Бердникова О.П., Андроник Н.А.

ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ДОПРОСОВ НА ПЕРВОНАЧАЛЬНОМ ЭТАПЕ РАССЛЕДОВАНИЯ УГОЛОВНЫХ ДЕЛ ПО МОШЕННИЧЕСТВАМ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

TACTICAL FEATURES OF INTERROGATIONS AT THE INITIAL STAGE OF INVESTIGATION OF CRIMINAL CASES ON FRAUD IN THE FIELD OF COMPUTER INFORMATION

В статье рассмотрены тактические особенности допросов потерпевших, свидетелей, подозреваемых в условиях бесконфликтной и конфликтной ситуации по мошенничествам в сфере компьютерной информации. Приведен наиболее типичный круг вопросов, которые необходимо выяснить на первоначальном этапе расследования мошенничества.

The article discusses the tactical features of interrogations of victims, witnesses, suspects in a conflict-free and conflict-free situation on fraud in the field of computer information. The most typical range of questions that need to be clarified at the initial stage of the fraud investigation is given.

Одной из особенностей современного периода развития общества является повсеместное внедрение технического прогресса, компьютеризация общества и распространение в обиходе глобальной сети Интернет, IT-технологий, которые стали неотъемлемой частью практически всех сфер жизни современного человека и охватывают все ресурсы, которые обеспечивают управление любой информацией. В настоящее время все больше информации о себе пользователи хранят в социальных сетях, в том числе персональные данные, включая подробности личной жизни и круг профессиональных интересов. Кроме того, гражданами ежедневно совершаются миллионы денежных операций по оплате товаров и услуг. Одновременно с этими законными процессами представители преступного мира находят новые способы совершения и сокрытия мошенничеств в сфере компьютерной информации. Данный вид мошенничества обладает повышенный общественной опасностью, которая возникает при совершении преступлений в «Киберпространстве». Это в полной мере подтверждается статистическими данными, согласно которым за январь – июль 2020 года уменьшились преступления против личности, при этом общее количество преступлений увеличилось на 0,5 %. Данный прирост связан с увеличением количества преступлений совершенных в сфере компьютерной информации. Так, к примеру, число преступлений, совершенных с использованием информационно-коммуникационных технологий, возросло на 94,6 %. По данным Генпрокуратуры на долю мошенничеств, совершенных с использованием компьютеров, интернета, мобильных телефонов, и других информационно-телекоммуникационных технологий, приходится более 67 %. В целом количество «киберпреступлений» за последние 5 лет увеличилось более чем в 6 раз – с 43,8 тысяч в 2015 году до 294,4 тысячи в 2019 году [1].

В связи с увеличением количества киберпреступлений, в том числе и мошенничеств, совершенных в сфере компьютерной информации, актуализируется потребность в совершенствовании методик расследования данных преступлений со стороны следственных органов. К сожалению, необходимо отметить, что зачастую данные преступления расследуют следователи, не имеющие глубокие познания, а также опыт расследования дел в сфере компьютерных технологий. Уголовно-процессуальный закон предусматривает ряд возможностей для восполнения недостатка специальных знаний в процессе собирания и проверки доказательственной базы, в том числе это привлечение специалиста узкого профиля для участия в следственных действиях. При расследова-

нии уголовных дел по мошенничеству в сфере компьютерной информации целесообразно наладить постоянное и непрерывное взаимодействие со специалистами в области компьютерной информации, так как по данным уголовным делам они могут привлекаться к проведению многих следственных действий, таких как: осмотр места происшествия; выемка и обыск, допросы подозреваемых, следственный эксперимент и конечно проведение судебных экспертиз.

В ходе изучения диссертационного исследования В.В. Коломинова, который, на основе изученных уголовных дел, а также анкетирования следователей выявил неоднозначное отношение следователей к привлечению специалистов к непосредственному проведению допроса. При этом 45 % опрошенных респондентов указали, что необходимо привлекать специалиста для участия в допросе; 50 % опрошенных указали, что присутствие специалиста негативно повлияло на ход допроса; 5 % затруднились ответить на данный вопрос [2, с. 112]. Данные цифры свидетельствуют о том, что 50 % опрошенных следователей предпочитают привлекать специалиста во время подготовки, к допросу заранее получив консультацию и тем самым быть готовым к допросу. Еще необходимо учитывать тот факт, что многие следователи предпочитают не показывать подозреваемым свою некомпетентность по некоторым вопросам, а присутствие специалиста на это будет прямо указывать.

