Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»
ЮРИДИЧЕСКИЙ ИНСТИТУТ
Кафедра «Уголовный процесс, криминалистика и судебная экспертиза»

МЕТОДИКА РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

ФГАОУ ВО «ЮУрГУ» (НИУ) – 40.03.01. 2016. 573.ВКР

Научный руководитель
канд. юрид. наук, доцент,
доцент кафедры
_____Галина Сергеевна Русман
_____ 2021 г.

Автор работы
студент группы Ю-573
_____Юлия Вячеславовна Лосева
_____ 2021 г.

Нормоконтролер,
преподаватель кафедры
_____Гончаренко Виталина Викторовна
_____ 2021 г.

Челябинск
2021

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Все больше информации обрабатывается и хранится в компьютерных сетях.Распространение интернет-банкинга,электронных платежей, личных кабинетов с персональными данными привели к тому, что злоумышленники стали активно использоватьдостижения научно-технического прогресса при совершении преступлений. Основныесредства, используемые при совершении мошеннических действий, связаны с использованиеИнтернета, а также компьютера и мобильных средств связи.Движимые корыстными мотивами преступники используют полный спектр возможностей компьютерных систем и создают новые мошеннические схемы. При этом жертвами преступных действий становятся не только физические, но и юридические лица, а также публично-правовые образования.Сложившаяся тенденция с годами только увеличивается. Сказанное подтверждают и данные статистики МВД за 2019-2020 год. В 2019 году было зарегистрировано 687 заявлений о мошенничестве в сфере компьютерной информации,в 2020 году показатели увеличились на 10 % и составили 761 заявление. А если учитывать тот факт, что мошенничество в сфере компьютерной информации имеет высокий уровень латентности, то реальный уровень данного виде преступности гораздо выше. Поэтому органы правопорядка активно ведут борьбу с мошенничеством в сфере компьютерной информации.С каждым годом методика расследования совершенствуется, основываясь на полученном опыте. Но все ещё есть множество пробелов, которые не позволяют в полной мере противостоять мошенникам.

Объектом выпускной квалификационной работывыступают общественные отношения, складывающиеся в процессе расследования мошенничества в сфере компьютерной информации.

Предметом исследования являютсяправовые и криминалистические проблемы расследования мошенничества в сфере компьютерной

информации, а также использование специальных познаний в сфере компьютерных технологий.

Целью выпускной квалификационной работы является выявление особенностей расследования мошенничества в сфере компьютерной информации.

Для достижения поставленной цели были определены следующие задачи:

1) рассмотреть понятие, сущность и содержание криминалистической характеристики мошенничества в сфере компьютерной информации;
2) изучить элементы криминалистической характеристики мошенничества в сфере компьютерной информации;
3) изучить особенности возбуждения уголовного дела по делам о мошенничестве в сфере компьютерной информации;
4) изучить особенности тактики первоначального и последующего расследования мошенничества в сфере компьютерной информации.

Методическая база исследования представлена следующими методами: методы анализа и синтеза, сравнительно-правовой, обобщения, системный, логический и диалектический методы научного познания.

Теоретическая основа. Несмотря на то, что мошенничество в сфере компьютерной информации это относительно новая сфера для уголовно-правовой науки, она не остается без внимания большого количества ученых. В специальной юридической литературе мошенничество в сфере компьютерной информации рассматривалось в исследованиях:В.В. Коломинова, В.П. АносоваА.В, А.А. Протасевича,О.Ю. Введенской, Старичков М.В и других авторов.

Нормативную и эмпирическую основу выпускной квалификационной работы составляют Уголовный кодекс РФ, Уголовно-процессуальный кодекс РФ, материалы судебной практики Верховного суда РФ и судов общей юрисдикции.

Структура выпускной квалификационной работы обусловлена целью и задачами настоящего исследования и состоит из введения, основной части (трех глав, двух параграфов), заключения и библиографического списка.

1 КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

1.1 Понятие, сущность и содержание криминалистической характеристики мошенничества в сфере компьютерной информации

Глобальная информатизация мирового сообщества и развитие сети Интернет продолжают набирать обороты. Все больше информации хранится и обрабатывается в компьютерных системах. Теперь все государственные органы, организации и просто частные лица пользуются компьютерно-техническими средствами. С одной стороны, большое количество компьютеров ускоряет обмен информацией и упрощает социально-экономические процессы, с другой стороны, появляются новые способы совершения преступлений, которые необходимо предупреждать, выявлять, раскрывать и расследовать. Для решения любой из этих задач учёные-криминалисты исследуют особенности и элементы информационной модели всех разновидностей преступлении и составляют характеристики, акцентирующие внимание на существенных чертах каждого вида противоправного деяния.

Так как преступление – это многогранное явление, то одной характеристики будет недостаточно, именно поэтому в обороте получили распространение несколько видов характеристик преступления, одной из которых является криминалистическая характеристика.

Первоначально понятие «Криминалистическая характеристика» было введено в оборот в 60-х годах XX века. В 1966 году Сергеев Л.А. в своем автореферате кандидатской диссертации применил термин «криминалистическая характеристика хищений».[1] Но, по общепринятому мнению, данное понятие вошло в оборот в 1967 году благодаря автореферату

[1] Сергеев Л.А. Расследование и предупреждение преступлений совершаемых при производстве строительных работ: автореф. дис. ... канд. юрид. наук. М., 1966. С. 16.

учёного-криминалиста Колесниченко Алексея Никифоровича, который прямо указал, что «К наиболее существенным положениям, общим для всех методик (расследования) относятся: а) общая криминалистическая характеристика данного вида преступлений;…»[1].

Отмечая важность криминалистической характеристики следует отметить, что в марте 1974 году проводился Всесоюзный семинар руководителей кафедр криминалистического цикла. По итогам данного семинара было принято решение включить изучение криминалистической характеристики каждого вида преступления в программу вузовского курса криминалистики.

При этом до сих пор нет единого понятия «Криминалистической характеристики». Так, например, Козлов В.Е. дает следующее понятие криминалистической характеристики преступлений: «это научная категория, в которой с определенной степенью общности описаны типовые признаки и свойства события, обстановки, способа совершения общественно опасных деяний определенной классификационной группы, процесса образования и локализации следов, типологические качества личности и поведения виновных, потерпевших, устойчивые особенности иных объектов посягательства, а также связи и отношения между всеми перечисленными структурными элементами».[2]

По мнению А.Ф. Лубина криминалистическая характеристика – это «сущностное выводное знание о преступной деятельности, которое выступает (наряду с техническими и организационными средствами) в качестве информационного средства расследования … это опережающие,

[1] Колесниченко А.Н. Научные и правовые основы расследования отдельных видов преступлений: автореф. дис. ... д-ра юрид. наук. Харьков, 1967. С. 27.

