меры по совершенствованию уголовного законодательства в ответ на появление новых видов преступлений. Например, в УК РФ была введена статья 159.3, которая предусмотрела ответственность за осуществление мошеннических действий с использованием электронных средств платежа. В редакции Федерального закона от 23.04.2018 г. №111-ФЗ был расширен предмет данного преступления, а именно, в него стали входить не только банковские карты, но и все электронные средства платежа.

Под последними понимается особый платёжный инструмент, который позволяет хранить денежные средства в интернете, а также свободно ими распоряжаться в данном пространстве. К таковым можно отнести «Яндекс. Деньги», «WebMoney» и др. Однако и это не позволило в полной мере эффективно организовать процесс расследования, поскольку практика отдельных регионов по квалификации конкретных преступных проявлений складывается далеко не единообразно, что говорит о недостаточной её наработанности на сегодняшний день.

Данный факт существенно усложняет расследование столь масштабного количества уголовных дел, по истечении срока предварительного следствия которых доказательственной информации оказывается недостаточно для дальнейшего производства по делу. В связи с этим требуется осуществлять более тесное и регулярное взаимодействие правоохранительных органов в вопросах обмена имеющимся опытом, поскольку в отсутствие этого, крайне часто органами предварительного следствия такие уголовные дела приостанавливаются по п. 1 ч. 1 ст. 208 УПК РФ, что очевидно, формирует отрицательную статистику.

Кроме того, Интернет-мошенничества характеризуются высокой степенью латентности, что не позволяет правоохранительным органам оценить реальный её уровень. Учитывая, что имеющегося практического опыта, а также численности следователей и сотрудников органов дознания, осуществляющих сопровождение таких уголовных дел, их знаний в сфере IT-технологий оказывается недостаточно даже для расследования того массива преступлений, который фактически был зарегистрирован, то не сложно представить, насколько сильно усложнился бы этот процесс при меньшей степени латентности.

Среди причин подобного явления обычно выделяют: недостаточный уровень доверия граждан к сотрудникам правоохранительных органов; отсутствие веры в возможность обнаружить преступника и привлечь его к ответственности; незначительность похищенной суммы денег, ради возвращения которой граждане не готовы вступать в уголовное судопроизводство.

Очевидно, что подобные проблемы все же должны решаться. В первую очередь, необходимо добиться правовой ответственности лиц, потерпевших от мошеннических действий в информационно-телекоммуникационном пространстве. Важную роль в данном вопросе играет правовая пропаганда, а также деятельность средств массовой информации о необходимости сообщения о произошедшем в правоохранительные органы, а также об основах поведения в сети Интернет, при поступлении звонков от неизвестных граждан и т.д. В ответ на это важно обеспечить полную штатную численность сотрудников органов предварительного следствия, в частности специализирующихся на расследовании преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. Кроме того, было

бы целесообразно осуществлять регулярное взаимодействие таких следователей с IT-специалистами, способными проводить разъяснительные лекции о способах совершения тех или иных действий мошенниками в работе с персональным компьютером, информационными сетями, смартфонами, о том, каким образом они преодолевают криптографические защиты и др.

Общение со специалистами на данные темы окажется крайне полезным для следователей, поскольку позволит напрямую узнать о принципе реализации преступником объективной стороны того или иного интернет-мошенничества. Для качественного проведения расследования, понимания плана предстоящих действий, способных изобличить мошенника, следователь должен быть компетентен в конкретном вопросе. В данном вопросе также важна и материальная составляющая.

Однако даже несмотря на сложность раскрытия рассматриваемой нами категории преступлений, следственная практика имеет хотя и минимальный, не всегда эффективный, но в некоторой степени стандартный план следственных и процессуальных действий, который позволяет расследовать, как минимум, несложные мошеннические схемы в информационно-телекоммуникационном пространстве.

Одно из возможных и достаточно информативных при грамотном проведении следственным действием выступает допрос потерпевшего лица о фактах совершённого в отношении него мошенничества. Практика показывает, что зачастую допросы проводятся формально, упускаются важные сведения события преступления.

В ходе проведения данного следственного действия важно детально узнать суть разговора/переписки с мошенником, точную сумму похищенного, тактику действий потерпевшего в сложившейся ситуации и т.д., приобщив при этом имеющиеся доказательства (например, скриншоты переписок) [6].

При наличии у пострадавшего от преступления лица чеков или квитанций, подтверждающих факт перевода денежных средств на тот или иной счёт злоумышленника, они могут быть подвергнуты выемке и также приобщены в качестве вещественных доказательств в соответствии с УПК РФ. В ходе приобщения важно соблюдать требования относимости, допустимости, достоверности и достаточности доказательств. Их процессуальное оформление должно позволять должным образом интерпретировать зафиксированные сведения, не содержать искажений и др.

Не стоит также умалять возможность опознания мошенника потерпевшим по голосу, который последний мог запомнить. Это может явиться поводом для назначения судебной фоноскопической экспертизы. Возможно, человек с подобным голосом в ином регионе уже привлекался к уголовной ответственности. В такой ситуации будет не лишней организация должного уровня взаимодействия органов предварительного следствия различных субъектов Российской Федерации. На практике такое взаимодействие не всегда выстраивается на доброжелательных началах, а время получения ответов затягивается, иногда необоснованно.

