УДК 343.1, 343.7, 343.72 DOI: 10.17223/23088451/16/6

О.В. Ханинева

ОБЩИЕ ПРИЧИНЫ И НЕКОТОРЫЕ ВИДЫ МОШЕННИЧЕСТВ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ, В РОССИЙСКОЙ ФЕДЕРАЦИИ

Описываются основные причины увеличения числа зарегистрированных мошенничеств, совершенных на территории Российской Федерации за последние 4 года. Также приводятся примеры наиболее распространенных видов мошенничеств, совершенных с использованием информационно-телекоммуникационных устройств, таких как «сообщение по телефону о совершенном родственником дорожно-транспортном происшествии»; «победа в розыгрыше, проводимом компанией-оператором сотовой связи»; «взлом страниц социальных сетей»; «сообщение от банка о блокировке карты»; «покупка товара на интернет-сайтах». Автором указываются первичные способы предупреждения и пресечения таких преступлений сотрудниками органов внутренних дел и меры, принимаемые самими гражданами.

Ключевые слова: *мошенничество, мобильные устройства, Интернет, пресечение, предупреждение.*

В течение последних нескольких лет на территории Российской Федерации, согласно официальной статистике, представленной Главным управлением правовой статистики и информационных технологий Генеральной прокуратуры Российской Федерации, совершение грабежей и разбойных нападений, предметом которых являлись мобильные телефоны и денежные средства граждан, сменились новым бесконтактным видом мошенничества.

Так, согласно отчетам о состоянии преступности в РФ, представленным порталом правовой статистики Генеральной прокуратуры РФ:

– за 2017 г. количество преступлений, совершенных в форме мошенничества (ст. 159–159.6 УК РФ), по сравнению с аналогичным периодом 2016 г. увеличилось на 6,6% и составило 222 772 преступления. Наибольший рост зарегистрированных преступлений данного вида наблюдается в Саратовской области (на 2 394; +124%), Калининградской области (на 1 247; +120,8);

– за 2018 г. более трети всех зарегистрированных преступлений (42,3%) составляют хищения чужого имущества, совершенные путем краж – 756 395 (–4,1%), грабежей – 50 111 (–11,9%), разбоев – 7 474 (–17,9%). Количество преступлений, совершенных в форме мошенничества (ст. 159–159.6 УК РФ), по сравнению с аналогичным периодом прошлого года снизилось на 3,5% и составило 215 036 преступлений. Наибольший рост мошенничеств наблюдается в Новосибирской области (на 1 883; +42,7%), Республике Крым (на 1 066; +57,6%), Краснодарском крае (на 1 028; +10,5%);

– за 2019 г. более трети всех зарегистрированных преступлений (42,5 %) составляют хищения чужого имущества, совершенные путем краж, – 774 159 (+2,3%), грабежей – 45 815 (–8,6%), разбоев – 6 739 (–9,8%). Количество преступлений, совершенных в форме мошенничества (ст. 159–159.6 УК РФ), по сравнению с аналогичным периодом прошлого года увеличилось на 19,6% и составило 257 187 преступлений. Наибольший рост мошенничеств наблюдается в г. Москве (на 4 895; +20,1%), Ростовской области (на 3 509; +59,2%), Краснодарском крае (на 2 869; +26,5%), Ставропольском крае (на 1 777; +35,6%);

