ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
«ВСЕРОССИЙСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Л. В. Яковлева, Е. И. Майорова, В. В. Улейчик

МОШЕННИЧЕСТВО В ЭПОХУ ЦИФРОВИЗАЦИИ: ОСОБЕННОСТИ СОВЕРШЕНИЯ И КВАЛИФИКАЦИИ

Научно-практический комментарий

МОСКВА 2024

УДК 343.1

Рекомендовано к опубликованию
редакционно-издательским советом ВНИИ МВД России

Р е ц е н з е н т ы:
Г. Г. Саркисян, кандидат юридических наук
(Академия управления МВД России);
С. И. Худиева, кандидат юридических наук
(Следственный департамент МВД России)

А в т о р ы:
Л. В. Яковлева, главный научный сотрудник НИЦ № 5,
доктор юридических наук, доцент;
Е. И. Майорова, ведущий научный сотрудник НИЦ № 5,
кандидат юридических наук, доцент;
В. В. Улейчик, заместитель начальника НИЦ № 5
(ВНИИ МВД России)

Яковлева, Л. В.
Мошенничество в эпоху цифровизации: особенности совершения и квалификации : научно-практический комментарий / Л. В. Яковлева, Е. И. Майорова, В. В. Улейчик. – Москва : ВНИИ МВД России, 2024. – 40 с.

Посвящен проблемам квалификации мошенничества в эпоху цифровизации. В нем раскрываются приемы, применяемые для совершения преступлений, связанные с использованием достижений научно-технического прогресса, особенно в сфере IT-технологий; проводится отграничение от смежных составов. На основе анализа теоретических источников и материалов судебной практики формулируются рекомендации по квалификации мошенничества в современных условиях.

Для следователей, руководителей и сотрудников органов внутренних дел, научных сотрудников научных и образовательных организаций системы МВД России.

Работа выполнена с использованием Справочной правовой системы КонсультантПлюс.

УДК 343.1

© ВНИИ МВД России, 2024

ВВЕДЕНИЕ

Эпоха цифровизации – такими словами можно охарактеризовать современный этап развития общества. Он отличается повсеместным внедрением цифровых технологий, в том числе в правовую систему.

С одной стороны, цифровизация помогает оптимизировать различные сферы жизнедеятельности общества, с другой, – возникли новые риски для социума, включая появление новых видов преступлений и способов их совершения. Прежде всего это касается хищений чужого имущества путем обмана или злоупотребления доверием с использованием электронных сетей или информационно-телекоммуникационных технологий, включая сеть Интернет.

Квалифицируются такие деяния по ст. 159 УК РФ «Мошенничество» или по ст. 159.3 УК РФ «Мошенничество с использованием электронных средств платежа». В таблице[1] представлены сведения о количестве зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий в 2019–2023 гг. Из таблицы видно, что в 2019–2020 гг. росло число преступлений, подпадавших под действие ст. 159.3 УК РФ, а начиная с 2021 г. их стало регистрироваться меньше. Данное обстоятельство обусловлено изменениями, внесенными Верховным Судом Российской Федерации в два постановления Пленума[2], в которых содержатся рекомендации по разграничению кражи с банковского счета, а равно в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ), и мошенничества, квалифицируемого по ст. 159.3 УК РФ. Тем не менее число преступлений в рассматриваемой сфере неуклонно растет, множится число пострадавших от действий недобросовестных лиц.

---

[1] См.: Состояние преступности в России за январь – декабрь 2019–2023 годы. М. : ГИАЦ МВД России, 2020–2024.

[2] О судебной практике по делам о краже, грабеже и разбое : постановление Пленума Верховного Суда Рос. Федерации от 27 дек. 2002 г. № 29 : ред. от 15 дек. 2022 г. // Бюллетень Верховного Суда Рос. Федерации. 2003. № 2; О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верховного Суда Рос. Федерации от 30 нояб. 2017 г. № 48 : ред. от 15 дек. 2022 г. // Бюллетень Верховного Суда Рос. Федерации. 2018. № 2.

Таблица

Сведения о количестве зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий (в сравнении с предыдущим годом)

Годы	Количество зарегистрированных преступлений, тыс. (АППГ)	Удельный вес в общем числе зарегистрированных преступлений (АППГ)	Из них тяжких и особо тяжких, тыс. (АППГ)	Удельный вес от числа преступлений в гр. 2	Из гр. 2 с использованием сети Интернет, тыс.	Из гр. 2 с использованием средств мобильной связи, тыс. (АППГ)	Кражи и мошенничества из гр. 2 (АППГ)	Из гр. 8 ст. 159 УК РФ	Из гр. 8 ст. 159.3 УК РФ
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
2019	294,4 (+ 68,5 %)	14,5 (+5,7 %)	142,7 (+149,0 %)	48,5 %	157,0 (+45,4 %)	116,2 (+89,5 %)	235,5 (+83,2 %)	119 903	16 119
2020	510,4 (+73,4 %)	25,0 % (+10,5 %)	267,6 (+87,5 %)	52,4 %	300,3 (+91,3 %)	218,7 (+88,3 %)	410,5 (+74,3 %)	210 493	25 820
2021	517,7 (+1,4 %)	25,8 % (+0,8 %)	288,3 (+7,7 %)	55,7 %	351,5 (+17,0 %)	217,6 (–0,5 %).	406,0 (–1,1 %)	238 560	10 258
2022	522,1 (+0,8 %)	26,5 % (+0,7 %)	272,2 (–5,6 %)	52,1 %	381,1 (+8,4 %)	213,0 (–2,1 %)	371,2 (–8,6 %)	249 984	7 288
2023	677,0 (+29,7 %)	34,8 % (+12,3 %)	342,6 (+25,9 %)	50,6 %	526,8 (+38,2 %)	302,9 (+42,2 %)	475,3 (+28,1 %):	353 201	2 461

Приведенные в таблице данные показывают, что в 2023 г. практически каждое третье преступление совершалось с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. За пять лет (с 2019–2023 г.) число таких преступлений увеличилось в 2,5 раза. По данным ЦБ России только за шесть месяцев 2023 г. у граждан было похищено более 8 млрд рублей, что на треть больше, чем за аналогичный период 2022 г. Возвращено владельцам было всего лишь 4,39 % от похищенной суммы (около 356,6 млн руб.)[3].

Эти показатели свидетельствуют об актуальности противодействия мошенничеству, совершаемому с использованием информационно-телекоммуникационных технологий.

В настоящее время в значительном числе случаев виновные лица прибегают к помощи социальной инженерии, которая представляет собой воздействие на психику людей с целью побуждения их к определенным действиям или к разглашению конфиденциальной информации (например, паспортных данных, логинов и паролей). При этом они гибко подстраиваются под обстоятельства, учитывают то, на что в обществе в конкретный период возникает наибольший спрос (например, в преддверии празднования Нового года создают поддельные сайты продажи билетов на различные культурно-зрелищные мероприятия; перед сдачей выпускниками школ единого государственного экзамена предлагают ответы на вопросы также на поддельных сайтах и пр.). Кроме того, оперативно меняют схемы совершения мошенничества, если о них становится известно широкому кругу людей благодаря разъяснительной работе со стороны правоохранительных органов, банков и пр.

[3] См.: Сетевой протокол: треть преступлений в России стали совершать с помощью IT. URL: https://news.mail.ru/society/58670659/?frommail=1 (дата обращения: 15.04.2024).

1. УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА МОШЕННИЧЕСТВА (СТАТЬИ 159, 159.3 УК РФ)

Под мошенничеством понимается хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием (ч. 1 ст. 159 УК РФ).

«Обман как способ совершения хищения или приобретения права на чужое имущество может состоять в сознательном сообщении (представлении) заведомо ложных, не соответствующих действительности сведений, либо в умолчании об истинных фактах, либо в умышленных действиях (например, в предоставлении фальсифицированного товара или иного предмета сделки, использовании различных обманных приемов при расчетах за товары или услуги или при игре в азартные игры, в имитации кассовых расчетов и т.д.), направленных на введение владельца имущества или иного лица в заблуждение.

Сообщаемые при мошенничестве ложные сведения (либо сведения, о которых умалчивается) могут относиться к любым обстоятельствам, в частности к юридическим фактам и событиям, качеству, стоимости имущества, личности виновного, его полномочиям, намерениям.

Злоупотребление доверием при мошенничестве заключается в использовании с корыстной целью доверительных отношений с владельцем имущества или иным лицом, уполномоченным принимать решения о передаче этого имущества третьим лицам. Доверие может быть обусловлено различными обстоятельствами, например, служебным положением лица либо его личными отношениями с потерпевшим.

Злоупотребление доверием также имеет место в случаях принятия на себя лицом обязательств при заведомом отсутствии у него намерения их выполнить с целью безвозмездного обращения в свою пользу или в пользу третьих лиц чужого имущества или приобретения права на него (например, получение физическим лицом кредита, аванса за выполнение работ, услуг, предоплаты за поставку

товара, если оно заведомо не намеревалось возвращать долг или иным образом исполнять свои обязательства)» [4].

Под имуществом при мошенничестве понимаются вещи материального мира, имеющие стоимость.

Специальным видом мошенничества является мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ).

Электронное средство платежа – 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[5].

Следует обратить внимание на то, что до 29 июня 2021 г. в постановлении Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» содержался п. 17, согласно которому по ст. 159.3 УК РФ квалифицировалось хищение имущества с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем сообщения уполномоченному работнику кредитной, торговой или иной организации заведомо ложных сведений о принадлежности указанному лицу такой карты на законных основаниях либо путем умолчания о незаконном владении им платежной картой[6].

