УДК 343.9 DOI: 10.17277/pravo.2021.02.pp.079-087

Предложен анализ положений действующего законодательства в сфере противодействия распространению хищений денежных средств, совершаемых дистанционным способом путем обмана или злоупотребления доверием. Основываясь на практических примерах, обоснована злободневность исследуемого вопроса, сделан вывод о недостаточности правового регулирования в данной области общественных отношений, возможности противодействия совершению кибермошенничеств посредством тех же самых инструментов, с использованием которых они совершаются. В ходе исследования не остаются в стороне конкретные вопросы выявления несовершенных положений законодательства, а также формулируются варианты его корректировки в целях повышения эффективности правоохранительной деятельности. Данная работа носит практико-ориентированный характер.

Ключевые слова: дистанционное мошенничество; Интернет; киберпреступность; мобильное приложение; сотовая связь.

Вадим Владимирович Крамской, *канд. юрид. наук, доцент,*
кафедра «Гражданское право и процесс»,
ФГБОУ ВО «Тамбовский государственный технический университет»,
Тамбов, Россия;
vkramskoy@mail.ru

Анастасия Николаевна Козодаева, *магистрант,*
ФГБОУ ВО «Тамбовский государственный технический университет»;
юрисконсульт, правовой отдел УМВД России по Тамбовской области,
Тамбов, Россия;
akozodaeva@mail.ru

ПРОТИВОДЕЙСТВИЕ РАСПРОСТРАНЕНИЮ КИБЕРМОШЕННИЧЕСТВА: НОВЫЕ ВОЗМОЖНОСТИ В РАССЛЕДОВАНИИ И ПУТИ СОВЕРШЕНСТВОВАНИЯ ЗАКОНОДАТЕЛЬСТВА

Введение. Научно-технический прогресс не стоит на месте – в обыденной жизни российских граждан за последние двадцать лет произошли кардинальные изменения, обусловленные стремительным развитием техники и в первую очередь в сфере обработки информации. Сегодня никого уже не удивят такие предметы, как планшетный компьютер, электронная книга, гаджеты виртуальной и дополненной реальности и, безусловно, смартфоны.

Образ жизни нынешнего человека все больше обретает цифровое качество – над живым общением начинает преобладать общение в социальных сетях и мессенджерах, налично-денежный оборот сменяется безналичным, на смену торговым точкам приходят интернет-магазины, а сетевые торговые площадки заменяют собой супермаркеты. Популярность современных информационных технологий объяснима удобством, которую они привносят в нашу жизнь.

Так, уже не нужно предварительно заказывать междугородние телефонные переговоры у оператора связи, нет необходимости носить с собой наличные денежные средства при существующей возможности оплаты товаров банковской картой или сотовым телефоном, поддерживающим технологию NFC (бесконтактная передача данных платежному и иному устройству), перевод денежных средств посредством мобильного приложения, установленного в смартфоне через сеть Интернет или GSM-канал связи и др. Несмотря на бесспорное повышение качества жизни современного человека, такой научно-технический прогресс имеет и обратную сторону – феномен роста количества хищений денежных средств, совершаемых дистанционно с использованием информационно-телекоммуникационных технологий. Результатом этого, в конечном итоге, стало появление отдельной категории преступлений, именуемой в криминологии и уголовно-правовой науке «IT-преступность». При этом в структуре самой IT-преступности особое место занимают так называемые кибермошенничества.

Но не только само общество столкнулось с проблемой IT-преступности и кибермошенничества, но и правоохранительные органы, которым приходится противодействовать данному социальному недугу, а в этой связи использовать те же самые информационные технологии в целях предотвращения появления новых преступлений и расследования уже совершенных. Широкое использование современных информационно-телекоммуникационных технологий не всегда может способствовать сдерживанию роста преступлений данного вида. Отдельное внимание в этом вопросе должно уделяться также и совершенствованию законодательства в указанной области общественных отношений.

Методы. В настоящей работе авторами широко используется привычный научный инструментарий, состоящий из формально-юридического метода, позволившего определиться с понятием кибермошенничества и уголовно-правовыми составами, его образующими. При проведении данного исследования широко использовался диалектический метод познания, что обусловлено необходимостью рассмотрения любого правового явления в динамике и признания стимулами его развития существующих противоречий в рамках правовой системы. Исследование проводилось с применением статистического метода, позволившего обосновать актуальность заданного вопроса, и принципа системного анализа факторов, влияющих на успешность расследования преступлений в сфере дистанционного мошенничества. Авторами в ряде случаев предпринят междисциплинарный подход в работе, с точки зрения сочетания криминологических и криминалистических выкладок, а также использования положений законодательства различной отраслевой принадлежности.

