2.2. Мошенничество.

Процесс доказывания такого преступления, как мошенничество, имеет некоторые особенности, определяемые несколькими обстоятельствами.

Во-первых, обстановка совершения преступления. При мошенничестве потерпевшие некоторое время, иногда довольно значительное, находятся с мошенниками в обычных стандартных условиях, то есть могут продолжать взаимодействовать с последними, не подразумевая о том, что стали их жертвами. Поэтому после совершения преступления потерпевшие способны дать более или менее полное описание внешности мошенника.

Во-вторых, личность мошенника. В большинстве случаев мошенничество совершают лица зрелого возраста, обладающие хитрым, изворотливым умом, умеющие привлечь к себе людей, заинтересовать их, произвести на них благоприятное впечатление.

Значительное число мошенничества совершается лицами, ранее судимыми за мошенничество и другие преступления против собственности. Это требует от следователя умелого применения при допросах мошенников разработанных криминалистикой приемов и методов расследования, использования данных криминалистических учетов.

В-третьих, совершению мошенничества зачастую способствует неправильное поведение отдельных граждан. Иногда они проявляют излишнюю доверчивость, простодушие и таким образом позволяют обмануть себя, иногда совершают поступки, противоречащие нормам морали, – проявляют алчность, стремятся обойти существующие порядки, в результате чего становятся жертвами ловких мошенников.

Следователь должен учитывать эти обстоятельства при проведении допроса потерпевшего для того, чтобы получить объективные показания.

Мошенничество, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием, относится к числу преступлений против собственности (ст. 159 УК РФ). При рассмотрении вопросов уголовно-процессуального доказывания мошенничества в отношении личного имущества граждан становится понятно, что наибольшее познавательное значение имеют сведения: о личности преступника и потерпевшего; об обстановке совершения преступления; о способах совершения преступления (подготовки и сокрытии); предмете преступного посягательства.

1) Сведения о личности преступников. В зависимости от личностных характеристик лица, совершающего преступление, зависит и способ совершения мошенничества. В настоящее время, как показывает практика, нет какого-то критерия по возрасту и половой принадлежности по многим преступлениям данной категории. К сожалению, мошенничество совершают и лица пенсионного возраста, хотя, казалось бы, им должны быть присущи более высокие нравственные устои, желание следовать во исполнение требований законов. В поисках какого-либо вознаграждения ввиду различных социальных причин на совершение данного вида преступления соглашаются студенты вузов, которые наряду со взрослой категорией преступников хорошо организуют, распределяют роли участников, понимают психологию людей.

2) Потерпевшими в основном становятся доверчивая, добродушная категория граждан, которые владеют какими-либо материальными ценностями, либо, в силу своего характера, хотят обогатиться за счет каких-либо заманчивых финансовых сделок, но в конечном итоге

становятся жертвами мошенников. Такие критерии, как половая принадлежность, профессия, не представляют интереса в ходе изучения личности потерпевшего, но возраст лица имеет достаточно важную характеристику. Например, по многим преступлениям в сфере мошенничества потерпевшими признают лиц возрастной категории пенсионного возраста ввиду недостаточной их информированности по состоянию и разновидности современной преступности, а также в силу рассеянности и чрезмерной доверчивости.

Кроме физических лиц, потерпевшими могут быть признаны и юридические лица, например, коммерческие организации, интересы которых в ходе предварительного расследования представляют их доверенные лица.

3) Обстановка совершения преступления. Особо выделяется обстановка совершения мошенничества в отношении личного имущества граждан, когда потерпевший некоторое время, иногда довольно значительное, общается с мошенником в спокойной обстановке. При этом потерпевший запоминает внешность преступника и может позже его описать и опознать. Мошенники активно используют благоприятную обстановку для совершения своих противоправных деяний. Естественно, что в общем смысле слова обстановка совершения преступления – это и время, и место. Но необходимо обратить внимание на то, что рассматриваемый вид мошенничества, как правило, реализуется в местах большого скопления людей: на рынках, вокзалах, улицах, в аэропортах, крупных магазинах. Иными словами, в тех местах, где люди чаще всего бывают с большими суммами денег. С другой стороны, большое скопление людей облегчает мошеннику выбор жертвы и последующее быстрое исчезновение.