Постановлением Пленума Верховного Суда РФ от 29 июня 2021 г. № 22 «О внесении изменений в отдельные постановления Пленума Верховного Суда Российской Федерации по уголовным делам»[7] данный пункт был исключен.

В определении Конституционного Суда Российской Федерации от 9 июля 2021 г. № 1374-О указывается, что таким образом Верховным Судом Российской Федерации устранена существовавшая в правоприменительной практике неопределенность в разграничении составов кражи, совершенной с банковского счета, а равно в

---

[4] См.: О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верховного Суда Рос. Федерации от 30 нояб. 2017 г. № 48 : ред. от 15 дек. 2022 г. // Бюллетень Верховного Суда Рос. Федерации. 2018. № 2.

[5] См.: О национальной платежной системе : Федер. закон от 27 июня 2011 г. № 161-ФЗ : ред. от 24 июля 2023 г. // Собр. законодательства Рос. Федерации. 2011. № 27, ст. 3872.

[6] См.: Бюллетень Верховного Суда Рос. Федерации. 2018. № 2.

[7] См.: Российская газета. 2021. № 159.

отношении электронных денежных средств, и мошенничества с использованием электронных средств платежа.

В частности, постановление Пленума Верховного Суда Российской Федерации от 27 декабря 2002 г. № 29 (ред. от 15 декабря 2022 г.) «О судебной практике по делам о краже, грабеже и разбое»[8] дополнено пунктом 25.1, в соответствии с которым тайное изъятие денежных средств с банковского счета или электронных денежных средств, например, если безналичные расчеты или снятие наличных денежных средств через банкомат были осуществлены с использованием чужой или поддельной платежной карты, надлежит квалифицировать как кражу по признаку «с банковского счета, а равно в отношении электронных денежных средств».

По п. «г» ч. 3 ст. 158 УК РФ квалифицируются действия лица и в том случае, когда оно тайно похитило денежные средства с банковского счета или электронные денежные средства, использовав необходимую для получения доступа к ним конфиденциальную информацию владельца денежных средств (например, персональные данные владельца, данные платежной карты, контрольную информацию, пароли).

В определении от 9 июля 2021 г. № 1374-О Конституционный Суд Российской Федерации также указал, что «использование обладателем чужой платежной карты в таком случае обмана (злоупотребления доверием) для введения в заблуждение уполномоченного работника организации, реализующей товары, выполняющей работы, предоставляющей услуги, относительно принадлежности платежной карты не может рассматриваться как мошенничество (покушение на мошенничество), поскольку указанный работник не наделен распорядительными полномочиями в отношении денежных средств на конкретном банковском счете. Соответственно, обман похитителем уполномоченного лица торговой или иной организации (злоупотребление его доверием) может расцениваться в качестве действий по созданию условий для тайного хищения денежных средств с банковского счета, т.е. кражи (п. «г» ч. 3 ст. 158 УК РФ)»[9].

---

[8] См.: О судебной практике по делам о краже, грабеже и разбое : постановление Пленума Верховного Суда Рос. Федерации от 27 дек. 2002 г. № 29 : ред. от 15 дек. 2022 г. // Бюллетень Верховного Суда Рос. Федерации. 2003. № 2.

[9] См. подробнее решения по конкретным делам: определения Судебной коллегии по уголовным делам Верховного Суда Рос. Федерации от 11 марта 2020 г. № 10-УДП20-1, от 29 сент. 2020 г. № 12-УДП20-5-К6, от 25 февр. 2021 г. № 81-УД21-1-К8, от 9 марта 2021 г. № 11-УД20-35-К6.

С., забрав в банкомате торгового центра забытую потерпевшим Ф. платежную карту ПАО «Сбербанк России», приобрел в магазине продукцию на сумму 2 135 руб., расплатившись этой картой.

С. был осужден по п. «г» ч. 3 ст. 158 УК РФ за кражу с банковского счета[10].

В связи с приведенными разъяснениями высших судебных инстанций суды переквалифицировали действия виновных лиц со ст. 159.3 УК РФ на п. «г» ч. 3 ст. 158 УК РФ по уже вынесенным приговорам.

Например, судом первой инстанции И. был признан виновным в совершении грабежа, а также мошенничества с использованием электронных средств платежа группой лиц по предварительному сговору с причинением значительного ущерба гражданину.

Согласно приговору И. применил насилие к А., не опасное для жизни и здоровья, после чего открыто похитил из внутреннего кармана куртки потерпевшего портмоне, в котором находились денежные средства и банковская карта ПАО «ВТБ».

Затем И. и лицо, уголовное дело в отношении которого выделено в отдельное производство, расплачивались похищенной у потерпевшего банковской картой в кафе и в магазинах, причинив потерпевшему значительный материальный ущерб. Действия И. были квалифицированы по ч. 2 ст. 159.3 УК РФ.

Апелляционным определением судебной коллегии по уголовным делам Московского городского суда от 14 апреля 2022 г. приговор в части квалификации содеянного не был изменен.

Однако в кассационной инстанции было отмечено, что по смыслу уголовного закона хищение денежных средств, совершенное с использованием виновным электронного средства платежа, образует состав преступления, предусмотренный ст. 159.3 УК РФ, в тех случаях, когда изъятие денежных средств было осуществлено путем обмана или злоупотребления доверием с использованием электронных средств платежа как способа совершения преступления. В соответствии с этим действия И. подлежат квалификации в этой части не по ст. 159.3 УК РФ, а по п. «г» ч. 3 ст. 158 УК РФ[11].

Таким образом под действие ст. 159.3 УК РФ подпадает мошенничество, при котором использование электронных средств платежа является способом его совершения.

---

[10] См.: Постановление Первого кассационного суда общей юрисдикции от 17 янв. 2023 г. № 77-376/2023 // СПС КонсультантПлюс.

[11] См.: Кассационное определение Второго кассационного суда общей юрисдикции от 17 янв. 2023 г. № 77-123/2023 // СПС КонсультантПлюс.

Так, например, С. из корыстных побуждений, желая путем обмана похитить денежные средства, вошел с помощью принадлежащего ему мобильного телефона посредством информационно-телекоммуникационной сети Интернет на сайт микрофинансовой организации ООО МКК «Академическая», где для заключения договора займа денежных средств внес паспортные данные своей знакомой Д. без ведома и согласия последней. Для получения денег он указал реквизиты своей банковской карты.

После этого уполномоченное лицо ООО МКК «Академическая», будучи введенным С. в заблуждение, заключило с Д. договор потребительского займа на сумму 3 тыс. руб. В тот же день с расчетного счета названной организации в АО «БАНК СНГБ» на открытую на имя С. банковскую карту ПАО «Сбербанк» были перечислены денежные средства в сумме 3 тыс. руб., которыми С. распорядился по своему усмотрению.

С. был осужден по ч. 1 ст. 159.3 УК РФ[12].

В судебной практике встречаются случаи переквалификации деяний со ст. 159.3 УК РФ на ст. 159 УК РФ.

Так, Ш. предлагал через сеть Интернет приобрести запасные части для автомобиля, которых у него не было. После получения предоплаты Ш. прекращал общение с покупателем. Судом первой инстанции действия Ш. были квалифицированы по ч. 2 ст. 159.3 УК РФ.

Суд апелляционной инстанции указал, что Ш. не использовал электронные средства платежа для введения в заблуждение потерпевших. Они применялись для перечисления Ш. денежных средств лицами, уже находившимися под влиянием обмана, то есть электронные средства платежа в данном случае не являлись способом совершения мошенничества.

При таких обстоятельствах приговор суда первой инстанции был изменен, а действия Ш. переквалифицированы на ч. 2 ст. 159 УК РФ как мошенничество, совершенное с причинением значительного ущерба гражданину[13].

Мошенничество признается оконченным с момента, когда денежные средства поступили в незаконное владение виновного или других лиц, и они получили реальную возможность пользоваться или распорядиться ими по своему усмотрению.

---

[12] См.: Приговор Ставропольского гарнизонного военного суда от 2 окт. 2023 г. № 1-50/2023 // СПС КонсультантПлюс.

[13] См.: Апелляционное постановление Верховного суда Республики Алтай от 23 нояб. 2023 г. по делу № 22-890/2023 // СПС КонсультантПлюс.

Если предметом преступления при мошенничестве являются безналичные денежные средства, в том числе электронные денежные средства, то преступление следует считать оконченным с момента изъятия денежных средств с банковского счета их владельца или электронных денежных средств, в результате которого владельцу этих денежных средств причинен ущерб.

Субъективная сторона мошенничества характеризуется прямым умыслом и корыстной целью, под которой понимается получение материальной выгоды для виновного или других лиц.

Рассматриваемые виды мошенничества следует отграничивать от мелкого хищения (ст. 158.1 УК РФ), кражи (п. «г» ч. 3 ст. 158 УК РФ) и мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ).

1. Отграничение от мелкого хищения следует проводить по размеру похищенных денежных средств и субъекту:

стоимость похищенного имущества должна составлять не более двух тысяч пятисот рублей;

виновный является лицом, подвергнутым административному наказанию за мелкое хищение чужого имущества стоимостью более одной тысячи рублей, но не более двух тысяч пятисот рублей.

При этом должны отсутствовать признаки преступлений, предусмотренных чч. 2–4 ст. 159 УК РФ.

Такого рода преступные деяния, как правило, совершаются следующим образом.