[2] Козлов В.Е. Теория и практика борьбы с компьютерной преступностью М.: Горячая линия – Телеком, 2002. С.10.

предпосылочные сведения о закономерностях функционирования объекта (предмета), которые обусловливают закономерности расследования»[1].

В.П. Лавров, под криминалистической характеристикой понимает систему сведений о типичных признаках определенной категории преступлений, анализ которых позволяет делать выводы об оптимальных путях их раскрытия и расследования[2].

Переходя к теме нашей работы, рассмотрим понятие криминалистической характеристики мошенничества в сфере компьютерной информации, но перед этим ознакомимся с определением, данным законодателем в УК РФ. В соответствии со ст. 159.6 УК РФ под мошенничеством в сфере компьютерной информации понимается: «хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей».[3]

Отдельно понятие криминалистической характеристики компьютерных преступлений было сформулировано Коломиновым В.В., который писал, что «это совокупность наиболее характерной, криминалистически значимой информации о признаках и свойствах такого рода преступлений, способной служить основанием для выдвижения версий о событии преступления и личности преступника, позволяющей верно оценить ситуации, возникающие в процессе раскрытия и расследования компьютерных преступлений,

[1] Лубин А.Ф. Методология криминалистического исследования механизма преступной деятельности: дис. … канд. юрид. наук / А.Ф. Лубин. Новгород, 1997. С. 94.
[2] Лавров, В.П. Криминалистика / В.П. Лавров. М.: Норма, 1999. С. 33.
[3] Уголовный Кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // СЗ РФ. 1996. № 25. Ст. 2347.

обусловливающей применение соответствующих методов, приемов и средств»[1].

Криминалистическая характеристика, в отличие от других видов характеристик, имеет ряд особенностей. Во-первых, содержит в себе только криминалистически значимые сведения о признаках преступлений. Во-вторых, сведения о признаках элементов описываются в количественно-качественном уровне, т.е. устанавливаются взаимосвязи и закономерности. Криминалистическая характеристика позволяет определить, что с чем связано, каким образом, что за чем следовало, с помощью чего может быть установлено и т.д. Таким образом, полученные при расследовании данные можно будет наложить на «теоретическую модель», сформулированную с помощью криминалистической характеристики. В таких условиях криминалистическая характеристика становится эффективным инструментом в расследовании преступлений. Как писал об этом Н.П. Яблоков: «зацепив одно звено в этой системе взаимосвязей, можно вытащить наружу всю цепь. В частности, при выявлении в преступлении одного звена цепочки с той или иной степенью вероятности можно судить о существовании другого, ещё не установленного элемента и определить направление и средства его поиска».[2] По мнению Уткина М.С., использование криминалистической характеристики на практике требует комплексного подхода и будет максимально эффективно в случае привлечения и других видов характеристик (уголовно-правовой, криминологической и т.д.).[3]

Криминалистическая характеристика – это сложная система, поэтому учёные всегда пытались её конкретизировать.

---

[1] Коломинов В.В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: дис. … канд. юрид. наук. Иркутск, 2017. С. 28.

[2] Яблоков Н.П. Информационные основы расследования и криминалистическая характеристика преступлений / Н.П Яблоков, Л.Д., Самыгин. М.: Бек, 1995 С. 12

[3] Уткин М.С. Некоторые вопросы общей методики расследования преступлений / М.С. Уткин. Омск: Омская высш. шк. милиции, 1986. С. 20.

По мнению Пантелеева И.Ф. в содержание криминалистической характеристики входят: характеристика типичных ситуаций разных видов преступлений, способы их совершения, используемые технические средства и способы их получения, характеристика типичных следов преступления, имеющих значение вещественных доказательств, способы сокрытия следов и другие следы маскировки преступников, типичные преступные связи.[1]

Более чёткая структура криминалистической характеристики сформулирована в виде отдельных элементов, которые основаны на значимой для конкретного дела информации.

Самойлов А.В. сформулировал основные требования к элементам криминалистической характеристики преступлений:

- теоретическая доказанность (в том числе подтвержденная практикой органов дознания и предварительного следствия);
- значимость тех или иных из них для научного и практического решения задач по выявлению, раскрытию преступлений и осуществлению уголовного преследования.[2]

До настоящего времени у учёных-криминалистов не выработано единой позиции относительно элементного состава криминалистической характеристики.

Так, например, С.А. Бессновым были выделены следующие элементы криминалистической характеристики:

- обстановка преступления (место, время и другие обстоятельства);
- способ совершения и сокрытия преступления;
- материальные следы преступления и вероятные места их
- нахождения (в том числе механизм следообразования);
- предмет преступного посягательства;
- личность потерпевшего;

---

[1]Пантелеев И.Ф. Методика расследования преступлений. М., 1975. С. 374.

[2]Самойлов А.В. Современное состояние учения о криминалистической характеристике преступлений // Российский следователь. М., 2010. № 22. С. 5.

 личность преступника».[1]

С.И. Коновалов составил свою иерархию элементов криминалистической характеристики, основываясь на частоте их использования для различных видов преступлений:

1. Способ и обстановка совершения преступления, особенности личности субъекта преступления, объект (предмет) преступного посягательства, следы преступления (механизм следообразования).

2. Связи между структурными элементами.

3. Личность жертвы, мотив, цель, условия совершения преступления, преступные связи, типичные ситуации совершения преступления, особенности сокрытия преступления, механизм преступления, типичные следственные ситуации (характер исходных данных и особенности их обнаружения), состояние борьбы с определенным видом преступления, связь с другими видами преступлений.

4. Средства, орудия и последствия преступной деятельности[2].

Если рассматривать вопрос об элементах криминалистической характеристики мошенничества в сфере компьютерной информации, то тут классификация была описана также несколькими учёными.

Так Гаврилин Ю.В. и Шурухунов Н.Г. включили в состав криминалистической характеристики компьютерных преступлений следующие элементы:

1. данные о способах подготовки, совершения и сокрытия преступления;
2. данные об орудиях (средствах) совершения преступления;
3. данные об обстановке и месте совершения преступления;
4. данные о следах;

---

[1]Бессонов С.А. К вопросу о структуре и природе криминалистической характеристики преступлений // Вестник Поволжского института управления. Саратов, 2014. № 4(43). С. 54.