Результаты. Согласно официальным статистическим данным о состоянии преступности в Российской Федерации, предоставленными ФКУ «ГИАЦ МВД России» за период с января по декабрь 2020 года отмечается общий рост преступлений, совершенных с использованием информационно-телекоммуникационных технологий на 73,4 %, в том числе с использованием сети Интернет – на 91,3 %, при помощи средств мобильной связи – на 88,3 % в сравнении с аналогичным периодом 2019 года.

В отдельных субъектах Российской Федерации темп прироста количества зарегистрированных преступлений указанного вида за 2020 год составляет более 100 %, в частности, в городе федерального значения Санкт-Петербург – 289,9 %, Калужской области – 159,4 %, Самарской области – 129,8 %, Карачаево-Черкесской Республике – 127,9 %.

Удельный вес названных преступных деяний от числа всех зарегистрированных в 2020 году составил порядка 25 %, а в 2019 году – 15 %.

Основная масса преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, приходится на кражи и мошенничества.

В то же время процент раскрываемости таких преступлений составляет примерно 20 %, то есть изобличить злоумышленника удается только в каждом пятом из общего числа зарегистрированных преступлений, связанных с использованием информационно-телекоммуникационных технологий [2].

Приведенные цифры позволяют прийти к следующим умозаключениям:

– информационные технологии и технические средства коммуникации активно используются населением;

– каждое четвертое зарегистрированное преступление в России – это кража либо мошенничество с использованием информационно-телекоммуникационных технологий;

– существующие правовые средства не позволяют сдерживать дальнейшее стремительное развитие негативного процесса киберпреступности;

– правоохранительный механизм нуждается в использовании новейших средств и методов идентификации лиц, причастных к киберпреступности.

Под киберпреступностью принято понимать преступления, совершаемые в виртуальном пространстве, а равно совершенные с использованием информационно-телекоммуникационных технологий [3, с. 111]. Это собирательное понятие, которое включает в себя множество составов уголовно наказуемых деяний, среди которых особое место занимают так называемые кибермошенничества или, говоря формально, – мошенничество с использованием электронных средств платежа или компьютерной информации, ответственность за совершение которого установлена соответственно в ст.ст. 159.3 и 159.6 Уголовного кодекса Российской Федерации.

Понятие электронного средства платежа нормативно установлено в Федеральном законе от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе», согласно которому это средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств. С учетом этого, предметом данного преступления выступает чужое имущество, представленное, как правило, денежными средствами, что обусловливает специфику данной формы хищения [1, с. 111].

Основной проблемой в раскрытии кибермошенничеств является процесс получения информации о реальном местонахождении преступника, так как преступные деяния данного вида совершаются дистанционно, носят межрегиональный характер, в связи с чем положительного результата в расследовании преступления можно достичь только при получении информации о его местонахождении (геолокации).

В этой связи непревзойденную актуальность обретают сами по себе информационно-телекоммуникационные технологии, с использованием которых и совершаются кибермошенничества. Рассмотрим их подробней.

Использование возможностей мобильных приложений по идентификации абонентского номера и получении информации об образе жизни абонента и его социальных связях.

В настоящее время существует множество мобильных приложений и интернет-ресурсов, использование которых способствует получению оперативно-значимой информации для расследования кибермошенничеств. К числу таковых относятся следующие: NumBuster, Getcontact, приложения онлайн-банкинга, NetMonitor, PhotoSherlock.

Мобильные приложения NumBuster и Getcontact предоставляют опцию по установлению данных о неизвестных абонентских номерах. Данная функция может быть использована для достижения следующих целей: предупреждения мошеннических действий и получения оперативной информации для изобличения лица, совершившего мошенничество дистанционным способом.

Функционал данных программ отражает сведения о том, каким образом тот или иной абонентский номер зафиксирован у других пользователей в телефонной книге смартфона, отзывы о владельце данного номера, а также оценка доверия к нему и комментарии пользователей названных приложений.

Так, пользователю смартфона, у которого установлены данные приложения, поступает звонок с неизвестного абонентского номера. В ходе идентификации пользователю смартфона предоставляется информация о том, что данный номер обладает низкой оценкой доверия, а также записан у ряда пользователей как «Мошенник», «Преступник» и др.