Х., являясь лицом, подвергнутым административному наказанию за мелкое хищение, предусмотренное ч. 2 ст. 7.27 Кодекса Российской Федерации об административных правонарушениях (далее – КоАП РФ), совершил мелкое хищение чужого имущества. В соответствии с постановлением по делу об административном правонарушении, вступившим в законную силу, Х. признан виновным в совершении административного правонарушения, предусмотренного ч. 2 ст. 7.27 КоАП РФ, за совершение мелкого хищения чужого имущества стоимостью более одной тысячи рублей, но не более двух тысяч пятисот рублей, путем кражи при отсутствии признаков преступлений, предусмотренных чч. 2, 3 и 4 ст. 158, 158.1 УК РФ.

Х., находясь в торговом зале магазина «Евроспар», убедившись в том, что за его действиями никто не наблюдает, подошел к стеллажу с выставленным на реализацию товаром и похитил с него товар стоимостью 144 руб. 95 коп., который спрятал во внутренний карман своей одежды. После чего, не имея намерения и возможности

рассчитаться за товар, прошел с похищенным имуществом мимо кассовых терминалов, скрылся с места преступления и в последующем распорядился похищенным по своему усмотрению. Своими противоправными действиями Х. причинил магазину материальный ущерб на сумму 144 руб. 95 коп.[14]

Х. был осужден по ст. 158.1 УК РФ.

Возможны случаи совершения мелкого хищения в форме мошенничества лицом, подвергнутым административному наказанию за мелкое хищение, предусмотренное ч. 2 ст. 7.27 КоАП РФ, если причиненный ущерб составляет не менее двух тысяч пятисот рублей и не более пяти тысяч рублей.

2. Уголовная ответственность за кражу с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159.3 УК РФ), установлена в п. «г» ч. 3 ст. 158 УК РФ. При совершении данного деяния лицо похищает безналичные денежные средства, воспользовавшись необходимой для получения доступа к ним конфиденциальной информацией держателя платежной карты (например, персональными данными владельца, данными платежной карты, контрольной информацией, паролями), переданной лицу самим держателем платежной карты под воздействием обмана или злоупотребления доверием.

Под действие данного пункта подпадают случаи:

безналичных расчетов или снятия наличных денежных средств через банкоматы с использованием чужой или поддельной платежной карты;

использования необходимой для получения доступа к чужим денежным средствам, размещенным на банковском счете, или электронным денежным средствам конфиденциальной информации их владельца (например, персональные данные владельца, данные платежной карты, контрольную информацию, пароли).

Так, например, П. совершил кражу с банковского счета (при отсутствии признаков преступления, предусмотренного ст. 159.3 УК РФ) при следующих обстоятельствах. П. нашел на улице банковскую карту ПАО «Сбербанк России», оформленную на незнакомого гражданина Б., и решил совершить хищение с банковского счета указанной банковской карты денежных средств путем проведения бесконтактной оплаты товаров в различных

[14] См.: Приговор Ленинского районного суда города Иваново от 11 окт. 2021 г. № 1-320/2021 // СПС КонсультантПлюс.

магазинах. В магазине «Лион Хлеб и Вино» через терминал, предназначенный для проведения операций по банковским картам без ввода пин-кода, П. произвел 4 операции по безналичному расчету за приобретенные товары на общую сумму 334 руб. 60 коп., тем самым тайно похитил указанные денежные средства Б. Аналогичным образом П. похитил принадлежащие Б. денежные средства путем приобретения товаров еще в двух магазинах. Таким образом, П. совершил преступление, предусмотренное п. «г» ч. 3 ст. 158 УК РФ[15].

Корыстная цель, которая свойственна всем формам хищения, зачастую приводит к тому, что лица совершают как кражу, так и мошенничество.

М. похитила смартфон марки «Samsung Galaxy J2 Core», принадлежащий О., под чехлом которого находилась банковская карта ПАО «Сбербанк России», открытая на имя О.

М. попыталась осуществить вход в приложение «Сбербанк Онлайн», установленное на данном смартфоне, однако возникла необходимость ввода пароля для осуществления входа. Для этого М. ввела данные банковской карты ПАО «Сбербанк», открытой на имя О., при подтверждении входа осуществила ввод пароля из СМС-сообщения от абонента 900. Таким образом М. стал доступен личный кабинет О. и открытые на имя последней банковские счета.

Далее М. посредством мобильного приложения «Сбербанк Онлайн» осуществила перевод в сумме 8 тыс. руб. на банковский счет банковской карты, открытой в ПАО «Сбербанк России» на имя Д., не осведомленного о преступных действиях М. Впоследствии Д. перевел на ее банковскую карту эти денежные средства, которыми она воспользовалась по своему усмотрению.

Она же, осознавая противоправность своих действий, используя тот же смартфон, посредством мобильного приложения «Сбербанк Онлайн», установленного в нем, воспользовавшись имеющимися там персональными данными О., от ее имени заполнила анкету-заявку на получение кредита в сумме 7 600 руб., указав способ получения денежных средств посредством перевода на банковский счет банковской карты МИР. После поступления на абонентский номер СМС-сообщения с кодом подтверждения М. ввела его в приложении «Сбербанк Онлайн», где в автоматическом режиме заключила договор потребительского кредита на сумму 7 582 руб. 82 коп. Эти денежные средства были зачислены на банковскую карту, которыми

[15] См.: Приговор Егорьевского городского суда Московской области от 20 апр. 2022 г. № 1-197/2022 // СПС КонсультантПлюс.

М. распорядилась по своему усмотрению.

М. была признана виновной в совершении преступлений, предусмотренных п. «г» ч. 3 ст. 158 УК РФ и ст. 159.3 УК РФ[16].

3. Для вменения лицу ст. 159.6 УК РФ (Мошенничество в сфере компьютерной информации) необходимо, чтобы оно совершило хищение чужого имущества теми способами, которые описаны в основном составе (например, путем ввода, удаления компьютерной информации и др.).

Вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей признается целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), смартфоны, снабженные соответствующим программным обеспечением, или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него.

При мошенничестве, ответственность за которое установлена в ст. 159 УК РФ и 159.3 УК РФ, лицо незаконно не воздействует на программное обеспечение серверов, компьютеров, информационно-телекоммуникационные сети. Верховный Суд Российской Федерации разъяснил, что в случае, если хищение чужого имущества или приобретение права на чужое имущество осуществляется путем распространения заведомо ложных сведений в информационно-телекоммуникационных сетях, включая сеть Интернет (например, создание поддельных сайтов благотворительных организаций, интернет-магазинов, использование электронной почты), то такое мошенничество следует квалифицировать по ст. 159, а не 159.6 УК РФ[17].

Так, например, К.И., Г.А., Б. совершили мошенничество в сфере компьютерной информации, совершенное группой лиц по предварительному сговору, с причинением значительного ущерба гражданину, при следующих обстоятельствах.

К.И. осуществил выход в сеть Интернет, где посредством информационно-телекоммуникационных сетей вступил с неустановленным лицом N. в преступный сговор на совершение

[16] См.: Приговор Ишимбайского городского суда Республики Башкортостан от 31 окт. 2023 г. по делу № 1-291/2023 // СПС КонсультантПлюс.

[17] См.: О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верховного Суда Рос. Федерации от 30 нояб. 2017 г. № 48 : ред. от 15 дек. 2022 г. // Бюллетень Верховного Суда Рос. Федерации. 2018. № 2.

мошенничества в сфере компьютерной информации путем несанкционированного блокирования поступления, чтения и отправки СМС-сообщений от ПАО «Сбербанк России» в память мобильных устройств с операционной системой на базе «Android», то есть путем вмешательства в функционирование средств хранения, обработки и передачи информации в информационно-телекоммуникационных сетях.

К.И. и N. распределили между собой роли при совершении преступления, согласно которым: N. посредством использования информационно-телекоммуникационных сетей должен был приискать путем мониторинга сайта бесплатных объявлений «www.avito.ru» владельца банковского счета банковской карты ПАО «Сбербанк России», направить в заранее обговоренный день на абонентский номер его абонентского устройства с операционной системой на базе «Android» программное вирусное обеспечение, посредством которого похитить со счета банковской карты денежные средств. К.И. на стадии приготовления к совершению преступления должен приискать двух соучастников преступления, роль которых заключалась в поиске банковских карт для использования при хищении денежных средств с банковских счетов граждан, без посвящения в совместный преступный умысел их владельцев, после чего передать сведения о номерах банковских карт N. для ввода программного вирусного обеспечения. При этом К.И. и N. договорились о порядке распоряжения похищенным имуществом: половину похищенного имущества К.И. должен переводить посредством электронного перевода на счет N., половину похищенного К.И. должен был разделить по своему усмотрению с другими привлеченными им для целей хищения соучастниками преступления.

К.И. для реализации умысла, направленного на хищение чужого имущества, предложил Б. за денежное вознаграждение подыскивать на сайте бесплатных объявлений «www.avito.ru» лиц, которые в своих объявлениях указывали абонентский номер своего телефона, подключенного к услуге дистанционного банковского обслуживания «Мобильный банк». На данное предложение Б. ответила согласием, после чего она предложила Г.А. вступить в преступную группу для совершения мошеннических действий в сфере компьютерной информации, на что Г.А. ответил согласием.

Г.А. за денежное вознаграждение предложил ранее знакомому З. сообщить ему номер своей банковской карты, на которую должны

были поступать денежные средства от обманутых граждан, полагавших, что они оплачивают покупку необходимого им товара. При этом З. не был посвящен в совместный преступный сговор К.И., Г.А., Б. и N. на совершение мошенничества в сфере компьютерной информации. Сведения о банковской карте, открытой на имя З., были переданы N. для использования данной карты в качестве средства хищения и обращения в свою пользу похищенных денежных средств.

