УДК 343.2/.7

Безденежных Надежда Сергеевна
студентка 3 курса
Волго-Вятский институт (филиал) Университета имени О.Е. Кутафина (МГЮА)
Россия, г. Киров
Ефремова Александра Олеговна
студентка 3 курса
Волго-Вятский институт (филиал) Университета имени О.Е. Кутафина (МГЮА)
Россия, г. Киров
Научный руководитель: Травина Ирина Геннадьевна, доцент кафедры уголовного права и криминологии Волго-Вятского института (филиала) Университета имени О.Е. Кутафина (МГЮА), кандидат юридических наук, доцент
Россия, г. Киров

МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ ВЫСОКИХ ТЕХНОЛОГИЙ

Аннотация: *Основной составляющей криминалистической характеристики мошенничества в сфере компьютерной информации является способ его совершения. В настоящей статье анализируются способы совершения мошенничества в сфере высоких технологий.*

Ключевые слова: *мошенничество, наказание, уголовные кодекс, интернет, высокие технологии*

Annotation: *The basic component of the forensic characteristics of fraud in the field of computer information is the method of its Commission. This article analyzes the ways of committing fraud in the field of high technology.*

Keywords: *fraud, punishment, criminal code, internet, high technology.*

Мошенничество в сфере высоких технологий на сегодняшний день занимает одно из первых мест не только среди преступлений против собственности, но и в общем количестве зарегистрированных преступлений.

Введением в Уголовный кодекс статей 159.3, 159.6 [1], законодатель предусмотрел защиту от мошеннических действий, совершенных с применением современных информационных технологий, т.е. с учетом развития технического прогресса. Однако ввиду сложности этих технических процессов значительный интерес представляют и сами способы совершения мошенничества.

С этой целью необходимо определить основные элементы взаимодействия в механизме преступного поведения. Полагаем, что к таким элементам относятся:

1) виновное лицо, которое совершает мошенничество в сфере компьютерной информации, полагаясь на эффективность своего обмана и нужный уровень доверия;

2) потерпевший, в качестве которого могут выступать как физические лица, так и их контрагенты, предоставляющие банковские услуги;

3) средства хранения, обработки или передачи компьютерной информации или информационно–телекоммуникационных сетей, которые используются в качестве инструментов совершения преступления;

4) контрагент, предоставляющий услуги связи, чьи информационно–телекоммуникационных сети используются для совершения преступлений;

5) третьи лица, возможности которых виновное лицо использует для совершения преступления в рамках реализации обмана или злоупотребления доверием [2. С. 283].

При совершении конкретного преступления не все эти элементы задействуются. Обязательными элементами являются виновное лицо, средства хранения, обработки или передачи компьютерной информации или информационно–телекоммуникационных сетей (ИТС) и потерпевший.

В настоящее время наиболее распространены следующие способы мошенничества в сфере высоких технологий:

1. Неправомерное завладение регистрационными данными разных учетных записей (googlemarket, appstore и т.п.) для последующей их реализации или дальнейшего использования при совершении мошеннических действий [3. С. 147].

2. Социальный инжиниринг как метод проникновения в защищенные системы, базирующийся на применении знаний из области социальной психологии. Его использование связано с применением компьютера или телефона для получения доступа к счету, упрощения такого доступа либо получения необходимой информации (в частности, адреса электронной почты лица) для хищения персональных данных.

3. Распространение вредоносного программного обеспечения (ПО), которое блокирует возможность использования компьютера либо затрудняет его использование (в частности, половину экрана закрывает изображение с требованием отправки SMS на короткий номер). Для разблокировки компьютера мошенники предлагают получить код, для чего необходимо направить платное SMS по указанному номеру. При этом, следует отметить, отправка SMS вовсе не гарантирует разблокировку компьютера.

4. Фишинг – способ мошенничества в сфере компьютерной информации, направленного на получение доступа к конфиденциальным данным пользователей – логинам и паролям. Фишинговые письма являются электронными сообщениями от мошенника в форме официального письма от банка, провайдера, которые направляются для получения логина и пароля пользователя к информационной системе [4. С. 128]. В подобных письмах имеется ссылка на сайт–копию организации, от имени которой якобы направлено данное письмо.

5. Кардинг (словообразование от англ. card – кредитная карточка) – незаконное использование принадлежащей третьим лицам информации о платежных средствах.

6. Использование платежных сервисов интернет–ресурсов при проведении платежных операций с последующим обналичиванием денежных средств или

покупкой различных товаров с использованием денежных средств, находящихся на счете жертвы (мошенники обладают необходимыми для осуществления транзакции данными карты жертвы).

7. Рассылка разного рода электронных писем на электронные почтовые ящики, текст которых вводит в заблуждение получателя, акцентируя его внимание на необходимости определенного рода платежей.

8. Проведение электронных торгов (с фиктивными лотами) или «интернет–аукционов» (продавцы–мошенники для завышения цены аукционного товара делают на него ставки).