4) Способ совершения преступления. При мошенничестве способ действий преступника носит информационный характер либо строится на особых доверительных отношениях, сложившихся между виновным и потерпевшим. При совершении мошенничества потерпевший сам передает имущество преступнику, полагая, что последний имеет право получить его. При этом именно обман или злоупотребление доверием побуждает собственника или иного законного владельца передать преступнику личное имущество или имущественное право. Обман или злоупотребление доверием, как один из способов завладения имуществом или приобретения права на имущество граждан, характеризует качественные особенности данной формы хищения.

5) Предметом преступного посягательства при хищениях личного имущества граждан являются: наличные деньги, иностранная валюта, ценные бумаги; изделия из драгоценных металлов (украшения); автомототранспортные средства; предметы старины (антиквариат), произведения искусства, коллекции монет, орденов, марок и пр.; изделия из кожи и меха; предметы одежды; носильные вещи (сумочки, чемоданы, дипломаты и др.). Похищенное имущество может реализовываться сразу после хищения или временно храниться в специально отведенных местах.

На сегодняшний день наиболее распространенными способами мошенничества в отношении личного имущества граждан являются преступления, совершаемые с использованием телекоммуникационных сетей. Преступники используют все более изощренные методы для обмана граждан. Наиболее распространёнными видами преступлений являются хищения в интернет-банкинге, телефонные мошенничества,

sms-мошенничества, фишинг, мошенничества в сфере финансовых пирамид, а также внесение сумм по поводу приобретения дорогостоящих БАДов, медицинского оборудования[7]. К основным способам мошенничества в глобальной сети относятся: организация мошенниками фиктивных «банков» и «инвестиционных фондов», обещающих непомерные проценты по вкладам; организация фиктивных интернет-магазинов, аукционов, торговых площадок; рассылки и сайты о якобы обнаруженных уязвимостях и черных ходах в платежных системах, позволяющие умножать свои деньги, например, переслав их на особый счет; предложение помощи в отмывании крупных сумм; организация интернет-казино и лотерей; интернет-благотворительность; спам рассылки и сайты с просьбой о материальной помощи под трогательную историю, просьбами внести денег в фиктивный благотворительный фонд; фишинг – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям путем обмана или злоупотребления доверием; подделка платежных систем и взлом аккаунтов, то есть записей, содержащих сведения, которые пользователь сообщает о себе некоторой компьютерной системе; кардинг – вид мошенничества, при котором производится операция с использованием платежной карты или ее реквизитов, не инициированная или не подтвержденная ее держателем; организация сайтов фиктивных брачных агентств, а также отдельные виртуальные невесты\женихи, стремящиеся путем обмана или злоупотребления доверием получить денежные средства пользователей; прямое вымогательство с использованием сети «Интернет»; мошеннические сайты и

[7] Полонский Д. Первые среди киберпреступников // Деньги. 2012. № 14 (871). 9 апр. URL: http://www.kommersant.ru/money/67687.

рассылки, предлагающие удаленную работу; мошенничество, связанное с блокированием программного обеспечения компьютеров. В настоящее время данный вид мошенничества очень распространен. В его основе лежит использование вредоносных программ в целях блокирования программного обеспечения компьютеров пользователей сети Интернет. Отдельными и самыми перспективными направлениями интернет-мошенничества можно выделить мошенничество в социальных сетях и онлайн-играх, учитывая их стремительное распространение и развитие. Механизм следообразования зависит от вида и способа совершения мошенничества в отношении личного имущества граждан. После совершения преступления часто остаются различные предметы. Или то, что имитировало предполагаемую вещь – фальшивые ценности, так называемые «куклы», документы. Эти предметы дают ценную и доказательственную информацию. Совершение интернет-мошенничества предполагает оставление обильных следов технического характера в любом случае, хотя преступники и принимают меры для сохранения анонимности. Виртуальные следы могут послужить доказательствами незаконного проникновения в память компьютера или иного устройства (взлома), возможного совершения или планирования определённого преступления конкретным лицом или группой лиц (например, при наличии доступа к терминалу только у определённого лица или группы лиц). Материальные следы, образуемые при совершении мошенничества, совершаемого с использованием сети Интернет, можно условно поделить на три группы:

- следы от размещения (рассылки) информации;
- следы от взаимодействия с потерпевшими;
- следы получения денежного перевода.