Впоследствии N. посредством использования информационно-телекоммуникационных технологий осуществил мониторинг сайта бесплатных объявлений «www.avito.ru», где У. разместил объявление с указанием абонентского номера своего телефона, подключенного к услуге дистанционного банковского обслуживания «Мобильный банк» его банковской карты. Далее N. посредством информационно-телекоммуникационных технологий направил на абонентский номер телефона У. сообщение в виде ссылки, при переходе по которой в мобильный телефон умышленно производился ввод вредоносного программного обеспечения, предназначенного для несанкционированного блокирования поступления, чтения и отправки СМС-сообщений от ПАО «Сбербанк России».

Получив посредством информационно-телекоммуникационных сетей сообщение со ссылкой на программное вирусное обеспечение, У., не подозревая о преступных намерениях К.И., Б., Г.А. и N., осуществил переход по полученной ссылке, из-за чего произошла модификация стандартного программного обеспечения мобильного телефона У. В результате К.И., Б., Г.А. и N. получили доступ на правах администратора к мобильному устройству У. и осуществили несанкционированный перевод денежных средств в сумме 7 380 руб. со счета банковской карты У. на банковскую карту З. Впоследствии Г.А. и З. обналичили эти денежные средства через банкомат. За использование его банковской карты З., не посвященный в преступный сговор, получил вознаграждение в сумме 500 руб., которые Г.А. оставил себе. В дальнейшем К.И., Б., Г.А. перевели на электронный счет N. 4 тыс. руб., а остальные 2 380 руб. оставили себе и распорядились ими по своему усмотрению, причинив У. значительный ущерб на сумму 7 380 руб.[18]

Вышеуказанные лица были осуждены по ч. 2 ст. 159.6 УК РФ.

По другому приговору Д. с третьими лицами установили на компьютере сотрудника ООО «№ 1» программы класса «Backdoor», которые относятся к вредоносным программам удаленного

[18] См.: Приговор Красноармейского городского суда Саратовской области от 1 февр. 2019 г. по делу № 1-10/2019 // СПС КонсультантПлюс.

администрирования, позволяющие управлять компьютером-жертвой дистанционно, посылая команды через канал IRC (класс «TrojWare» – вредоносная программа, занимающаяся уничтожением, блокированием, модификацией или копированием информации, нарушением работы компьютеров или компьютерных сетей, и при этом не попавшая ни в один из классов троянских программ). Это позволило им получить доступ к забронированным и оплаченным проездным документам на железнодорожный транспорт и произвести оформление железнодорожных проездных документов на имя Д. Затем Д. оформил возврат билетов и получил за них денежные средства.

Суд действия Д. обоснованно квалифицировал по п. «в» ч. 3 ст. 159.6 УК РФ, так как данное преступление совершено путем иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации. Хищение денежных средств стало возможным в результате целенаправленного воздействия на компьютер сотрудника ООО «№ 1» вредоносных программ удаленного администрирования. Он был осужден по п. «в» ч. 3 ст. 159.6 УК РФ[19].

[19] См.: Апелляционное определение Пермского краевого суда от 20 мая 2021 г. по делу № 22-2970/2021 // СПС КонсультантПлюс.

2. ПРИЕМЫ, ПРИМЕНЯЕМЫЕ ПРИ СОВЕРШЕНИИ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ IT-ТЕХНОЛОГИЙ

Как отмечалось выше, мошенничество в настоящее время часто совершается с помощью социальной инженерии. Одной из схем социальной инженерии является фишинг.

Фишинг – это тип киберпреступления, при котором преступники выдают себя за надежный источник в Интернете, чтобы вынудить жертву передать им личную информацию (например, имя пользователя, паспортные данные, номер банковской карты и пр.).

Фишинговая атака может принимать различные формы, и хотя она часто происходит по электронной почте, существует множество различных способов, которые мошенники используют для выполнения своих схем.

С целью получения доступа к банковским картам, страницам социальных сетей и сайту «Госуслуги», которые привязаны к абонентскому номеру, потерпевшему поступают звонки на мобильный телефон, в том числе через мессенджеры «WhatsApp», «Viber», «Telegram», а также путем рассылки СМС-сообщений или писем по электронной почте.

Виновные лица могут представляться сотрудниками службы безопасности банка или операторов сотовой связи Билайн, Теле2, МТС, Мегафон (техподдержки мессенджера); руководителями организаций, где работают потерпевшие; сотрудниками правоохранительных органов либо иных государственных структур (например, налоговых органов); родственниками и пр.[20]

При этом они в одних случаях создают для потерпевшего обстановку тревожности, убеждая его в необходимости срочного проведения определенных операций, сообщая, например, получателю, что его личный счет был взломан и с него в данный момент пытаются похитить денежные средства. Цель таких манипуляций состоит в том, чтобы в созданной ситуации риска утраты потерпевшим своего

[20] См.: В киберполиции сообщили о вновь появившихся видах дистанционного мошенничества. URL: https://rg.ru/2024/03/18/nash-razgovor-budet-opasen.html (дата обращения: 02.05.2024); О новых способах мошенничества с использованием информационных технологий. URL: https://elizsp.ru/novosti/o-novykh-sposobakh-moshennichestva-s-ispolzovaniem-informatsionnykh-tekhnologij (дата обращения: 03.05.2024).

имущества он под воздействием обмана перешел по вредоносной ссылке.

В других случаях недостоверные сообщения содержат предложения о получении различного рода привилегий (например, высокооплачиваемой работы, выигрыша в лотерее, удачного вложения денег и др.).

Так, например, виновные лица могут сообщать о необходимости:

произвести замену номера телефона, прикрепленного к лицевому счету, чтобы предотвратить мошеннические действия, либо обновить приложение оператора связи или улучшить тарифный план. Для осуществления этих изменений предлагается установить на мобильный телефон приложения «RustDesk» и «Zoom». С помощью данных приложений лица получают возможность дистанционно управлять мобильным телефоном потерпевшего и открывать приложения «Онлайн банка». При вводе пароля в приложении «Онлайн банка» у потерпевшего производится списание всех денежных средств;

отменить заявку на удаление аккаунта в мессенджере. Для ее отмены рекомендуется перейти на сайт с дизайном, похожим на интерфейс мессенджера, ввести номер телефона и код безопасности. Таким образом лица получают доступ к аккаунту, перепискам и управлению каналами, администрируемыми потерпевшим;

продлить срок действия сим-карты абонента, для чего потерпевшему необходимо сообщить лицу код из сообщения. После этого подключается переадресация звонков и СМС-сообщений на другой номер, и виновные получают доступ к «Онлайн банку», социальным сетям и мессенджерам потерпевшего для входа по номеру телефона;

продлить срок действия договора по оказанию услуг сотовой связи. В противном случае номер будет передан другому абоненту. При этом предлагается это сделать по телефону, продиктовав код из СМС-сообщения. В дальнейшем для потерпевшего могут наступить следующие последствия. В одних случаях после передачи кода из СМС-сообщения, лицо получает доступ в личный кабинет сотового оператора и заказывает перевыпуск сим-карты потерпевшего с материального носителя на виртуальный (E-SIM). В результате лицо получает доступ ко всем банковским картам, страницам социальных сетей, привязанным к абонентскому номеру. В других – потерпевшему необходимо будет перейти по присланной ссылке, где нужно ввести еще один код. В итоге он не продлевает договор, который на самом деле является бессрочным, а предоставляет данные для входа в личный кабинет на портале «Госуслуги» и всю информацию о себе, которая там хранится;

обновить приложения банков, чтобы счета потерпевшего не были заблокированы. Ему предлагается скачать приложение, которое на самом деле устанавливает на телефон программу для его удаленного администрирования;

сохранить денежные средства, которые якобы пытаются похитить. Во избежание этого в качестве временной меры ему следует перевести средства на «безопасный» счет в ЦБ РФ, с которого впоследствии эти деньги обещают возвратить владельцу;

установить приложение для поиска вирусов, которое в реальности представляет собой вредоносное программное обеспечение, открывающее доступ к телефону потерпевшего и содержащимся в нем данным и пр.

Вместе с тем в сообщениях может содержаться:

предложение получить какую-либо госвыплату, компенсацию или субсидию от имени Госуслуг. Для ее получения необходимо перейти по ссылке на сайт, копирующий дизайн Госуслуг, и там нажать на «активировать предложение», где потерпевшему придется вводить свои логин и пароль. В результате чего виновные лица получат доступ к реальному личному кабинету на портале Госуслуг;

требование оплатить штраф, например, за нарушение Правил дорожного движения (далее – ПДД). В этих случаях владелец автотранспортного средства получает от ГИБДД МВД России письмо, содержащее копию постановления о совершенном им административном правонарушении, связанном с нарушением ПДД, которое зафиксировано специальными техническими средствами фото- и видеоконтроля нарушений, работающими в автоматическом режиме. В письмо вложена квитанция на уплату штрафа, содержащая недостоверные реквизиты счета, принадлежащего не ГИБДД МВД России, а виновному лицу[21];

выгодные предложения о заработной плате. В одних случаях рассылается информация о привлекательных условиях труда (например, с высокой зарплатой, неполной занятостью и пр.). При этом у лица берутся все паспортные данные, а также данные карты, на которую обещают перечислять зарплату, либо просят внести аванс для того, чтобы эта должность была закреплена за потерпевшим. В других случаях предложения о лжевакансиях размещаются на популярных сайтах объявлений. Для замещения вакансии лицу требуется пройти собеседование с будущим работодателем по видеозвонку, в процессе

[21] См.: Моя экономическая безопасность. Как не стать жертвой аферистов. Квитанция на кражу. URL: 35.мвд.рф/press/consultation/профилактика-разных-видов-мошенничест/econbez (дата обращения: 11.05.2024).