9. Осуществление взлома электронных кошельков (в частности, путем рассылки вредоносного программного обеспечения или ссылок на него) и последующее хищение денежных средств (их обналичивание), перевод на другие счета, оплата услуг либо товаров через электронные платежные системы («Webmoney», «YandexMoney», «Qiwi», «PayPal» и др.). Рассмотренные способы наиболее часто встречаются в судебной и следственной практике, однако их перечень не является исчерпывающим и может постоянно пополняться. Проиллюстрируем данные выше положения на статистических примерах.

В России, по данным Росстата, произошел рекордный за последние три года всплеск мошенничества. В первом полугодии 2019–го в стране зарегистрировано 122,8 тыс. таких преступлений, и это на 10,9% больше, чем было зафиксировано за аналогичный период прошлого года. Последний раз мощный всплеск по этому виду преступлений фиксировали три года назад, в первом полугодии 2016–го был резкий рост сразу примерно на 25% в годовом выражении [5].

Генеральная прокуратура РФ в «Ежемесячном сборнике о состоянии преступности в России» подтверждает рост количество преступлений, совершенных в форме мошенничества за январь–июнь 2019–го по сравнению с аналогичным периодом прошлого года почти на 11%. Там отмечают, что на 5,3% выросло число (34,2 тыс.) предварительно расследованных преступлений этого вида, из которых 27,5 тыс. направлены в суд. По данным Генеральной

прокуратуры [6], наибольший рост мошенничеств отмечен в Ростовской области – 62%, в Свердловской области 35,2%, в Башкирии – 31,5% и Ставропольском крае – 28,1%. В Москве тоже вполне заметный рост – на 7,5%.

Как сообщило Главное управление МВД по Свердловской области, ежесуточно в регионе ставится на учет от 10 до 20 преступлений данного вида. В Нижнем Тагиле, например, из 153 уголовных дел по фактам мошенничества в 148 эпизодах фигурирует телефон. Злоумышленники выдают себя за представителей банковских служб безопасности и настаивают на передаче номеров карт и цифровых кодов. Люди сами отдают деньги: на Сахалине в начале августа четыре жителя за день перевели злоумышленникам от 9 до 620 тыс. руб. А 6 августа мошенники, представившиеся сотрудниками службы безопасности банка, списали с карты москвича 3,5 млн руб. В 2018 году, по данным центра мониторинга и реагирования на компьютерные атаки FinCERT Банка России, мошенники похитили почти в 1,5 раза больше, чем в 2017–м, денег с карт россиян. Речь идет об 1,4 млрд руб.

Распространяется мошенничество при оформлении квартир, потому что выливается, по сути, в кражу имущества ценой в миллионы. За последние пять лет число случаев мошенничества на вторичном рынке недвижимости растет, их стало больше на 7,5%, сообщили ранее специалисты агентства «ИНКОМ–Недвижимость».

Всплеск активности мошенников заметили и после того, как они начали продавать жителям поддельные газовые счетчики. Эта тема возникла после череды взрывов газа в жилых домах в разных городах страны.

В России растет и число мошенничеств с использованием электронной подписи. По данным компании «Микрофинансирование и развитие», микрокредитов, оформленных таким путем, по сравнению с прошлым годом стало в три раза больше, сообщала пресса. За первое полугодие число займов, оформленных на третье лицо с помощью электронной подписи, достигло 15,4% от общего объема.

Эта ситуация так скажем «подтолкнула» законодателей и правительство

принимает экстренные меры: внесены поправки в закон «О государственной регистрации недвижимости» [7], которые накладывают запрет на удаленную передачу права на недвижимость физического лица по электронной подписи без предварительного уведомления об этом Росреестра.

Эксперты не исключают, что активизация мошенников стала следствием как сокращающихся уже шестой год подряд доходов населения, так и упрощения криминальных действий за счет современных технологий.

Указанные факты свидетельствуют о несовершенстве правоприменительной практики, обусловленном наличием ряда проблемных вопросов. В самом широком смысле под высокими технологиями понимают сложные технологии, включающие в себя электронику и робототехнику, явившиеся результатом научно–технической революции.

Высокие технологии требуют для своей разработки привлечения научных подходов в той или иной степени. Чем сложнее технология, тем выше уровень ее наукоемкости [8.С. 9-10].

Мошенничество в сети Интернет характеризуется прямым умыслом на незаконное получение чужого имущества или приобретение права на него путем обмана или злоупотребления доверием, который возник до совершения названных действий, а также корыстной целью.

К примеру, в приговоре Октябрьского районного суда г. Барнаула от 12 мая 2016 года по делу №1-154/2016 указывается, что по факту мошенничества в отношении потерпевшего П. виновность Щетинина О. С. подтверждается следующими доказательствами.

Показаниями подозреваемого Щетинина О. С. подтверждается, что ДД.ММ.ГГГГ он приехал в <адрес> на постоянное место жительства. ДД.ММ.ГГГГ около 16 часов в квартире, расположенной по адресу: <адрес>, встретившись с Ф., он согласился арендовать указанное жилое помещение. В этот же день около 18 часов он вместе с Ш. и ребенком приехал в квартиру по указанному адресу, где с Ф. заключил договор аренды, подписанный им и Ф. от имени Ч. За первый месяц проживания в квартире он перечислил Ф. 9000 рублей.