Здесь необходимо отметить, что, несмотря на консультации со стороны специалистов, следователь является должностным лицом, уполномоченным осуществлять предварительное следствие и от его знаний, опыта и профессионализма зависит ход и результат расследования. Поэтому до проведения вышеуказанных следственных действий должна осуществляться тщательная предварительная подготовка. Хотелось бы подробнее остановиться на тактических особенностях проведения такого следственного действия как допрос (потерпевших, свидетелей, подозреваемых) в связи с тем, что именно данное следственное действие проводится в 100 % случаев при расследовании мошенничеств в сфере компьютерной информации, от качества проведения которого зависит объем полученной информации. Кроме того от уровня проведения допроса подозреваемого лица во многом зависит ход дальнейшего расследования, если следователь во время первого допроса покажет свою некомпетентность, то подозреваемый займет конфликтную позицию и не будет давать правдивых показаний, что отрицательно повлияет на ход всего расследования.

Вышесказанное свидетельствует о том, что по данным уголовным делам в не зависимости от процессуального положения допрашиваемого лица следователю необходимо тщательно подготовиться до проведения допроса. До начала допроса необходимо проконсультироваться с оперативным сотрудником отдела «К», который может помочь в выяснении следующих вопросов: каков характер предмета преступного посягательства; посредствам чего осуществлялся неправомерный доступ к информации; какое именно воздействие или вмешательство было осуществлено преступником; последствия преступных действий; какой уровень специальных познаний у предполагаемого преступника; один человек или группа лиц могла совершить мошенничество. Данный круг вопросов не является исчерпывающим, носит ориентировочный характер и варьируется в зависимости от конкретного преступления.

Точный ответ на ряд перечисленных вопросов требует производства длительных исследований, однако специалист, ознакомившись с имеющейся информацией, может высказать свои предположения, которые помогут выдвинуть следственные версии и спланировать тактику допроса [3, с. 97].

На практике, как правило, потерпевшие на первоначальном этапе расследования допрашиваются в условиях бесконфликтной ситуации, так как являются заинтересованными лицами в установлении и поимке предполагаемого преступника. Свидетели могут принимать различные позиции как благоприятные для расследования так и наоборот, это зависит от того на чьей стороне свидетель, и какова его заинтересованность в исходе дела. Подозреваемые, как правило, занимают конфликтующую сторону и пы-

таются оказать как пассивное, так и активное противодействие следователю. Так, в большинстве случаев подозреваемые обладают углубленными знаниями в области высоких информационных технологий. Они имеют специализированное образование или самообразование, особые криминальные навыки работы с компьютерной техникой, которые постоянно совершенствуются [4, с. 47].

Остановимся подробнее на тактических особенностях проведения допросов потерпевших, свидетелей и подозреваемых в зависимости от ситуации (бесконфликтная, конфликтная), в которой протекает допрос.

Тактика допроса потерпевшего должна строиться с учетом его криминалистического типа. Небезынтересна точка зрения В.М. Быкова, который типизируя потерпевших, исходит из занятой ими позиции в ходе предварительного следствия и их поведении, выделяя четыре типа: активных и неактивных добросовестных потерпевших, неустойчивых, а также недобросовестных потерпевших [5, с. 27].

При первоначальном допросе потерпевших, как правило, используются следующие традиционные тактические приемы в условиях бесконфликтной ситуации: установление психологического контакта; выслушивание свободного рассказа; задавание уточняющих вопросов, вызывание ассоциативных связей. К нетрадиционному тактическому приему можно отнести демонстрацию действий потерпевшего, которые он совершал ранее с помощью телефона, компьютера, планшета или других технических устройств, и которые повлекли преступные последствия. Здесь важно исключить факт тактического риска, то есть наступления негативных последствий вследствие повторения данных действий на другом техническом устройстве. Данный тактические прием является эффективным и наглядно помогает увидеть следователю виртуальный путь совершения мошенничества, но в тоже время не применим, если может повлечь повторные преступные последствия.

Кроме того, у потерпевших необходимо выяснить следующую информацию:

- какое компьютерно-техническое средство было подвергнуто преступному посягательству;

- уровень навыка работы на персональном компьютере, или другом техническом устройстве и уровень пользования мобильными телефонами;

- наличие знаний о программных средствах, установленных на компьютере или технически сложном устройстве;

- с каким оператором (провайдером) заключен договор на оказание услуг по предоставлению сети Интернет и на каких условиях;

- как потерпевший узнал о совершении в отношении него мошеннических действий;

- при каких обстоятельствах проходило преступное событие с указанием всех данных, которые могут изобличить преступников и установить цепочку преступного события;

- был ли визуальный контакт с преступниками, если да то при каких обстоятельствах, кто мог быть свидетелями встречи и подробное описание внешности.

Данный перечень вопросов, в основном, выясняется у физических лиц, что касаемо юридических лиц, в отношении которых совершено мошенничество в сфере компьютерной информации, то перечень вопросов расширяется в зависимости от конкретной следственной ситуации, в которой протекает расследование.