которого кандидат заполняет анкету с указанием паспортных данных и данных банковских карт якобы для перечисления зарплаты. Впоследствии с банковских карт потерпевшего похищаются денежные средства;

предложения об участии в различных инвестиционных проектах с обещанием получить большую прибыль. Потерпевшему предлагается зарегистрировать аккаунт на электронной торговой площадке (бирже), которая якобы имеет официальный статус. Представившиеся сотрудниками инвестиционных компаний лица обещают ему консультативную помощь при проведении торгов, чтобы совершаемые им сделки гарантировано приносили прибыль. На первоначальном этапе лицу позволяют заработать незначительную сумму денег и вывести ее на свой банковский счет. Затем убеждают его с целью получения еще более высоких доходов перевести на подконтрольные виновным счета крупные суммы денег. Под видом выгодных сделок потерпевший совершает заведомо убыточные операции и теряет все накопления с лицевого счета;

поддельные сообщения на электронную почту, как правило, от известных компаний, в которых содержится поздравление с победой в каком-либо конкурсе, проводимом компанией. При этом для получения приза необходимо перейти по ссылке, данной в письме;

предложение приобрести билеты на различные культурно-зрелищные мероприятия. Потерпевшему по мессенджеру поступает ссылка на поддельный сайт, при переходе по которой открывается окно оплаты, внешне схожее с официальным сайтом билетных касс. После внесения потерпевшим реквизитов банковской карты его денежные средства списываются;

предложение оплатить услугу или товар по поддельному QR-коду, который приводит не на официальный сайт сервиса, а на поддельный ресурс.

Кроме того, существует еще несколько схем мошенничества:

1. Так, с целью получения доступа к мессенджеру потерпевшего виновные лица просят продиктовать код, необходимый для доступа к его аккаунту, либо включить демонстрацию экрана или программу удаленного доступа, что позволяет им получить код самостоятельно. Контроль над аккаунтом потерпевшего третьи лица могут получить при его подключении к бесплатной открытой сети Wi-Fi, если, получив сообщение о необходимости регистрации через аккаунт в «Telegram», потерпевший отправляет им код доступа. В результате виновные получают полный контроль над аккаунтом, а владелец

утрачивает доступ к нему.

2. В магазине приложений «App Store» лица создают поддельные сайты банков, например, схожие по названию с существующими банками. При этом внешний вид сайта оформлен как реальный сайт банка. Например, ПАО «Сбербанк России», ВТБ и др.

3. Нередко уже известные схемы усовершенствуются и наполняются новым содержанием. В качестве примера можно привести схему, которую условно можно назвать «Родственник попал в беду». Если ранее виновные лица пытались имитировать голос родственника потерпевшего, то в настоящее время они научились синтезировать чужой голос с помощью нейросети, используя для этого реальные образцы его звучания. Для получения таких образцов потерпевшему предварительно могут позвонить и предложить поучаствовать в конкурсе или опросе либо использовать видеоролики потерпевшего из соцсетей.

4. Получение третьими лицами доступа к электронной цифровой подписи потерпевшего, в результате чего они могут без ведома владельца от его имени заключать договоры купли-продажи, дарения, в том числе на жилые помещения.

5. Новым способом, порожденным сложившейся геополитической обстановкой, является следующий. Третьи лица звонят потерпевшему, представляются сотрудниками правоохранительных органов и сообщают, что сотрудник банка, клиентом которого является потерпевший, похитил его персональные данные и осуществляет с его счета переводы в пользу ВСУ. При этом говорят, что он также несет ответственность как соучастник в государственной измене.

3. МОШЕННИЧЕСТВО, СВЯЗАННОЕ С РЕАЛИЗАЦИЕЙ ТОВАРОВ И ОКАЗАНИЕМ УСЛУГ В СЕТИ ИНТЕРНЕТ

Виновные применяют нередко несколько схем одновременно. В качестве иллюстрации можно привести мошенничества, связанные с реализацией товаров и оказанием услуг в сети Интернет[22].

Под реализацией товаров или оказанием услуг в сети Интернет признается передача на возмездной основе (в том числе обмен товарами или услугами) права собственности на товары, возмездное оказание услуг одним лицом другому лицу. Однако при совершении мошенничества гражданско-правовые обязательства не исполняются, товары не поставляются, услуги не оказываются.

Под имуществом при мошенничестве, связанном с реализацией товаров в сети Интернет, понимаются вещи материального мира, имеющие стоимость, которые являются **товаром** по договору купли-продажи. В соответствии с п. 1 ст. 454 Гражданского кодекса Российской Федерации (далее – ГК РФ)[23] товаром по договору купли-продажи могут быть любые вещи, за исключением тех, которые ограничены или запрещены в обороте (например, оружие, наркотические средства).

Так, например, Б. совершил мошенничество с причинением значительного ущерба гражданину. Он из корыстных побуждений предлагал через сеть Интернет незнакомым лицам бытовую и электронную технику, а также иные товары. Оплата товаров должна была производиться путем перечисления денежных средств на банковскую карту, указанную Б.

Для этого Б. в социальной сети «ВКонтакте» в группе «Вам все – по карману» разместил объявление о продаже двух мобильных телефонов марки «iPhone 11», которое заинтересовало Н.

---

[22] В данном разделе использованы материалы см.: Рязанцев В.А., Улейчик В.В., Майорова Е.И., Яковлева Л.В. Расследование мошенничеств, связанных с реализацией товаров и оказанием услуг в сети Интернет : методические рекомендации. М.: ВНИИ МВД России, 2022. URL: https://49.xn--b1aew.xn--p1ai/citizen/Razjasnenija_MVD_Rossii/методические-рекомендации-расследование.

[23] См.: Гражданский кодекс Российской Федерации (часть вторая) : утв. Федер. законом от 26 янв. 1996 г. № 14-ФЗ : ред. от 24 июля 2023 г. // Собр. законодательства Рос. Федерации. 1996. № 5, ст. 410.

В ходе переписки была обсуждена цена. Б. обещал доставить мобильные телефоны покупателю. Н., не зная о преступных намерениях Б., посчитала, что данные условия сделки для нее выгодны, так как стоимость продукции ее устраивала и сроки поставки продукции непродолжительны. Тем самым, будучи введенной в заблуждение, Н. перевела денежные средства на оформленную на Б. банковскую карту, номер которой он ей продиктовал.

Отправленные Н. денежные средства Б. получил, после чего обналичил их и распорядился ими, не отправив обещанные мобильные телефоны.

Б. был осужден по ч. 2 ст. 159 УК РФ.[24]

Под **услугой** понимается определенное действие или деятельность, которые исполнитель осуществляет по заданию заказчика на основании договора. Согласно п. 1 ст. 779 ГК РФ по договору возмездного оказания услуг исполнитель обязуется оказать услуги (совершить определенные действия или осуществить определенную деятельность), а заказчик обязуется оплатить эти услуги. Услуги могут оказываться в различных сферах жизнедеятельности.

Так, например, Х., не имея постоянного источника дохода, в ходе просмотра размещенной в сети Интернет информации обратил внимание на интернет-сайт «Ati.su», через который осуществляются грузоперевозки по территории Российской Федерации. У него возник умысел, направленный на хищение чужого имущества путем обмана в крупном размере. Для этого он зарегистрировался на вышеуказанном сайте под вымышленным именем.

Х. для того, чтобы его преступные действия не были обнаружены, используя сеть Интернет, заказал и приобрел для совершения вышеуказанного преступления водительское удостоверение и паспорт со своими фотографиями на чужое имя, а также два государственных регистрационных знака. После этого он зарегистрировался на интернет-сайте «Ati.su» под вымышленным именем и проследовал на строительный рынок, где арендовал по устной договоренности за 60 тыс. руб. в месяц у С. автомобиль «ГАЗ-3302». Впоследствии Х. обнаружил на сайте заявку Г. о перевозке товара со склада ООО. После этого он позвонил Г. и, введя последнего в заблуждение относительно своих намерений, заключил с ним в

[24] См.: Приговор Савеловского районного суда города Москвы от 9 нояб. 2023 г. № 1-177/2023 // СПС КонсультантПлюс.

устной форме договор на перевозку принадлежащего Г. товара.

Не имея намерения на осуществление грузоперевозки, Х. отправил Г. фотографии ранее приобретенных им поддельных документов. Будучи введенным в заблуждение, Г. оплатил по безналичному расчету сумму в размере 421 800 руб. за приобретенный им товар, который должен был перевезти Х. Тот на арендованном автомобиле «ГАЗ-3302» приехал к складу ООО, осуществил погрузку товара на общую сумму 421 800 руб., после чего с похищенным грузом скрылся, распорядившись им впоследствии по своему усмотрению[25].

При совершении мошенничеств, связанных с оказанием услуг, следует иметь в виду, что услуги могут и не регулироваться нормами гражданского права, а относиться к нетрадиционным способам воздействия на человека – заговоры, гадание и пр.

Так, например, В., осознавая общественную опасность своих действий, с помощью мобильного телефона, имеющего соединение с сетью Интернет, в сервисе для создания и просмотра видео «TikTok» на личной странице пользователя под ником «@gadalka_zarina», открытой для публичного доступа, разместила заведомо ложное объявление об оказании услуг экстрасенсорного характера. При этом В. не имела соответствующих навыков, умений и способностей для оказания данных услуг. Для связи она указала номер мобильного телефона, подключенный к мессенджеру «WhatsApp».