[2]Коновалов С.И. Теоретико-методологические проблемы криминалистики. Ростов-на-Дону: РЮИ МВД России, 2001. С. 85.

5. данные о предмете преступного посягательства;

6. данные о виновных лицах.[1]

А.А. Протасевич и Л.П. Зверянская в своей работе выделили следующие элементы криминалистической характеристики преступлений в сфере компьютерной информации:

- способ совершения преступления;
- особенности следовой информации;
- особенности обстановки совершения преступления (место совершения преступления, время совершения преступления и др.);
- личностная характеристика преступника;
- особенности непосредственного предмета преступного посягательства.[2]

На наш взгляд мнение А.А. Протасевича и Л.П. Зверянской более содержательное, поэтому в дальнейшем в нашей работе за основу мы возьмем иерархию, предложенную этими авторами.

Все элементы криминалистической характеристики являются фрагментами действительности, которые взаимодействуют друг с другом в процессе подготовки, совершения и сокрытия преступного деяния. Поэтому, все предложенные учёными элементы сходны.

Проблема компьютерной преступности до сих пор является новой и недостаточно изученной, но несмотря на это, у ученых сформировались две точки зрения по отношению к элементам криминалистической характеристики данной группы преступлений.

Первая точка зрения основывается на том, что сами структурные элементы криминалистической характеристики компьютерной преступности

---

[1]Гаврилин Ю.В. Расследование неправомерного доступа к компьютерной информации. М.: ЮИ МВД РФ, 2004. С. 137.

[2] Протасевич А.А., Зверянская Л.П. Криминалистическая характеристика компьютерных преступлений // Российский следователь. 2013. № 11. С. 45-47.

ничего не дают для их классификации. Только взаимосвязи позволяют выделить такой класс преступлений как компьютерная преступность.[1]

Другие же считают, что необходимо выделить особенные элементы криминалистической характеристики компьютерных преступлений, указывая в этом перечне способ совершения, следы, условия преступления и личность преступника.[2] Ряд ученых, например, В.Б. Вехов считает, что особую роль в криминалистической характеристике играет криминалистически значимая информация о личности преступника, его мотивах и целях.[3]

В тоже время, следует учитывать особенности отдельных видов компьютерных преступлений. Говоря о мошенничестве в сфере компьютерной информации, особенно следует отметить способы и механизмы следообразования, способы, обстановку, предмет и объект преступления, а также место его совершения.

В современной криминалистике до сих пор не утихают споры о том, какое место занимает криминалистическая характеристика, какое у неё значение и насколько она необходима при разработке частных методик расследования отдельных видов преступлений.

Вся концепция криминалистической характеристики прошла долгий путь в рамках отечественной юриспруденции: от всеобщего одобрения до сомнений и отрицания. До сих пор ученые-криминалисты имеют несколько позиций по данному вопросу. Первоначальная положительная позиция была подорвана отрицательным мнением авторитетного учёного Р.С. Белкина. В своей работе «Понятие, ставшее “криминалистическим пережитком”» он высказал мнение, что само понятие «Криминалистическая характеристика» не соответствует научным требованиям. Поэтому предлагал от него

---

[1] Дударчик Я.Ю. Анализ взглядов на криминалистическую характеристику преступлений // Вестник Академии МВД. Краснодар, 2017. № 2. С. 46.

[2] Старичков М.В. Способ совершения как элемент криминалистической характеристики мошенничества в сфере компьютерной информации // Криминалистика: вчера, сегодня, завтра. 2018. № 4. С. 177-179.

[3] Вехов В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и сведений. Волгоград, 2008. С. 88-91.

полностью избавиться и вернутся к практике указания в криминалистической методике элементов и специфических особенностей предмета доказывания по той или иной категории уголовных дел[1]. После этого часть исследователей восприняли данное высказывание буквально, исключив при разработке частных методик расследования отдельных видов преступлений их криминалистическую характеристику, либо вернулись к указанию особенностей предмета доказывания.

На наш взгляд, криминалистическая характеристика имеет место быть в методике расследования отдельных видов преступлений как разделе науки криминалистика и является важным структурным элементом. Благодаря ей можно увидеть связи между элементами преступления, которые являются криминалистически значимыми для расследования. Особенно в случаях, если на первоначальных этапах расследования недостаточно информации. Например, для расследования мошенничества в сфере компьютерной информации на первоначальных этапах расследования у следователя порой очень мало информации о фактически расследуемом преступлении. И в условиях недостатка исходной информации всегда требуется «ориентир», которым и является криминалистическая характеристика.

Криминалистическая характеристика – это концепция, которая несмотря на неоднозначное отношение со стороны ученых, вошла в обиход среди практикующих следователей. Связано этом с тем, что она содержит в себе обобщенное описание системы криминалистически значимой информации о признаках и свойствах отдельных видов преступлений, благодаря чему, может послужить опорой на первоначальных этапах расследования. Особенно это касается дел, где первоначального количества данных недостаточно, например, в делах о мошенничестве в сфере компьютерной информации. При правильном понимании и применении информации, полученной из криминалистической характеристики, можно

[1]Белкин, Р.С., Понятие, ставшее «криминалистическим пережитком» / Р.С. Белкин. М., 2000. С. 11−12.

выдвигать типичные версии о событиях преступлений, личности преступника и определять направление расследования.

1.2 Значимые элементы криминалистической характеристики мошенничества в сфере компьютерной информации

Как мы уже ранее описывали в предыдущей главе, криминалистическая характеристика состоит из элементов. В данной главе мы рассмотри эти элементы подробнее, взяв за основу иерархию А.А. Протасевича и Л.П. Зверянской.

Предметом мошенничества в сфере компьютерной информации выступает непосредственно сама компьютерная информация.

Согласно п. 1 ст. 2 Федерального закона от 27.07.2006 г № 149-ФЗ «Об информации, информационных технологиях и защите информации», под информацией принимаются сведения (сообщения, данные) независимо от формы их представления.[1]

В соответствии со ст. 272 УК РФ под компьютерной информацией понимаются сведения (сообщения и данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

При этом, формулировку понятия «компьютерная информация» данную в Уголовном кодексе сложно считать корректной, т.к. сведения, представленные в форме электрических сигналов это слишком неточное определение. В данном случае под такое определение может подпадать не только компьютерная информация, но и, например, радио.

