МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»
Институт права
(наименование института полностью)

Кафедра «Уголовное право и процесс»
(наименование)

40.03.01 Юриспруденция
(код и наименование направления подготовки, специальность)

Уголовно-правовой
(направленность (профиль)/специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (БАКАЛАВРСКАЯ РАБОТА)

на тему «Дистанционное мошенничество: понятие, виды, особенности расследования»

Студент Н.Ю. Быкова
(И.О. Фамилия) (личная подпись)

Руководитель канд. юрид. наук, доцент, П.А. Кабанов
(ученая степень, звание, И.О. Фамилия)

Тольятти 2022

Аннотация

Актуальность выпускной квалификационной работы состоит в том, что в условиях развития информационных технологий посредством трансформации правовых норм в уголовном праве существует определенный риск совершения преступлений. Однако остается и нерешённой проблема применения информационных технологий и адаптации криминалистической деятельности при расследовании преступлений.

Преобладание цифровой экономики привело к необходимости реформатировании не только уголовного и уголовно-процессуального законодательства, но и гражданского права. Поскольку объектами гражданских прав, а также элементами преступлений в уголовном праве выступают не только имущество, нематериальные блага, но и цифровые права и средства индивидуализации, неправомерные действия лиц, запрещенные уголовным законом, осуществляются в нарушении норм уголовного и гражданского права.

Цель выпускной квалификационной работы – уголовно-правовой анализ преступлений, связанных с дистанционным мошенничеством, раскрытие вопросов расследования.

Для реализации данной цели были поставлены следующие задачи:

- рассмотреть дефиниции и терминологию, используемые для описания дистанционного мошенничества;
- определить понятие и признаки дистанционного хищения;
- определить специальные понятия, используемые для описания дистанционного мошенничества;
- проанализировать виды и способы дистанционного мошенничества;
- провести общую уголовно-правовую характеристику мошенничества;
- охарактеризовать отдельные виды и способы дистанционного мошенничества;

- исследовать особенности расследования дистанционного мошенничества;
- изучить некоторые особенности выявления дистанционного мошенничества первоначального этапа расследования;
- определить тактические особенности производства следственных действий при расследовании дистанционного мошенничества.

Объектом исследования выпускной квалификационной работы выступают общественные отношения в сфере привлечения к уголовной ответственности за преступные деяния, совершаемые с применением дистанционного мошенничества.

Предметом исследования выпускной квалификационной работы выступают уголовно-правовые нормы, отражающие специфику рассматриваемых правоотношений.

Структура выпускной квалификационной работы состоит из введения, трех глав с шестью параграфами, заключения и списка используемой литературы и используемых источников.

Оглавление

Введение 5
Глава 1 Дефиниции и терминология, используемые для описания дистанционного мошенничества 8
1.1 Дистанционные хищения: понятие и признаки 8
1.2 Специальные понятия, используемые для описания дистанционного мошенничества 13
Глава 2 Виды и способы дистанционного мошенничества 28
2.1 Общая уголовно-правовая характеристика мошенничества 28
2.2 Характеристика отдельных видов и способов дистанционного мошенничества 36
Глава 3 Особенности расследования дистанционного мошенничества 52
3.1 Некоторые особенности выявления дистанционного мошенничества первоначального этапа расследования 52
3.2 Некоторые тактические особенности производства следственных действий при расследовании дистанционного мошенничества 59
Заключение 69
Список используемой литературы и используемых источников 73

Введение

Актуальность выпускной квалификационной работы состоит в том, что в условиях развития информационных технологий посредством трансформации правовых норм в уголовном праве существует определенный риск совершения преступлений. Однако остается и нерешённой проблема применения информационных технологий и адаптации криминалистической деятельности при расследовании преступлений.

Преобладание цифровой экономики привело к необходимости реформатировании не только уголовного и уголовно-процессуального законодательства, но и гражданского права. Поскольку объектами гражданских прав, а также элементами преступлений в уголовном праве выступают не только имущество, нематериальные блага, но и цифровые права и средства индивидуализации, неправомерные действия лиц, запрещенные уголовным законом, осуществляются в нарушении норм уголовного и гражданского права.

Федеральный закон от 29.11.2012 № 207-ФЗ (ред. от 03.07.2016) «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» в Уголовный Кодекс Российской Федерации (далее – УК РФ) введена новая норма, устанавливающая уголовную ответственность за совершение мошенничества с использованием платежных карт.

Вместе с тем, преступления, связанные с применением обмана или злоупотребления доверия можно квалифицировать и по ст. 137 УК РФ, по ст.ст. 159, 159.6 УК РФ, а также ст. 272 УК РФ. Проблемы уголовно-правовой квалификации связаны не только с преступным деянием, но и наступившими общественно-опасными последствиями его совершения.

Цель выпускной квалификационной работы – уголовно-правовой анализ преступлений, связанных с дистанционным мошенничеством, раскрытие вопросов расследования.

Для реализации данной цели были поставлены следующие задачи:

- рассмотреть дефиниции и терминологию, используемые для описания дистанционного мошенничества;
- определить понятие и признаки дистанционного хищения;
- определить специальные понятия, используемые для описания дистанционного мошенничества;
- проанализировать виды и способы дистанционного мошенничества;
- провести общую уголовно-правовую характеристику мошенничества;
- охарактеризовать отдельные виды и способы дистанционного мошенничества;
- исследовать особенности расследования дистанционного мошенничества;
- изучить некоторые особенности выявления дистанционного мошенничества первоначального этапа расследования;
- определить тактические особенности производства следственных действий при расследовании дистанционного мошенничества.

Объектом исследования выпускной квалификационной работы выступают общественные отношения в сфере привлечения к уголовной ответственности за преступные деяния, совершаемые с применением дистанционного мошенничества.

Предметом исследования выпускной квалификационной работы выступают уголовно-правовые нормы, отражающие специфику рассматриваемых правоотношений.

Методологическую основу исследования выпускной квалификационной работы составили сравнительный и системный методы исследования, методы теоретического анализа нормативно-правовых источников, метод аналитического обобщения мнений выдающихся ученых-юристов по теме исследования.

Методика исследования выпускной квалификационной работы – сравнительно-правовой анализ нормативных источников.

Нормативные источники, на которых базируется выпускная квалификационная работа, представлены Конституцией Российской Федерации; кодексами, такими как Уголовный кодекс Российской Федерации, Кодекс Российской Федерации об административных правонарушениях; федеральными законами, такими как Федеральный закон «Об оперативно-розыскной деятельности» [42] , Федеральный закон «О связи» [43], Федеральный закон «Об информации, информационных технологиях и о защите информации» [44]; постановлениями, такими как Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», Постановление Пленума Верховного Суда РФ от 27.12.2002 № 29 (ред. от 29.06.2021) «О судебной практике по делам о краже, грабеже и разбое» и др.

Теоретические источники на которых базируется выпускная квалификационная работа, монографии, диссертации, учебники, учебные пособия, научные статьи. В ходе исследования были использованы научные труды отечественных и зарубежных ученых в области уголовного, гражданского права.

Структура выпускной квалификационной работы состоит из введения, трех глав с шестью параграфами, заключения и списка используемой литературы и используемых источников.

Глава 1 Дефиниции и терминология, используемые для описания дистанционного мошенничества

1.1 Дистанционные хищения: понятие и признаки

Распространенное в последние годы использование преступниками сети Интернет, сотовой связи, компьютерных программ, социальных сетей для совершения хищений получило в практике и научном сообществе название «дистанционное мошенничество». Однако четкого понимания, что такое «дистанционное мошенничество», нет [4, с. 15].

При помощи компьютерных устройств, сети Интернет, иных компьютерных технологий в настоящее время совершаются различные преступления, объекты которых «разбросаны» по всей Особенной части УК РФ: преступления против личности, экономические преступления, преступления против основ конституционного строя и безопасности государства и др. Это создает определенные сложности при квалификации таких преступлений [5, с. 58].

Понятие «дистанционное мошенничество» законодательного закрепления не получило, но с учетом практики правоохранительных органов можно выделить отдельную категорию мошенничества, объединенную спецификой, основанной на способе совершения.

Способы совершения данных преступлений постоянно меняются, что влечет за собой изменения уголовного законодательства. Последнее такое изменение было внесено 23 апреля 2018 г. в ст. 158 и 159 УК РФ. Так, Федеральным законом от 23 апреля 2018 г. № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» ч. 3 ст. 158 УК РФ была дополнена пунктом «г», в котором определена ответственность за кражу, совершенную с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159.3 УК РФ).

Пока термин «дистанционное хищение» охватывает три вида преступлений: подпункт «д» ч. 3 ст. 158, ст. 159.3, ст. 159.6 УК РФ. Попытки дать определение этому виду преступления предпринимались и другими исследователями [1, с. 29].

Действительно пункт «д» ч. 3 ст. 158 УК РФ посвящена хищению денег с банковской карты, расчетного счета, путем перевода средств через интернет, мобильный банкинг, Сбербанк-онлайн и т.д.

Кража, то есть тайное хищение чужого имущества, с банковского счета, а также в связи с электронными деньгами – наказывается штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода за период от одного года до трех лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до полутора лет или без такового, либо лишением свободы на срок до шести лет со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев или без такового и с ограничением свободы на срок до полутора лет или без [25, с. 41].

Другой вид в пункте «д» части 3 ст. 158 УК РФ – электронные деньги. Они также используются для безналичных расчетов. Как справедливо заметил А.А. Рудых, «электронные деньги представляют собой определенную информацию, преобразованную в эквивалент, выраженный в стоимостной или натуральной единице (деньги, минуты, количество поездок, литры)» [34, с. 6].

Согласно Постановлению Пленума Верховного Суда Российской Федерации от 29 июня 2021 г. о хищениях с банковского счета и карты (п. «д» ч. 3 ст. 158 УК РФ): «Тайное снятие денежных средств с банковского счета или электронных денег, например, если снятие наличных в безналичном или банкоматном порядке осуществлялось с использованием чужой или поддельной платежной карты, это будет квалифицироваться как хищение по признаку «с банковского счета». Согласно п. «д» ч. 3 ст. 158 УК

РФ действия лица также правомерны в случае, если оно тайно похитило денежные средства с банковского счета или электронные деньги с использованием конфиденциальной информации владельца денежных средств, необходимой для доступа к ним (например, персональные данные владельца, реквизиты платежной карты, контрольная информация, пароли)» [32].

Ответственность за использование чужого доверительного управления с целью завладения денежными средствами, привязанными к платежной карте, предусмотрена ст. 159.3 УК РФ.

Согласно части 1 ст. 159.3 УК РФ под мошенничеством с использованием платежных карт понимается хищение чужого имущества, совершенное с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем введения в заблуждение уполномоченного работника кредитной, торговой или иной организации.

Это деяние наказывается штрафом в размере до 120 тыс. рублей или в размере заработной платы или иного дохода за период до одного года, либо обязательными работами на срок до 360 часов, либо исправительными работами в принудительном порядке на срок до одного года. на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на срок до двух лет [39].

В этой статье также приведены отдельные признаки классификации.

Недавно в Уголовный кодекс были внесены изменения, согласно которым лицо, впервые совершившее вышеуказанные преступления, освобождается от уголовной ответственности, если в течение 2 месяцев со дня возбуждения уголовного дела полностью возместило задолженность по выплате заработной платы, пенсий, стипендий, пособий и иных установленных законодательством выплат, а также процентов (денежной компенсации выплаченных) в порядке, определяемом законодательством

Российской Федерации, и если ваши акции не содержат иного уголовное преступление.

Электронные платежные средства не считаются объектом хищения в статье 159.3 УК РФ, а именно как средство вывода денежных средств, а объектом являются только безналичные денежные средства, находящиеся на банковском или сводном счете держателя карты. То есть по смыслу ст.159.3 УК РФ электронное платежное устройство выступает ключом к банковскому сейфу, содержащему деньги [39].

Согласно части 1 ст. 159.6 УК РФ под мошенничеством в области компьютерной информации понимается хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, изменения компьютерной информации либо в любом случае вмешательства в ее функционирование средств хранения, обработки или передачи информации, или компьютерных и телекоммуникационных сетей [39].

За данное преступление предусмотрена ответственность в виде штрафа до 120 000 рублей, либо размер заработной платы или иного дохода осужденного за период до одного года, либо обязательные работы на срок до 360 часов, либо исправительные работы на срок до одного года, либо ограничение лишение свободы на срок до двух лет, либо принудительные работы на срок до двух лет, либо арест на срок до четырех месяцев.

Мошенничество в сфере компьютерной информации, совершенное путем неправомерного доступа к компьютерной информации либо путем создания, использования и распространения вредоносных программ для ЭВМ, требует дополнительной квалификации по ст. 272, 273 или 274.1 УК РФ [39].

Дистанционное хищение совершается при активном участии владельца средств. Последний под руководством мошенника часто осуществляет очень сложные действия по переводу своих средств на чужой счет. Под руководством нападающего и под его руководством объект убеждения

впадает в состояние иллюзии. Он соглашается действовать по инструкции оператора, после чего добровольно совершает действия, в результате которых теряет свои деньги [46].

Механизм совершения дистанционной кражи также уникален. Преступник осуществляет действия на расстоянии от потерпевшего, не вступая в непосредственный контакт с потерпевшим, вводит потенциального потерпевшего в заблуждение, а затем похищает у него деньги.

Хищение средств происходит по следующему алгоритму: жертвы сами сообщают информацию мошеннику, потому что их ввели в заблуждение. Преступник получает доступ к счету мобильного телефона или кредитной карте, с которых впоследствии похищаются деньги. Бывают случаи, когда потерпевшие сами под влиянием обмана переводят деньги.

В связи с этим дистанционное воровство можно разделить на три группы:

- хищения, совершенные с использованием сотовой связи и сети Интернет. Предлоги, которые используют преступники для получения информации о банковской карте, счете, разнообразны. К ним относятся: разблокировка банковской карты; купля-продажа товаров на интернет-сайтах в случаях, когда размещенные на них товары являются лишь предлогом для вызова потенциальной жертвы; компенсация за ранее купленные лекарства, компенсация из Пенсионного фонда России и т. д.;
- кража, совершенная с использованием сотовой связи и прямого контакта с потерпевшим. Как правило, этот способ характерен при использовании предлога - у родственника проблемы, авария, полиция и т.п.;
- хищения, совершенные только с использованием интернет-ресурсов. Покупка, продажа товаров на различных интернет-площадках, в том числе с использованием «зеркал» (сайтов, аналогичных оригинальным, которые принадлежат известным

организациям), взлом страниц в социальных сетях и отправка запросов на перевод денег от имени пользователя страницы в социальной сети [51, с. 97].