К первой группе следов можно отнести, в первую очередь, различные рассылки информации – спам. Под спамом (англ. spam) следует понимать рассылку коммерческой и иной рекламы или иных видов сообщений (информации) лицам, не выражавшим желания их получать. Помимо спама следами от рекламирования и распространения мошеннической информации могут служить следы взаимодействия с рекламными площадками, а также системами обмена баннерами. Также, особенно при организации фиктивных интернет-магазинов, важное значение для сотрудников, расследующих мошенничество, имеют регистрационные данные на доменное имя, лог-файлы от взаимодействия с регистратором доменных имен; следы от проведения платежа этому регистратору. Это могут быть следы при настройке DNS сервера, поддерживающего домен-мошенников. (DNS-сервер, он же name server – приложение, предназначенное для ответов на DNS-запросы по соответствующему протоколу. Также DNS-сервером могут называть хост, на котором запущено приложение.)

Важное значение для раскрытия преступления могут представлять следы от взаимодействия с хостинг-провайдером, у которого размещен сайт мошенников и куда происходил залив контента. (Хостинг-провайдер – компания, занимающаяся предоставлением услуг размещения оборудования, данных и web-сайтов на своих технических площадках. При взаимодействии с потерпевшими, в первую очередь, это следы при приеме заказов – по электронной почте, по ICQ, через вебформу, а также, в последнее время все чаще, через получившие широкое распространение социальные сети; следы от переписки с потерпевшими. При передаче сообщения от мошенника к потерпевшему и

наоборот через электронную почту остается достаточный объем следов: это копия сообщения на компьютере отправителя и получателя, следы в логах провайдеров (например, статистика трафика), запись в логе каждого МТА, через который сообщение прошло, логин антивирусов и программ, предназначенных для фильтрации информации и защиты от спама, иные следы. Также это могут быть данные о телефонных переговорах между мошенником и потерпевшим, посредством которых обсуждались детали мнимой сделки, данные абонента, на имя которого зарегистрирован телефон. При получении денег от обманутых пользователей мошенники, как правило, оставляют следы при осуществлении ввода, вывода и перевода денег в платежных системах. Наиболее распространенными платежными системами являются Webmoney, e-gold, StormPay, RUpay, RBKMoney, Qiwi, Яндекс-деньги, МОНЕТА.РУ. На серверах платежных систем остаются данные об операциях с интересующими нас счетами, данные пользователей, конкретное время проведения операций со счетами, следы от дистанционного управления мошенниками своими счетами, их открытия и закрытия, а также многие другие сведения. Реквизиты счетов, на которые осуществлен перевод денежных средств, можно узнать как от потерпевшего, так и в рассылках, рекламе, на сайте мошенников и другими способами.

На сегодняшний день одним из наиболее распространённых способов мошенничества является хищение имущества под предлогом совершения сделки по купле-продаже через сеть Интернет. Рассмотрим актуальные вопросы предмета доказывания данной категории уголовных дел.

Объективная сторона данного типа хищений может выполняться в следующих вариантах:

1. Потерпевший, например, на сайте «www.avito.ru» находит объявление о продаже товара, связывается путём переписки или по указанному преступником абонентскому номеру телефона, после чего мнимый продавец предлагает потерпевшему перечислить денежные средства в счёт предоплаты (либо аванса).

Потерпевший перечисляет нужную сумму денежных средств со своей банковской карты на банковские счета либо через платёжный терминал на абонентские номера телефонов (электронные кошельки платёжных систем), после чего связь с преступником прекращается.