Свидетелями, как правило, становятся так называемые сведущие лица, которые имеют определенные познания о произошедшем событии и могли быть очевидцами его совершения. В случае мошенничества с одним лицом, как правило, свидетелями являются родные или близкие потерпевшего, а также коллеги по работе. Если потерпевший – юридическое лицо, то свидетелями могут являться сотрудники, занимающие должность директора, системного администратора, техника, бухгалтера, менеджера и т.п. В условиях бесконфликтной ситуации у свидетелей выясняются вопросы, которые касаются их осведомленности о совершенном мошенничестве и устанавливаются все

сведения, которые могут быть полезными для расследования. В условиях конфликтной ситуации необходимо применять большинство тактических приемов, которые будут описаны ниже при производстве допроса подозреваемого.

Рассмотрим допрос, который следует проводить сразу же после задержания подозреваемого. В зависимости от совершенного преступления круг вопросов увеличивается, изменяется или сужается. Приведем наиболее типичные вопросы задаваемые подозреваемым:

- когда у него возник умысел на совершение мошеннических действий в сети Интернет;
- почему именно такой способ обмана выбрал;
- имелись ли у него соучастники; если да, то кто именно и какова их роль в совершенном преступлении; кто был организатором мошеннических действий;
- где приобретали продукцию, которую реализовывали через интернет-магазин;
- на чье имя был зарегистрирован сайт, домен, у какого хостинг-провайдера размещен веб-сайт;
- кто принимал заказы и вел переписку с потерпевшими;
- почему именно через определенную платежную систему оплачивался товар;
- с какого компьютера выходили в Интернет, кому он принадлежит;
- сколько совершили преступных эпизодов и т.д.

Для наглядности приведем конкретный пример совершения мошенничества в сфере компьютерной информации в крупном размере и определим, какие типичные вопросы необходимо выяснить у подозреваемого при первоначальном допросе. Так, И.А. Варданян с целью личного обогащения путем ввода, модификации компьютерной информации и вмешательства в функционирование средств хранения, будучи осведомленным о порядке и правилах доступа к автоматизированной услуге «мобильный банк» ПАО «Сбербанк» и возможности перевода денежных средств без использования самой карты, используя sim-карту осуществил sms сообщение на незнакомый абонентский номер (принадлежащий А.И. Гордееву) с текстом «Ваша карта заблокирована, информация № 752». Гордеев, введенный в заблуждение, перезвонил на номер Варданяна, который представился сотрудником банка. Варданян обманным путем получил информацию о номере банковской карты и кодовом слове, пояснив, что служба безопасности банка осуществляет контроль лицевых счетов, привязанных к картам клиентов, сумма на которых превышает 5 млн. рублей. Далее Варданян с помощью неустановленной техники, имеющей доступ в «Интернет», произвел вмешательство в функционирование средств хранения и, используя полученные данные, осуществил доступ к лицевому счету Гордеева и перевел денежные средства на подконтрольный ему счет [6].

Определим вопросы, подлежащие выяснению у подозреваемого Варданяна:

- личные данные, наличие судимостей, состоит ли на учете, уровень образования и другая информация, указывающая на наличие или отсутствие специальных знаний;
- подробные обстоятельства совершения данного эпизода (в том числе, случайным ли образом осуществлял дозвон или по наводке, если да, то кто навел, где и как приобрел сим-карту, где находится телефон, через который осуществлял разговор с потерпевшим);
- где и на какого открыл подконтрольный счет, есть ли другие счета;
- у кого приобрел и какое использовал техническое устройство для несанкционированного проникновения и где оно сейчас находится;
- как распорядился денежными средствами;
- действовал один или в составе преступной группы;
- причастен ли к совершению других преступных эпизодов.

Приведены основные вопросы, которые необходимо выяснить в ходе допроса, данные перечень вопросов не является исчерпывающим.

В случае возникновения конфликтной ситуации на допросе позиция следователя должна быть максимально тактически выверенной и избирательной. Следует избегать

ситуаций тактического риска, оперирования ненадежными доказательствами [7]. Анализ эмпирического материала позволил выделить наиболее эффективные тактические приемы подозреваемого в условиях конфликтной ситуации: оглашение неопределенной информации без конкретизации, то есть создание представления о большой осведомленности, чем на самом деле; неоднократное задавание одного и того же вопроса на протяжении всего допроса в различных вариациях, что может привести к проговору; предъявление доказательств во время допроса (результаты экспертизы, фрагмент допроса соучастника и другое); маскировка главного вопроса среди второстепенных; разъяснение зоны ответственности за содеянное преступление; обращение к положительным качества ранее несудимых подозреваемых и разъяснение о смягчении наказание за содействие следствию и признание вины [8].