С другой стороны, компьютерная информация может представляться в форме не только электрических сигналов (например, носители компьютерной информации – лазерные оптические диски, а также практически вышедшие из употребления перфокарты и перфоленты). Наконец, под сигналом в

[1] Федеральный закон «Об информации, информационных технологиях и защите информации» от 27 июля 2006 г. № 149-ФЗ // СЗ РФ. 2006. № 31 (часть I) ст. 3448.

теории информации и связи понимается материальный носитель информации, используемый для передачи сообщений в системе связи. Сигналом может быть любой физический процесс, параметры которого изменяются в соответствии с передаваемым сообщением[1]. Поэтому определения, включающие в формулировку «хранение» сигнала, абсурдны с точки зрения физики.

Именно поэтому учёные, понимая неточность закрепленных в законе понятий, предлагают свои формулировки.

Так, например, Зигура Н.А. понимает под компьютерной информацией: «сведения, представленные в электронно-цифровой форме на материальном носителе, создаваемые аппаратными и программными средствами фиксации, обработки и передачи информации, а также набор команд (программ), предназначенные для использования в электронно-вычислительной машине (ЭВМ), системе ЭВМ или управления ими.»[2]

Мещеряков В.А. считает, что компьютерная информация является: «информацией, представленной в специальном (машинном) виде, предназначенном для ее автоматизированной обработки, хранения и передачи, которая находится на материальном носителе и имеет собственника, установившего порядок ее создания (генерации), обработки, передачи и уничтожения».[3]

Стоит отдельно отметить позицию Шаркова А.Е., который выделил следующие признаки компьютерной информации:

- она объёмна и быстро обрабатываема;
- она очень быстро и просто бесследно уничтожаема;

---

[1]Старичков М.В. Понятие «Компьютерная информация» в российском уголовном праве. URL: https://cyberleninka.ru/article/n/ponyatie-kompyuternaya-informatsiya-v-rossiyskom-ugolovnom-prave/viewer.

[2]Зигура Н.А. Компьютерная информация как вид доказательств в уголовном процессе России: яис. ... д-ра юрид. наук. Челябинск. 2010. С. 125.

[3] Степанов-Егиянц В.Г. Понятие «компьютерная информация» с точки зрения её уголовно- правовой защиты. URL: https://cyberleninka.ru/article/n/ponyatie-kompyuternaya-informatsiya-s-tochki-zreniya-ugolovno-pravovoy-zaschity.

 она обезличена, т.е. между ней и лицом, которому она принадлежит, чаще всего нет жесткой связи;

 она может находиться лишь на машинном носителе (дискете, магнитной ленте, лазерном диске, полупроводниковых схемах и др.), в самой ЭВМ (оперативной памяти – ОЗУ);

 она может создаваться, изменяться, копироваться, применяться только с помощью ЭВМ;

 она легко передаётся по телекоммуникационным каналам связи компьютерных сетей, причём практически любой объём информации можно передать на любое расстояние;

 она относительно проста в пересылке, преобразовании, размножении; при её изъятии, в отличие от изъятия вещи, она легко сохраняется в первоисточнике; доступ к одному и тому же файлу, содержащему информацию, могут одновременно иметь несколько пользователей.

Следующим криминалистически значимым признаком мошенничества в сфере компьютерной информации является способ совершения преступления. Именно способ совершения данного вида преступлений является одним из определяющих элементов криминалистической характеристики.

Под способом совершения преступления понимают объективно и субъективно обусловленную систему поведения субъекта до, в момент и после совершения преступления, оставляющего различного рода характерные следы, позволяющие с помощью криминалистических приемов и средств получить представление о сути происшедшего, своеобразии преступного поведения правонарушителя, его отдельных личностных данных

и соответственно определить наиболее оптимальные методы решения задач раскрытия преступления.[1]

Для мошенничества в сфере компьютерной информации способом совершения преступления может быть обман или злоупотребление доверием с целью получения чужого имущества или информации, распространение вредоносного ПО, незаконное завладение, путем введения владельца в заблуждение, и т.д.[2]

Учитывая сложный характер рассматриваемой нами преступной деятельности, преступление делится на стадии подготовки к совершению мошенничества, непосредственной реализации преступного умысла и сокрытия следов преступления.

При этом, данная структура имеет свои особенности. Так, на этапе подготовки к совершению преступления сразу же происходит и сокрытие следов. В качестве примера можно привести разработку вредоносных программ, которые проникают в компьютер жертвы без предварительного согласия на установку.

Также бывают случаи, когда лицо, помогающее в разработке программы, не предполагает, что её в дальнейшем могут использовать для распространения вредоносного программного обеспечения.

Исчерпывающего перечня способов совершения мошенничества в сфере компьютерной информации нет. Прогресс не стоит на месте и каждый раз злоумышленники придумывают новые способы обмана.

Но тем не менее попытки классификации предпринимались не раз. Так, например, кодификатор рабочей группы Интерпола предлагает определять в обобщенном виде компьютерные мошенничества и классифицировать их следующим образом:

---

[1] Введенская О.Ю. Лекции МВД: Особенности расследования преступлений в сфере компьютерной информации на первоначальном этапе / О.Ю. Введенская. Краснодар., 2016. С.16.

[2] Комарова А.А. Интернет-мошенничество: проблемы детерминации и предупреждения: монография. М.: Юрлитинформ, 2013. С. 9.

 мошенничества в сфере компьютерной информации, направленных на хищение денежных средств из банкоматов;

 мошенничества путем создания поддельных устройств и интернет-ресурсов;

 мошенничества, связанные с игровыми автоматами;

 мошенничества в сфере компьютерной, связанные с платежными средствами;

 телефонное мошенничество путем посягательства на протоколы и процедуры компьютеров, обслуживающих телефонные системы.[1]

Белицкий В.Ю. отмечает, что на данный момент в сети Интернетраспространены следующие способы мошенничества:

1. Фишинг – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальной информации пользователя: паролям, логинам, реквизитам банковских карт, расчетным счетам и т.д.

2. Способы получения такой информации различные: от рассылок на электронных писем от имени знаменитых брендов или выигрышами крупных денежных сумм до телефонных звонков от имени банка или СМС-рассылок.

3. Нигерийские письма – интернет-мошенничество, суть которого заключается в направлении на электронную почту потенциального потерпевшего письма, содержащего просьбу мнимого высокопоставленного чиновника развивающейся и терпящей бедствие страны оказать ему содействие в вывозе денег за вознаграждение. Для этого мошенники просят оплатить счет на определенную сумму денег на почтовые расходы.