В. ответила на пришедшее в мессенджер сообщение от З., заинтересованной в получении услуг экстрасенсорного характера, представилась ей лицом, владеющим такими навыками и оказывающим помощь в решении семейных проблем. Желая завладеть путем обмана принадлежащими З. денежными средствами, выяснив, что последняя является держателем банковской карты ПАО «Сбербанк России» с подключенной услугой «Мобильный банк», убедила последнюю посредством безналичного расчета перевести на банковскую карту ПАО «Сбербанк России» на чужое имя, но находящуюся в пользовании В., денежные средства на общую сумму 100 900 руб.

З., будучи уверенной, что В. действительно обладает экстрасенсорными способностями и помогает ей в решении семейных проблем, посредством безналичного расчета с банковской карты ПАО «Сбербанк России», подключенной к ее абонентскому номеру, посредством услуги «Мобильный банк», перевела несколько

[25] См.: Приговор Волоколамского городского суда Московской области от 17 марта 2022 г. по делу № 1-81/2022 // СПС КонсультантПлюс.

раз на счет банковской карты ПАО «Сбербанк России», находящейся в пользовании В., денежные средства на общую сумму 100 900 руб.

Тем самым, В. совершила хищение денежных средств путем обмана, причинив З. ущерб, который с учетом материального и социального положения последней, является для нее значительным. Действия В. квалифицированы по ч. 2 ст. 159 УК РФ[26]*.*

Несмотря на то, что денежные средства потерпевшая З. переводила неоднократно, действия В. охватывались единым умыслом на хищение всей суммы, находящейся на счете З., о чем В. было известно, и поэтому были квалифицированы как единое преступление.

Возможны следующие разновидности совершения такого рода деяний:

1. Отсутствие у виновного лица обещанных для реализации товаров или возможности для оказания соответствующих услуг.

Например, Г. в социальной сети «ВКонтакте» создавал страницы («Т», «О») и сообщества, где, выступая в качестве посредника, размещал рекламу, фотографии товаров со страниц поставщиков оптового рынка «Садовод», условия поставки товаров, одним из которых была полная предварительная оплата заказов и стоимости его услуг. Он решил похищать перечисленные ему денежные средства за предоплаченные товары.

Никаких товаров у Г. не имелось. Он выбирал заказчиков из других регионов, с которыми общался посредством сети «ВКонтакте», чтобы иметь возможность блокировать страницы. Принимая заказы на страницу «Т», а также переводы денежных средств за них, часть денег из разных заказов забирал и расходовал на собственные нужды, а, получив требования от покупателей о возврате денег, блокировал данную страницу и создал новую страницу «О». Впоследствии по той же причине он не отвечал на сообщения и звонки, продолжал блокировать страницы и с целью хищения денежных средств создавать новые, на которые продолжал принимать заказы, получал денежные средства на счета банковских карт, открытых на его имя, имена его жены и матери, и продолжал их похищать. Также за указанный период им были созданы страницы и сообщества в сети «ВКонтакте», для создания которых он приобрел шесть сим-карт. Похищенные деньги покупателей переводил со счетов, открытых на его имя и имя его матери, на свой счет, с которого снимал их в банкоматах. За указанный период Г.

[26] См.: Приговор Ленинского районного суда Тульской области от 28 дек. 2021 г. № 1-228/2021 // СПС КонсультантПлюс.

похитил денежные средства, не исполнив обязательств по доставке заказанных ими товаров[27].

Таким образом, действия Г. квалифицированы по ч. 3 ст. 159 УК РФ (мошенничество, совершенное в крупном размере).

2. Виновное лицо вместо обещанных товаров поставляет иные вещи.

Г., имея умысел, направленный на хищение чужого имущества – денежных средств, принадлежащих Ф., путем обмана, заведомо не намереваясь исполнять принимаемые на себя обязательства, используя с корыстной целью доверительные отношения с последним, в ходе общения посредством использования интернет-сайта, предназначенного для размещения объявлений, заключил с ним устный договор купли-продажи коллекционных игрушек, в соответствии с которым он должен был отправить в адрес Ф. указанный товар почтовым отправлением.

Ф. под воздействием обмана, используя систему дистанционного банковского обслуживания (мобильный банк), перечислил со своего счета на счет Г. принадлежащие ему безналичные денежные средства в размере 2 230 руб. в качестве оплаты за товар, который Г. в действительности поставлять не собирался. Далее вместо ранее указанного предмета сделки (коллекционные игрушки) Г. упаковал в полиэтиленовый почтовый конверт фрагмент подошвы обуви и отправил данный фальсифицированный товар в адрес Ф. При этом в ходе общения с использованием интернет-сайта сознательно сообщил последнему заведомо ложные, не соответствующие действительности сведения о том, что выполнил условия ранее указанного договора купли-продажи и направил в его адрес коллекционные игрушки, предоставив фотографию кассового чека об отправке.

В тот же день Г., продолжая реализацию своего единого преступного умысла путем обмана и заведомо не намереваясь исполнять принимаемые на себя обязательства, заключил с Ф. еще один устный договор купли-продажи коллекционных игрушек на сумму 4 600 руб. В качестве оплаты за товар, который Г. в действительности продавать не собирался, Ф. перечислил Г. указанную сумму, после чего Г. завладел денежными средствами в общей сумме 6 830 руб., обратил их в свою пользу[28].

---

[27] См.: Приговор Володарского районного суда города Брянска от 10 июня 2021 г. по делу № 1-66/2021 // СПС КонсультантПлюс.

[28] См.: Приговор Егорьевского городского суда Московской области от 11 марта 2022 г. по делу № 1-87/2022 // СПС КонсультантПлюс.

В приведенном приговоре Г. с целью получения от потерпевшего большей суммы денег пытался придать правомерный вид сделке купли-продажи и направил фото кассового чека об отправке заказанного потерпевшим товара по первому договору. В результате введенный в заблуждение потерпевший перечислил Г. еще одну денежную сумму по второму договору.

3. У виновного лица имеются товары, качество которых не соответствует обещанному.

4. У виновного имеется заявленный товар, однако он поставляет его не в полном объеме.

Для совершения мошенничеств, связанных с реализацией товаров или оказанием услуг в сети Интернет, лица используют следующие схемы:

создают страницы в социальных сетях, на которых рекламируют товары, которые не собираются реализовывать, или предлагают услуги, которые не планируют оказывать;

создают аналогичные сайты, которые минимально отличаются от соответствующих официальных сайтов различных известных фирм, но указывают на них данные своих банковских расчетных счетов либо создают полностью фальшивые сайты (например, туроператоров или авиакомпаний);

создают подменную страницу для оплаты товаров и предлагают оплатить покупку через Интернет, утверждая, что на сайте не работают кнопки оформления заказа и присылают ссылку для оплаты товаров. Так, например, если лицо приобретает или продает какой-то товар на сайте «Авито», то и ссылка должна быть только на этот сайт – www.avito.ru. В случае, если адрес схожий, но иной (например, avito-dostavka.ru или avitto.ru), то это подменный сайт;

для совершения сделки просят продиктовать CVV/CVC-код банковской карты или код из СМС-сообщения от банка от имени службы безопасности банка для подтверждения подлинности карты, с которой предполагается оплатить товар;

настаивают на том, чтобы вести общение не во встроенном мессенджере на сайте объявлений, а, например, в WhatsApp, Telegram или по телефону;

взламывают и перехватывают письма по электронной почте, высылая покупателю поддельное письмо с приложенным счетом с указанием реквизитов фирмы-мошенника в случаях, если компания не имеет собственного почтового сервера, а пользуется бесплатными сервисами.

Лица, реализующие товары и оказывающие услуги в сети

Интернет, как правило, действуют следующим образом:

устанавливают цены существенно ниже рыночных;

требуют предоплату с использованием анонимных платежных систем, электронных денег или при помощи банковского перевода на карту, выданную на имя частного лица;

не предлагают курьерскую доставку и самовывоз товара;

не размещают контактную информацию и сведения о продавце. Контактная информация представлена лишь формой обратной связи и номером мобильного телефона. Отсутствует адрес продавца либо указан несуществующий адрес;

интернет-магазин или учетная запись продавца зарегистрированы всего несколько дней назад, отсутствуют отзывы об этом магазине или продавце;

при совершении покупки продавец торопит с оплатой, убеждая в том, что если не заказать товар сейчас, то цена изменится или товар будет снят с продажи;

продавец высылает отсканированное изображение паспорта для подтверждения своей личности. Это не может свидетельствовать о подлинности личности продавца, поскольку не представляет сложности изготовить фальшивое отсканированное изображение.

Мошенничества имеют сходство с нарушениями гражданско-правовых договоров, таких как договоры купли-продажи, договоры поставки, договоры возмездного оказания услуг, и совершаются под прикрытием правомерной гражданско-правовой сделки.

Публичное предложение продавца любому лицу заключить на его условиях договор купли-продажи товара, в том числе в сети Интернет, является офертой. Оферта вступает в силу с момента ее размещения на интернет-сайте и действует до ее отзыва.

Реклама и иные предложения, адресованные неопределенному кругу лиц, рассматриваются как приглашение делать оферты, если иное прямо не указано в предложении (п. 1 ст. 437 ГК РФ).

Договором признается соглашение двух или нескольких лиц об установлении, изменении или прекращении гражданских прав и обязанностей (ст. 420 ГК РФ). При реализации товаров и оказании услуг в сети Интернет у сторон из договоров возникают обязательства, в силу которых одно лицо обязано совершить в пользу другого лица определенное действие, например, передать имущество, выполнить работу, оказать услугу, уплатить деньги и т.п.