Говоря о получении информации с помощью указанных мобильных приложений, следует отметить, что абонентские номера используются мошенниками не только для совершения звонков, но также и для регистрации на отдельных интернет-ресурсах – электронных почтах, социальных сетях, досках объявлений. Проверяя и обобщая сведения через приложения NumBuster и Getcontact по всем абонентским номерам мошенника, можно установить его данные, а в некоторых случаях даже и анкетные данные.

Приложения онлайн-банкинга, такие как «СберБанк» или «ВТБ» могут быть источником получения дополнительных сведений о владельце абонентского номера.

Например, в 2019 году начала свою работу «Система быстрых платежей», позволяющая переводить безналичные денежные средства из одного банка в другой по номеру мобильного телефона, сопряженного с банковской картой. Оформляя заявку на перевод денежных средств по абонент-

скому номеру через приложения банков, можно узнать, банковские карты какого банка находятся в пользовании у мошенника, и запросить информацию по ним в установленном порядке. Из информации о движении денежных средств можно узнать о покупках в интернет-магазинах, а в последующем о доставках товара; о других абонентских номерах, пополняемых злоумышленником, а также о местах общего пользования, где он часто пребывает (кафе, бары, кинотеатры и др.). В этой связи, можно запросить у банка IP-адреса посещения личного кабинета по банковской карте мошенника, что в последующем может помочь узнать реальный адрес его местонахождения. Приложение «СберБанк», помимо указанной информации, предоставляет частичные сведения о держателе банковской карты в формате «Иван Иванович И.», что также может нести в себе полезные сведения для расследования преступления.

NetMonitor – сервис обобщения информации о зоне покрытий операторов стандарта GSM, а также о расположении их базовых станций. Базовая станция – это комплекс приемопередающей аппаратуры, которая обслуживает абонентов в своей зоне действия. В момент совершения вызова абонентский номер «привязывается» к ближайшей базовой станции, что позволяет ориентировочно определить район его местонахождения при получении расширенной детализации звонков. Обозначенное приложение, используемое совместно с полученной детализацией, помогает получить более детальные характеристики базовых станций, а именно: силу сигнала, азимут направленности и точное географическое положение, общий анализ которых помогает вычислить более узкий сектор местности, в котором находился мошенник во время совершения вызова.

Мобильное приложение PhotoSherlock – сервис по поиску картинок и людей в сети Интернет по фотографии. Рассмотрим ситуацию, когда движение похищенных денежных средств было отслежено до момента их снятия в банкомате или совершения покупки в торговой точке. Опытный сотрудник органов внутренних дел, собравший эти сведения оперативно, сможет запросить видеоматериалы до момента их удаления с жесткого диска видеорегистратора в связи с истечением сроков хранения, однако лицо, снимающее денежные средства, на первоначальном этапе раскрытия преступления остается неизвестным. В случае, если видеоматериал хорошего качества, возможно получить скриншот с изображением интересующего лица, а приложение PhotoSherlock окажет содействие при идентификации личности мошенника путем поиска страниц его социальных сетей, страниц с сайтов знакомств, а также совместных фото со страниц его друзей в социальных сетях.

Использование возможностей опции «геолокация» мобильных приложений при расследовании кибермошенничеств.

Так, каждый современный смартфон оснащен системой геопозиционирования – функционалом определения реального местоположения электронного устройства, подключенного к сети Интернет. Практически каждое программное приложение смартфона запрашивает разрешение на получение информации о геолокации используемого смартфона, в целях облегчения работы со своим пользователем. Программное приложение

смартфона осуществляет подбор информации о временно́м поясе, погодных условиях региона, строит траектории движения пользователя, выявляет несанкционированные доступы к аккаунтам пользователя, отображает ближайшие банкоматы, остановки общественного транспорта и многое другое, правоохранители могут использовать данную функцию в своих целях.

К примеру, если в ходе следствия становится известно, что злоумышленник в своем арсенале может иметь определенное приложение (в преступных схемах преимущественно используют электронные кошельки «Яндекс.Деньги» и «Киви», что говорит о высокой степени вероятности использования злоумышленником и одноименных приложений – «Яндекс.Деньги» и «Киви»), то путем направления запроса администратору приложений можно получить сведения о местонахождении мошенника в момент подключения к приложению.