Таким образом, термин «дистанционное хищение» охватывает три вида преступлений: п. «д» п. 3 ст. 158, ст. 159.3, ст. 159.6 УК РФ. Их объединяют следующие признаки: изъятие денежных средств осуществляется в неочевидных условиях, когда преступник и потерпевший не видят друг друга и, как правило, не знают друг друга; преступник не только не видит потерпевшего, но обычно находится в другом субъекте РФ, возможно, в местах лишения свободы; предметом таких преступлений являются только деньги, которые являются безличными, они могут быть переданы преступнику как в не денежной, так и в денежной форме.

1.2 Специальные понятия, используемые для описания дистанционного мошенничества

Распространенное в последние годы использование преступниками сети Интернет, сотовой связи, компьютерных программ, социальных сетей для совершения хищений получило на практике и в научном сообществе название «дистанционного мошенничества». Достаточно часто под дистанционным мошенничеством правоохранительные органы понимают телефонное мошенничество, совершаемое с использованием сотовой связи, реже фиксированной телефонной связи в условиях отсутствия личного контакта между преступником и потерпевшим [2, с. 17].

В данном пункте проведем анализ специальных понятий, используемых для описания дистанционного мошенничества.

Во-первых, понятие сотовой связи и базовых станций. Для определения правовой природы понятий «сотовая связь» и «базовые станции» необходимо рассмотреть признаки указанных категорий, содержащихся в действующих нормативных правовых актах. Федеральным законом от 07.07.2003 № 126-ФЗ

(ред. от 30.12.2021) «О связи» (далее – Закон «О связи») из определения «пользователь услуг связи» можно сделать вывод, что услуги связи могут быть, как оказаны, так и использованы в зависимости от соглашений, заключаемых потребителями услуг. При этом условия соглашений о предоставлении услуг связи должны быть направлены на обеспечение прав и свобод не только сторон договора, но и других лиц, интересы которых застрагиваются предметом договора, то есть оказываемыми услугами связи.

Статьей 44 указанного Закона «О связи» определены условия предоставления подвижной радиотелефонной связи потребителям услуг – физическому и юридическому лицу. При этом потребителями услуг связи выступают абоненты. Вместе с тем услуги связи предоставляются на основании сведений об абоненте, достоверность которых является обязательным условием. Ответственность за предоставление сведений ненадлежащим образом или предоставление недостоверных сведений установлена Кодексом об административных правонарушениях – для юридических лиц и субъектов, осуществляющих предпринимательскую деятельность, уголовная – для физических лиц [43].

Услуги связи предоставляются пользователям на основании договора об оказании услуг. Услуги оказываются операторами связи на основании правил оказания услуг связи в зависимости от вида услуг. Следует учесть, что договор об оказании услуг связи в обязательном порядке должен содержать сведения об абоненте, позволяющих его идентифицировать. Однако в случае непредоставления сведений или предоставления недостоверных сведений, оператор может быть привлечен к административной ответственности, предусмотренной ст. 13.30 КоАП РФ.

Предоставление услуг связи неразрывно связано с их использованием и передачей, которые осуществляются различными способами. К таким способам относится порядок передачи услуг связи через сеть «Интернет», а также использования пользовательского оборудования, позволяющего идентифицировать пользователя услуг связи.

Базовые станции сотовой связи представляют собой определенные средства передачи связи. При этом базовые станции отвечают признакам объекта капитального строительства и объекта недвижимости, поскольку являются сложными объектами, неразрывно связаны с землей в силу наличия у них фундамента, технологически образуют единое целое, части которого взаимосвязаны [6, с. 45]. К тому же, базовые станции являются постройками, имеющий постоянный характер и единое целевое назначение, соответственно не могут быть признаны в качестве самовольных и временных построек. Отличительной особенностью базовых станций является их назначения. Они активно применяются в хозяйственной деятельности и связаны с имуществом организаций.

Еще одним понятием, имеющим важное значение при использовании услуг связи, является «сеть связи», которая предназначена для электрической и почтовой связи. Порядок осуществления почтовой и электрической связи определяется положениями Закона «О связи». Законом предусмотрено, что сети связи представляют собой технологическую систему, имеющую сложную структуру и ограниченные сферы использования [43].

Следует учесть, что объекты сетей связи можно выявить визуально или с применением специальных приборов. При этом к таким объектам связи относятся линии связи и вооружения. К сетевым объектам относятся линейные объекты связи, абонентское оборудование и точки доступа. Вместе указанные элементы образуют сетевые объекты.

Таким образом, сотовая связь определяется не только, исходя из ее назначения, но и в соответствии с источником хранения связи. Так, сотовая связь предназначена для получения, передачи, хранения и использовании информации посредством использования технических средств и программных устройств. Использование сотовой связи, в том числе ее передача осуществляется с помощью базовых станций. Следует учесть, что предоставление услуг должно быть осуществлено на основании законности

добровольности, недопустимости нарушения прав и законных интересов потребителей услуг.

Во-вторых, понятие IMEI. При осуществлении расследовании преступлений, процессуальный порядок которых предусмотрен УПК РФ [40], органы следствия и оперативно – розыскной деятельности совершают неотложные действиями и используют полученные доказательства для раскрытия преступления. Однако при исследовании следов преступления в рамках криминалистической деятельности органы внутренних дел сталкиваются с понятием «перепрошивка», которое используется с целью сокрытия следов преступления, IMEI-номеров похищенных сотовых телефонов.

Действующее законодательство не имеет достаточных нормативно-правовых инструментов для противодействия кражам мобильных телефонов, в то время как, например, изменение идентификационного номера мобильного телефона наказывается лишением свободы на срок до двух лет в Австралии и до пяти лет лишения свободы в Великобритании [12, с. 34].

Макаров А.В., Страмилова Т.П., Куприянова А.В., Федурина Ю.О. отмечают, что проблемами правового регулирования установления уголовной ответственность является применение ст. 158 УК РФ и ст. 159 УК РФ за совершение хищения сотовых телефонов. Так, если хищение произошло с злоупотреблением доверия, когда потерпевший знал о хищении, то такие действия могут быть квалифицированы по ст. 159 УК РФ. Если хищение мобильного телефона произошло при его обнаружении, когда лицом не был заранее обдуман умысел на похищение, то такие действия попадают под признаки кражи, предусмотренные ст. 158 УК РФ [24, с. 42].

Применение связано с осуществлением неправомерного доступа к компьютерной информации. Так, указанное преступление имеет место при изменении IMEI-номера. Изменение IMEI номера в теории уголовного законодательства не может быть отнесено к признакам преступления, предусмотренного ст. 272 УК РФ.

Такое разночтение закона может быть обусловлено тем, что средства связи, в том числе радиотелефоны и сотовые телефоны практически затруднительно отнести к вычислительной технике. Трудности возникают и в связи с тем, что нормативными правовыми актами четко не сформулировано понятие электронно-вычислительной техники, а в ст. 272 УК РФ дается лишь упоминание об ЭВМ.

Дать законодательно закрепленное понятие сотового мобильного телефона как электронно-вычислительной машины для квалификации действий преступников по перепрограммированию индивидуального идентификатора мобильного устройства по ст. 272 и ст. 273 УК РФ возможно, если рассматривать под ЭВМ банкоматы, контрольно-кассовые машины, электронные платежные терминалы. Эти предположения основаны на определении IMEI по международному праву, согласно которому IMEI выступает в качестве международного идентификатора сотового оборудования, используемого для хранения информации об устройстве [25].

Существенную проблему в сфере борьбы с хищениями сотовой связи вызывает отсутствие единого учета их номеров IMEI. Это связано с тем, что данные номера IMEI содержатся в международных сетях и системах, не подпадающих под действие российского законодательства. В результате преступники имеют возможность беспрепятственно пользоваться украденными сотовыми телефонами в различных уголках страны.

В целях установления факта использования мобильного устройства при проведении расследования исследуют данные не только о IMEI-номерах, о и соединениях абонента, места нахождения абонента, число и виды зарегистрированных мобильных устройств. Поскольку идентификационные сведения о сотовом телефоне не могут указать на принадлежность к конкретному пользователю, в целях изобличения лиц, совершивших преступление с использованием средств сотовой связи, мобильных телефонов, устанавливается маршрут передачи данных всех операторов связи.

Однако китайские производители присваивают международный идентификатор целой партии сотовой продукции. Соответственно отследить сотовые телефоны сотрудникам правоохранительных органов при расследовании преступлений достаточно сложно. Для решения указанной проблемы необходимо предусмотреть собственный порядок идентификации по российскому законодательству.

Такой порядок в связи с отсутствием идентификационных сведений должен быть определен, исходя из конкретного региона, в котором находится сотовый телефон. Однако такое решение не является достаточным. Необходимо решать указанные проблемы на международном уровне посредством заключения соглашений о международном сотрудничестве в конкретной сфере применения.

Информация об абонентском номере, в том числе о соединениях, хранении данных и их использование, информация, полученная в текстовых и голосовых сообщениях, как правило находится у оператора связи.

Однако в случае нарушения тайны переговоров, конституционного права на неприкосновенность информации и частной жизни, требуется постановление суда. В связи с тем, что право на защиту телефонных переговоров и тайны переписки может быть ограничено на основании постановления судебных органов, выдаваемого в случае проведения расследования преступления или проверки информации о готовящемся преступлении.

При обращении правоохранительных органов и органов обеспечения безопасности операторы обязаны предоставить сведения об абонентах и абонентских номерах. В вязи с необходимостью приостановления оказания услуг связи оператор приостанавливает действие договора связи. Восстановить получение услуги возможно при получении разрешения органов, осуществляющих оперативно – розыскную деятельность [8, с. 12].

Таким образом, предоставление сведений о международном идентификаторе сотового телефона имеет важное значение при

расследовании и раскрытии преступлений, предусмотренными несколькими разделами УК РФ. Решение проблем для получения сведений об IMEI – номере должно осуществляться на международном уровне не только между странами, имеющими торговые отношения, но и государствами, использующими средства идентификация для защиты права и законных интересов пользователь услуг.

Понятие IP-адреса и VPN. Искусственный интеллект, информационные технологии, а также системы, имеющие признаки «человекоподобного» интеллекта являются технологиями, применяемыми во всех сферах общественной жизни, во взаимосвязи государства, общества и личности [33, с. 109].

Искусственный интеллект широко используется в компьютерных программах и персональных компьютерах, при их использовании потребителями услуг. Кроме того, Искусственный интеллект применяется в информационно – телекоммуникационной сети «Интернет».

По мнению Морхата П.М., в настоящее время Интернет представляет собой особое информационное пространство, содержащее постоянно изменяющийся объем информации с точки зрения ее качественных и количественных характеристик. При этом Интернет выступает как так называемое «виртуальное пространство», в котором формируется собственная система социальных коммуникаций, важная для частной жизни, деловой деятельности, государственного управления [35, с. 262].

В большинстве случаев для подключения к сети используются IP-адреса, что дает провайдеру возможность обслуживать больше клиентов, чем реальное количество свободных адресов, принадлежащих провайдеру. Следовательно, динамические IP-адреса Интернет-соединения могут быть одинаковыми для разных устройств связи, если Интернет-соединения были установлены в разное время. Сам динамический IP-адрес определяется не компьютером, а очень часто сервером, расположенным, например, в офисном здании.

Гуляев К.С. отмечает, что использование IP-адреса и VPN способствует не только применением информационных технологий во всех сферах жизнедеятельности, но и раскрытию преступлений в экономической деятельности. Так, Управление уголовных расследований Налоговой службы США (IRS-CI) ежегодно направляет в Министерство юстиции США сотни материалов проверок в отношении граждан и организаций, занимающихся оборотом криптовалюты и извлечением как законного, так и незаконного дохода [10, с. 29]. Осуществление указанных проверок направлено на борьбу с киберпреступностью в финансовой и налоговой сферах.

Усилия IRS-CI по расследованию киберпреступности сосредоточены на субъектах, использующих Интернет в качестве основного средства совершения преступления, оставаясь анонимными, ускользая от правоохранительных органов и скрывая финансовые операции, владение активами.

В Российской Федерации противодействие преступлениям осуществляется не только в отношении информационных технологий и использованием сети «Интернет», но и при предоставлении отчетности о доходах государственных служащих. В ходе 18-го заседания генеральных прокуроров государств – членов Шанхайской организации сотрудничества Генеральный прокурор РФ заявил о том, что государственные служащие в России обязаны декларировать виртуальные валюты наряду с другими активами. При этом требуется сообщать именно о сделках по приобретению виртуальных активов, цифровой валюты. При этом нелегальным признается сам факт владения государственным служащим криптовалютой, даже без целей обмена.

Таким образом, применение IP-адресов и VPN осуществляется в целях предупреждения и пресечения международных и национальных преступлений в экономической и финансовой деятельности. Следовательно, правовое регулирования порядка производства расследований по указанным преступлениям должно осуществляться в соответствии с международными

договорами и принципами международного права. Следует учесть, что для всех государственных и гражданских служащих необходимо установить прямой запрет не только на счета в иностранных кредитных организациях, но и иностранной валюте с целью конфиденциальности государственной и правоохранительной деятельности, а также с целью пресечения возможности совершения должностных преступлений.

Используемые ресурсы для перевода и хранения похищенных денежных средств. Повышение уровня уголовно-правовой защиты граждан осуществляется не только посредством установления уголовной ответственности за совершение преступления, а также уголовного наказания, но и усиление мер ответственности за преступление. Так, в 2018 году в положения УК РФ, регулирующие квалификацию преступлений за хищение денежных средств с банковских карт, совершаемых путем применения платежных систем. Так, нормами Федерального закона «О внесении изменений в УК РФ» от 23.04.2018 года № 111-ФЗ банковские счета определены в качестве электронных денежных средств.