Подводя итоги, необходимо еще раз отметить, что от качественной подготовки к допросу лиц по мошенничеству в сфере компьютерной информации зависит результат следственного действия. Задача следователя состоит не только в том, чтобы выступить с инициативой о необходимости передать ему информацию ее носителем, но и в том, чтобы держать под постоянным контролем ход и результаты допроса, анализировать информацию, выявлять упущения, неточности, пробелы, противоречия в показаниях, сопоставлять их с данными из других источников.

ЛИТЕРАТУРА

1. В 2020 году число мошенничеств с платежными системами выросло на 120 % [Электронный ресурс]. URL: http://aif.ru.

2. Степаненко Д.А. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: дис. … канд. юрид. наук. Иркутск, 2017. 207 с.

3. Расследование преступлений в сфере компьютерной информации и высоких технологий: учебное пособие / О.П. Грибунов, М.В. Старичков. М.: ДГСК МВД России, 2017. 160 с.

4. Поляков В.В. Региональные особенности криминалистической характеристики преступлений в сфере компьютерной информации // Вестник криминалистики. 2016. № 2 (58). С. 47 – 52.

5. Быков В.М. Допрос потерпевшего // Законность. 2014. № 6. С. 27 – 32.

6. Приговор суда по ч. 3 ст. 159.6 УК РФ № 1-144/ 2017 [Электронный ресурс]. URL: svd-praktika.ru.

7. Поляков В.В. Следственные ситуации по делам о неправомерном удаленном доступе к компьютерной информации // Российский юридический журнал. 2010. № 1 (21). С. 46 –50.

8. Савельева М.В., Смушин А.Б. Следственные действия. М., 2011. 176 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Бердникова Ольга Петровна. Доцент кафедры криминалистики. Кандидат юридических наук, доцент.

Уральский юридический институт МВД России.

Служебный адрес: 620057, Российская Федерация, г. Екатеринбург, ул. Корепина, д. 66.

Berdnikova Olga Petrovna. Assistant professor of the chair of Criminalistics. Candidate of legal sciences, associate professor.

Ural Law Institute of the Ministry of Internal Affairs of Russia.

Work address: 620057, Russian Federation, Yekaterinburg, st. Korepina 66.

Андроник Наталья Аureловна. Старший преподаватель кафедры криминалистики.
Уральский юридический институт МВД России.
Служебный адрес: 620057, Российская Федерация, г. Екатеринбург, ул. Корепина, д. 66.

Andronic Natal'ya Aurelovna. Senior teacher of the chair of Criminalistics.
Ural Law Institute of the Ministry of Internal Affairs of Russia.
Work address: 620057, Russian Federation, Yekaterinburg, st. Korepina 66.

Ключевые слова: мошенничество; компьютерная информация; допрос; тактические приемы; потерпевший; свидетель; подозреваемый.
Keywords: fraud; computer information; interrogation; tactical techniques; victim; witness; suspect.

УДК 343.98.068

Бондарева М.В., Першин А.Н.

ИСПОЛЬЗОВАНИЕ КРИМИНАЛИСТИЧЕСКИХ УЧЕТОВ И ИНЫХ БАЗ ДАННЫХ В РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ ЭКОНОМИЧЕСКОЙ НАПРАВЛЕННОСТИ

USE OF FORENSIC RECORDS AND OTHER DATABASES IN THE DETECTION AND INVESTIGATION OF ECONOMIC CRIMES

Преступления экономической направленности наносят существенный вред бюджетной системе Российской Федерации. Поэтому совершенствование деятельности по выявлению виновного в экономическом преступлении лица и доказыванию его вины является важной задачей для правоохранительных органов. Статья посвящена использованию криминалистических учетов и иных баз данных органов внутренних дел в раскрытии и расследовании преступлений экономической направленности. Отмечается, что криминалистические учеты либо не используются вовсе, либо используются неэффективно и без должной оценки следственной ситуаций по делу. Следователи недостаточно внимания уделяют личность подозреваемого по преступлениям экономической направленности и всего объема информации, содержащейся в учетах, которая может помочь собрать сведения, характеризующие эту личность. Кроме того, предлагается совершенствовать систему учетов по способу совершения преступлений экономической направленности.

Economic crimes cause significant damage to the budget system of the Russian Federation. Therefore, improving the activities of identifying the person guilty of an economic crime and proving his guilt is an important task for law enforcement agencies. The article is devoted to the use of forensic records and other databases of internal affairs bodies in the detection and investigation of economic crimes. It is noted that forensic records are either not used at all, or are not used effectively and without a proper assessment of the investigative situation in the case. Investigators do not pay enough attention to the identity of the suspect in economic crimes and the entire volume of information contained in the records, which can help to collect information that characterizes this person. In addition, it is proposed to improve the system of accounting for the method of committing economic crimes.