В то же время широко используемые мошенниками одноименные приложения сотовых операторов, к примеру, «Мой МТС», «МойTele2» и др. собирают информацию о геолокации устройства лишь в фоновом режиме, ввиду чего получение сведений от оператора связи о географическом положении смартфона, при использовании которого было запущено названное приложение, затруднительно для правоохранительных органов. При этом мошенниками данные приложения используются достаточно часто, что обусловлено возможностью перевода денежных средств по лицевому счету абонентского номера при их помощи. Повышенный интерес к данным приложениям у злоумышленника обусловлен еще и тем, что, как правило, используемый им номер сотового телефона оформлен на несуществующее лицо, а следовательно, общение злоумышленника и оператора связи происходит исключительно только через данное приложение.

Однако действующее правовое регулирование в данном вопросе не полноценно, поскольку на операторов связи не возложена обязанность по учету сведений о геолокации пользователей мобильных приложений.

Так, в силу ч. 1 ст. 64 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи» операторы связи обязаны хранить на территории Российской Федерации только:

1) информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи – в течение трех лет с момента окончания осуществления таких действий;

2) текстовые сообщения пользователей услугами связи, голосовую информацию, изображения, звуки, видео-, иные сообщения пользователей услугами связи – до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки.

Часть 1.1 ст. 64 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи» предусматривает обязанность операторов связи предоставлять уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, указанную выше информацию, информацию о пользователях услугами связи и об оказанных им услугах связи и иную информацию, необходимую для выполнения возложенных на эти органы задач, в случаях, установленных федеральными законами.

Сходным предписаниям операторов связи корреспондирует п. 12 Правил взаимодействия операторов связи с уполномоченными государствен-

ными органами, осуществляющими оперативно-розыскную деятельность, утвержденных постановлением Правительства Российской Федерации от 27 августа 2005 г. № 538.

Изложенное позволяет предложить идею о внесении изменения в ст. 64 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи» в части дополнения перечня сведений, подлежащих хранению и предоставлению уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность, операторами связи, информацией о геолокации пользователей услуг связи. Это, безусловно, сделает более эффективным процесс реализации оперативно-розыскных мероприятий по установлению местонахождения мошенника, а также будет мерой превентивного воздействия на лиц, вынашивающих преступный план.

Еще одним аспектом, заслуживающим внимания в ключе рассматриваемых вопросов, является совершенствование механизма оказания услуг связи в свете противодействия распространению кибермошенничеств и предоставление более широкого инструментария органам, осуществляющим оперативно-розыскную деятельность, в этом процессе.

Так, органам внутренних дел Российской Федерации в своей деятельности зачастую приходится сталкиваться с ситуацией, когда в дежурную часть обращается гражданин с заявлением о проведении проверки в отношении лица, которое путем обмана завладело его денежными средствами посредством электронного средства платежа и осуществляет их расходование, о чем заявителю поступают информационные сообщения от банковской или иной кредитной организации.

Как правило, списание денежных средств осуществляется с использованием смс-команд, задаваемых злоумышленником, или действиями самого потерпевшего, осуществляющего перевод денежных средств в пользу злоумышленника на указанный им абонентский номер сотовой связи и пр.

В этой связи видится целесообразным введение в арсенал правоохранительных органов такого механизма, как инициирование процедуры приостановления оказания услуг связи, чтобы избежать наступления тяжких последствий совершаемого хищения денежных средств.

Анализ законодательства в указанной сфере общественных отношений показал, что имеются пробелы правового характера в реализации предоставленного абзацем первым п. 1 ч. 1 ст. 15 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» органам, уполномоченным осуществлять оперативно-розыскную деятельность, права на прерывание предоставления услуг связи в случае возникновения непосредственной угрозы жизни и здоровью лица, а также угрозы государственной, военной, экономической, информационной или экологической безопасности Российской Федерации. Согласно абзацу первому п. 3 ст. 64 Федерального закона от 7 июля 2003 года № 126-ФЗ «О связи», приостановление оказания услуг связи юридическим и физическим лицам осуществляется операторами связи на основании мотивированного решения в письменной форме одного из руководителей органа, осуществляющего оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации в случаях, установленных федеральными законами. Из приведенных правоположений следует, что приостановление оказания услуг связи юридическим и физическим лицам в рамках проведения оперативно-розыскных мероприятий в полной мере невозможно, поскольк-

ку в абзаце первом п. 1 ч. 1 ст. 15 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» речь идет о прерывании, а не о приостановлении услуг связи, и вместе с тем речь идет о случаях возникновения непосредственной угрозы жизни и здоровью лица, а также угрозы государственной, военной, экономической, информационной или экологической безопасности Российской Федерации, но не угрозе нарушения прав, свобод и законных интересов физических и юридических лиц, что часто прослеживается по мошенническим действиям с использованием средств связи.