Изменения у положения УК РФ коснулись не только определений и понятий. Используемых при регулировании уголовного законодательства, но и уголовной ответственности за совершение мошенничества с использованием электронных средств платежа. Если до редакции лишение свободы устанавливалось на срок до четырех месяцев, то в действующей редакций срок лишения свободы увеличен до трех лет [15, с. 23].

Применение технических средств при совершении мошенничества позволять затруднить идентификацию лица, совершившего преступление, поскольку преступление осуществляется посредством использования ресурсов сети «Интернет» [14, с. 40].

В теории уголовного права совершение преступлений в отношении банковских средств могут быть квалифицированы, как кража и как мошенничество. Однако применение одной и той же квалификации недопустимо при расследовании преступлений и назначении наказания.

Единственным признаком квалификации преступления, совершенные с использованием платежных систем, является отсутствие признаков состава преступления, предусмотренного ст. 159.3 УК РФ [19, с. 87].

Мошенничество следует отличать от кражи при совершении незаконного изъятия денежных средств с банковских счетов. Преступление может быть признано в качестве кражи, если при подготовке к его совершению использовались конфиденциальные данные, позволяющие идентифицировать владельца счета. В данном случае к конфиденциальным сведениям относятся персональные данные и данные банковской карты и средств платежа.

При квалификации преступлений против собственности важнейшим признаком является способ совершения преступления. Именно определяет уголовно – правовую квалификацию и признаки разграничения преступления. Если мошенничество в отличие от кражи совершается при использовании платежных систем в момент совершения преступления, а кража при использовании данных о владельце банковских счетов и карт, то мошенничество в сфере компьютерной информации осуществляется посредством вмешательства в порядок передачи и хранения информации, в том числе при ее размещении в сети «Интернет».

Способами получения денежных средств при совершении указанных видов преступлений является обналичивание денежных средств. Например, лицо, совершившее преступление по хищению денежных средств с электронного счета, может перечислить средства на банковских счет и впоследствии обналичить их путем получения. Следует учесть, что преступные действия при совершении мошенничества были реализованы посредством удаления персональных даны о собственнике банковского счета, что само по себе затрудняет реализацию права собственности на денежные средства, находящиеся в кредитных организациях [16, с. 42].

Таким образом, совершение преступлений против собственности посредством хищения денежных средств может быть квалифицировано в

качестве кражи и в качестве мошенничества. При этом для установления правильной квалификации необходимо исследовать все элементы состава преступления, в том числе способы и предметы преступления.

Интернет сайт понятие и схема получения информации. Правовое регулирование размещения информации в сети «Интернет» осуществляется Федеральным законом от 27.07.2006 № 149-ФЗ (ред. от 30.12.2021) «Об информации, информационных технологиях и о защите информации». При этом предоставление информации и ее размещение неразрывно связано с защитой авторских прав, предусмотренных нормами ГК РФ. При этом сеть интернет представляет собой электронный ресурс, в котором размещается информация с использованием технических средств.

Интернет-портал, или «веб-портал», как категория общего характера не раскрывается в действующем законодательстве, но в федеральных законах, подзаконных нормативных правовых актах определяются особенности конкретных специализированных порталов, созданных для реализации публичных функций.

Единый портал может быть создан для размещения официальной информации, а также официальных сайтов о деятельности органов государственной власти [18, с. 415]. При предоставлении государственных и муниципальных услуг используется портал государственных и муниципальных услуг. При этом информационный портал является средством получения информации гражданам организациями о деятельности органов государственной власти, органов местного самоуправления, а также с целью получения государственных услуг, связанных с регистрацией прав на объекты недвижимости, прав в жилищной и образовательной сферах. К тому же, информационный портал содействует взаимодействию субъектов права с органами государственной власти.

Следует учесть, что информационные порталы используются и применяются не только при предоставлении государственных и муниципальных услуг, но и для создания базы данных пространственных

данных. Правовое регулирования создания информационных порталов осуществляется в соответствии с нормами Федерального закона от 30.12.2015 № 431-ФЗ «О геодезии, картографии и пространственных данных и о внесении изменений в отдельные законодательные акты Российской Федерации».

В сфере обеспечения занятости населения используется сайт «Работа в России», который функционирует в соответствии с Законом РФ от 19.04.1991 № 1032-1 «О занятости населения в Российской Федерации». При этом указанный сайт включает базу вакансия, используемую для поиска работы и лиц, готовых осуществлять трудовую деятельность.

Осуществление правосудия, как и право на судебную защиту непосредственно связано с принципом доступности правосудия, который реализуется не только посредством обращения в органы судебной власти, но и посредством получения информации, размещаемой в сети «Интернет». В рамках осуществления судебной деятельности предусмотрено создание системы данных об основах осуществления правосудия с целью получения информации о правоприменительной деятельности судов общей юрисдикции, арбитражных судов, специализированных судов и судов, имеющих высший правовой статус. Так, получить указанную информацию можно в системе ГАС «Правосудие» [21, с. 99].

Интернет-портал является совокупностью программ, применяемых с использованием технических средств и информационных технологий, и иной информации, содержащейся в информационной системе. Таким образом, интернет-портал включает массивы информации, объединенных по определенному признаку, обеспечивает обмен данными, обработку посредством единых информационных технологий и технических средств.

Законный доступ к интернет-порталу осуществляется с помощью сети Интернет по сетевым адресам, позволяющим идентифицировать сайты. Вследствие этого интернет-порталы открыты для широкого круга

пользователей и обращение к ним возможно с любого устройства, подключенного к сети.

Интернет портал обладает множеством функций и сфер применения, что предполагает наличие различных информационных ресурсов, услуг в электронной форме и сервисов. В том числе интернет-портал обычно предусматривает средства поиска, навигации, перехода по внешним ссылкам к другим информационным системам. Примером является это обращение к сведениям через портал государственных услуг, размещенным в государственных и муниципальных информационных системах, с целью получения информации с ГАС «Правосудие».

Публикация на интернет-портале осуществляется единообразным способом, поэтому с точки зрения пользователя массив воспринимается как единое целое даже в случае обмена данными, которые обеспечивают взаимодействие между интернет-порталом и внешними информационными системами.

Правовой режим публичных государственных и муниципальных интернет-порталов основан на общедоступности информации и сервисов, которые предназначены для неопределенного круга лиц, обеспечении на бесплатной основе доступа к информации о деятельности органов государственной власти и местного самоуправления, судов в Российской Федерации.

По результатам исследования первой главы можно сделать ряд выводов и обобщений:

- сотовая связь предназначена для получения, передачи, хранения и использовании информации посредством использования технических средств и программных устройств. Использование сотовой связи, в том числе ее передача осуществляется с помощью базовых станций. Следует учесть, что предоставление услуг должно быть осуществлено на основании законности добровольности,

недопустимости нарушения прав и законных интересов потребителей услуг.

- предоставление сведений о международном идентификаторе сотового телефона имеет важное значение при расследовании и раскрытии преступлений, предусмотренными несколькими разделами УК РФ. Решение проблем для получения сведений об IMEI – номере должно осуществляться на международном уровне не только между странами, имеющими торговые отношения, но и государствами, использующими средства идентификация для защиты права и законных интересов пользователь услуг.
- применение IP-адресов и VPN осуществляется в целях предупреждения и пресечения международных и национальных преступлений в экономической и финансовой деятельности. Следовательно, правовое регулирования порядка производства расследований по указанным преступлениям должно осуществляться в соответствии с международными договорами и принципами международного права.
- предупреждение совершения преступлений, равно как и расследование и раскрытие преступлений сталкивается с проблемами осуществления идентификации устройств связи. Такие проблемы обусловлены отсутствием единого нормативного правового акта, регулирующего понятие и признаки сотовой связи, услуг связи, а также признаков идентификации сотовых телефонов и мобильных устройств, что во многом способствовало предупреждению совершения преступлений, а также защиты персональных данных граждан без нарушения принципа неприкосновенности частной жизни и тайные телефонных переговоров.
- под термин «дистанционное хищение» подпадают три состава преступлений: п. «г» ч. 3 ст. 158, ст. 159.3, ст. 159.6 УК РФ.

–

Глава 2 Виды и способы дистанционного мошенничества

2.1 Общая уголовно-правовая характеристика мошенничества

В 2021 году мошенничество стало одним из наиболее распространенных хищений – таким способом преступники завладели денежными средствами и имуществом других людей в 16.3% случаях. В результате в структуре преступности их доля увеличилась с 12,7% до 16,4%. Наиболее распространены мошенничества в Мурманской области (350,6 факта на 100 тыс. жителей), Республике Коми (345,2) и г. Москве (342,0), наименее – в Чеченской Республике (31,8), республиках Дагестан (63,3) и Ингушетия (68,2) [46].

В соответствии с ч. 1 ст. 159 УК РФ мошенничеством признается хищение чужого имущества либо приобретение права на чужое имущество путем обмана или злоупотребления доверием. ч. 2 ст. 159 УК РФ предусматривает квалификацию признаков мошенничества – таких как: совершение мошенничества группой лиц по предварительному сговору, лицом с использованием своего служебного положения либо причинение значительного вреда гражданину. В части 3 этой статьи перечислены три особо уважительных признака – это совершение мошенничества организованной в особо крупном размере группой либо лицом, ранее дважды и более судимым за растрату или вымогательство.

Анализ литературы и судебной практики показывает, что под мошенничеством законодатель понимает хищение чужого имущества или приобретение прав на чужое имущество путем обмана или злоупотребления доверием. Ответственность за данное преступление предусмотрена общей нормой (ст. 159 УК РФ) и рядом частных норм (ст.ст. 159.1-159.6 УК РФ) [23, с. 41].

В настоящее время современное определение «мошенничество» включает в себя множество противоправных действий в самых разных

сферах, включая банковскую деятельность, сотовую связь и современные информационные технологии. Несмотря на различия в технологиях, все эти действия имеют ряд общих характеристик:

- обманные действия;
- злоупотребление доверием;
- умышленное искажение фактов или умолчание;
- хищение чужой собственности;
- незаконное приобретение прав на чужую собственность [3, с. 7].

В целом мошенничество, исходя из недостаточного разнообразия трактовок этого понятия, следует понимать, как:

- право собственности – право собственности, которое является наиболее широким, включающим в себя все имущественные права: собственник имеет право владеть, пользоваться и распоряжаться своим имуществом в соответствии с гражданским законодательством;
- право собственности следует рассматривать как совокупность гражданско-правовых норм, регулирующих обязанности;
- имущественные права – вещные права получают лица, не являющиеся законными собственниками [22, с. 15].

В целом, исходя из законодательной трактовки мошенничества и доктринальных точек зрения, все же можно сделать вывод, что оно представляет собой все-таки не кражу в прямом смысле слова, а причинение вреда имуществу потерпевшего.

В большинстве случаев жертва мошенничества самостоятельно и добровольно передает свое имущество или права преступникам.

Исходя из определения мошенничества, можно выделить два вида мошенничества – хищение самого имущества и приобретение права на чужое имущество, а также указание на конкретные способы его совершения, отличающие мошенничество от других форм хищения. - мошенничество и злоупотребление доверием.

Некоторые авторы не считают хищением приобретение прав на чужое имущество путем мошеннических действий. Так, Шевченко Е.С. утверждает, что рассматриваемое деяние не является кражей, поскольку не связано с изъятием и (или) обращением чужого имущества в пользу виновного или других лиц. Особенность этого вида мошенничества заключается в том, что лицо, совершающее данный вид деяния, не присваивает чужое имущество, а лишь приобретает право на него. Таким образом, некоторые признаки хищения, перечисленные в юридическом определении, отсутствуют [48, с. 160].

Мошенничество относится к имущественным преступлениям, уголовный закон дифференцирует ответственность за такие преступления в зависимости от способа их совершения. Общая норма о мошенничестве часто подвергается реформированию законодателем, который то увеличивает санкции, то включает новые виды мошенничества, то исключает их из уголовного законодательства. Специальные нормы о мошенничестве были введены единовременно в Уголовный кодекс РФ Федеральным законом от 29 ноября 2012 г. № 207-ФЗ.

Мошенничество основано на знании психологии и стереотипов поведения человека и используется людьми, в данном случае мошенниками, которые ставят себя выше жертвы и намеренно игнорируют нормы морали. Стратегия и тактика мошенничества, как правило, хорошо продуманы. Они нацелены на достижение цели с минимальным риском для мошенника. Конкретные методы обмана могут быть самыми разными. Иногда это самые простые и примитивные уловки, но в некоторых случаях мошенники реализуют сложный план, действуют группой, постоянно двигая жертву по заранее запрограммированному пути, чтобы ввести ее в заблуждение [50, с. 76].

Мошенничеством по смыслу статьи 159 УК РФ является сообщение заведомо ложных сведений либо недопущение сведений, сообщение которых было обязательным при данных обстоятельствах. Обман может быть

активным или пассивным. При пассивном обмане человек умалчивает о фактах, которые он должен был сообщить. Вводящие в заблуждение действия могут принимать форму устного обмана, письменного обмана и активного обмана.

В настоящее время п. 2 Постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, хищении и растрате» определяет мошенничество как совершенное:

- путем сообщения ложных, не соответствующих действительности сведений;
- путем умолчания об истинных фактах;
- путем совершения умышленных действий, направленных на введение в заблуждение [32].

Его суть заключается в сознательном стремлении одного из партнеров создать у другого ложное представление о теме обсуждения. Обман всегда связан с умыслом, обманом, который необходимо установить при квалификации мошенничества. Отличительной особенностью данного преступления является то, что виновный путем обмана формирует у себя криминогенную ситуацию, позволяющую ему достичь своей цели. Обман необходимо воспринимать как покушение на истину, но обман есть не искажение самой истины, а создание определенного субъективного представления о ней, цель которого не только ввести другого человека в состояние иллюзии, а убедить его совершить определенные действия. Кроме того, обман может быть совершен через обманутую волю. В таких случаях потерпевший подвергается влиянию других людей, введенных в заблуждение.

Обращаясь к криминальной характеристике мошенничества, необходимо раскрыть его объективную сторону. Поэтому объективной стороной мошенничества является хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления

доверием. Действующее российское законодательство предусматривает два способа совершения мошенничества: обман и злоупотребление доверием [20, с. 190].