В дальнейшем, нуждаясь в денежных средствах, он решил пересдать квартиру третьим лицам. С этой целью в сети Интернет на сайте «без посредников» разместил объявление о сдаче вышеуказанной квартиры в аренду. ДД.ММ.ГГГГ около 13 часов в квартиру по адресу: <адрес> приехал П., чтобы ее посмотреть. Он, обманывая последнего, пояснил, что приобрел квартиру несколько месяцев назад, документы на которую находятся у родителей. Чтобы более заинтересовать мужчину, он сообщил, что П. может снимать квартиру до лета 2016 года, а если внесет предоплату в размере 10000 рублей, то сумма арендной платы будет составлять 5000 рублей в месяц. Около 19 часов этого же дня в указанной квартире он собственноручно написал договор, в котором указал, что сдает однокомнатную меблированную квартиру по адресу: <адрес> П., оплата произведена за два месяца в сумме 10000 рублей. Далее около 19 часов 30 минут ДД.ММ.ГГГГ П. передал ему деньги в сумме 10000 рублей, о чем он (Щетинин О. С.) написал расписку. ДД.ММ.ГГГГ около 14 часов П. он передал ключи от указанной квартиры, после чего уехал. Он понимал, что данная квартира ему не принадлежит, и распоряжаться ею ему никто не разрешал (л.д. 126-131, 153-154)

Показаниями обвиняемого Щетинина О. С. подтверждается, что последний свою вину в совершении преступления, предусмотренного ч. 2 ст. 159 УК РФ, признал полностью, пояснив, что 16 ноября путем обмана он похитил у П. денежные средства в сумме 10000 рублей, сдав ему квартиру, расположенную по адресу: <адрес>, не имея на то права. Вырученные денежные средства потратил на собственные нужды (л. д. 167-168) [9].

Как видим из указанного примера, Щетинин О. С., зная о том, что квартира была заранее арендована, умышленно путем обмана сдал квартиру заново другому лицу.

Общественная опасность мошенничества в сфере высоких технологий обусловлена в первую очередь способом его совершения. Об особенностях отдельных информационных технологий осведомлены далеко не все граждане, при этом большинство населения использует банковские карты, далеко не всегда разбираясь в технических процессах поступления денежных средств на карту и

их списания.

Одной из причин, обусловливающих общественную опасность мошенничества в сфере высоких технологий в общем и в сфере компьютерной информации в частности, является недобросовестность работников сферы обслуживания, нарушающих требования информационной безопасности и злоупотребляющих своим служебным положением [10. С. 24]. Немаловажную роль в повышении степени общественной опасности рассматриваемых преступлений является общедоступность последних, что отрицательным образом сказывается на выработке мер по предупреждению правонарушений в указанной сфере. Также к наиболее общим причинам широкого распространения данного вида мошенничества выступает слабая осведомленность потерпевших о характере совершаемых ими действий.

Перечисленные факторы указывают на необходимость выработки специфических мер предупреждения преступлений данного вида и определяют основные направления противодействия им.

Литература:

1. Уголовный кодекс Российской Федерации от 13.06.1996 N 63–ФЗ (ред. от 04.11.2019) // Собрание законодательства РФ. 1996. N 25. Ст. 2954.

2. Коломинов В.В., Смирнова И.Г. К вопросу о формировании криминалистического знания о мошенничестве в сфере компьютерной информации // Уголовно–процессуальные и криминалистические средства обеспечения эффективности уголовного судопроизводства: материалы науч.–практ. конф. – 2014. – С. 283–289.

3. Коломинов В.В. О способе совершения мошенничества в сфере компьютерной информации // Человек: преступление и наказание. – 2015. – № 3. – С. 147.

4. Зверянская Л.П. Современные проблемы исследования криминалистических особенностей киберпреступлений // Приоритетные научные направления: от теории к практике. – 2015. – Вып. № 15. – С. 128.

5. Мошенники осваивают высокие технологии // http://www.ng.ru (Дата доступа 10.12.2019).

6. ФГИС Единый реестр проверок Генеральной прокуратуры Российской Федерации [Электронный ресурс]. URL: http://genproc.gov.ru (Дата обращения 10.12.2019).

7. Федеральный закон от 13.07.2015 N 218–ФЗ (ред. от 02.08.2019) "О государственной регистрации недвижимости" (с изм. и доп., вступ. в силу с 16.09.2019) // http://www.consultant.ru (дата доступа 10.12.2019).

8. Бархатова Е.Н. Об общественной опасности мошенничества в сфере высоких технологий // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. – 2018. – № 16–2. – С. 9–10.

9. Приговор Октябрьского районного суда г. Барнаула от 12 мая 2016 года по делу № 1154/2016 [Электронный ресурс]. - Режим доступа: http://sudact.ru/regular/doc/9Tug2D2AqPUp/ (дата обращения 17.12.2019).

10. Хайдаршина Р.Ф. Способы мошенничества в сфере высоких технологий // Перо науки. – 2019. – № 11 (11). – С. 21–24.