– за январь–май 2020 г. уже более половины всех зарегистрированных в стране преступлений составляют хищения чужого имущества. Каждый пятый факт связан с кражей денежных средств с банковского счета (58 993 из 289 386), большинство подобных случаев выявлено в г. Москве (6 111). Наряду с этим в России заметно сократилось количество грабежей (–10,4%, 17 245) и разбоев (–19,3%, 2 320). Увеличилось число преступлений, совершенных путем мошенничества, по сравнению с аналогичным периодом прошлого года на 22,2%. Каждое седьмое деяние зарегистрировано в г. Москве (16 006 из 107 543). На долю мошенничеств, совершенных с использованием интернета, мобильных средств связи, компьютерной техники или других информационно-телекоммуникационных технологий, приходится 66% (71 162, +60%). Более чем вдвое увеличилось количество мошенничеств с использованием электронных средств платежей (+113,3%, 11 248). Среди субъектов Российской Федерации наиболее негативно выделяются Омская область (1 012, +209,5%) и Пермский край (816, +325%). За январь–май 2020 г. их количество возросло более чем на 85% (до 180,5 тыс.). Если годом ранее такими деяниями было каждое десятое регистрируемое преступление, то сегодня это уже каждое пятое. Больше половины из них (56,6%) совершается с использованием сети Интернет (+74,1%, 102,2 тыс.), свыше 40% – при помощи средств мобильной связи (+99,7%, 76,6 тыс.). Три четверти таких преступлений совершается путем кражи или мошенничества (+96,2%, 143 тыс.).

Средства массовой информации также выражают опасения населения в «пабликах», сообщая, что, как следует из данных Росстата, по итогам первого полугодия случился рекордный за последние три года всплеск различных мошеннических преступлений – сразу на 11% по сравнению с аналогичным периодом 2018 г.

В России произошел рекордный за последние три года всплеск мошенничества. В первом полугодии 2019 г. в стране зарегистрировано 122,8 тыс. таких преступлений, и это на 10,9% больше, чем было зафиксировано за аналогичный период 2018 г. Последний раз мощный всплеск по этому виду преступлений фиксировали в первом полугодии 2016 г., был резкий рост сразу примерно на 25% в годовом выражении.

К аналогичному выводу приходили и иные авторы, исследовавшие более ранний период времени рассматриваемого вопроса (2003–2008 гг.), который показал общий рост преступности в РФ на 16,5%, а по мошенничествам – на 120,1% [1. С. 34–40].

Для начала приведем результаты проведенного анализа правоприменительной практики за рассматриваемый период времени, который показал, что основными видами мошенничеств, совершаемых с использованием информационно-телекоммуникационных технологий, продолжают оставаться такие, как:

– совершение телефонного звонка или направление sms преступником в адрес неопределенного круга лиц, и ложное сообщение о совершении их родственником / другом, дорожно-транспортного происшествия. За «решение» проблем, по которому «попавшему в беду» требуется некоторая сумма денежных средств, которые последний должен отдать сотруднику полиции / пострадавшему в ДТП / оплатить эвакуатор или штраф-стоянку, диктуя при этом банковский счет или номер мобильного телефона, привязанного к карте преступников;

– направление sms от имени компаний операторов сотовой связи или иных организаций с информацией о выигрыше потерпевшим приза, при этом запрашивая у такого абонента данные банковской карты и sms-кодов для «перевода» денежной суммы на счет «победителя». Получив доступ к ним, используя специальные программы, преступники переводят на свои счета все денежные средства с карт и счетов потерпевших;

– написание сообщения в социальных сетях путем «взлома» личных страниц с просьбой одолжить денежные средства от имени «друзей» с указанием банковского счета или номера мобильного телефона преступников для пополнения баланса;

– звонки или sms от представителей банков под предлогами «ваша карта заблокирована», с просьбой сообщения реквизитов своих карт и CVC-кодов для якобы разблокировки счетов, и под другими благовидными предлогами, помогающими преступникам завладеть информацией, позволяющей впоследствии совершать операции с денежными средствами от имени потерпевших без их непосредственного участия;

– размещение на сайтах, подобных «Avito», объявлений о продаже «товара», для приобретения которого требуется 100% предоплата в адрес продавца с указанием в переписке номеров карт и счетов, по факту не отправляя в адрес покупателя приобретенный «товар» или отправляя «муляж».

Примерно таким же способом совершаются мошенничества с использованием «зеркальных сайтов». Это далеко не полный перечень способов совершения обмана собственников имущества с целью его хищения.