Объектом мошеннического преступления являются имущественные отношения, принадлежащие одному лицу или группе лиц. Общим объектом мошенничества, как состава преступления, предусмотренного главой 21 УК «Преступления против собственности», всегда являются общественные имущественные отношения между людьми в отношении материальных благ.

Отношения собственности – это, прежде всего, межличностные отношения в процессе общественного производства, обмена и потребления произведенного продукта, т. е. материальные (экономические) отношения. При этом они регламентированы и закреплены в нормативных актах. В результате эти отношения создают право собственности. Нарушая эти отношения, вы нарушаете защищенный законом закон, который определяет, является ли действие (например, мошенничество) незаконным [13, с. 52].

Существующие в Российской Федерации формы собственности (частная, государственная, муниципальная) должны быть признаны непосредственным предметом мошенничества.

Одним из наиболее сложных элементов преступления при его расследовании является установление субъективной стороны преступления.

Субъективная сторона преступления традиционно определяется в науке уголовного права как психическое отношение субъекта к своему общественно опасному деянию и его последствиям в виде умысла или неосторожности [11, с. 130].

Мошенничество, как и другие виды хищений, всегда совершается с прямым умыслом. Преступник, руководствуясь корыстной целью и мотивом, осознает, что он незаконно завладел чужим имуществом или получил право собственности, путем обмана, предвидит, что в результате его действий чужое имущество будет обращено в его пользу, либо в пользу других лиц,

которые не имеют права собственности на это имущество, либо приобретают право собственности и желают его [7, с. 24].

Субъектом является физическое лицо, возраст которого на момент совершения преступления достигает не менее 16 лет. Кроме того, субъектом может быть признано лицо, занимающее определенную должность, совершившее деяние с использованием своего служебного положения [17, с. 13].

Субъективной стороной является вина в виде прямого умысла и корыстной цели. Человек осознает, что завладевает чужим имуществом незаконно, путем обмана или злоупотребления доверием. Кроме того, обязательным признаком субъективной стороны данного преступления является корыстная цель, заключающаяся в обращении имущества преступника в свое собственное. В основе корыстного мотива лежит стремление преступника удовлетворить свои материальные потребности за счет других путем конфискации имущества, на которое он не имеет права.

Характерным признаком мошенничества является как бы добровольная передача имущества или прав на него виновному лицу. Потерпевший, действуя под влиянием обмана, либо передает имущество потерпевшему, либо предлагает третьему лицу передать имущество, принадлежащее потерпевшему, виновному. Он может осудить имущество, которым уже владеет или ранее передано ему с какой-то целью (но не в собственности). При этом потерпевший как бы добровольно, без давления со стороны виновного (или третьих лиц) передает ему свое имущество или права. Без участия потерпевшего (пусть и неосознанного, механического) такая передача права собственности из одних рук в другие просто невозможна.

Объектом мошенничества может быть только чужое имущество, то есть имущество, которое не находится в совместной, долевой или законной собственности самого мошенника. Похищенное имущество другого лица следует понимать, как имущество, которое не является собственностью или иным законным владением преступника. Таким образом, чужое имущество –

это имущество, на которое мошенник не имеет законных прав. В случае мошенничества автор с целью завладения чужим имуществом или правом на него использует обман лица, владеющего, владеющего или распоряжающегося имуществом, после чего это лицо, введенное в заблуждение, добровольно уступает право собственности автору [9, с. 24].

Как отмечает Пильников С.Г., мошеннические действия являются преступлениями новой формации, становятся дистанционными и совершаются в большей мере с использованием информационно-коммуникационных систем [28, с. 13].

Калюжный А.Н. отмечает, что «дистанционное мошенничество, с одной стороны, является результатом эволюции традиционного мошенничества, поскольку некоторые его виды встречаются в Интернете без каких-либо серьезных изменений в методике реализации преступного замысла; с другой стороны – это качественно новая группа преступлений, так как при схожести методов реализации конкретные способы имеют существенные отличия» [11, с. 118].

Дистанционное мошенничество – это мошенничество, совершаемое с помощью компьютеров, информационных технологий, вводящее в заблуждение потерпевшего с целью получения его имущества на расстоянии [29, с. 123].

Дистанционное мошенничество предполагает наличие интеллектуально-информационного аспекта в деятельности мошенника. В результате воздействия на волю потерпевшего виновный достигает намеченной цели [26, с. 16].

Необходимо констатировать тот факт, что виновный очень часто выдает себя за профессионала в какой-либо сфере деятельности, банковского служащего, оператора мобильной связи и других лиц в зависимости от легенды, которую он использует для воздействия на потерпевшего.

Исходя из способов совершения такого рода мошеннических действий, считаем, что лица, совершившие такие преступления, обладают высокими

навыками убеждения, находчивостью, природной изобретательностью, неотъемлемым признаком является хорошо развитая устная речь, посредством которой потерпевший вводится в заблуждение. Поскольку в процессе совершения мошеннических действий активно используются достижения научно-технического прогресса, логично предположить, что это лица в возрасте от 18 до 35-40 лет, активно использующие гаджеты с доступом в Интернет.

Непосредственным объектом дистанционного мошенничества является собственность конкретных физических и юридических лиц [47, с. 22].

С одной стороны, в случае мошенничества, это имущество, а с другой – право собственности.

Объективная сторона является составной частью состава преступления, характеризующего внешнее проявление конкретного общественно опасного поведения, причинившего вред объекту, охраняемому уголовным законом.

Объективная сторона мошенничества имеет важное значение для квалификации. Некоторые преступления можно отличить только по признакам объективной стороны [27, с. 19].

Мошенничество считается оконченным с момента, когда имущество фактически незаконно передано во владение виновного и он имеет возможность использовать или распоряжаться им по своему усмотрению, а также с момента, когда право на имущество потерпевший незаконно передан виновнику [30, с. 42].

Например, при наличии объективных признаков мошенничества с использованием электронных средств платежа в отношении денежных средств, находящихся на банковском счете (иной кредитной организации), клиент, открывший такой счет, имеет право свободно распоряжаться денежными средствами. Если лицо, не имеющее права распоряжаться указанными денежными средствами, отдает такое распоряжение и денежные средства списываются со счета владельца счета в корыстных целях, переводятся на счет другого лица, «учитываются» и, как следствие, владелец

(или лица уполномочен управлять от имени собственника) теряет над ними контроль, поэтому речь должна идти не о приобретении прав, а о хищении чужого имущества [36, с. 44].

Субъект удаленного мошенничества: вменяемое лицо, достигшее шестнадцатилетнего возраста, есть исключение, в этом случае субъектом может быть только лицо, занимающее служебное положение [41].

Субъективная сторона мошенничества с дистанционными электронными платежами выражается в прямом умысле и корыстной цели [45].

Таким образом, мошенничество является одним из наиболее распространенных общественно опасных деяний, ущемляющих право собственности. Уголовный кодекс Российской Федерации устанавливает несколько признаков, квалифицируемых как мошенничество. Появление новых современных видов мошенничества, отличающихся нетрадиционными способами совершения, диктует необходимость их целенаправленного изучения.

2.2 Характеристика отдельных видов и способов дистанционного мошенничества

Мошенничество с использованием информационных технологий находятся в динамике, то есть с течением времени появляются новые способы мошенничества, другие же мошеннические схемы постепенно теряют свою актуальность, это обуславливается работой служб безопасности организаций, изменением политики сервисов, в том числе и работой правоохранительных органов. Именно поэтому необходимо производить постоянный мониторинг и исследование новых методов и способов мошенничества [19, с. 227].

Преступники используют различные способы обмана и мошенничества, что вынуждает законодателя корректировать уголовное

законодательство. Так, Федеральным законом от 23 апреля 2018 г. № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» внесены изменения в ст. 159.3 (мошенничество с электронными средствами платежа), 159.6 (мошенничество с компьютерной информацией), связанные с незаконными действиями преступников с электронными деньгами потерпевших.

В рамках выпускной квалификационной работы проведем анализ специфических видов и способов совершения дистанционного мошенничества:

Дистанционное мошенничество со взломом страниц социальных сетей. Конституцией РФ предусмотрено право на неприкосновенность частной жизни, а также на защиту тайны переписки и телефонных переговоров. Данное право охраняется не только нормами конституционного, но и уголовного права. Уголовная ответственность на нарушение права на неприкосновенность частной жизни предусмотрена ст. 137 и 138 УК РФ.

Одним из распространенных преступлений, связанных с нарушением неприкосновенности частной жизни, является взлом страниц в социальных сетях, в том числе незаконное чтение чужой переписки. Однако при совершении указанных преступлений потерпевший и преступник могут находиться, как в одном, так и разных городах. Одними из способов мошенничества посредством взлома социальных сетей являются: незаконное списание денежных средств с банковских карт, покупки в сети «Интернет» от имени пользователя. При этом деяние считается уголовно – наказуемым, если преступник осуществляет несанкционированный доступ к определенным программам. Однако специфика совершения преступлений в социальных сетях в настоящее время не нашла своей отражение, ни в диспозициях, ни в санкциях уголовно – правовых норм [37, с. 101].

Особенностями совершения преступлений, связанных со взломом социальных сетей являются: молодой возраст лиц, совершающих преступления и лиц, пострадавших от их совершения; анонимность, большой

масштаб совершения; принципы построения и изменения способов использования социальных сетей, что приводит к разработке новых способов и методов, а также новых видов мошенничества.

На данном этапе особенности и признаки такого преступления еще не нашли своего прямого отражения в Уголовном Кодексе Российской Федерации. Однако, автор считает, что преступные посягательства, совершаемые в рамках новых беспрецедентных условиях – должны рассматриваться индивидуально. Первой проблемой можно назвать вопросы квалификации такого преступления по статье 159 УК РФ или 159.6 УК РФ.

Для уточнения этого положения необходимо рассмотреть содержание этих статей. Статья 159 УК РФ содержит следующие признаки преступления: во-первых, две формы совершения – хищение чужого имущества и приобретение права на чужое имущество путем обмана или злоупотребления доверием, и во-вторых – способы владение, такое как обман или злоупотребление доверием. Статья 159.6 УК РФ аналогична основному составу преступления тем, что как обычное мошенничество, так и компьютерное мошенничество всегда являются хищением чужого имущества или приобретением права на чужое имущество путем обмана или злоупотребления доверием.

Соответственно мошенничество в социальных сетях также содержит в себе этот первый признак. Далее следует говорить о различиях. Статья 159.6 УК РФ предусматривает использование электронных технологий и техники. Хоть мы и говорим о том, что в первую очередь совершение такого преступления возможно исключительно посредством использования современных компьютерных технологий, статья содержит в себе прямое уточнение, каким именно образом это возможно, а именно «…путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей» [31, с. 10].

Таким образом, рассматривая данное преступление с точки зрения действий лица, которые он совершает с компьютерной информацией. Постановление Пленума Верховного Суда Российской Федерации дано разъяснения в постановлении от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», поясняет, что 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) и т.д. [31].Однако, если говорим о мошенничестве, совершаемом в социальных сетях, для изменения данных и воздействия на потерпевших не всегда обязательно использование специальных программных средств. Например, чтобы использовать чужой аккаунт в социальных сетях для мошеннических действий. Если рассматривать данное деяние, как использование учетных данных собственника или иного владельца имущества независимо от способа получения доступа к таким данным, то Верховный Суд Российской Федерации рекомендует квалифицировать такое деяние по статье 158 УК РФ «Кража». Нам представляется это не совсем корректным, в виду несоответствия способа совершения преступления «путем обмана или злоупотребления доверием».

Таким образом, квалификация по статье 158 УК РФ – не корректна, квалифицировать по статье 159 УК РФ, это значит снизить общественную опасность данного деяния, поскольку статья 159.6 УК РФ является квалифицированным составом. Диспозиция же статьи 159.6 УК РФ не в полной мере соответствует совершенному деянию.

Таким образом, детально УК РФ рассматривает дистанционное мошенничество, связанное со взломом страниц социальных сетей лишь во взаимосвязи со ст. 159. 6 УК РФ, предусматривающей уголовную ответственность только к привязке к компьютерной информации, то есть за

совершение вмешательства посредством ввода, удаления, блокировки или модификации информации. Однако применение указанных норм не является обоснованных по отношению к преступлениям, связанных со взломом страниц в социальных сетях, которые совершаются посредством обмана и злоупотребления доверием с целью получения денежных средств.

Одними из способов совершения дистанционного мошенничества, связанного со взломом страниц социальных сетей, является финансовое или маркетинговое и нефинансовое мошенничество. Указанная классификация представлена В.А. Смирновым, который к указанным видам мошенничества относит: получение обманным способов идентификационных сведений об электронных платежных системах, в то числе электронном кошельке, сообщение ложных сведений для получения денежных средств, заведомо ложное предложение о получении заемных средств, предоставлении кредита, а также предложение об увеличении капитала [37, с. 101].

Другие авторы, такие как А. Шеслер к видам мошенничества, связанным со взломом страниц социальных сетей относят: взлом страницы и собирание денежных средств на помощь «близким», переход по ссылке и отправка зараженных сайтов, осуществление предоплаты за приобретение товара, а также предложение «легкого» дополнительного заработка [49, с. 67].

К основным и наиболее распространенным способам мошенничества, связанных со взломом страниц социальных сетей относятся: мошенничество под чужим именем, использование актуальной новостной информации, которая может быть распространена в наиболее глобальных масштабах, «романтическое» мошенничество, мошенничество в сфере услуг, создание фейковых опросников. Мошенничество под чужим именем и создание фейковых опросников можно объединить в одну группу, поскольку при использовании данного метода создается фейковый аккаунт известной медийной личности путем распространения ложной информации, проведения опросов. К тому же указанный способ предполагает рассылку сообщений

контактам пользователя с просьбой об оказании финансовой помощи. Такой способ является наиболее популярным и «эффективным», поскольку информация поступает от знакомого лица, уровень доверия к которому наиболее велик.

Следует учесть, что наиболее эффективным способом борьбы с мошенничеством, связанным со взломом страниц в социальных сетях является проверка персональных данных и усиления уровня защиты аккаунтов. Такие меры могут использоваться путем обращения к администрации социальных сетей с указанием «подозрительных» страниц и пользователей.