Говоря о взаимодействии, хотелось бы обозначить имеющую место быть достаточно серьёзную проблему в рассматриваемом нами вопросе. В целом, в ходе расследования Интернет-мошенничеств, а также мошенничеств с использованием сотовой связи, информация, предоставляемая следователю по его запросу от операторов сотовой связи, банков, различных Интернет-сервисов, платёжных систем играет большую роль, однако: нередко время ожидания ответа растягивается на несколько месяцев, что существенно затягивает сроки расследования; используются недоста-

точно конкретные формулировки в запросах и даются такие же абстрактные ответы; существует деление сотовых компаний на макро-филиалы, которые не всегда могут предоставить информацию обо всех абонентах их оператора в России, ограничиваясь при этом только теми из них, кто находится в пределах их филиала [7]; при перегрузке базовой сотовой станции (вышки) сигнал может передаваться на ближайшую станцию, что и фиксируется операторами сотовой связи. Однако, в связи с этим возникают ложные предположения о нахождении звонящего лица в том или ином месте, хотя фактически он находился в другом [8].

Указанные нюансы следует учитывать при направлении запросов, не допускать абстрактности в их формулировке и направлять их в первые же дни после начала производства предварительного следствия по уголовному делу.

В случае с расследованием преступлений по факту мошеннических звонков, следует помнить, что зачастую запрос в сотовую компанию направляется с целью получения информации о соединениях между абонентами и абонентскими устройствами, для чего предварительно требуется получить судебное решение. Копии материалов дела, передаваемые при этом в суд, должны отражать всю суть расследуемого дела, предоставлять судье полную информацию о нём. В сотовую организацию необходимо направлять вместе с запросом исключительно оригинал судебного решения, чтобы в случае его отсутствия не получить ответ о невозможности предоставления запрашиваемых сведений.

Необходимо обозначить одну из наиболее злободневных проблем – отсутствие должного международного сотрудничества. В ситуациях, когда есть необходимость установления IP-адреса подозреваемого, может быть выявлен факт его регистрации на территории иностранного государства. В данном случае встаёт вопрос о направлении запроса по линии Интерпола, срок ответа на который зачастую крайне длителен, в том числе и по объективным причинам (например, IP-адрес анонимен). Ещё один недостаток в данном направлении – не всегда добросовестная и оперативная работа в ходе ответа на запрос со стороны правоохранительных органов иностранного государства [9].

Решением подобной проблемы может стать подписание договоров об оказании правовой помощи в расследовании преступлений, совершённых с использованием ИТКТ, между Российской Федерацией и зарубежными странами.

На первый взгляд можно полагать, что следователем при расследовании информационно-телекоммуникационных мошенничеств предпринимается достаточный объём действий. Но несмотря на это, многие из них, как показывает практика, остаются не раскрытыми. Так, из зарегистрированных 522 065 преступлений, совершённых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации в 2022 г. раскрыто лишь 142 384 из них [10]. Масштабное приостановление таких уголовных дел объясняется совершенствованием схем преступной мошеннической деятельности, к которым можно отнести, например, применение при переходе на конкретный сайт VPN сервисов, маскирующих реальный IP-адрес или использование абонентских номеров, не способных отобразиться на конкретной базовой станции ввиду отсутствия у номера физического носителя.

Обобщая сказанное, мы можем сделать вывод о том, что следственные действия, не приносящие должных результатов, из-за существования множества маскирую-

щих истинное лицо мошенника сервисов, лазеек, заводят следствие в тупик. Это является стимулом для того, чтобы лица, производящие расследование мошенничеств, совершённых с использованием ИТКТ, стремились к развитию своих знаний в IT-сфере, тем самым идя, как минимум, «в ногу» со злоумышленниками и пытаясь предугадать схему их действий в каждом конкретном случае, без использования формализованных шаблонов, не подстроенных под особую следственную ситуацию.

Список литературы:

1. Вестов Ф.А., Шамьенов Н.Р. Актуальность проблем DoS и DDoS-атак в уголовном праве в сфере компьютерной информации // Базис. 2020. № 1 (7). С. 13-16.
2. Иванов С.И. Особенности проведения оперативно-разыскных мероприятий в сети Интернет // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2018. № 18-1. С. 23-24.
3. Зоз В.А., Лагуточкина А.С. Личность интернет-преступника и отдельные способы их выявления в глобальной информационной сети // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2023. Т. 9. № 2. С. 306-312.
4. Бондаренко Т.Г. К проблеме мошенничества с использованием банковских карт в РФ// Инновационная наука. 2016. № 21. С.6.
5. Бадиков Д.А., Елисеева К.А. Алгоритм действий следователя при расследовании мошенничества с использованием электронных средств платежа // Закон и право. 2023. № 4. С. 153-155.
6. Денисов, Е. А. Скриншоты в системе уголовно-процессуальных доказательств: вопросы теории и практики // Скиф. Вопросы студенческой науки. 2017. № 15(15). С. 179-183.
7. Сезонова, Т.В. Проблемы расследования мошенничеств, совершенных с использованием сети «Интернет» и сотовой связи / Т.В. Сезонова, В.И. Чувальникова // Проблемы уголовно-процессуального права и криминалистики: сборник научных статей / Редколлегия: Н.В. Морозова [и др.]. Орел : Орловский юридический институт Министерства внутренних дел Российской Федерации имени В.В. Лукьянова, 2021. С. 108-113.
8. Ковтун Ю.А., Жукова Н.А., Лагуточкин А.В. Актуальные вопросы раскрытия и расследования мошенничеств, совершенных с использование средств мобильной связи: учебно-практическое пособие / Белгород, 2015.
9. Науменко О.А. Проблемы в расследовании уголовных дел о мошенничестве, совершенном с использованием информационно-телекоммуникационной среды // Вестник Краснодарского университета МВД России. 2019. № 3(45). С. 60-64.
10. Краткая характеристика состояния преступности в Российской Федерации за январь - декабрь 2022 года: [Электронный ресурс]. URL: https://мвд.рф/reports/item/35396677/ (Дата обращения: 29.03.2023).

Badikov D.A., Zoz V.A. Towards problematic aspects of investigating internet and mobile phone frauds // Scientific notes of V.I. Vernadsky crimean federal university. Juridical science. – 2024. – T. 10 (76). № 2. – C. 223–228.

This article discusses the most pressing problems today that arise in investigative practice during the investigation of fraud committed using information and telecommunication technologies (ITCT). Particular attention is paid to the study of procedures for collecting and forming an evidence base in such cases, taking into account the specifics existing in practical activities, on the basis of which possible options for solving existing shortcomings are proposed. It is noted that the main problem that arises during the investigation of this type of crime is caused by the non-standard (peculiarity) of the environment in which they are committed, gaps in the special knowledge of law enforcement officers, necessary both when seizing electronic storage media and when carrying out other necessary investigative actions that have their own specifics.

Key words: Internet fraud, information and telecommunication technologies, features of the investigation, criminal activity, deception and abuse of trust, electronic means of payment, bank cards.

Spisok literatury:

1. Vestov F.A., SHam'enov N.R. Aktual'nost' problem DoS i DDoS-atak v ugolovnom prave v sfere komp'yuternoj informacii // Bazis. 2020. № 1 (7). S. 13-16.
2. Ivanov S.I. Osobennosti provedeniya operativno-razysknyh meropriyatij v seti Internet // Aktual'nye problemy bor'by s prestupleniyami i inymi pravonarusheniyami. 2018. № 18-1. S. 23-24.
3. Zoz V.A., Lagutochkina A.S. Lichnost' internet-prestupnika i otdel'nye sposoby ih vyyavleniya v global'noj informacionnoj seti // Uchenye zapiski Krymskogo federal'nogo universiteta imeni V.I. Vernadskogo. YUridicheskie nauki. 2023. T. 9. № 2. S. 306-312.
4. Bondarenko T.G. K probleme moshennichestva s ispol'zovaniem bankovskih kart v RF// Innovacionnaya nauka. 2016. № 21. S.6.

5. Badikov D.A., Eliseeva K.A. Algoritm dejstvij sledovatelya pri rassledovanii moshennichestva s ispol'zovaniem elektronnyh sredstv platezha // Zakon i pravo. 2023. № 4. S. 153-155.
6. Denisov, E. A. Skrinshoty v sisteme ugolovno-processual'nyh dokazatel'stv: voprosy teorii i praktiki // Skif. Voprosy studencheskoj nauki. 2017. № 15(15). S. 179-183.
7. Sezonova, T.V. Problemy rassledovaniya moshennichestv, sovershennyh s ispol'zovaniem seti «Internet» i sotovoj svyazi / T.V. Sezonova, V.I. CHuval'nikova // Problemy ugolovno-processual'nogo prava i kriminalistiki: sbornik nauchnyh statej / Redkollegiya: N.V. Morozova [i dr.]. Orel : Orlovskij yuridicheskij institut Ministerstva vnutrennih del Rossijskoj Federacii imeni V.V. Luk'yanova, 2021. S. 108-113.
8. Kovtun YU.A., ZHukova N.A., Lagutochkin A.V. Aktual'nye voprosy raskrytiya i rassledovaniya moshennichestv, sovershennyh s ispol'zovanie sredstv mobil'noj svyazi: uchebno-prakticheskoe posobie / Belgorod, 2015.
9. Naumenko O.A. Problemy v rassledovanii ugolovnyh del o moshennichestve, sovershennom s ispol'zovaniem informacionno-telekommunikacionnoj sredy // Vestnik Krasnodarskogo universiteta MVD Rossii. 2019. № 3(45). S. 60-64.
10. Kratkaya harakteristika sostoyaniya prestupnosti v Rossijskoj Federacii za yanvar' - dekabr' 2022 goda: [Elektronnyj resurs]. URL: https://mvd.rf/reports/item/35396677/ (Data obrashcheniya: 29.03.2023).

.