4. Поддельные торговые сайты или интернет-магазины – этот вид мошенничества связан с созданием клонов сайтов известных магазинов или производителей, или использование готовых интернет-платформ (Avito.ru, Youla.ru, Auto.ru) на котором размещаются объявления о продаже товаров. В

[1] Коломинов В.В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: дис. … канд. юрид. наук. Иркутск, 2017. С. 27.

дальнейшем, если пользователь что-то оплачивает на таком сайте, то мошенники либо отправляют более низкокачественный товар, либо игнорируют заказ покупателя.

5. Брачные аферы – вид мошенничества при котором виновные знакомятся на специальных интернет-сайтах с людьми, желающими создать семью, после чего, под разными предлогами получают финансовую помощь от наивных потерпевших.

6. Мошеннические благотворительные организации – вид мошенничества в котором виновные попрошайничают деньги, спекулируя на чувствах наивных людей.

7. Предложение работы мошенниками – схема при которой мошенники, претворяясь представителями разным компаний приглашают на работу соискателей, обещая высокие заработную плату, работу за границей и т.д. После того, как соискатель соглашается на данную работу, мошенники посредством телефонного звонка просят отправить им денежную сумму для оформления документов (например, виз), пошива униформы и т.д. После получения денежной суммы виновные больше не выходят на связь с потерпевшим.[1]

На данный момент наиболее распространенными способами мошенничества в этой сфере являются:

- незаконное завладение данными различных учетных записей и их использованием в различных мошеннических схемах;
- применение платежных сервисов для дальнейшего обналичивания денежных средств или приобретения товаров с использованием платежных данных потерпевшего;
- использование ложной информации для введения в заблуждение потенциальных жертв на специально разработанном сайте;

[1]Белицкий В.Ю. Распространенные виды мошенничеств в сети интернет // Актуальные проблемы современности. Барнаул. 2020. №2(28). С 32.

 взлом электронных кошельков и перевод денежных средств на другой счет или приобретение товаров, через электронные платежные сервисы;

 рассылка спам-писем на электронную почту, содержащих вредоносное программы;

 создание мошенниками сайтов-двойников известных интернет-магазинов для хищения платежных данных жертв.

 проведение электронных торгов с несуществующими лотами;

 проведение благотворительных акций через Интернет, где в рамках помощи предлагается перевести денежные средства для больных, инвалидов, детей оставшихся без попечения родителей и т.д.

 хищение платежных данных посредством вредоносного программного обеспечения.

Данные списки далеко не исчерпывающие и будут ни раз пополняться новыми видами мошенничества в сфере компьютерной информации.

Следующим элементом криминалистической характеристики являются следы преступления. Опять же из-за специфики данной категории противоправного деяния следы можно разделить на два вида: традиционные следы и компьютерные (виртуальные) следы.

К традиционным следам относятся следы человека, транспортных средствах, средствах связи и т.д.

К компьютерным следам же относят информацию о любых действиях с компьютерами или программами, которые фиксируются в:

 журналах администрирования, журналах безопасности отображаются такие действия, как включение, выключение, различные операции с содержимым памяти компьютера;

 реестре компьютера (reg-файлах) отражаются действия с программами (установка, удаление, изменение и т.д.);

 log-файлах отображаются сведения о работе в сети Интернет, локальных и иных сетях;

 свойствах файлов отображаются последние операции с ними (например, даты создания, последних изменений).[1]

Компьютерные устройства, как следообразующие объекты выступают, как носители информации об объективной стороне преступного деяния и как носители информации о самом субъекте преступления.

Местом преступления является место, реализации объективной стороны. В данном случае, это место нахождение компьютерно-технического средства, с которого отправлялись команды.

Мошенничеством в глобальной сети занимается большое количество людей. Преступники встречаются как квалифицированные специалисты, так и простые дилетанты. Всех их можно разделить на два вида:

 лица, знакомые с потерпевшим, например, находящиеся в деловых или трудовых отношениях (технический персонал, программисты, инженеры, операторы и др.);

 лица, незнакомый с потерпевшим.

К последним чаще всего относятся люди с более глубокими познаниями в области компьютерных технологий.

В настоящее время существует абстрактный портрет типичного компьютерного преступника. Чаще всего это человек, который рано освоил компьютер и считает это смыслом жизни, это социальный отщепенец, игнорирующий окружающий мир и имеющий много разных комплексов. Хакерство становится привлекательным для многих несовершеннолетних лиц, которые считают это занятие настоящим достижением в жизни.[2]

Чаще всего возраст злоумышленника от 14-40 лет. В пять раз чаще такие преступления совершаются мужчинами, однако в последнее время

---

[1] Протасевич А.А., Зверянская Л.П. Криминалистическая характеристика компьютерных преступлений // Российский следователь. 2013. №11. С. 45-47.

[2]Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж, 2012. С. 94-119

увеличивается доля женщин. Чаще всего это лица с оконечным или неоконченным техническим образованием.[1]

В.Б. Вехов обозначил три группы мошенников в сфере компьютерной информации:

 лица, которые отличаются профессионализмом в сфере компьютерной техники и программного обеспечения с определенным фанатизмом в собственной изобретательности;

 лица, имеющие психические отклонения, вызванные компьютерными фобиями и информационными болезнями;

 профессиональные мошенники с явными корыстными интересами.[2]

Так, например, рассмотрим приговор Приволжского районного суда города Казани. В рамках данного дела Редозубов А.Г., действуя из корыстных побуждений, специально разработал Интернет-ресурс, дизайн которого полностью имитировал распространенный в сети Интернет платежный сервис с помощью которого собирал персональный данные (логины и пароли) пользователей платёжной системы. После чего использовал, полученную незаконным способом информацию и переводил денежные средства на другие интернет-кошельки.[3]

Отдельно хотелось бы остановиться на жертвах мошенничества в сфере компьютерной информации. Ими могут быть как физические, так и юридические лица. Очень часто физические лица становятся пострадавшими из-за низкого уровня познаний в области компьютерной информации, проявления излишнего доверия к злоумышленникам или программам и т.д. Также немаловажную роль играет обеспечение компьютерной безопасности. Многие физические лица, не обращают на это внимания, но именно этим и пользуются злоумышленники. По данным отчета МВД за 2020 год было

---

[1] Лавров В.П. Криминалистическая характеристика преступления // Криминалистика. М., 2004. С. 150.

[2]Вехов, В.Б. Компьютерные преступления. Способы совершения, методики расследования. М.: Право и закон, 1996. С. 52.