Таким образом, мошенничество в социальных сетях на данный момент является новым видом преступления, содержащим в себе ряд признаков, пока не охватываемых действующими составами преступления.

Дистанционное мошенничество через сайты объявлений. Одним из самых распространенных способов мошенничества, который основан на доверии, является размещение объявлений о продаже товаров на электронных досках объявлений. Одной из причин совершения данного преступления является привлечение граждан заниженными ценами и выгодными предложениями. При этом способом оплаты товаров и услуг является перечисление денежных средств на электронный кошелек.

Фишинг представляет собой один из способов введения пользователь сети «Интернет» в заблуждение с использованием поддельного сайта. Такой сайт может виртуальной имитировать банковскую систему. Однако при пользовании услугами сайта пользователям необходимо предоставить персональные данные. Одним из распространенных форм фишинга являются: спам, рассылка поддельных писем, реклама товаров и услуг, а также «выуживание» отсканированных документов пользователей для их последующего применения [38].

Одной из задач спама является запугивание пользователей проблемами с платежными системами, путём требования предоставления информации,

связанной с разблокировкой счета или проведением каких – либо транзакций. При этом пользователи осуществляют немедленную авторизацию, предоставляя необходимую информацию для совершения мошеннических действий.

Еще одной разновидностью фишинга является рассылка поддельных писем, которая заключается в том, что от имени банка производится рассылка писем с просьбой уточнить номер или данные авторизации, отправив их по адресу, указанному на интернет – сайте.

Реклама товаров и услуг, которые размещены на досках объявлений в сети «Интернет», также является способом совершения мошенничества. Данный вид мошенничества осуществляется путем размещения сайтов о товарах или услугах, для ознакомления с которыми пользователям необходимо перейти на сайт фирм – однодневок, использующих персональные данные пользователем для совершения незаконных финансовых операций.

Так называемое «выуживание» у пользователей сканы документов, позволяющих идентифицировать граждан, предполагает последующее оформление кредитов от имени пользователя. Способом такого мошенничества является СМС – рассылка информации о выигрыше в лотерее или интернет – лотерее при дальнейшем переходе пользователей на подложный «Интернет – сайт». Для применения данного способа мошенники используют логотипы известных компаний, а также стиль оформления и схожие электронные адреса. При этом в СМС – рассылке мошенники просят провести проверку персональных данных для устранения рисков либо подозрительной активности аккаунтов, либо подозрительной активности при использовании платежных систем переводов [38].

Также на сегодняшний день одни из популярных способов дистанционного мошенничества является на способ совершения мошенничества, посредством использования сервиса «Авито доставка».

В данной системе и работают мошенники, они осуществляют свои действия некоторыми способами:

- подмена товара. Суть данной схемы заключается в следующем. Злоумышленник находит на сервисе «Авито» нужный ему товар, находящийся в другом городе, связывается с продавцом и предлагает отправить товар через сервис «Авито доставка», продавец отправляется на почту, почтовый сервис (сервисов, оказывающих данную услугу достаточно большое количество, например, в Нижнем Новгороде их около 100 шт.) и отправляет товар. Покупатель же, получая уведомление о поступлении посылки в свой город отправляется для приемки товара, во время проверки своей покупки он попросту подменяет товар на схожий, например, дорогостоящие компьютерные комплектующие (процессоры, видеокарты, оперативную память) на их дешёвые аналоги, существенно уступающие, как в техническом, так и в материальном качестве. Подменить можно, например, и одеж ду, то есть любой товар на сходный. Таким образом, покупатель получает желаемый товар, при этом отправляя продавцу «подменный товар», как не отвечающий требованиям и получает свои деньги обратно. Данная схема достаточно распространена, в сети «Интернет» присутствует огромное количество историй мошенничества с помощью «подмены товара».
- требование предоплаты. Данная схема используется не только в «Авито доставке», но в любом сервисе покупок. Суть её заключается в требовании продавца отправить ему денежные средства в качестве предоплаты за товар, которая составляет 10-20 % от суммы товара, объясняет он это необходимостью быть уверенным в покупке товара, так как на товар претендует несколько «потенциальных покупателей», которых попросту не существует. После перечисления покупателем предоплаты за товар, продавец

исчезает, перестаёт выходить на связь. Продавец может даже не обладать «продаваемым» товаром, а позаимствовать фотографии в сети «Интернет», кроме этого, мошенники используют поддельные аккаунты «Авито», с ложными отзывами и продажами, чаще всего данные аккаунты покупаются у других лиц.

– использование подставных сайтов. По нашему мнению, данная схема является наиболее распространенной, так как не требует от злоумышленника очного посещения организаций [52, с. 55].

Проанализируем примеры из судебной практики по данному виду дистанционного мошенничества. Реализуя совместный корыстный преступный умысел, Анчугов И.Л., в дневное время, находясь по месту проживания, со своего мобильного телефона «Honor 8C» зашел на сайт бесплатных объявлений «Авито», зарегистрировался под вымышленным именем «Дмитрий» и разместил объявление о продаже мобильного телефона «iPhone 7 plus, 128 gb». Далее совместно с Мамонтовым В.А. стал ждать звонка предполагаемого покупателя. По номеру телефона, указанному Анчуговым И.Л. в объявлении, позвонила ранее ему незнакомая N у которой Анчугов И.Л. и Мамонтов В.А., действуя по предварительной договоренности, решили похитить принадлежащие ей денежные средства [30]. С этой целью Анчугов И.Л., действуя по предварительному сговору с Мамонтовым В.А., согласно отведенной ему роли, заведомо не собираясь продавать указанный в объявлении мобильный телефон «iPhone 7 plus, 128 gb», в ходе телефонного разговора предложил N перечислить денежные средства в качестве оплаты по ссылке, которую готов выслать ей посредством телекоммуникационной сети Интернет в приложении «WhatsApp». После оплаты приобретенного товара, указанного в объявлении, доставить купленный ФИО13 мобильный телефон «iPhone 7 plus, 128 gb» службой «Авито-доставка». На данное предложение Анчугова И.Л. введенная в заблуждение N согласилась. После чего, посредством телекоммуникационной сети Интернет в приложении «WhatsApp» Анчугов

И.Л. отправил N созданную им самостоятельно поддельную ссылку для перевода денежных средств «Авито-доставка», к которой была подключена Яндекс-карта, зарегистрированная на имя Анчугова И.Л. Не подозревая о совместных преступных намерениях Анчугова И.Л. и Мамонтова В.А., обманутая и введенная в заблуждение N, используя телекоммуникационную сеть Интернет, со своего мобильного телефона «iPhone SE», получив от Анчугова И.Л. вышеуказанную поддельную ссылку для перевода денежных средств, осуществила оплату покупки мобильного телефона «iPhone 7 plus, 128 gb» и перевела принадлежащие ей денежные средства со счета своей банковской карты на электронное средство платежа Анчугова И. Л. – Яндекс-карту. После этого Мамонтов В.А., действуя по предварительному сговору с Анчуговым И.Л., согласно ранее распределенных ролей, после перевода денежных средств в сумме 14179 рублей 55 копеек Анчугова, перевел данные денежные средства путем приобретения и продажи криптовалюты – Биткоинов на неустановленном следствием сайте сети Интернет на банковскую карту Анчугова И.Л., впоследствии распорядившись похищенным совместно по своему усмотрению.

Судом Мамонтов В.А. и Анчугов И.Л., были признаны виновными в совершении преступления, предусмотренного ч. 2 ст. 159 УК РФ «Мошенничество, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину», виновным было назначено наказание в виде лишения свободы на срок 11 месяцев 14 дней, с отбыванием наказания в колонии-поселении [30].

Таким образом, обобщая вышесказанное, можно прийти к выводу, что дистанционное мошенничество через сайты объявлений с использованием ложных ссылок является наиболее общественно опасным, так как вводит потерпевшего в заблуждение. Также данный способ мошенничества является латентным, так как не всегда потерпевший из-за нескольких тысяч рублей готов отправляться в органы внутренних дел, во многом из-за недоверия правоохранительной системе и нежелании тратить своё время, тем самым

оставляя злоумышленников безнаказанными. Справедливо отметить, что при использовании злоумышленников должных мер защиты и анонимности вычислить его достаточно проблематично. По нашему мнению, большинство граждан, привлечённых к ответственности являются «новичками» в данной сфере, а профессионалы остаются безнаказанными.

Дистанционное мошенничество с банковскими картами. Отличительная черта этого вида мошенничества – таргетированность на конкретные группы граждан: конечной целью злоумышленников является перевод средств жертв на их счета, при этом средства ее достижения варьируются.

Проанализируем наиболее популярные виды мошеннических действий с использованием банковских карт:

- скимминг – похищение реквизитов платежной карты при помощи скиммера. Скиммер представляет собой устройство, снимающее с магнитной полосы данные карты, а ПИН-код получают при помощи мини-камеры. С помощью данного устройства в расположении мошенников оказываются все данные, которые помогают реализовать денежные средства картой-клоном потерпевшего;
- ливанская петля – вид мошенничества, когда в картоприемник вставляется устройство, которое удерживает карту от возврата её владельцу. Возле жертвы мошенничества появляется прохожий, который рассказывает о похожей ситуации и сообщает, что нужно набрать определенную комбинацию и ввести ПИН-код. Жертва мошенничества сообщает ПИН-код мошеннику, но после того, как комбинация не помогла, тот же самый человек советует немедленно обратиться в банк. Тем временем карта изымается из устройства и с нее списываются денежные средства.
- вишинг – средство совершения мошеннических действий при помощи телефона. Клиенту поступает звонок от «сотрудника» банка, который предупреждает его о попытке незаконного списания

денежных средств со счета клиента и просит позвонить на указанный им номер. Соответственно, клиент, позвонив по данному номеру, попадает к подставному сотруднику банка, который просит указать данные платежной карты.

– траппинг – мошенничество с использованием банкомата. В банкомат устанавливается специальное задерживающее устройство, в результате вставленная в него платежная карта застревает. Мошенники, находящиеся поблизости, подсматривают ПИН - код и пока жертва идет в банк, чтобы решить данную проблему, просто достают карту и снимают все денежные средства.

Способами получения денежных средств при совершении указанных видов преступлений является обналичивание денежных средств. Например, лицо, совершившее преступление по хищению денежных средств с электронного счета, может перечислить средства на банковских счет и впоследствии обналичить их путем получения. Следует учесть, что преступные действия при совершении мошенничества были реализованы посредством удаления персональных данных о собственнике банковского счета, что само по себе затрудняет реализацию права собственности на денежные средства, находящиеся в кредитных организациях [21, с. 45].

Мошенничество, совершенное под предлогом предотвращения списания денежных средств или разблокировки банковской карты, в теории и практике уголовного права классифицируют по ст. 159. 3 УК РФ, то есть мошенничество с использованием электронных средств платежа. В свою очередь под электронным средством платежа в соответствии с п. 19 ст. 3 Федеральный закон от 27.06.2011 № 161-ФЗ (ред. От 02.07.2021) «О национальной платежной системе» (с изм. и доп., вступ. в силу с 01.12.2021) следует понимать средства, с помощью которых пользователь может удостоверять, передавать распоряжения в целях перевода денежных средств, осуществляющих посредством безналичных расчетов и электронных систем.

Мошенничество, предусмотренное ст. 159.6 УК РФ отличается от мошенничества по ст. 159.3 УК РФ широкой сферой применения, то есть предметом совершения преступления. Если предметом мошенничества и использование банковских счетов являются денежные средства, то предметом мошенничества с использованием информационных технологий осуществляется и использованием самого права на владение банковскими счетами и платежными системами.

В 2018 году в часть 3 статьи 158 УК РФ внесены изменения и дополнения пунктом «д», которым предусмотрена ответственность за тайное хищение чужого имущества с банковского счета, а также в отношении электронных средств (при отсутствии признаков преступления, предусмотренного ст.159.3 УК РФ).

В связи с этим уточнение в постановлении Пленума Верховного Суда РФ от 30.11.2017 № 48: если лицо похитило денежные средства с использованием персональных данных владельца платежной карты (ПИН-кода), то действия преступника должно квалифицироваться как кража. Эти нововведения создали конкуренцию между статьей 159.3 УК РФ и пунктом «г» части 3 статьи 158 УК РФ.

Посмотрим, как эти акты разграничиваются на практике. Так, гр. Б. был осужден за совершение преступления, предусмотренного ч. 1 ст. 159.3 УК РФ. Преступление было совершено при следующих обстоятельствах: с. Б. в ночь с 28 на 29 июня 2019 г. прошел возле дома гр. А. и увидел его скутер. Подойдя к скутеру, он увидел ключи в замке зажигания и решил сесть на него. Приехав в кафе «Вегас», он оставил самокат на стоянке и зашел в кафе, где пробыл некоторое время и решил пойти домой. Когда он ехал домой, скутер начал глохнуть, поэтому гр. Б. остановился на заправке и решил посмотреть, что в бардачке. В нем он нашел черный кошелек, в котором находилась банковская карта N на имя гр. А. Гр. Б. знал пин-код, так как ранее, когда с гр. А. выпил алкоголь, последний отправил его в магазин и дал ему эту карту, сказав пин-код.

Сначала впервые заправил 2-х литровый скутер примерно за 80 рублей, а при оплате понял, что есть деньги, которые можно потратить на свои цели. В связи с этим он пошел дальше и решил купить алкоголь, зашел в кафе, начал употреблять алкоголь. При этом он расплатился картой, принадлежащей гр. А. По этой карте он сделал около семи или восьми покупок пива, пока не закончились деньги. После этого он положил карту обратно в кошелек в бардачке скутера [29, с. 124].

Или, гр. М. совершил кражу, то есть тайное хищение чужого имущества с причинением значительного ущерба гражданину (п. «д» ч. 3 ст. 158 УК РФ) (при отсутствии признаков состава 253 преступления, предусмотренного ст. 159.3 УК РФ), с банковских счетов, при следующих обстоятельствах: 28.07.2019 гр. М., имея разовый постоянный умысел, направленный на тайное хищение денежных средств, действуя из корыстных побуждений, с использованием принадлежащих гр. Н. банковской картой ПАО Сбербанк с технологией бесконтактной оплаты, оплачены покупки банковской картой в магазинах Пятерочка, M-Style и др. на общую сумму 12 263 руб. 99 копеек, распорядился ими по своему усмотрению, чем причинил значительный ущерб потерпевшему на указанную сумму [29, с. 125].