Главным отличительным признаком мошенничеств от нарушений гражданско-правовых договоров является установление

прямого умысла на хищение чужого имущества, а также отсутствие у лица цели исполнить свои обязательства. Следует установить, что лицо заведомо не собиралось отвечать по своим обязательствам. Прежде всего это обстоятельство может подтверждаться отсутствием у лица реальной возможности исполнить обязательства (например, отсутствие у лица предлагаемых товаров), неподтвержденными надуманными причинами о невозможности их исполнения (ссылки на технический сбой при оплате товаров) либо создание видимости исполнения взятых обязательств (отсылка сканов кассовых чеков об оплате услуг по доставке товаров).

Поскольку главным отличительным признаком мошенничества и гражданско-правового договора является наличие либо отсутствие цели завладения чужим имуществом, следует особенно тщательно ее устанавливать, проверяя всю совокупность данных по каждому конкретному случаю. Нельзя ориентироваться только на такой признак, как безвозмездность изъятия имущества ввиду того, что мошенники нередко частично возмещают ущерб потерпевшему (например, передают товар меньшей стоимости или худшего качества, чем было определено договором поставки и пр.).

Для квалификации деяния как мошенничества необходимо устанавливать момент возникновения умысла на завладение чужим имуществом. При мошенничестве лицо преднамеренно (до момента вступления в гражданские правоотношения) не собирается исполнять взятые на себя обязательства. В случае, если лицо добросовестно исполняло взятые на себя обязательства, но в силу сложившихся уже после заключения сделки обстоятельств, препятствующих их исполнению, перестало их исполнять, действия лица не образуют состава мошенничества и должны оцениваться как гражданско-правовые отношения.

4. МОШЕННИЧЕСТВО, СОВЕРШАЕМОЕ ПУТЕМ ПОДМЕНЫ АБОНЕНТСКОГО НОМЕРА

В последние годы значительно увеличилось количество преступлений, совершаемых с использованием IT-технологий с применением различных вышерассмотренных схем.

Способы совершения рассматриваемых преступлений в целом схожи, отличия могут заключаться в последовательности совершения определенных действий.

Центральным местом в способе хищений, совершенных с использованием информационно-телекоммуникационных технологий путем подмены абонентского номера, является использование возможностей SIP-телефонии, представляющей собой технологию передачи голоса через сеть передачи данных, когда взаимодействие между устройством и сервером осуществляется по протоколу SIP, позволяющему организовать телефонию (телефонные соединения) с использованием доступного подключения к сети Интернет или к компьютерной сети.

Подсудимый Ф. в ходе судебного заседания, а также в ходе предварительного следствия вину в совершении преступления признал полностью и показал, что он через приложение «App Store», скачал приложения «WPN PROKSI MASTER» и «Team Viewer Quick Support» в свой мобильный телефон с абонентским номером – № оператора «Теле 2», который зарегистрирован на его имя. Это приложение было платным, так как там находилась информация по банковским картам различных клиентов банков, а именно: ФИО, последние 4 цифры банковской карты, абонентские номера телефонов. Это так называемый Dark Net. Приложение «Team Viewer Quick Support» давало доступ к телефону пользователя с его разрешения. При помощи приложения он засекретил свой абонентский номер телефона, выбрав регион «Москва и Московская область», цифры в номере также заменил сам на произвольные, после чего при осуществлении звонков с его абонентского номера у собеседника высвечивался не его достоверный номер[29].

Использование технологии по подмене телефонного номера для

[29] См.: Приговор Советского рационного суда города Липецка от 28 марта 2022 г. № 1-96/2022 // СПС КонсультантПлюс.

достижения преступных целей при звонках на устройства, оснащенные автоматическим определителем номера, помимо прочего, позволяет, с одной стороны, ввести в заблуждение, обезличить звонящего абонента, с другой – добиться соответствующего уровня доверия к звонящему, так как подменный номер телефона может быть знаком потерпевшему (этот номер есть в памяти устройства и принадлежит конкретному абоненту – родственнику, знакомому и пр.), либо информировать потерпевшего, что звонок ему поступает именно из той службы, учреждения, организации, работником которой представляется звонящий (номер 900 – ПАО «Сбербанк России», другие номера системы правоохранительных органов и пр.).

Кроме того, следует учитывать, что телефонные звонки с применением технологии подмены номера могут быть использованы не только для обмана граждан, но и для звонков на горячие линии банковских организаций. В случаях, когда система антифрода[30] колл-центров банков пропускает такие звонки, появляется возможность получить конфиденциальную информацию о состоянии банковского счета, данных о последних операциях и других сведений. Полученные данные в дальнейшем могут быть использованы при общении с клиентом банка при совершении рассматриваемых преступлений.

В ходе совершения преступления виновные лица могут использовать программы модуляции голоса, для передачи конфиденциальных сведений применяют роботов (ботов). Специализированное программное обеспечение применяется не только для подмены телефонного номера звонящего, но и для отправки СМС-сообщений.

Соответствующие уровни доступа, полученные в ходе взлома программ, виновные лица используют для совершения рассматриваемых преступлений с использованием социальных сетей и мессенджеров.

Кроме того, при совершении дистанционных хищений денежных средств виновные лица используют персональные данные, полученные из различных баз данных – «утечек», распространяемых в сети Интернет (в том числе в его «теневой» части). В таких базах данных могут содержаться персональные данные и иная конфиденциальная информация, которые могут быть использованы для оказания психологического воздействия (психологического манипулирования), прежде всего направленного на принуждение к совершению

[30] Система верификации между операторами, в соответствии с которой происходит автоматический запрос от одного оператора другому о совершенном вызове, т.е. что в данный момент абонент Х, абонентский номер которого принадлежит одному оператору, набрал номер абонента другого оператора. Если это подтверждается, то звонок пропускается. Если нет, то блокируется.

определенных действий, формирование соответствующего образа восприятия (должностного лица сотрудника правоохранительного органа, сотрудника банка и пр.).

Операторы связи обязаны прекратить оказание услуг связи и услуг по пропуску трафика в свою сеть связи при поступлении звонков и СМС-сообщений, идущих из-за рубежа в Российскую Федерацию с подменных номеров.

Указанные новеллы получили свое дальнейшее развитие в положениях Федерального закона от 4 августа 2023 г. № 473-ФЗ «О внесении изменений в Федеральный закон «О связи»[31]. В частности, расширен перечень информации, которую операторы подвижной радиотелефонной связи обязаны представлять в Роскомнадзор для мониторинга соблюдения обязанности по проверке достоверности сведений об абонентах и сведений о пользователях услугами связи.

Нарушения требований к пропуску трафика через технические средства преследуются в административном и уголовно-правовом порядке (ст. 13.42 КоАП РФ, ст. 274.2 УК РФ).

Рассматриваемые хищения совершаются путем передачи компьютерной информации по информационно-телекоммуникационным сетям с использованием протокола TCP-IP с использованием прокси-серверов и программных технологий VPN, TOR, SSL, позволяющих менять IP-адрес пользователя сети Интернет, создавать динамические и нераспознаваемые IP-адреса, или уникальный код идентификации посредством SIP-телефонии[32].

Рассматриваемые хищения совершаются путем кражи (п. «г» ч. 3 ст. 158 УК РФ) или мошенничества (ст. 159 УК РФ).

Так, например, Ф. совершил мошенничество, то есть хищение чужого имущества путем обмана группой лиц по предварительному сговору с причинением значительного ущерба гражданину при следующих обстоятельствах.

Неустановленные лица, обладая достаточными познаниями и практическими навыками работы в глобальной информационной сети Интернет и в системе безналичных банковских расчетов, действуя умышленно, из корыстных побуждений, вступили между собой в преступный сговор с целью хищения денежных средств путем обмана Х. под предлогом пресечения несанкционированного их списания.

---

[31] См.: Собр. законодательства Рос. Федерации. 2023. № 32 (часть I), ст. 6205.

[32] См.: Собирание электронных доказательств по уголовным делам на территории России и зарубежных стран: опыт и проблемы : монография / Е.А. Архипова, Е.В. Быкова, П.А. Литвишко и др.; под общ. и науч. ред. С.П. Щербы. М. : Проспект, 2022. 168 с.

Они договорились с Ф., на банковский счет которого за денежное вознаграждение возможно будет перечислить со счета потерпевшей похищенные денежные средства посредством сети Интернет и мобильного приложения «Telegram».

Неустановленные следствием лица, действуя согласованно в составе группы лиц по предварительному сговору с Ф., при помощи неустановленных следствием устройств связи, имеющих доступ к сети Интернет, используя сервис подмены исходящего номера, исключающий возможность идентифицировать абонента и исходящий сигнал, подменив номера, осуществили телефонные звонки Х. на ее абонентский номер, и, представившись сотрудником АО «Альфа Банка», а также сотрудником МВД России, под вымышленными данными «…», под предлогом сохранения денежных средств потерпевшей от несанкционированного доступа злоумышленников к ее банковскому счету АО «Альфа Банк» путем обмана в ходе телефонного разговора с Х. убедили ее для сохранности денежных средств на ее банковском счете перевести деньги на якобы страховой счет банковской карты «…», принадлежащей Н. и подконтрольной злоумышленникам.

Х., будучи введенная в заблуждение, не подозревая об их преступных намерениях, перевела денежные средства в сумме 42 360 руб., из которых 2 360 руб. комиссия, со своей банковской карты АО «Альфа Банк», к которой привязан банковский счет «…», на банковскую карту ПАО Банк «ФК Открытие», номер которой был продиктован неустановленным следствием лицом. Таким образом, Ф. получил доступ к денежным средствам Х., поступившим на счет указанной банковской карты и возможность распорядиться данными денежными средствами.

