УДК 343.7

© Руслан Алексеевич Митрофанов,
старший советник юстиции,
заместитель прокурора г. Владимира

© Иван Вадимович Листратов,
студент факультета права,
Владимирский филиал РАНХиГС,
г. Владимир
e-mail: listratoff25@yandex.ru

ДИСТАНЦИОННЫЕ ХИЩЕНИЯ: ТЕОРЕТИЧЕСКИЕ И ПРАКТИЧЕСКИЕ ВОПРОСЫ

Remote theft: theoretical and practical issues

Аннотация: *в статье рассматриваются вопросы, связанные с распространением дистанционных хищений в современной России. Авторами исследуются особенности преступлений данного вида, а также способы и механизмы их совершения. Проводится анализ проблем, возникающих при квалификации и расследовании дистанционных хищений. Предлагаются пути решения выявленных проблем, уделяется внимание направлениям деятельности по противодействию данным преступлениям и их профилактике на территории России.*

Abstract: *The article deals with issues related to the spread of remote theft in modern Russia. The author explores the features of crimes of this type, as well as the ways and mechanism of their commission. He analyzes the problems that arise in the qualification and investigation of remote theft. Ways of solving the identified problems are proposed, attention is paid to the areas of activity to counter these crimes and their prevention in Russia.*

Ключевые слова: *дистанционные хищения, дистанционное мошенничество, кража, безналичные денежные средства, информационные технологии, преступление, профилактика.*

Keywords: *remote theft, remote fraud, theft, non-cash funds, information technology, crime, prevention.*

В настоящее время повсеместно происходит развитие телекоммуникационных сетей, компьютерных технологий, высокотехнологичных систем по работе с информацией; в цифровое пространство переносится значительная часть общественных отношений. Естественный ход научно-технического прогресса сопровождается повышением доступности его достижений для широких масс, ввиду чего современные информационные технологии начинают активно использоваться различными социальными категориями для достижения

всевозможных целей. В этой связи неизбежным становится рост преступности, основанной на использовании возможностей цифровых технологий.

Одной из наиболее актуальных проблем в данной сфере можно считать распространение преступлений против собственности, совершаемых с использованием информационно-телекоммуникационных технологий (ИТТ), поскольку во многих случаях такие деяния отличаются сложностью квалификации, расследования и профилактики. На сегодняшний день для обозначения рассматриваемых преступлений в практике и научном сообществе укрепился термин «дистанционные хищения», которым в зависимости от обстоятельств дела именуются отдельные составы мошенничества и кражи [6, с. 65]. Однако юридического закрепления данного наименования, как и его единообразного понимания, не было достигнуто до сих пор.

Различные толковые словари русского языка, в том числе словарь под редакцией Д. Н. Ушакова, описывают мошенничество как корыстный обман [9, с. 311]. Определяя мошенничество в Уголовном кодексе Российской Федерации, законодатель указывает в дефинициях отличительные черты составов, в соответствии с которыми в случае мошенничества хищение имущества осуществляется путем обмана или злоупотребления доверием, предоставления заведомо ложных или недостоверных сведений и др. [1]. В основе мошеннических способов завладения чужим имуществом лежит добровольная передача потерпевшим имущества или права на него преступнику при уверенности, что последний действует правомерно. Именно внешняя добровольность многими авторами называется ключевым признаком мошенничества, отличающим его от других форм хищения [5, с. 16].

Можно констатировать, что мошенничество, совершенное с использованием информационно-телекоммуникационных технологий, имеет ряд особенностей. Его главным отличием является осуществление преступной деятельности в условиях, исключающих непосредственный личный контакт злоумышленника и жертвы. Субъект преступления не вступает в живое взаимодействие с потерпевшим; более того, он может находиться на территории другого субъекта Российской Федерации или даже иностранного государства. Зачастую происходят случаи, при которых дистанционное мошенничество совершается лицами, содержащимися в местах лишения свободы по приговору суда. В ходе совершения преступления используются средства связи, сеть «Интернет», посредством которых жертва переводит денежные средства на счет преступника. Иногда поведение потерпевшего может не носить характер активных действий, направленных на перевод платежных средств, а отличаться пассивностью, при которой он не препятствует их переводу (например, в случае совершения деяния путем распространения вредоносного программного обеспечения) [8, с. 346]. Характеризуя дистанционное мошенничество, еще

одним признаком и одновременно достоинством Н. Д. Литвинов называет тот факт, что оно никогда не перерастет в грабеж или разбой, так как при отсутствии положительного отклика на свои «предложения» со стороны потенциальной жертвы субъект просто перейдет к поискам другого объекта [7, с. 78].