[3]Уголовное дело № 1- 588/18 по обвинению Редозубов А.Г. по ч. 2 ст. 159.6, ч. 2 ст. 273 УК РФ URL: https://sudact.ru/regular/doc/o3PSlcynw8Lv/ (дата обращения 10.03.2021).

зарегистрировано 761 заявление[1], по сравнению с 2019 годом количество заявленных преступлений увеличилось на 10%. [2]

Если говорить о юридических лицах, то основываясь на статистике, представленной Group-IB за 2020 год самой атакуемой отраслью стало производство, Половина всех атак пришлось на сферу торговли, здравоохранения, строительства, образования, а также на государственные сервисы.[3] Это же подтверждает статистика, представленная Лабораторией Касперского. В их отчете указано, что около 60% опрошенных компаний заявили, что сталкивались с какими-либо киберинцедентами. В сравнении со статистикой за 2018-2019 год этот показатель вырос с 51%. Также в отчете Касперского указано, что во многих случаях сами сотрудники компании являются источниками угрозы безопасности. Отчасти это является следствием недостаточной информированности, особенно в случае новых цифровых систем автоматизации ТП. Около 48% опрошенных компаний обозначили планы повышения инвестиций в инструктаж и обучение кадров.[4]

Криминалистическая характеристика мошенничества в сфере компьютерной информации это обобщенное описание комплекса криминалистически значимой информации, а именно: способ совершения преступления; особенности следовой информации; особенности обстановки совершения преступления (место совершения преступления, время совершения преступления и др.); личностная характеристика преступника; особенности непосредственного предмета преступного посягательства.Все эти элементы взаимосвязаны меду собой и позволяют следователям

1Статистические данные о состоянии преступности в России за январь-декабрь 2019 года. Официальный сайт Министерства Внутренних Дел. URL: https://xn--b1aew.xn--p1ai/reports/item/19412450/ (дата обращения 12.02.2021).

[2]Статистические данные о состоянии преступности в России за январь-декабрь 2020 года. Официальный сайт Министерства Внутренних Дел. URL: https://xn--b1aew.xn--p1ai/reports/item/22678184/ (дата обращения 12.02.2021).

[3] Статистические данные Hi-Tech Crime Trends за 2020 – 2021 год. URL: https://www.group-ib.ru/blog/trends20_21 (дата обращения 27.01.2021).

[4] Менце Т. Кибербезопасность систем промышленной автоматизации в 2019 году. URL: https://ics.kaspersky.ru/media/Kaspersky-ARC-ICS-2019-Trend-Report-Ru.pdf (дата обращения 27.01.2021).

составить «фундамент» и продумать план дальнейших следственных действий.

Резюмируя все вышесказанное, можно сказать, что мошенничество в сфере компьютерной информации относительно новый вид преступлений для российского законодательства. На данный момент можно сказать, что из-за быстрого развития технологий, многие понятия и положения в законах начинают терять актуальность. Законодатель не всегда успевает за новыми технологиями. Связано это либо с быстрым изменением форм и видов компьютерной информации, либо с новыми быстроразвивающимися видами мошенничества, либо в недостаточной «подкованности» в технических вопросах со стороны учёных-юристов, законодателей, а порой и правоприменителей. Тем не менее, практикующие криминалисты уже составили основу в виде криминалистической характеристики, которая будет в дальнейшем развиваться и дорабатываться вместе с законодательством.

2 ОСОБЕННОСТИ ВОЗБУЖДЕНИЯ УГОЛОВНОГО ДЕЛА ПО ДЕЛАМ О МОШЕННИЧЕСТВЕ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Расследование преступлений – это сложный процесс, который можно разделить на 3 части: сбор доказательств, их исследование и использование. Весь процесс расследования делится на две стадии – первоначальную и последующую.

Первоначальной стадией расследования считается стадия возбуждения уголовного дела. Каждый вид преступления имеет свою специфику, влияющую на алгоритм действий следователя при обнаружении признаков преступления. Все эти признаки влияют на ход расследования, а также выбор сил, средств и способов дальнейших действий следователя. Кроме этого, процесс возбуждения уголовного дела зависит от законодательных актов, регламентирующих данную стадию, так, например, порядок рассмотрения сообщений установлен ст. 144 УПК РФ.

Стадия возбуждения уголовного дела подразумевает следующий алгоритм действий: приём, регистрацию, проверку сообщений о преступлении и принятие решения об отказе или о возбуждении уголовного дела. Именно на этой стадии проводится предварительная проверка и принимается решение о наличии или отсутствии оснований для возбуждения уголовного дела.[1]

До сих пор среди ученых и практикующих следователей ведутся споры о том, стоит ли проводить проверки заявлений и сообщений о готовящихся преступлениях. По данным опроса, проведенного Коломиновым В.В. 85% опрошенных работников, считают, что предварительная проверка нужна в любом случае, 10% считают, что проверки необходимо проводить только в

[1] Конин В.В. Тактико-криминалистическое обеспечение предварительной проверки заявлений и сообщений в рамках стадии возбуждения уголовного дела // Криминалистика: вчера, сегодня, завтра. Иркутск, 2020. №2 (14) С. 34.

случае неочевидных преступлений и 5% считают, что это неразумная трата времени.[1]

Предварительная проверка – это необязательная процедура, которая применяется в случае, если наличие противоправных действий неочевидно. В противном случае можно сразу же возбуждать уголовное дело.

Что касается мошенничества в сфере компьютерной информации, то по итогам изучения следственной и судебной практики возбуждению такого рода дел всегда предшествовала предварительная проверка.

На наш взгляд, это обусловлено тем, что мошенничество в сфере компьютерной информации как правило не имеет ярко выраженных субъективных признаков и для их обнаружения порой требуется ряд сложных процессуальных и следственных действий.

В целом наша точка зрения, подтверждается большинством учёных-криминалистов. Они также придерживаются позиции, что для мошенничества в сфере компьютерной информации проведение предварительной проверки является обязательной. Например, Шаров А.В. аргументирует данную точку зрения тем, что данный вид дел имеет ряд сложностей для установления признаков мошенничества и требует помощи со стороны квалифицированных специалистов, которые окажут содействие в обнаружении и исследовании следов.[2]

Основания для осуществления предварительной проверки установлены ст. 140 УПК РФ, которая включает в себя:

- заявление о преступлении;
- явка с повинной;
- сообщение о совершенном или готовящемся преступлении, полученное из иных источников;

---

[1]Коломинов В.В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: дис. … канд. юрид. наук. Иркутск, 2017. С. 84-85.