Ввиду этого в абзаце первом п. 1 ч. 1 ст. 15 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» слова «прерывать предоставление услуг связи в случае возникновения непосредственной угрозы жизни и здоровью лица, а также угрозы государственной, военной, экономической, информационной или экологической безопасности Российской Федерации» представляется рациональным заменить словами «прерывать (приостанавливать) предоставление услуг связи в случае возникновения непосредственной угрозы жизни и здоровью лица, угрозы нарушения прав лица, а также угрозы государственной, военной, экономической, информационной или экологической безопасности Российской Федерации».

Обсуждение. Динамика роста преступлений, связанных с использованием информационно-телекоммуникационных технологий и направленных на хищение денежных средств дистанционным способом во взаимосвязи со сравнительно низким показателем их раскрываемости, констатирует существующие проблемы в расследовании данных преступлений правоохранительными органами, а также обнаруживает неполноту правового регулирования деятельности операторов связи в контексте противодействия распространению киберпреступлений. Справедливым будет утверждение о том, что результативность борьбы с ними напрямую зависит от разработки новых методик противодействия данным преступлениям, мониторинга возможных изменений схем и средств их совершения, повышения квалификации сотрудников правоохранительных органов в сфере использования высоких технологий, а главное – от совершенствования законодательной базы.

Заключение. Предложенные средства и способы противодействия распространению кибермошенничеств, изобличения лиц, их совершивших, а также нормотворческие инициативы, безусловно, не искоренят данное явление, но их реализация совершенно точно поспособствует повышению эффективности правоохранительной деятельности.

Список литературы

1. **Комментарий** к Уголовному кодексу Российской Федерации (постатейный) / Под ред. д-ра юрид. наук, проф. Л. В. Иногамовой-Хегай. М.: НИЦ ИНФРА-М, 2013. 572 с.

2. **Официальный сайт** в сети «Интернет» Министерства внутренних дел Российской Федерации [Электронный ресурс]: URL: http://мвд.рф/reports/item/22678184/ (дата обращения: 01.03.2021).

3. **Федоров А. В.** Информационная безопасность в мировом политическом процессе. М.: МГИМО-Университет, 2006. 220 с.

References

1. **Inogamova-Khegay L.V. (Ed.)** *Kommentariy k Ugolovnomu kodeksu Rossiyskoy Federatsii (postateynyy)* [Commentary on the Criminal Code of the Russian Federation (itemized)]. Moscow: NITS INFRA-M, 2013. 572 p. (In Rus.)
2. **Available at:** http://mvd.rf/reports/item/22678184/ (accessed 01 Mart 2021).
3. **Fedorov A.V.** *Informatsionnaya bezopasnost' v mirovom politicheskom protsesse* [Information security in the global political process]. Moscow: MGIMO-Universitet, 2006. 220 p. (In Rus.)

Countering the Spread of Cyber Fraud: New Opportunities in the Investigation and Ways to Improve the Legislation

V.V. Kramskoy, *Cand. Sci. (Law), Associate Professor,*
Department of Civil Law and Procedure,
Tambov State Technical University, Tambov, Russia;
vkramskoy@mail.ru

A. N. Kozodaeva, *Master's Student,*
Tambov State Technical University;
Legal Adviser, Legal Department of the Russian MIA Administration
for the Tambov Region, Tambov, Russia;
akozodaeva@mail.ru

The analysis of the provisions of the current legislation in the field of counteracting the spread of theft of funds committed remotely by deception or abuse of trust is offered. Based on practical examples, the topicality of the issue under study is substantiated; a conclusion about the inadequacy of legal regulation in this area of public relations is made; the possibility of counteracting the commission of cyber fraud using the same tools with which they are committed is explored. In the course of the study, specific issues of identifying imperfect provisions of the legislation are not left aside, and options for adjusting it in order to increase the efficiency of law enforcement are formulated. The study is practice-oriented.

Keywords: remote fraud; Internet; cybercrime; mobile app; cellular.

Статья поступила в редакцию 14.04.2021

При цитировании использовать:

Крамской В. В., Козодаева А. Н. Противодействие распространению кибермошенничества: новые возможности в расследовании и пути совершенствования законодательства // Право: история и современность. 2021. № 2(15). С. 79 – 87. doi: 10.17277/pravo.2021.02.pp.079-087