Поступки, идентичные с объективной точки зрения, квалифицируются по-разному. Такое разнообразие репрессивных практик рассматриваемого состава преступления свидетельствует об отсутствии единого понимания признаков данного преступления. В первом случае суд признал наличие обмана в действиях подсудимого, а во втором – его отсутствие.

Полагаем, что для четкого разграничения смежных преступлений, таких как хищение имущества с банковского счета и мошенничество с использованием электронных средств, Верховному Суду РФ необходимо уточнение и уточнение. Так, в постановлении Пленума Верховного Суда Российской Федерации от 27 декабря 2002 г. № 29 «О судебной практике по делам о кражах, грабежах и грабежах» необходимо уточнить, что следует понимать под хищением банковского счета, а также в отношении

электронных денег. В п. 17 Постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, хищениях и растратах» следует уточнить, что следует понимать под «молчанием о незаконном владении платежной картой», то есть при мошенническом приобретении товара в коммерческой организации при оплате чужой банковской картой, когда сведения о владельце не уточняются продавцом и не сообщаются покупателем.

Выводы по второй главе:

- уголовное законодательство Российской Федерации содержит запрет на мошенничество – то есть хищение чужого имущества или приобретения права на чужое имущество путем обмана или злоупотребления доверием.
- дистанционное мошенничество, как один из видов преступления не детализирован ни нормам УК РФ, ни нормами действующего законодательства. Разработка понятий и способов совершения мошенничества в настоящее время находится исключительно на доктринальном уровне, что приводит к различным проблема квалификации преступлений.
- виды и способы дистанционного мошенничества, которые следует относить к способам совершения преступления классифицируются не только по различным нормам УК РФ, но и имеют различный родовой объект совершения преступления
- особенность рассматриваемых способов совершения дистанционного мошенничества, которая заключается в том, что в качестве мер борьбы с преступностью относятся не меры принуждения или установление запрета на свершение определенных действий, а меры профилактики, которые размещаются на интернет- порталах официальных сайтов правоохранительных органов.

– проблемы уголовно-правовой квалификации заключаются не только в отсутствии уголовно-правовых норм, предусматривающих способы конкретного дистанционного мошенничества, но и в привлечении к уголовной ответственности за данный вид преступления, в том числе и назначения наказания.

Глава 3 Особенности расследования дистанционного мошенничества

3.1 Некоторые особенности выявления дистанционного мошенничества первоначального этапа расследования

Раскрытие и расследование мошенничеств, совершенных дистанционным способом, остается довольно сложной задачей. Имеющиеся проблемы обусловлены двумя основными факторами – техническим аспектом и сложностью установления лица, подлежащего привлечению к уголовной ответственности [2, с. 14].

Отличительной чертой данного вида преступлений является совершение преступлений издалека, в ходе которых их раскрытие и расследование основывается на своевременном проведении комплекса оперативно-розыскных, следственных мероприятий, направленных на документирование преступной деятельности лиц. совершение преступления, проведение детального анализа используемых преступниками расчетных счетов, абонентских номеров, мобильных устройств, интернет-сайтов.

Существующая следственная и судебная практика свидетельствует о недостаточной эффективности работы органов дознания при расследовании уголовных дел по анализируемой категории преступлений [5, с. 228].

В делах о дистанционном мошенничестве самым сложным в организации является начальный этап расследования. Последовательность и тактические особенности производства следственных действий, направленных на выявление указанных мошенничеств, во многом определяются следственными ситуациями, складывающимися на начальном этапе [6, с. 227].

На данном этапе очень часто при получении сведений о совершении мошеннических операций неизвестным практическим органам способом уголовное дело возбуждается без достаточных оснований или, наоборот, с

предварительным длительным ознакомлением с материалами, имеющими признаки преступления.

Изучение следственной практики показывает, что ключевыми факторами, влияющими на рост нераскрытых преступлений указанного вида, являются:

- отсутствие поэтапного алгоритма следственных и оперативно-розыскных действий, которые необходимо проводить по сложившейся следственной обстановке на первоначальном этапе расследования;
- несвоевременное реагирование на заявления и сообщения о преступлениях;
- срок выяснения оснований для возбуждения уголовного дела;
- многолетнее выполнение банками, организациями, оказывающими услуги через сеть Интернет и сотовую связь, запросов о предоставлении криминалистической информации, имеющей значение для уголовного производства;
- отсутствие отлаженных механизмов реагирования и расследования приводит к тому, что следственные органы склонны отказываться от возбуждения таких уголовных дел, чтобы не снижать раскрываемость;
- отсутствие реальной возможности привлечения к участию в производстве следственных действий специалистов, обладающих знаниями в соответствующей области знаний;
- во многих случаях для получения криминалистически важной информации, которая могла бы помочь в раскрытии преступлений, следователям необходимо взаимодействие с банковскими учреждениями, находящимися за пределами России, а также оперативная помощь зарубежных коллег, что затруднительно, а иногда и невозможно из-за отсутствия договорные отношения между странами [7, с. 52].

Эти концептуальные проблемы во многом приводят к сужению комплекса следственных и иных процессуальных действий, проводимых на рассматриваемой и последующих стадиях, а также к ненадлежащему сбору доказательств и иных криминалистически значимых сведений по уголовному делу, что не позволяет выявить состав преступления. лица, совершившие анализируемые преступления. Поэтому изучение организационно-тактических особенностей начального этапа дистанционного расследования мошенничества, выявление типичных следственных ситуаций для эффективного раскрытия и расследования преступления, выявление мошенника, действующего дистанционно, имеет важное значение для противоправной деятельности.

Деятельность следователя или дознавателя на первоначальном этапе расследования уголовных дел данной категории заключается в последовательном выполнении действий по оценке и анализу полученных сведений о преступлении, проверке заявления или сообщения, содержащих сведения о преступном деянии, которые наступило, вынесение процессуального решения о возбуждении уголовного дела, а также процессуальное оформление этого решения, уведомление прокурора и заявителя о возбуждении уголовного дела [8, с. 75].

Изучение судебно-следственной практики по уголовным делам данной категории позволило сделать вывод о том, что на первоначальном этапе расследования складываются следующие типичные следственные ситуации:

- потерпевший сообщил о признаках мошенничества с использованием методов социальной инженерии. Подозреваемый установлен и арестован;
- потерпевший сообщил о признаках мошенничества с использованием методов социальной инженерии. Подозреваемый арестован, но отрицает свою причастность к преступлению;

– потерпевший сообщил о признаках мошенничества с использованием методов социальной инженерии. Информация о личности подозреваемых отсутствует;
– в результате оперативно-розыскных мероприятий выявлены признаки мошенничества с использованием методов социальной инженерии. По предварительной информации о преступлении установлены сведения о личности подозреваемого (подозреваемых), а также механизм следственной деятельности, подозреваемые не задержаны, данные о личности подозреваемого потерпевшего отсутствуют. Такая ситуация возникает, когда жертва не знает о мошеннических операциях, совершенных против нее [9, с. 54].

Далее рассмотрим последовательность следственных действий и иных процессуальных мероприятий в ходе предварительного расследования в рамках возбужденного уголовного дела по факту совершения дистанционного мошенничества, когда на телефон потерпевшего поступает телефонный спам-звонок в целях получения конфиденциальной информации о банковском счете и похищения денежных средств с его банковского счета.

Следователь либо дознаватель имеет возможность, обратившись к общедоступным базам данных, установить первоначальную информацию, необходимую для дальнейшего производства по уголовному делу на первоначальном этапе предварительного расследования, используя информацию об операторах сотовой связи интернет-услуг, организациях, предоставляющих услуги IP-телефонии, доменных имен, хостингов и др.

С целью сокращения времени, необходимого для производства по уголовному делу на первоначальном этапе предварительного расследования, и с учетом соблюдения разумных сроков уголовного судопроизводства для установления первоначальной информации, имеющей доказательственное значение по уголовному делу, следователь (дознаватель) может инициативно истребовать у потерпевшего выписку о движении безналичных денежных средств по его банковскому счету и установить, куда они были перечислены

с его счета. В кратчайшие сроки потерпевший также может инициативно по указанию должностного лица, производящего предварительное расследование, получить информацию от оператора связи о телефонных соединениях со злоумышленником.

При этом необходимо отметить ряд технических сложностей, возникающих при расследовании данной категории дел, которые следователь (дознаватель) не имеет возможности решить самостоятельно в сжатые сроки:

- проведение оперативно-розыскных мероприятий в рамках оперативно-розыскной деятельности по установлению организаций, оказывающих злоумышленникам услуги IP-телефонии (Voice overIP-телефонии) и искусственного изменения входящего номера телефона (спуфинг);
- установление местонахождения подозреваемого в случае использования VPN-шифрования каналов интернет-связи;
- усложненная процедура получения личной информации об абоненте по номеру международного идентификатора (IMEI) мобильного устройства с учетом необходимости соблюдения конституционных прав и свобод граждан;
- вопросы оперативной блокировки банковских счетов и банковских карт с учетом необходимости получения судебного разрешения на указанную операцию [11, с. 120].

Несмотря на имеющиеся сложности, следователь (дознаватель) имеет возможность самостоятельно установить предварительную информацию об актуальном операторе связи, смене оператора связи, абонентском номере телефона звонящего, устройстве для звонков (телефон, планшет, компьютер и т. д.) путем использования программных средств, представленных на интернет-сайтах: www.zniis.ru; www.htmlweb.ru и др. После чего направить запросы актуальным операторам связи, предоставляющим в том числе услуги IP-телефонии злоумышленника использующим средства связи для совершения дистанционного мошенничества.

В рамках исследовательской работы отметим ситуации дистанционного мошенничества с использованием интернет-соединений, когда необходимо установить IP-адрес точки выхода в интернет, с которой подозреваемый в преступлении совершал противоправные действия. В такой ситуации возможно использование информации с сайта https://who.is/, с использованием которого в случае имеющегося IP-адреса или наименования домена (сайта) можно получить контакты администрации организации, зарегистрировавшей домен злоумышленника, и отправить ей запрос о представлении соответствующей информации о клиенте.

При этом должностным лицам, производящим предварительное расследование, необходимо отслеживать вопросы, связанные с оплатой злоумышленником услуги интернет-связи, обслуживания домена, хостинга (хранилища), где размещена информация, непосредственно отображенная на интернет-сайте, с оплатой услуг сотовой связи. Так, подозреваемое лицо, используя VPN-шифрование в ходе совершения мошеннических действий, может допустить просчет и произвести оплату за услуги со своей личной банковской платежной карты либо карты своего знакомого, родственника и др. Таким образом, помимо запроса о представлении общей информации об установочных данных злоумышленника у оператора связи (интернет-, сотовая связь и т. д.), интернет-услуг (VPN, IP-телефония и т. д.), необходимо получить информацию обо всех платежах, произведенных злоумышленником (данные банковского счета, банковской платежной карты, IP-адрес, с которого производился платеж, наименование интернет-кошелька, его номер, какой криптовалютой совершен расчет и т. д.).

С учетом участившихся случаев использования криптовалют в ходе осуществления противоправной деятельности следует отметить создание на базе Федеральной службы по финансовому мониторингу программного средства «Прозрачный блокчейн», которое положительно зарекомендовало себя и было использовано при раскрытии ряда резонансных преступлений.

Можно выделить ряд причин, влияющих на качество и эффективность деятельности по организации расследования мошенничеств, совершенных дистанционным способом:

- трудность определения места окончания противоправного деяния в случае межрегионального характера его совершения;
- необходимость в закреплении сотрудников по расследованию мошенничеств, совершенных дистанционным способом, а также создания специализированных специальных групп по данному направлению;
- отсутствие должного и достаточного количества специалистов в сфере компьютерных технологий;
- отсутствие качественного обучения и последующего непрерывного повышения квалификации сотрудников органов внутренних дел, специализирующихся на выявлении, раскрытии и расследовании такого рода мошенничеств;
- отсутствие должного, качественного взаимодействия между подразделениями территориального органа МВД России, а также между сотрудниками органов внутренних дел и банковскими организациями, операторами сотовой связи, электронными платежными системами;
- отсутствие оснащения органов внутренних дел новыми техническими средствами обработки информации [17, с. 282].

В заключение отметим, что анализируемые примеры – это часть имеющейся проблемы по раскрытию фактов дистанционного мошенничества, связанной с установлением цифровых следов преступной деятельности злоумышленников, так как в дальнейшем могут появиться сложности в рамках международного взаимодействия – длительный обмен информацией с учетом международных соглашений, ряд других зарегулированных бюрократических моментов, которые могут возникнуть в случае международной координации преступниками своей противоправной

деятельности. В завершение анализа рассматриваемой проблематики следует акцентировать внимание на том, что наиболее сложным и трудоемким, требующим от следователя значительных усилий для успешного проведения следственных и иных процессуальных действий, как правило, является первоначальный этап расследования уголовного дела.

3.2 Некоторые тактические особенности производства следственных действий при расследовании дистанционного мошенничества

В целях исследования особенностей принятия тактико-управленческих решений на различных этапах производства следственных действий при расследовании дистанционного мошенничества, следует выделить:

- типовые ситуации при проверке сообщения о дистанционном мошенничестве (с момента получения сообщения о преступлении до возбуждения либо отказа в возбуждении уголовного дела);
- типовые ситуации первоначального этапа расследования дистанционных мошенничеств (с момента возбуждения уголовного дела до предъявления обвинения по уголовному делу);
- типовые ситуации последующего этапа расследования дистанционных мошенничеств (с момента предъявления обвинения до окончания предварительного расследования) [18, с. 415].

В условиях удаленного мошенничества в конкретной среде возможна одновременная преступная деятельность одного лица в нескольких регионах и стирание границ интернет-преступности. Указанную особенность дистанционного мошенничества можно проиллюстрировать на примере из следственной практики Управления уголовного розыска МВД России по Нижегородской области. После раскрытия серии дистанционных афер, совершенных с использованием сети Интернет, было установлено, что преступная деятельность преступника, проживающего в Нижегородской

области, насчитывала более двадцати эпизодов и распространялась на Хабаровск, Иркутск, Москву, Ярослав, Калугу, Ростов.