[2]Шаров А.В. Методика проведения доследственной проверки материалов, содержащих признаки мошенничества, при отчуждении квартир, находящихся в собственности граждан // Вестник криминалистики. М., 2002. С. 62.

 постановление прокурора о направлении соответствующих материалов в орган предварительного расследования для решения вопроса об уголовном преследовании.1

Применительно к исследуемому мошенничеству в сфере компьютерной информации В.Е. Козлов предлагает следующий, достаточно расширенный перечень поводов для проведения проверки и дальнейшего возбуждения уголовного дела:

1.Заявление о преступлении:

 должностных лиц организаций, предприятий, учреждений;

 граждан.

2.Сообщение о преступлении, полученное из иных источников:

 непосредственное обнаружение органом дознания, следователем или прокурором сведений, указывающих на признаки преступления;

 в результате проверки сообщения о совершенном или готовящемся преступлении, в сфере компьютерной информации, поступившего из оперативных источников;

 в ходе проведения специальных оперативно-розыскных мероприятий;

 по материалам контрольно-ревизионных и иных документальных проверок;

 при задержании лица с поличным;

 непосредственное обнаружение признаков преступления в сфере компьютерной информации при производстве по уголовным делам о преступлениях других видов;

 сообщения в средствах массовой информации.[2]

---

[1]Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ // СЗ РФ.2001. № 249. Ст. 4921.

[2] Козлов В.Е. Теория и практика борьбы с компьютерной преступностью М.: Горячая линия – Телеком, 2002. С. 37.

Примерно аналогичной точки зрения, с некоторыми уточнениями придерживаются и другие ученые. Так, например, ряд авторов указывают, что «основаниями для возбуждения уголовных дел по мошенничеству в сфере компьютерной информации могут быть следующие:

1. Заявление потерпевшего от мошеннических действий в сети Интернет.

2. Сообщение представителей благотворительных организаций о клонировании их сайтов.

3. Сообщение в печати об обнаруженном мошенничестве в сети Интернет.

4. Обнаружение правоохранительными органами признаков мошенничества в сети Интернет»[1].

Анализ судебной практики показывает, что на период получения сведений о совершенном преступлении может складываться две ситуации:

1. Преступление ещё длится, т.е. связь между преступником и жертвой сохраняется

2. Преступление окончено и связь между преступником и жертвой отсутствует.

Первый исход для следователя является наиболее благоприятным и при правильном подходе позволяет раскрыть дело по «горячим следам», поймав преступника с поличным или собрать большой объем доказательств и ориентирующей информации. Второй исход, наоборот, увеличивает объем работы следователей.

После получения правоохранительными органами заявления или сообщений о преступлениях, следователи приступают к проведению проверочных действий. Для успешного процесса проведения проверок процессуальный закон определяет перечень процессуальных и иных действий, которые могут быть реализованы органами следствия. В

[1]Чистов Л.Е. Методика расследования отдельных видов мошенничества. М.: МосУ МВД России, 2014. С. 41.

соответствии со ст. 144 УПК РФ: «При проверке сообщения о преступлении дознаватель, орган дознания, следователь, руководитель следственного органа вправе получать объяснения, образцы для сравнительного исследования, истребовать документы и предметы, изымать их в порядке, установленном настоящим Кодексом, назначать судебную экспертизу, принимать участие в ее производстве и получать заключение эксперта в разумный срок, производить осмотр места происшествия, документов, предметов, требовать производства документальных проверок, ревизий, исследований документов, предметов, привлекать к участию в этих действиях специалистов, давать органу дознания обязательное для исполнения письменное поручение о проведении оперативно-розыскных мероприятий».

Для мошенничества в сфере компьютерной информации наиболее часто используемыми процессуальными действиями являются:

- получение объяснений;
- осмотр места происшествия;
- истребование необходимых материалов;
- проведение оперативно-розыскных действий.

Принятие решения о проведении конкретных проверочных действий зависят от обстоятельств совершенного преступления. Даже ситуация, сложившаяся на момент получения заявления о преступлении, влияет на дальнейшие действия следователей. Обусловлено это источником и характером полученных данных.

В зависимости от статуса лица, предоставившего сведения, зависит объем действий. Например, источниками информации могут быть как физические, так и юридические лица. Например, у юридических лиц необходимо будет выявить и проверить документы, имеющие отношение к делу и опросить сотрудников организации. Что касается физических лиц, то тут круг проверки на этапе получения заявлений существенно меньше.

Также отличается объем информации, который поступает от этих категорий заявителей. В случае с юридическими лицами, преступники чаще прибегают к разным средствам сокрытия следов. Также почти всегда перед подачей заявления в полицию в организациях проводится внутренняя проверка. А в связи с тем, что далеко не все службы или должностные лица обладают навыками и средствами, необходимыми для оперативного обнаружения и выявления следов, тратится лишнее время, которое позволяет преступнику скрыть большее количество следов преступления. Данный фактор необходимо устанавливать и учитывать при проведении проверок.

При мошенничестве в сфере компьютерной информации, объяснения нужно получить у:

- системных-администраторов;
- программистов, занимающихся разработкой или сопровождением программного обеспечения;
- инженеров средств связи и телекоммуникационному оборудованию;
- специалистов по обеспечению безопасности систем
- провайдеров и т.д.

Круг опрашиваемых лиц, зависит от того, кто является пострадавшим. Для юридических лиц необходимо опрашивать тех, кто отвечает за компьютерно-технические средства. Для купных компаний наличие IT-службы является нормой, а для более мелких организаций следует проводить опрос руководства, отвечающего за организацию работы. При этом, при опросе таких лиц не следует исключать их причастность к совершенному преступлению. Также необходимо опросить сотрудников, которые знали или могли знать о том, кто мог совершить мошенничество. Как показывает анализ судебной практики именно сотрудники юридических лиц чаще всего совершают противоправные деяния.