Сегодня практика знает немало схем дистанционных мошеннических действий. Субъект преступления может завладевать денежными средствами путем введения потерпевшего в заблуждение о пребывании его родных или близких в трудных жизненных обстоятельствах, зачастую представляясь при этом сотрудником полиции. Мошенники могут представляться сотрудниками службы безопасности банка, стремящимися пресечь «несанкционированный доступ» к счетам потенциальной жертвы; создавать специальные сайты под видом реализации продукции, не имея в действительности таковой цели. Дистанционным мошенничеством может являться и завладение безналичными денежными средствами физических и юридических лиц путем неправомерного получения доступа к терминалам, системам банковского обслуживания при помощи вредоносного программного обеспечения.

От рассматриваемых преступлений следует отличать схожие деяния, которые квалифицируются по Уголовному кодексу Российской Федерации как кража, т.е. тайное хищение чужого имущества (как правило, охватываются п. «г» ч. 3 ст. 158 УК РФ). Так, согласно п. 17 постановления Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» действия злоумышленника будут считаться кражей в случае похищения безналичных денежных средств с использованием необходимой для получения доступа к ним конфиденциальной информации, переданной преступнику самим держателем платежной карты под воздействием обмана или злоупотребления доверием [3].

В юридической литературе отмечается, что дистанционные хищения характеризуются высоким уровнем эффективности при минимальных финансовых и организационных затратах, значительной прибылью, возможностью удаленного воздействия на жертву, высокой степенью конспиративности и вероятностью избежать ответственности, что обусловливает широкое распространение преступлений данного вида [7, с. 78]. В 2021 году на территории Российской Федерации зарегистрировано 406 041 хищение, совершенное с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что составляет приблизительно 20 % от общего числа зарегистрированных в стране преступлений; при этом за указанный период было раскрыто менее 64 тысяч удаленно совершенных хищений [4]. Неутешительную статистику можно видеть и в отдельных регионах: например, в административном центре Владимирской области за 2021 год более 24 % от общего числа преступлений составили дистанционные

хищения. Таким образом, каждое четвертое регистрируемое в городе Владимире преступление является хищением, совершенным с использованием ИТТ, в то время как раскрываемость остается на сравнительно низком уровне – 5 % по составам дистанционного мошенничества и 24,7 % по кражам, совершенным с банковских счетов или в отношении электронных денежных средств.

В настоящее время ситуация осложняется существованием большого количества разноплановых проблем, которые создают препятствия на пути качественного расследования дистанционных хищений, а также их эффективной профилактики. Многие из них могут быть справедливо отнесены к причинам многочисленности данных преступлений и низких показателей раскрываемости.

Как отмечалось ранее, характерной особенностью дистанционных хищений является отсутствие непосредственного контакта злоумышленника и жертвы. Находясь на территории одного субъекта Российской Федерации, лицо может пострадать от действий преступника из другого субъекта; денежные средства при этом могут быть переведены на счет, открытый в третьем субъекте. Это приводит к фактическому несовпадению места непосредственного совершения преступления с местом наступления преступных последствий, что вызывает массу сложностей в ходе расследования.

Кроме того, гражданин может пользоваться счетом, открытым в подразделении банка, находящемся за пределами субъекта его фактического проживания. В случае, если он станет потерпевшим по делу, связанному с дистанционной кражей, трудности начнутся еще до начала расследования, так как согласно новому пункту 25.2 постановления Пленума Верховного Суда РФ от 27.12.2002 № 29 «О судебной практике по делам о краже, грабеже и разбое» местом окончания кражи, предусмотренным п. «г» ч. 3 ст. 158 УК РФ, считается место нахождения подразделения банка, в котором владельцем был открыт счет или велся учет электронных денежных средств [2].

Так, в мае 2021 года в г. Владимире гражданином К. в подъезде хостела похищен мобильный телефон. При осмотре похищенного устройства К. обнаружил, что на указанном телефоне отсутствуют защитные пароли и имеется дистанционный доступ к банковскому счету. В течение последующих двух дней с целью хищения денежных средств с банковского счёта гражданин К. трижды переводил денежные средства на свой счёт и баланс своего абонентского номера, причём последние 2 перевода, а также приобретение товара в магазине осуществлялись с территории деревни Бараки Судогодского района Владимирской области. Банковский счёт, с которого удаленно похищены денежные средства, открывался потерпевшим в г. Новотроицке Оренбургской области, ввиду чего место окончания преступления юридически располагается более чем в полутора тысячах километров от мест непосредственной реализации

преступного умысла. Более того, с местом непосредственного совершения преступного деяния не совпадает и местонахождение суда, который будет рассматривать исследуемое дело.

Среди существующих проблем стоит также упомянуть сложность надлежащей идентификации владельцев счетов, на которые переводятся денежные средства, а также СИМ-карт, которые преступники используют для связи с жертвами. Формально владельцами могут числиться умершие или вовсе не существующие люди, иностранные граждане или иные лица, которые не имеют фактического отношения к счету или СИМ-карте. Целесообразным мы находим ужесточение требований по удостоверению личности в ходе приобретения соответствующих услуг, потому как данный шаг способен повысить эффективность расследования и снизить сложность доказывания.