В совершении таких преступлений придумываются все новые и новые способы, разрабатываются специальные программы, позволяющие использовать ip-телефонию, sip-телефонию, совершать телефонные звонки якобы со стационарных номеров телефонов, например +7(495), +7(8-800) и т.п., что еще в большей степени позволяет вводить в заблуждение население страны, которое предполагает, что звонок действительно осуществляется банковскими работниками головных офисов, расположенных в г. Москве.

Для размещения похищенных денежных средств преступники, помимо предприятий, находящихся в оффшорных зонах, и таких же банковских счетов, примерно с 2018 г. активно стали использовать перевод денежных знаков в криптовалюту, в частности, в биткоины (Bitcoin), что значительно усложнило выявление лиц, совершивших преступление, их связи, а также отслеживание похищенного имущества и тем более его изъятие и возврат законному владельцу.

При этом при обращении к сети Интернет с вопросом о возможности перевода денег в биткоины, поисковая система Яндекс выдает более 12 млн результатов. В том числе и с использованием популярнейшего приложения «Сбербанк онлайн».

Учитывая вышеописанные способы, такие мошенничества принято считать совершенными «дистанционно». Определение дистанционному мошенничеству в своей работе дал Р.В. Кудрявцев: «Дистанционное мошенничество – это совершение такого вида мошенничества, при котором виновный, чаще всего, используя компьютерные и телефонные сети, воздействует на сознание потерпевшего путем обмана, склоняет к передаче имущества удаленным образом» [2. С. 218–221].

По мнению автора, совершению подобного рода мошенничеств в Российской Федерации способствовал ряд причин, например таких, как:

1. Значительное развитие информационно-телекоммуникационных возможностей у населения страны в целом. Современное общество и ритмы жизни диктуют развитым странам необходимость активно внедрять в повседневную жизнь новейшие разработки в области информационных технологий, проходить глобализацию информационных процессов. И российское общество этому не исключение.

Такие возможности используются во всех значимых отраслях жизнедеятельности, например таких, как: образование всех видов и уровней, начиная от начальной школы и вплоть до высших учебных заведений, в которых происходит демонстрация материала, участие удаленным способом в видеоконференциях, дистанционное обучение и т.д.; в медицине, включая консультации, операции, апробацию медицинского оборудования; в торговле – заключение сделок и отправка документов посредством электронной почты, а также совершение оплаты и т.п.

2. Снижение цен на мобильные телефоны и иные мобильные устройства, что позволило значительной части граждан стать их владельцами. В связи с активной покупательской способностью и перенасыщением рынка сбыта мобильных телефонов и тому подобных

гаджетов (планшетов и т.п.) ценовая политика производителей стала более доступной для российских граждан. По этой причине практически у каждого человека различной возрастной категории имеется как минимум один мобильный телефон.

Данные нововведения, как следствие, сделали общество активными пользователями: социальных сетей, мобильных приложений, электронной почтой и другими возможностями, предоставленными сетью Интернет, как в личных целях (переводы денежных средств для оплаты коммунальных услуг, обучения, и т.п.), так и в рабочих (оплата товара по договорам, выплата заработной платы работникам и т.п.).

3. Внедрение в пользование лиц зарплатных проектов, переход на электронные платежные системы и др. Одним из социальных факторов, способствующих увеличению роста количества совершаемых мошенничеств рассматриваемой категории, автор считает глобальное внедрение банковских продуктов населению, таких как пластиковые дебетовые и кредитные карты (включая зарплатные, студенческие и пенсионные проекты), виртуальные счета, мобильный банкинг, интернет-магазины, работа с которыми осуществляется через личный кабинет, а равно посредством использования сети Интернет.