Как правило, общение между потерпевшим и злоумышленником осуществляется посредством сотовой связи, а также через обмен электронными сообщениями. Поэтому при расследовании указанной категории преступлений с целью установления лиц, причастных к его совершению, установления обстоятельств совершённого преступления, а также возможных фактов совершения аналогичных преступлений в отношении иных лиц, следователю необходимо в порядке, предусмотренном ч. 7 ст. 185 и ст. 186^1 УПК, обратиться в суд с ходатайством о разрешении получения информации о соединениях абонентов и пользовательского оборудования, осмотре и выемки электронных сообщений или иных передаваемых по сетям электросвязи сообщений, а именно сведений о:

- лице, на имя которого зарегистрирован адрес электронной почты (аккаунт) «prestupnik@bk.ru», дате создания;

- IP-адресе (с указанием точного времени: дата, час, минута, секунда), с которого осуществлялся вход в момент создания аккаунта (в момент его активации/авторизации);

- точном времени (дата, час, минута, секунда) отправки каждого сообщения с адреса электронной почты (аккаунта) «prestupnik@bk.ru» за интересуемый орган предварительного следствия период времени;

- содержании переданных и принятых сообщений посредством адреса электронной почты (аккаунта) «prestupnik@bk.ru» за интересуемый орган предварительного следствия период времени;

- IP-адресах (с указанием точного времени: дата, час, минута, секунда), с которых осуществлялся вход на сайт в момент отправления каждого сообщения с адреса электронной почты (аккаунта) «prestupnik@bk.ru» за интересуемый орган предварительного следствия период времени;

- лицах, на которых зарегистрированы адреса электронной почты (аккаунты), осуществлявшие в интересуемый орган предварительного следствия период времени обмен сообщениями с пользователем адреса электронной почты (аккаунтом) «prestupnik@bk.ru».

2. На контактный номер телефона потерпевшего (указанный последним в объявлении о продаже товара, например, на сайте «www.avito.ru») поступает звонок злоумышленника, который сообщает, что ему очень понравился товар, он срочно хочет его купить, однако находится в другом городе, не имеет возможности прибыть лично к потерпевшему в нужный адрес, поэтому желает срочно перевести на счёт потерпевшего предоплату (либо аванс) за товар, посредством безналичного перевода денег на банковскую карту потерпевшего, но для этого ему необходимо сообщить: данные о номере банковской карты,

сроке действия, а также CVV-код, CVC-код, расположенный на оборотной стороне карты, либо сообщить текст смс-сообщения с кодами-подтверждения, которые потерпевший получит в момент общения. Сведения, сообщаемые потерпевшим злоумышленнику, являются важной персональной информацией, необходимой для облегчения доступа преступника к счёту (счетам). При получении подобных показаний потерпевшего одной из главных версий совершения преступления должна стать версия о хищении денежных средств посредством использования услуги по моментальному переводу денежных средств с карты на карту (например, перевод через сервисы: «Card2Card», «Moneysend», «VISA Transfer, «VISA Direct» и проч.) посредством использования сайта банка-эквайрера.

Как правило, при таких типичных ситуациях с момента размещения потерпевшим объявления о продаже товара до момента поступления звонка от злоумышленника, момента начала совершения преступления проходит не более суток. В связи с этим необходимо обратить внимание сотрудников органов предварительного следствия, что помимо выполнения алгоритма по раскрытию преступлений в случае проведения преступниками моментальных переводов с карты на карту через WEB-сайт банка-эквайрера, необходимо выяснить у потерпевшего, на каком сайте тот разместил объявление о продаже, каковы его номер, дата, время размещения, в течение какого периода времени (с момента размещения) с потерпевшим связался злоумышленник.

Посредством использования информации о номере объявления потерпевшего, размещённого на том или ином сайте, путём направления в порядке, предусмотренном ч. 4 ст. 21 УПК, запроса на сайт объявлений необходимо выяснить:

- количество просмотров объявления за период, прошедший с момента его размещения до начала совершения преступления (как правило, количество просмотров не превышает числа 20), с каких IP-адресов с указанием точного времени (дата, час, минута, секунда), номера TCP/UDP порта осуществлялся вход на сайт в момент каждого просмотра. После чего полученную информацию можно использовать в целях раскрытия преступления, а также в качестве доказательственной базы в совокупности с иными полученными доказательствами.