В связи с этим на процессы проверки и расследования мошенничества на расстоянии в наименьшей степени влияют географические и другие факторы, связанные со спецификой разных регионов, что позволяет установить универсальность рассмотренных типовых следственных ситуаций и алгоритм действий следователя. действия на разных стадиях расследования рассматриваемых преступлений.

Рассмотрим типовые ситуации при дистанционном расследовании сообщения о мошенничестве. При изучении сообщения о совершении интернет-мошенничества были выявлены следующие типичные ситуации в зависимости от источника и объема информации.

Ситуация 1: информация об удаленном мошенничестве, полученная в результате проведения оперативно-розыскных мероприятий; достаточно информации для принятия окончательного процессуального решения.

В этой ситуации результаты оперативно-розыскных мероприятий, предоставленные для решения вопроса о возбуждении уголовного дела, подлежат рассмотрению с точки зрения достаточности данных, указывающих на признаки преступления; наличие сведений о месте, времени, обстоятельствах преступления, признаки которого обнаружены; о лицах, совершивших дистанционное мошенничество (если они известны); о местонахождении предметов, которые могут стать вещественными доказательствами.

Ситуация 2: информация об удаленном мошенничестве получена из заявления потерпевшего, других неофициальных источников; недостаточно информации для принятия окончательного процессуального решения.

В этой ситуации рекомендуются следующие проверочные действия: получить объяснения от истца и от лиц, указанных в исходных сведениях в качестве возможных понятых; запросить справку о движении денежных средств с банковского счета потерпевшего; осмотр места происшествия,

компьютеров и других устройств с привлечением специалистов в области информационных технологий с целью выявления и фиксации данных, свидетельствующих о совершении преступления.

В рассматриваемой ситуации осуществляется по месту нахождения компьютерной техники потерпевшего. При этом особое внимание при данной проверке следует уделить выявлению и исправлению цифровых следов, таких как данные учетных записей пользователей в социальных сетях, переписка между потерпевшим и виновником преступления в социальных сетях и почтовых серверах, данные из журнала посещений Интернета жертвой, следы вывода средств, лог-файлы, отчеты и статистика работы антивирусного программного обеспечения [18, с. 418].

В протоколе осмотра места происшествия в связи с дистанционным расследованием мошенничества должны быть указаны: сведения о местонахождении компьютера и других устройств, их цвете, фирменных маркировках и обозначениях, серийных номерах, состоянии и повреждения, другие индивидуальные характеристики (например, MAC-адрес, IP-адрес устройства), физические следы, обнаруженные на устройствах; сведения о наличии подключения компьютерных устройств к сети Интернет, типе сетевого подключения и оборудовании, используемом для подключения (модем); состояние компьютерного оборудования на момент осмотра (включено или выключено), описание изображения экрана, открытых файлов, запущенных программ и процессов, запущенных при включении оборудования [21, с. 124]; порядок действий, выполняемых с оборудованием, последовательность открытия веб-страниц, окон и файлов, содержащих цифровые следы мошенничества (например, в отношении просмотра страницы жертвы в социальной сети, в первую очередь, способ доступа к странице, личный идентификатор страницы, информация о содержании главной страницы пользователя, его персональные данные, затем осуществляется последовательный переход на страницы «Настройки», «Безопасность» для установления информации об истории активности, на

страницу «Сообщения», страницы других пользователей с записью криминалистической информации в протокол); применимые дополнительные методы фиксации цифровых следов (скриншоты и т.п.); наименование файлов, подлежащих копированию при проверке (лог-файлы, записанные веб-страницы, электронные документы), способ копирования с указанием используемых программно-аппаратных средств, носителей информации, количество сделанных копий; порядок выключения и изъятия компьютеров и сетевых устройств (устройства ЭВМ изымаются в выключенном состоянии или в «спящем режиме» для сохранения данных оперативной памяти в случае изъятия ноутбуков; рекомендуется согласовывать вопросы, связанные с процессом изъятия отключение ИТ-устройств вместе со специалистом во избежание потери важных следов).

На практике ситуации первого типа чаще всего возникают на этапе рассмотрения заявления о возбуждении уголовного дела, который характеризуется недостаточностью первичной информации о наличии признаков преступления (95%), значительно реже встречаются ситуации второго типа (5%), что подтверждается результатами опроса исследователей, проведенного в рамках настоящего исследования [46].

Окончательным процессуальным решением на этой стадии является постановление об отказе в возбуждении уголовного дела или постановление об открытии уголовного дела, которое служит основанием для возбуждения предварительного следствия.

Рассмотрим далее типовые ситуации на начальном этапе дистанционного расследования мошенничества (от возбуждения уголовного дела до предъявления обвинения по уголовному делу). На начальном этапе дистанционного расследования мошенничества в зависимости от содержания исходной информации определяются следующие типовые ситуации.

Ситуация 1: Установлен способ совершения дистанционного мошенничества, установлены потерпевшие и свидетели, установлены

отдельные цифровые следы, данные о лице, совершившем преступление, отсутствуют.

В данной ситуации выявлены отдельные цифровые следы (например, следы неправомерного доступа к аккаунту в социальных сетях, доменное имя мошеннического сайта интернет-магазина и следы заказа на сайте, следы связи между подписчиками устройства, следы снятия денежных средств с банковских счетов) могут служить источником информации о лице, совершившем преступление. Направление следствия в данной ситуации заключается в установлении сведений о лице, совершившем дистанционное мошенничество, на основании оставленных следов.

Для указанной съемочной ситуации характерен определённый алгоритм действий: анкетирование потерпевших. В ходе анкетирования в зависимости от применяемого метода дистанционного мошенничества и вида выявленных цифровых следов должны быть уточнены следующие вопросы: имеется ли у потерпевшего персональный компьютер, телефонный ноутбук, планшет с выходом в Интернет на месте место жительства или работы; имеет ли кто-либо, кроме потерпевшего, доступ к компьютеру, мобильному телефону, планшету; зарегистрирована ли жертва в социальных сетях и под каким аккаунтом; если введенные данные (логин, пароль) для доступа к профилю в социальной сети известны лицу, отличному от потерпевшего; есть ли у потерпевшего банковские счета, карты и в каких банках, есть ли у потерпевшего услуги «Интернет-банкинг», «Мобильный банкинг», если реквизиты карты/счета потерпевшего известны третьим лицам; производились ли платежи потерпевшим от имени сайтов, интернет-магазинов, физических лиц и на какие цели, с каких банковских счетов и на какие; какими техническими средствами была произведена оплата; как осуществлялось общение жертвы с мошенником (номера мобильных телефонов, смс-переписка, электронная почта, мессенджеры); если у мошенника были какие-то причуды голоса, он говорит; сталкивался ли потерпевший с фактами несанкционированного удаленного доступа к

персональному компьютеру; есть ли на компьютерном устройстве жертвы программы, препятствующие несанкционированному удаленному доступу; устанавливались ли программы на устройства компьютера жертвы, после чего на устройствах проявлялась подозрительная активность (автоподключение к сети, появление необычных ошибок, автоматический запуск программ и файлов, выключение устройства).

Следующим этапом является изучение выписок о движении денежных средств на банковских счетах потерпевшего. В рамках этого этапа производят направление запросов в банки и кредитные организации о предоставлении реквизитов владельца счета, на который были переведены денежные средства в результате мошенничества; направление запросов регистраторам доменных имен на предоставление сведений об администраторе (владельце) доменного имени сайта мошеннического интернет-магазина; направление запроса информации оператору связи о человеке, на которого зарегистрирован абонентский номер; направление запросов к провайдерам на предоставление информации об интернет-подключениях абонента или абонентского устройства (указанная информация, предоставляемая провайдером, может содержать информацию о дате и времени добавления записи на основе системного времени логин-сервера; IP-адрес маршрутизатора, обслуживающего данную сессию, логин пользователя, имя линии, тип логина, тип записи (старт, стоп, обновление) и дополнительные параметры); Информация о подключении к Интернету важна для удаленных расследований мошенничества и позволяет определить, кто использовал известный IP-адрес в течение определенного периода времени (используя такие записи, как стоп).

В рассматриваемой следственной ситуации практикующие специалисты сталкиваются с трудностями, вызванными отсутствием необходимой и своевременной помощи со стороны банков, интернет-провайдеров, регистраторов доменных имен при предоставлении ответов на запросы. [46].

Следующим этапом является проведение опроса свидетелей, в число которых в силу специфики преступления могут входить лица, обладающие криминалистически значимой информацией в силу своего профессионального статуса (представители регистратора доменных имен, хостера, работники банков и кредитных организаций).

Допрос представителей регистраторов доменных имен, компаний-провайдеров, банковских служащих может проводиться по иным вопросам с уточнением и уточнением сведений, предоставленных по запросу следователя в рамках расследования уголовного дела. В рамках этой стадии проводятся дополнительные мероприятия по назначению и проведению необходимых проверок: направление в следственные органы предписания о проведении оперативно-розыскных мероприятий по установлению лиц, причастных к совершению мошенничества на расстоянии; при возможности принять необходимые меры к задержанию подозреваемых с последующим допросом задержанных.

Таким образом, решение типовых следственных ситуаций на начальном этапе дистанционного расследования мошенничества сводится к сбору и исследованию максимального количества доказательств и установлению лиц, причастных к совершению преступления.

Типовые ситуации последующего этапа расследования удаленного мошенничества (с момента сообщения до окончания расследования). Последующий этап расследования, в отличие от первоначального, обычно характеризуется наличием необходимого объема собранных по делу доказательственных сведений и в большей степени направлен на закрепление и проверку имеющихся по уголовному делу доказательств. На последующем этапе расследования дистанционного мошенничества определяются типичные ситуации по степени признания вины обвиняемого и достаточности доказательств.

Ситуация 1: Подсудимый признает себя виновным в совершении преступления, но материалы уголовного дела содержат недостаточные доказательства его вины.

Направлением следствия в указанной ситуации является получение новых доказательств по делу, предопределяющее следующие действия: проведение повторных допросов обвиняемых, свидетелей, потерпевших, с целью установления дополнительных источников доказательств; использование в ходе исследования специальных знаний в виде опросов и экзаменов. В качестве примера эффективного использования специальных знаний в анализируемой следственной ситуации можно привести уголовное дело по факту мошенничества с использованием интернет-магазина в Тюменской области. По настоящему делу подсудимый в ходе своих показаний подтвердил, что принимал решения в компании, которая действовала через мошеннический интернет-магазин, был ее реальным начальником, давал указания менеджерам, составлял «скрипты» диалогов с покупателями.

Данные показания подтвердились в ходе допросов сотрудников компании, а также в ходе судебно-почерковедческой экспертизы, согласно заключениям которой рукописные записи, подписи в договорах компании, в том числе в договоре на оказание услуг по созданию мошеннической сайт интернет-магазина, были сделаны обвиняемым, а не номинальным директором компании [52, с. 115]. Предписания, адресованные органам дознания, о проведении оперативно-розыскных мероприятий, направленных на получение новых данных, относящихся к предмету доказывания.

Ситуация 2: обвиняемый полностью или частично отрицает свою вину в совершении преступления, но в материалах дела содержится достаточное количество доказательств, подтверждающих вину.

В этой ситуации возможно активное сопротивление подсудимого следствию в виде дачи ложных показаний или отказа от дачи показаний. Основным направлением следствия в данной ситуации является

систематизация имеющихся источников доказательственной информации и поиск новых, проверка (опровержение или подтверждение) показаний, данных обвиняемым.

В данной следственной ситуации необходимо принять следующие меры: повторный допрос обвиняемого с применением различных тактик допроса. В то же время наиболее эффективна следующая тактика при расследовании преступлений в сфере информационных технологий: главную проблему прикрыть второстепенными; Информирование допрашиваемого о возможности установления определенного факта путем допроса, создание впечатления, что следователь лучше осведомлен об обстоятельствах преступления [50, с. 76]. Тактические приемы допроса в данной следственной ситуации должны применяться с учетом личностных особенностей допрашиваемого. Например, при допросе удаленных мошенников, не ведущих активной общественной жизни вне виртуального пространства, в том числе не имеющих устойчивых криминальных связей, эффективным методом воздействия может стать разъяснение тяжести и последствий ответственности за совершенное преступление. При допросе лиц, обладающих высоким уровнем знаний в области информационных технологий (например, лиц, совершивших мошенничество, сопровождающееся использованием компьютерных вирусов и программ), целесообразно акцентировать внимание на положительных качествах и профессиональных навыках. Уточнение роли обвиняемого в подготовке, совершении, сокрытии преступления; установление других лиц, причастных к преступному событию.

Итак, на основе изучения материалов судебной практики по уголовным делам о дистанционном мошенничестве выявлены тактические особенности производства следственных действий в ходе расследования – при проверке сообщения о преступлении, ситуации начальной и последующей стадии расследования.

Выводы по третьей главе:

– для эффективного раскрытия и расследования необходимо незамедлительное реагирование на показания и сообщения о преступлении; принимать своевременное и обоснованное решение о возбуждении уголовных дел; рациональное планирование группой следственно-оперативной и разведывательной деятельности; разработка эффективной тактики проведения отдельных следственных и оперативно-розыскных мероприятий в целях выявления, расследования и закрепления механизма создания следов преступлений; проверять в ходе расследования достоверность, допустимость и относимость доказательств, полученных по уголовному делу;
– организовать эффективное взаимодействие с работниками, осуществляющими оперативно-розыскную деятельность, работниками негосударственных организаций, в частности, финансово-кредитных учреждений, операторов мобильной связи, интернет-провайдеров и специалистами, обладающими специальными знаниями;
– разработка типовых следственных ситуаций и тактических особенностей производства следственных действий в ходе расследования и рекомендаций по их разрешению имеет важное значение для совершенствования теоретических и прикладных прогнозов методики дистанционного расследования мошенничества. Практическая значимость этих положений определяется их общей направленностью на совершенствование и повышение эффективности расследования указанных преступлений.

Заключение

Важнейший признак мошенничества – способ совершения преступного деяния, который в конечном счете сводится к обману или злоупотреблению доверием владельца имущества и получению преступным путем имущественной выгоды. Совершение данных преступных деяний требует от мошенников творческого подхода, знания психологии, умения войти в доверие к ничего не подозревающему гражданину.