Важным ориентиром, на наш взгляд, является повышение уровня защиты персональных данных пользователей, поскольку утечка клиентских баз компаний различного уровня может становиться почвой для совершения преступлений с использованием ИТТ. Более того, многие жертвы преступлений по указаниям субъекта оформляют кредит и в дальнейшем переводят злоумышленникам полученные денежные средства, потому борьбе с дистанционным мошенничеством может способствовать более четкое выяснение целей получения кредитов гражданами в банках и кредитных организациях, а также дополнительная информационная работа с потенциальными заемщиками.

Без сомнений, вклад в повышение эффективности и качества деятельности по организации расследования хищений, совершенных с использованием информационно-телекоммуникационных технологий, вносит специальная подготовка кадров и создание специализированных следственных и оперативных групп по рассматриваемому направлению. Так, например, на базе УМВД Владимирской области в декабре 2019 года создан специализированный отдел по раскрытию данных преступлений, включающий 10 оперативных сотрудников в аппарате. Кроме того, в территориальных отделениях полиции выделены конкретные сотрудники либо группы, за которыми закреплена линия по раскрытию дистанционных краж и мошенничеств.

Наконец, следует расширять масштабы информационной работы с населением в целях профилактики хищений, совершенных дистанционным способом. Ключевую роль в указанной деятельности играют правоохранительные органы на любом территориальном уровне.

Обратившись за примером к административному центру Владимирской области, можно увидеть, что УМВД России по г. Владимиру в целях пресечения совершения преступлений в рассматриваемой сфере на постоянной основе проводится комплекс информационно-пропагандистских мероприятий. Осуществляются публикации в региональной печатной прессе с разъяснением методов, которые

используются преступниками, чтобы войти в доверие к гражданам, приводятся примеры преступлений, проводятся беседы с гражданами. Организуются выступления представителей УМВД России по г. Владимиру в передачах регионального телевидения и радио, осуществляются публикации в социальных интернет-сетях. Изготовлены специальные видеоролики, распространяются памятки с призывами соблюдать бдительность и разъяснением порядка действия в ситуациях, последствием которых может быть хищение денежных средств и другого имущества.

На примере деятельности прокуратуры города Владимира можно также видеть активное проведение профилактической работы, направленной на предупреждение преступлений, связанных с посягательствами на информационную безопасность в сфере использования информационно-коммуникационных технологий, в том числе хищений, совершенных дистанционным способом. Работниками городской прокуратуры на постоянной основе осуществляется деятельность по проведению лекций, бесед, иных выступлений перед гражданами, изготавливаются информационные материалы, даются интервью средствам массовой информации. Так, например, помощником прокурора города Владимира К. в мае 2021 проведена лекция перед студентами Владимирского филиала РАНХиГС на тему «Противодействие преступлениям в сфере информационно-коммуникационных технологий и ответственность за совершение дистанционных хищений».

Подводя итог вышеизложенному, можно констатировать, что вопрос борьбы с дистанционными хищениями в нашей стране сегодня изобилует множеством проблем теоретического и практического плана. Ключом к решению этих проблем нам представляются их тщательное научное исследование и разработка на его основе грамотных мер практического характера, способных повысить эффективность правотворческой и правоприменительной деятельности, их результатов и, в конечном счете, качество жизни граждан Российской Федерации.

Список литературы

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 28.01.2022) // Собр. законодательства Рос. Федерации. – 1996. – № 25, ст. 2954.

2. О судебной практике по делам о краже, грабеже и разбое: постановление Пленума Верховного Суда РФ от 27.12.2002 № 29 (ред. от 29.06.2021) // Рос. газ. – 2003. – № 9.

3. О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 29.06.2021) // Рос. газ. – 2017. – № 280.

4. Состояние преступности в Российской Федерации за январь-декабрь 2021 года [Электронный ресурс] // ГИАЦ МВД России [Сайт]. URL: https://мвд.рф/reports/item/28021552 (дата обращения: 15.02.2022).

5. Богданов А. В., Ильинский И. И., Хазов Е. Н. Киберпреступность и дистанционное мошенничество как одна из угроз современному обществу // Криминологический журнал. – 2020. – № 1. – С. 15-20.

6. Евтушенко И. И., Венедиктов А. А. Дистанционные хищения: понятие и признаки // Гуманитарные, социально-экономические и общественные науки. – 2020. – № 12-2. – С. 65-67.

7. Литвинов Н. Д., Федоров А. Н. Мошенничество с использованием средств мобильной связи (дистанционное): понятие и особенности совершения // JSRP. – 2015. – № 12 (32). – С. 73-80.

8. Семенихина Т. Н. Порядок проверки факта дистанционного мошенничества, совершенного с использованием сети «Интернет» // Вестник ВИ МВД России. – 2021. – № 2. – С. 346-350.

9. Ушаков Д. Н. Толковый словарь современного русского языка. – М. : Аделант, 2014. – 800 с.