При этом для совершения операции по счетам разработчиками сайтов и владельцами интернет-магазинов запрашивается информация о кодах CVV2/CVC2, указанных банком, выпускающим пластиковые карты, расположенных на их оборотной стороне, зная которые, можно совершить любые денежные операции в пределах установленных банком лимитов. Отмена таких операций даже через обращение в банк практически не возможна.

Все вышеперечисленное способствует тому, что население РФ, вне зависимости от возраста, в 70% случаев перестало хранить наличные денежные средства при себе, в связи с чем количество совершаемых грабежей и разбойных нападений снизилось ввиду отсутствия предмета хищения и вместе с тем увело преступность в «безналичное пространство». Вследствие этого совершению таких мошенничеств подверглась практически вся взрослая часть общества, имеющая право и возможность пользования банковскими продуктами и мобильными устройствами.

Ущерб, причиняемый таким видом мошенничества, исчисляется миллионами рублей в год, как показывают официально опубликованные данные.

Кроме этого, как показывает практика, многие из потерпевших сразу после совершения в отношении них преступления не принимают мер к обращению в правоохранительные органы под влиянием заблуждения, в которое они были введены преступниками (в качестве примера можно привести уголовное дело, возбужденное по ч. 3 ст. 159 УК РФ в отношении неустановленного лица. Согласно материалам уголовного дела, летом 2017 г. гражданин А. приобрел посредством сети Интернет в фирме Х биологически активные добавки (далее – БАДы), однако должного эффекта от их приема не получил. Спустя год неустановленное лицо позвонило на мобильный телефон гражданину А. 1972 года рождения и, представившись сотрудником прокуратуры г. Москвы, пояснило, что он имеет право на компенсационные выплаты в сумме 580 000 руб. за то, что ранее приобретенные потерпевшим БАДы, не вылечили его болезнь. При этом неустановленное лицо пояснило, что для получения вышеуказанной компенсации мужчина должен заплатить налог в сумме 34 800 руб. на указанный преступником счет, которые якобы впоследствии вернутся на его счет обратно вместе с компенсацией. Гражданин А., будучи введенным в заблуждение, не осознавая истинные намерения преступников, с помощью онлайн-банкинга совершил неоднократные переводы, в общей сложности на 440 000 руб. Обратился в правоохранительные органы с заявлением о хищении спустя 3 месяца, так как все это время ожидал перевода в размере 1 020 000 руб. в качестве компенсации) [3].

Причинами «большой популярности» совершения мошенничеств вышеописанными бесконтактными способами у преступников являются: 1) расширенный круг потенциальных потерпевших; 2) возможность донести некую ложную информацию до потерпевших, оставаясь незамеченным; 3) обеспечение собственной анонимности и безопасности, исключение возможности опознания внешности и демонстрации голоса, по которому возможно было бы провести фоноскопическую экспертизу; 4) возможность удаленного получения от жертвы денежных средств в различных суммах; 5) возможность нахождения потерпевшего и участников преступной группы относительно друг друга на значительном территориальном удалении – от разных субъектов РФ до разных стран.

Все эти факторы делают раскрытие и расследование такого вида мошенничества крайне сложными.

Таким образом, в настоящее время преступники получили реальную возможность воспользоваться складывающейся ситуацией некоего замешательства правоохранительных органов в регулировании методов выявления, документирования и расследования данного вида преступлений, поняв, что для получения незаконного обогащения не обязательно совершать «опасные для себя» виды преступлений, связанные с нападением, применением насилия в отношении потерпевших и т.п., при этом оставаясь длительное время не установленными.

Зачастую представители преступного мира, избирая новый способ совершения преступлений, успевают выработать свои методы и тактику, опробовать технические средства, используемые при совершении преступления, а также подобрать соучастников из числа лиц, обладающих специальными познаниями. Чего нельзя в настоящее время сказать о сотрудниках правоохранительных органов, которые в большинстве случаев не успевают переориентироваться и надлежащим образом противостоять неизвестным методам совершения преступлений, в том числе ввиду отсутствия общей стратегии поведения в борьбе с мошенничествами.