Дистанционное мошенничество, как один из видов преступления не детализирован ни нормам УК РФ, ни нормами действующего законодательства. Разработка понятий и способов совершения дистанционного мошенничества в настоящее время находится исключительно на доктринальном уровне, что приводит к различным проблема квалификации преступлений.

Проблемы уголовно-правовой квалификации заключаются не только в отсутствии уголовно-правовых норм, предусматривающих способы конкретного мошенничества, но и в привлечении к уголовной ответственности за данный вид преступления, в том числе и назначения наказания.

В судебной практике Российской Федерации при постановлении обвинительных приговоров по фактам мошеннических действий с использованием информационных технологий все чаще используются термины «дистанционное мошенничество» либо «мошенничество, совершенное дистанционным способом». В настоящее время единого подхода к определению термина «дистанционное мошенничество» в уголовно-правовой доктрине Российской Федерации не выработано. С учетом способов совершения мошеннических действий с использованием информационных технологий в ситуации удаленного нахождения злоумышленника под дистанционным мошенничеством понимаем хищение безналичных денежных средств и (или) электронных денежных средств с

использованием электронных средств платежа и технологий обмана информационно-телекоммуникационным или телефонным способом.

Таким образом, термин «дистанционное хищение» охватывает три вида преступлений: п. «д» п. 3 ст. 158, ст. 159.3, ст. 159.6 УК РФ. Их объединяют следующие признаки: изъятие денежных средств осуществляется в неочевидных условиях, когда преступник и потерпевший не видят друг друга и, как правило, не знают друг друга; преступник не только не видит потерпевшего, но обычно находится в другом субъекте РФ, возможно, в местах лишения свободы; предметом таких преступлений являются только деньги, которые являются безличными, они могут быть переданы преступнику как в не денежной, так и в денежной форме.

Виды дистанционного мошенничества, которые следует относить к способам совершения преступления классифицируются не только по различным нормам УК РФ, но и имеют различный родовой объект совершения преступления.

Особенностью рассматриваемых способов совершения дистанционного мошенничества, которая заключается в том, что в качестве мер борьбы с преступностью относятся не меры принуждения или установление запрета на свершение определенных действий, а меры профилактики, которые размещаются на интернет – порталах официальных сайтов правоохранительных органов.

В рамках выпускной квалификационной работы установлено, что этапу проверки сообщения о совершении дистанционного мошенничества, в зависимости от источника и объема информации, присущи две ситуации: а) недостаточно первичной информации о наличии признаков преступления, что обусловливает необходимость проведения проверочных действий (истребование выписок о движении денежных средств с банковского счета потерпевшего, осмотр места происшествия и компьютерных устройств с применением специальных технических средств и программ и др.); б) информации для принятия итогового процессуального решения достаточно;

имеющиеся материалы подлежат рассмотрению с точки зрения достаточности данных, указывающих на признаки преступления; сведений о месте, времени, обстоятельствах преступления, признаки которого обнаружены о местоположении предметов, которые могут стать вещественными доказательствами, и др.

Первоначальный этап расследования дистанционных мошенничеств, в большинстве случаев характеризуется отсутствием сведений о мошеннике, при наличии данных о способе совершения преступления, установлении потерпевших и свидетелей, выявлении цифровых следов. Расследование осуществляется путем установления информации о лице, совершившем дистанционное мошенничество, по оставленным следам.

Ситуации последующего этапа расследования данных преступлений выделены в зависимости от степени признания вины обвиняемого и достаточности доказательств. Выявлены ситуации, когда: обвиняемый признает свою вину в совершении преступления, но в материалах уголовного дела содержится недостаточное количество доказательств его виновности (расследование направлено на получение новых доказательств по делу); обвиняемый отрицает свою вину в совершении преступления полностью или частично, но в материалах дела содержится достаточное количество доказательств, подтверждающих вину (расследование направлено на систематизацию имеющихся и поиск новых источников доказательственной информации, проверку – опровержения или подтверждения данных обвиняемым показаний) (6%) (по результатам изучения материалов судебной практики).

Разработка типовых следственных ситуаций и рекомендаций по их разрешению имеет существенное значение для совершенствования теоретико-прикладных положений методики расследования дистанционных мошенничеств. Практическая значимость данных положений определяется их общей направленностью на совершенствование и повышение эффективности деятельности по расследованию указанных преступлений.

Современную основу эффективного противодействия оперативно-розыскной и уголовно-процессуальной деятельности составляет использование преступниками в совокупности неограниченных возможностей ресурсов сети Интернет, средств обеспечения связи и инновационных компьютерно-технических и программных решений, и результатом их применения выступает анонимизированная в сети Интернет личность преступника.

Предупреждение совершения преступлений, равно как и расследование и раскрытие преступлений сталкивается с проблемами осуществления идентификации устройств связи. Такие проблемы обусловлены отсутствием единого нормативного правового акта, регулирующего понятие и признаки сотовой связи, услуг связи, а также признаков идентификации сотовых телефонов и мобильных устройств, что во многом способствовало предупреждению совершения преступлений, а также защиты персональных данных граждан без нарушения принципа неприкосновенности частной жизни и тайные телефонных переговоров.

Список используемой литературы и используемых источников

1. Авдулова Т.П. Уголовное право России. Части общая и особенная: учебник и практикум для академического бакалавриата. М. : Издательство Юрайт, 2019. 394 с.
2. Алексеева Т.А., Ахмедшин Р.Л., Юань В.Л. Исследование личности обвиняемого посредством анализа материала социальных сетей // Уголовно-процессуальные и криминалистические чтения на Алтае: проблемы и перспективы противодействия преступлениям, совершаемым с применением информационных технологий: сб. науч. статей. Барнаул : Изд-во Алт. унта, 2018. Вып. XV. С. 7-14.
3. Ахмедшин Р.Л. Некоторые психологические аспекты проведения обыска // Вестник Томского государственного университета. 2019. № 38. С. 18.
4. Богданов А.В., Ильинский И.И., Хазов Е.Н. Киберпреступность и дистанционное мошенничество как одна из угроз современному обществу // Криминологический журнал. 2020. № 1. С. 15.
5. Борзенков Г.Н. Ответственность за мошенничество (вопросы квалификации) // Уголовное право. 2019. № 6. С. 233.
6. Валеев Д.Х., Маколкин Н.Н. Прогнозирование динамики судебной защиты в условиях цифровизации // Вестник гражданского процесса. 2020. № 3. С. 227-243.
7. Волохова О.В. Современные способы совершения мошенничества: особенности выявления и расследования // Государство и право. 2018. № 8. С. 128.
8. Гавло В.К., Кругликова О.В. Криминалистическая методика предварительного следствия и судебного разбирательства по делам о мошенничествах, совершаемых в сфере потребительского кредитования. // Барнаульский юридический институт МВД РФ. Барнаул. 2019. С. 78.

9. Григорян Г.Р. Юридическая характеристика объекта мошенничества в сфере компьютерной информации // Общество и право. 2017. № 2 (60). С. 54-57.

10. Гуляев К.С. Право человека на Интернет, права в Интернете и при использовании интернет-вещей: новые тенденции // Прецеденты Европейского суда по правам человека. 2018. № 1. С. 29-37.

11. Калюжный А.Н. Использование возможностей средств сотовой связи в раскрытии и расследовании преступлений, посягающих на свободу личности // Вестник Восточно-Сибирского института МВД России. 2018. N 1 (84). С. 118-124.

12. Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет: дис. …канд. юрид. наук. М., 2018. 197 с.

13. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ). [Электронный ресурс] // Информационно-правовая система Консультант Плюс.

14. Кузнецова Е.Г. Обман как способ хищения при мошенничестве // Вестник Уральского института экономики, управления и права. 2017. № 3 (40). С. 40-44.

15. Кузнецова Е.Г. Мошенничество в сфере компьютерной информации: вопросы квалификации // Правопорядок: история, теория, практика. 2017. № 4 (15). С. 87-90.

16. Кулешова Н.Н. Христофорова Е.И. Особенности квалификации мошенничества в сфере компьютерной информации // Вопросы науки и образования. 2018. № 14 (26). С. 41-46.

17. Кучебо И.В. Классификация информационных преступлений /В сборнике: Актуальные вопросы публичного права // Материалы XIX

Всероссийской научной конференции Студентов и молодых ученых. Екатеринбург, 2020. С. 282-287.

18. Кучебо И.В. Информационное преследование как угроза неприкосновенности личности информационной сфере // Вопросы российской юстиции. 2020. № 6. С. 415-422.

19. Лазарев А.М. Вопросы разграничения кражи и присвоения найденного чужого имущества // Вестник Волжской государственной академии водного транспорта. 2017. № 53. С. 227-233.

20. Лебедкин В.В. Актуальные вопросы квалификации преступлений против хищения имущества // Безопасность бизнеса. 2016. № 1. С. 112.

21. Лопашенко Н.А. Преступления против собственности. В 4 книгах: авторский курс: монографии. Кн. 1. Общетеоретическое исследование посягательств на собственность: монография. Москва: Юрлитинформ, 2019. 294 с.

22. Любан В.Г., Молянов А.Ю., Хазов Е.Н. Распространенные способы мошенничеств в сфере информационно-телекоммуникационных технологий // Вестник Московского университета МВД России. 2019. № 1. С. 190-194.

23. Мазуров И.Е. Методика расследования хищений, совершенных с использованием интернет-технологий: дис. … канд. юрид. наук. 12.00.12. 2017. Ростов н/Д., 2017. С. 130-156.

24. Макаров А.В., Страмилова Т.П., Куприянова А.В., Федурина Ю.О. К вопросу о разграничении кражи и присвоения найденного // Российский следователь. 2021. № 7. С. 41-46.

25. Мещеряков В.А. Криминалистика в цифровой век // Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения): Материалы международной научно-практической конференции (г. Москва, 18 мая 2018 г.) / Редакторы: С.В. Валов, А.В. Красильников, Е.А. Ефремова. Москва: Академия управления МВД России, 2018. С. 180-185.

26. Нестеренко А.К. Реформа корпоративного права в России продолжается // Закон. 2019. № 1. С. 16.

27. Опальский А.П., Смирнов А.И. О деятельности информационно-поисковой системы по противодействию дистанционному мошенничеству // Алтайский юридический вестник. 2017. № 3 (19).

28. Пильников С.Г. Уголовно-правовая и криминологическая характеристика отдельных видов хищений чужого имущества: закон, теория, практика: монография. Москва: Проспект, 2021. 96 с.

29. Поляков В.В., Ширяев А.В. Проблемы тактики допроса по делам о компьютерных преступлениях // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2015. № 15 (1). С. 123-126.

30. Приговор от 19 мая 2020 г. по делу № 1-200/2020. [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_40412/ (дата обращения 20.01.2022 г.).

31. Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // «Российская газета», 11 декабря 2017 г. № 280.

32. Постановление Пленума Верховного Суда РФ от 27.12.2002 № 29 (ред. от 29.06.2021) «О судебной практике по делам о краже, грабеже и разбое» [Электронный ресурс] // Информационно-правовая система Консультант.

33. Россинская Е.Р. К вопросу о частной теории информационно-компьютерного обеспечения криминалистической деятельности. Известия Тульского государственного университета. Серия: Экономические и юридические науки. 2016. № 3-2. С. 109-117.

34. Рудых А.А. Трансформация криминалистической и преступной деятельности в условиях развития информационных технологий // Российский следователь. 2020. № 2. С. 3-6.

35. Себякин А.Г. Возможности использования контекстного поиска информации на компьютерных носителях в целях выявления, расследования

и профилактики преступлений // Всероссийский криминологический журнал. 2019. № 2. С. 262-270.

36. Сергеев С.М. Некоторые проблемы противодействия использованию в преступной деятельности средств обеспечения анонимизации пользователя в сети Интернет [Электронный ресурс]. URL: доступа: https://cyberleninka.ru/ (дата обращения: 16.04.2022 г.).

37. Смирнов В.А. Присвоение найденного: некоторые проблемы, возникающие в практике судов и органов предварительного расследования / В.А. Смирнов // Сибирский юридический вестник. 2016. № 4 (75). С. 101-103.

38. Тенишев А.П., Тесленко А.В. Антикартельный пакет: «экстраполномочия» или оправданные меры? [Электронный ресурс] // Информационно-правовая система Консультант.

39. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ [Электронный ресурс] // Информационно-правовая система Консультант.

40. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 08.12.2020) (с изм. и доп., вступил в силу с 19.12.2020). [Электронный ресурс] // Информационно-правовая система Консультант Плюс.

41. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». [Электронный ресурс] // Информационно-правовая система Консультант Плюс.

42. Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ (ред. 30.12.2020). [Электронный ресурс] // Информационно-правовая система Консультант Плюс.

43. Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ [Электронный ресурс] // Информационно-правовая система Консультант Плюс.

44. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ Электронный ресурс] // Информационно-правовая система Консультант Плюс.

45. Федеральный закон от 29.11.2012 № 207-ФЗ (ред. От 03.07.2016) «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» [Электронный ресурс] // Информационно-правовая система Консультант Плюс.

46. Хайдаров А.А. Дистанционное мошенничество. Расследование преступления и доказывание в суде [Электронный ресурс]. URL: https://elibrary.ru/ (дата обращения: 16.04.2022 г.).

47. Хилюта В.В. Кража и присвоение найденного имущества: монография / В.В. Хилюта. - Москва : Юрлитинформ, 2018. 222 с.

48. Шевченко Е.С. Социально-технологические детерминанты следственных действий при расследовании киберпреступлений // Актуальные проблемы российского права. 2016. № 10 (71). С. 160.

49. Шеслер А. Мошенничество: проблемы реализации законодательных новелл // Уголовное право. 2017. № 2. С. 67.

50. Шульгина И.В. Криминалистическая характеристика личности мошенника // Наука и образование сегодня. 2018. № 5 (28). С. 76-78.

51. Шут О.А. Мошенничество в социальных сетях и способы его осуществления // Вестник Омского университета. Серия «Право». 2020. Т. 17, № 4. С. 97-106.

52. Чернова Е.В. Информационная безопасность человека: учеб. пособие. 2-е изд., испр. и доп. Москва : Юрайт, 2020. 243 с.