В целях доведения преступного умысла до конца Ф., действуя согласованно в составе группы лиц по предварительному сговору с неустановленными следствием лицами, после поступления денежных средств на вышеуказанный счет произвел их снятие, причинив тем самым потерпевшей Х. значительный материальный ущерб в сумме 42 360 руб.[33]

Согласно другому приговору Г. совершил мошенничество группой лиц по предварительному сговору в крупном размере при следующих обстоятельствах.

Г. был зарегистрирован в приложении «Telegram». Неустановленные лица, уголовное дело в отношении которых выделено в

[33] См.: Приговор Тетюшского районного суда Республики Татарстан от 14 февр. 2023 г. по делу № 1-9/2023 // СПС КонсультантПлюс.

отдельное производство, с корыстной целью решили совершать хищения чужого имущества путем обмана неограниченного числа пожилых людей, проживающий на территории г. Тула. Они предложили Г. присоединиться к ним.

Неустановленные лица путем случайного подбора абонентских номеров стационарных телефонов жителей г. Тулы с использованием SIP-телефонии подыскивали пожилых людей и в ходе общения с ними представлялись сотрудниками правоохранительных органов. Вводя их в заблуждение, они сообщали потерпевшим заведомо ложные сведения о том, что их родственник, управляя автомобилем, стал виновником дорожно-транспортного происшествия. Для решения возникшей проблемы родственника они требовали денежные средства якобы для того, чтобы избежать уголовного преследования со стороны правоохранительных органов.

При этом они изменяли голос и интонацию, а в случае возникновения сомнений в правдивости их слов, объясняли причины изменения голоса результатами полученных телесных повреждений, эмоциональным напряжением и приемом лекарственных препаратов. При согласии пожилых людей передать денежные средства в обговоренной сумме неустановленные лица просили их сообщить свой домашний адрес. Полученные сведения они передавали Г. путем интернет-переписки в приложении «Telegram». Г. являлся к обманутым гражданам лично, подтверждая слова других участников преступной группы.

Затем Г. получал от пожилых людей денежные средства в оговоренной по телефону сумме, которые обращал в пользу членов преступной группы путем перевода на неустановленные различные банковские счета, реквизиты которых ему поступали на учетную запись в ходе интернет-переписки в приложении «Telegram» от неустановленных лиц с последующим распоряжением ими по своему усмотрению.

Таким образом, Г. и неустановленные лица, действуя группой лиц по предварительному сговору, путем обмана похитили денежные средства в сумме 320 тыс. руб., чем причинили материальный ущерб в крупном размере (ч. 3 ст. 159 УК РФ)[34].

Вместе с тем возможны случаи совершения лицом кражи с банковского счета, а также мошенничества и квалификации его действий по совокупности преступлений – п. «г» ч. 3 ст. 158 УК РФ, ст. 159 УК РФ.

Так, например, Ф., имея умысел на тайное хищение чужих

[34] См.: Приговор Привокзального районного суда г. Тулы от 31 мая 2023 г. по делу № 1-76/2023 // СПС КонсультантПлюс.

денежных средств с банковского счета, используя приложение «WPN PROKSI MASTER», установленное в его мобильном телефоне «iPhone 8» («Айфон 8»), подменил находящийся у него в пользовании абонентский номер телефона «…» на «…» и позвонил на абонентский номер «…», принадлежащий В. Он представился сотрудником службы безопасности ПАО «Сбербанка России», пояснив В., что с ее расчетного счета, открытого в ПАО «Сбербанк России», происходит списание денежных средств, и что для предотвращения несанкционированного списания денежных средств с ее банковского счета ей необходимо установить в свой мобильный телефон приложение «Team Viewer Quick Support».

В., будучи введенной в заблуждение Ф. и уверенной в законности его действий, установила на свой мобильный телефон «Honor Huawei 7x» («Хонор Хуавей 7икс») вышеуказанное приложение. Таким образом, Ф. получил доступ к программному обеспечению мобильного телефона В. и установленным в нем приложениям, в том числе к приложению «Сбербанк Онлайн». Далее, Ф., используя приложение «Сбербанк Онлайн», установленное в мобильном телефоне В., оформил онлайн-заказ в интернет-магазине «Эльдорадо» на общую сумму 178 980 руб., приобретя при этом смартфон «Apple IPhone 11 Pro Max 256 Gb Midnight Green M» («Эпл Айфон 11 Про Макс 256 Гб Миднайт Грин М») на сумму 113 990 руб. и смартфон «Apple IPhone 11 128 Gb (Product) Red (MWM32RU/A)» («Эпл Айфон 11 128 Гб (Продукт) Ред (МВМ32РУ/А») на сумму 64 990 руб., и оплатил заказ с вышеуказанного банковского счета В., тем самым похитил принадлежащие ей денежные средства.

Он же, Ф., имея умысел на хищение чужого имущества путем обмана из корыстных побуждений, используя приложение «WPN PROKSI MASTER» («ВПН ПРОКСИ МАСТЕР»), установленное в его мобильном телефоне «iPhone 8» («Айфон 8»), подменил находящийся у него в пользовании абонентский номер телефона «…» на «…» и под видом сотрудника службы безопасности ПАО «Сбербанк России» убедил В., что для обеспечения сохранности ее денежных средств, находящихся на счетах в ПАО «Сбербанк России», ей необходимо перевести указанные денежные средства на резервный счет.

В., будучи введенная в заблуждение Ф. и уверенная в законности его действий, по указанию Ф. самостоятельно с расчетного счета «…», открытого в отделении ПАО «Сбербанк России», используя приложение «Сбербанк онлайн», установленное в ее мобильном телефоне, произвела перевод денежных средств в размере 185 тыс. руб.

на расчетный счет, открытый в отделении ПАО «Сбербанк России» на ее имя.

Далее В. по указанию Ф. в банкомате сняла со своего расчетного счета денежные средства в сумме 150 тыс. руб. После этого она также по указанию Ф. через банкомат АО «Тинькофф Банк» осуществила перевод наличных денежных средств на общую сумму 150 тыс. руб. одиннадцатью операциями на лицевой счет «…», открытый дистанционным способом в АО «Тинькофф Банк» на имя Ф.

В дальнейшем Ф. полученными денежными средствами распорядился по своему усмотрению, причинив В. значительный материальный ущерб на сумму 150 тыс. руб.

В результате Ф. был осужден по п. «г» ч. 3 ст. 158 УК РФ, ч. 2 ст. 159 УК РФ[35].

Как правило, совершение рассматриваемых преступлений происходит по типичной схеме, включающей элементы (этапы), следующие друг за другом, большинство из которых были описаны выше (например, звонок от родственника, о блокировке банковской карты и др.).

Совершение рассматриваемых преступлений сопряжено с использованием умений и навыков, связанных со способностью быстро и точно составлять суждения о людях, понимать их чувства, мысли, намерения участников общения, выстраивать стратегию своего поведения для достижения преступной цели. Кроме того, необходимы материально-технические средства. Для этого приобретаются и используются персональные компьютеры, роутеры, средства SIP-телефонии, различные мобильные телефоны, в том числе с сим-картами различных операторов связи абонентские номера которых зарегистрированы, как правило, на подставных лиц[36].

[35] См.: Приговор Советского районного суда города Липецка от 28 марта 2022 г. по делу № 1-96/2022 // СПС КонсультантПлюс.

[36] См.: Приговор Советского районного суда города Нижнего Новгорода от 28 дек. 2022 г. № 1-366/2022 // СПС КонсультантПлюс.

ЗАКЛЮЧЕНИЕ

В противодействии мошенничеству большое значение имеет профилактическая работа. Органы государственной власти, правоохранительные органы, банки через официальные сайты, телевидение, плакаты в транспорте и иными способами доводят до граждан информацию о том, чтобы они не доверяли свои персональные данные посторонним лицам, не совершали необдуманных операций со своими денежными средствами под влиянием третьих лиц, с осторожностью переходили по ссылкам на интернет-сайты, если такие ссылки содержатся в письмах электронной почты или в сообщениях в мессенджерах.

С другой стороны, определенные меры, как отмечалось выше, предпринимаются операторами сотовой связи, блокирующими звонки, если они осуществляются с подменой телефонного номера.

Банки увеличивают срок зачисления денежных средств на счет, если операция по их переводу представляется им сомнительной, либо блокируют подозрительные счета.

К такому поведению их обязывают нормы соответствующих законодательных актов, чья роль в противостоянии мошенничеству в эпоху цифровизации продолжит оставаться одной из самых важных.

ОГЛАВЛЕНИЕ

План-график выпуска изданий
ВНИИ МВД России, 2024, поз. 16

Лариса Владимировна Яковлева
Елена Ивановна Майорова
Виктор Владимирович Улейчик

МОШЕННИЧЕСТВО В ЭПОХУ ЦИФРОВИЗАЦИИ: ОСОБЕННОСТИ СОВЕРШЕНИЯ И КВАЛИФИКАЦИИ

Научно-практический комментарий

Редактор *И. П. Стоянова*
Компьютерная верстка *С. В. Первовой*

Подписано в печать 03.07.2024 Тираж 45 экз.
Формат 60Х84 1/16 Печ. л. 2,5 Уч.-изд. л. 2,0 Заказ № 18

Издатель: ВНИИ МВД России
121069, Москва, ул. Поварская, д. 25, стр. 1

Группа ОП РИО ВНИИ МВД России