Подводя итоги, сделаем несколько выводов.

1. Нынешнее время диктует необходимость совершенствования уровня профессиональных знаний и

умений у сотрудников органов внутренних дел, которые в силу своих должностных обязанностей принимают участие в выявлении, раскрытии и расследовании рассматриваемого вида преступлений.

2. Для решения возникающих проблем в качестве консультантов и исполнителей направляемых в рамках расследования уголовных дел запросов и постановлений суда следует привлекать к взаимодействию организации, такие как операторы сотовой связи, банки, интернет-провайдеры и иные, с помощью которых возможно будет наладить оперативное получение данных, блокирование денежных средств на счетах при попытках совершения финансовых операций с использованием номеров телефонов, сайтов и т.п., ранее замеченных при совершении преступлений или противоправных действий.

3. Говоря о предупреждении и пресечении совершения мошенничеств в отношении граждан, следует отметить отсутствие у населения страны в целом должной реакции на сведения, распространяемые правоохранительными органами с помощью средств массовой информации, а также личных профилактических бесед о мерах по реагированию на действия преступников, направленных на хищение имущества, путем обмана и злоупотребления доверием.

4. Данную работу надлежит продолжать, доводя до населения страны информацию о новых способах совершения преступлений и противостояния им, основной упор делая на запрет сообщать посторонним лицам данные о номерах своих банковских счетов, sms-кодов и паролей для входа в онлайн-банкинг, личный кабинет и т.п.

ЛИТЕРАТУРА

1. *Петров С.А.* Анализ состояния мошенничества в России // Российский следователь. 2009. № 13. С. 34–40.
2. *Кудрявцев Р.В.* Организация деятельности по раскрытию дистанционных мошенничеств // Молодой ученый. 2019. № 24. С. 218–-221.
3. *Уголовное* дело № 11801120011000317 от 21.09.2018 данные ИЦ УМВД России по Астраханской области // СПС «КонсультантПлюс» (дата обращения: 20.04.2020).

General Causes and Some Types of Fraud Committed With the Use of Information and Telecommunication Technologies in the Russian Federation

Ugolovnaya yustitsiya – Russian Journal of Criminal Law, 2020, no. 16, pp. 28−31. DOI: 10.17223/23088451/16/6
Olga V. Khanineva, Krasnodar University of the Ministry of Internal Affairs of Russia (Krasnodar, Russian Federation). E-mail: hanineva83@mail.ru
Keywords: fraud, mobile devices, Internet, suppression, prevention.

The article describes the main reasons for the increase in the number of registered frauds committed in the Russian Federation over the past 4 years and provides examples of the most common types of fraud committed with the use of information and telecommunication devices. The author analyzes the reasons for committing frauds using communication facilities and information and communication technologies, with the focus on their types, ways of commission, categories of citizens most susceptible to these crimes. The author lists the most common types of fraud and their nature and proposes improvements for further activities of law enforcement officers to promote cooperation with other organizations involved in transferring and storing funds of citizens (banks) and providing communication services via the Internet (providers, companies of cellular operators) with the aim to curb the growth of crimes and achieve the high-quality prevention and protection of information about citizens and their funds.

References

1. Petrov, S.A. (2009) Analiz sostoyaniya moshennichestva v Rossii [Fraud in Russia]. *Rossiyskiy sledovatel' – Russian Investigator*. 13. pp. 34–40.
2. Kudryavtsev, R.V. (2019) Organizatsiya deyatel'nosti po raskrytiyu distantsionnykh moshennichestv [Organization of activities to disclose remote fraud]. *Molodoy uchenyy*. 24. pp. 218–221.
3. Russian Federation. (2018) *Criminal case No. 11801120011000317 of September 21, 2018, data of the IC UMVD of Russia for the Astrakhan Region*. [Online] Available form: SPS "KonsultantPlus" (Accessed: 20th April 2020). (In Russian).