В качестве примера рассмотрим дело Советского районного суда г. Владивостока. В рамках данного дела подсудимый Мишланов Д.Е. при

выполнении возложенных на него должностных обязанностей, имея доступ к служебной компьютерной информации, а именно, осуществляя доступ под своим логином и паролем к базам данных и переоформлять абонентские номера сим-карт организации. Воспользовавшись своим служебным положением Мишланов, реализуя свой единый преступный умысел, искал номера категории «Серебро» и «Золото», за которые взымается плата в размере: за категорию «Серебро» - 3 000 руб., за категорию «Золото» - 15 000 руб., незаконно переоформлять абонентские номера, перевыпускал сим-карту и реализовывал.[1]

Полученные в рамках предварительной проверки объяснения всегда являлись определяющими для практиков. Ранее среди ученых возникали вопросы о том стоит ли относить объяснения к доказательствам. Но сейчас данное положение закреплено УПК РФ. Основным плюсом объяснений, как доказательств, является то, что они могут быть оперативно и своевременно получены. По мнению Корнакова С.В., объяснения не имеют четкой процессуальной формы, но, как правило, в них содержится достоверная информация. Во-первых, из-за того, что при оперативном получении информации, детали события остаются свежи в памяти. Во-вторых, лица дающие объяснения, пока не испытывают негативного воздействия со стороны лиц, заинтересованных в исходе проверки сообщения о преступлении.[2]

После опросов, необходимо сразу же преступить к осмотру места нахождения компьютерно-технических средств и других устройств, с помощью которых могло быть совершено мошенничество. Поэтому органами следствия могут быть истребованы документы и прочие необходимые материалы, например, журнал сбоев в работе компьютерной

[1]Уголовное дело № 1-277/2020 по обвинению Мишланова Д. Е. по .3 ст.30, п.«б» ч.3 ст.159.6 УК РФ, / Архив Советского районного суда г. Владивостока. URL: https:// sudact.ru/regular/doc/4AyuDmz7J9oX/ (дата обращения 18.03.2021).
[2]Корнакова С.В. Процессуальный статус прокурора в стадии возбуждения уголовного дела. М.: Юрлитинформ, 2015.С. 34.

сети, журнал учета рабочего времени операторов ЭВМ или компьютеров сети, системный блок, жесткие диски, список лиц, имеющих доступ к определенной компьютерной информации и т.д.

Как правильно отметили Гаврилов Ю.В. и Шипилов В.В., прежде всего следы преступной деятельности остаются на носителях информации и содержат в себе все изменения, хранящихся в них данных. В данном случае речь идет о следах модификации информации, содержащихся на жестких дисках (реестры, базы данных, файлы-отчеты, текстовые файлы и т.д.).[1]

В данном случае в идеале, чтобы подобные дела расследовал следователь, обладающий высоким уровнем знаний в области компьютерной информации. Но в связи с тем, что базовое образование следователей не углубляется в особенности работы с компьютерно-техническими средствами, то целесообразно привлекать для помощи специалистов данной сферы, а также тесно взаимодействовать со всеми подразделениями и службами, принимающими участие в проверке.

Выявлению следов и другой информации помогает использованию специальных технических устройств, например, портативный аппаратно-программный комплекс для съема и исследования данных из мобильных устройств UFED, XRY, CellXtract, MOBILedit, Tarantula и т.д. Использование подобных аппаратно-технических комплексов позволяет работать не только с телефонами, а почти с любыми мобильными устройствами, независимо от производителей, операционной системы, например, планшетами, навигаторами и дронами. Особенность работы с такими устройствами заключается в том, что они позволяют извлечь даже удаленные данные,

[1]Гаврилин Ю.В., Шипилов В.В. Особенности следообразования при совершении мошенничеств в сфере компьютерной информации // Российский следователь. 2013. №23. С. 2-6.

заходить в систему в обход логинов и паролей, работать с устройствами без аккумулятора или только с сим-картой.[1]

Как заверяют производители, с помощью данных устройств можно получить данные о телефоне (IMEI/ESN); сим-карте (ICCID и IMSI), расшифровывать фотографии, видео, записи, извлекать историю звонков, контакты, текстовые сообщения, элементы календаря, заметки, файлы данных, историю браузера, Cookie-файлы, пароли и данные «Skype», «Dropbox», «Facebook», «WhatsApp», «Viber», «WeChat», «Вконтакте» и т.д.[2]

Но использования данных аппаратно-технических средств недостаточно, следователю необходимо также напрямую взаимодействовать со специалистами социальных сетей и провайдерами.

Наибольшее количество ресурсов и технического потенциала в ходе расследования и проведения проверок концентрируется в рамках отдела «К», которые с помощью технических средств могут перехватить информацию, передаваемую подозреваемыми по каналам связи. Полученную информацию в дальнейшем можно будет приобщить к делу в качестве вещественных доказательств в деле о мошенничестве в сфере компьютерной информации.

В целом вся специфика компьютерных преступлений не позволяет традиционными способами и методами устанавливать признаки преступлений. Для оснований возбуждения уголовного дела одним из основных средств принятия решения, является возможность и необходимость назначения и производства компьютерно-технической экспертизы.[3]

Анализ судебной практики показывает, что несмотря на то, что производство компьютерной экспертизы является базовой для

---

[1]Аносов А.В. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий. М.: Академия управления МВД России, 2019. С. 64.

[2] Сайт производителя MOBILedit оборудования для цифровой криминалистики URL: https://www.mobiledit.com/forensic-express (дата обращения 18.03.2021).

[3]Коломинов, В.В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: дис. … канд. юрид. наук. Иркутск, 2017. С. 98.

предварительной проверки по мошенничеству в сфере компьютерной информации, но у и неё есть ряд проблем. Основная проблема заключается в том, что производство компьютерной экспертизы требует длительного времени. Это обусловлено в первую очередь не только самими экспертными методиками, а высокой загруженностью экспертных подразделений.

Изъятие предметов и документов в рамках предварительной проверки по делам о мошенничестве в сфере компьютерной информации может быть осуществлено в рамках осмотра места происшествия или истребованы на основании постановления должностного лица, осуществляющего проверку.

В ходе предварительной проверки очень важно обращать внимание на места обналичивания денежных средств, незаконно полученных от пострадавших. Если это происходило в банковских терминалах, то благодаря встроенным техническим средствам фиксации камеры могли запечатлеть мошенника или иного подставного лица. В случае непосредственного взаимодействия с сотрудниками банка следует произвести опрос, истребовать документы, фиксирующие финансовые операции, документы, на которых могли остаться следы рук, подписи, образцы почерка и т.д.

Анализ судебной практики показывает, что мошенники часто пользуются помощью подставных лиц, которые обналичивают денежные средства или оформляют на свое имя договоры услуг связи, банковские карты и т.д. При чем стоит помнить о том, что мошенники могут ввести в заблуждение и поставное лицо может не осознавать, что оказывает содействие совершению преступления.

Также всегда есть вероятность, что указанные лица могут находится в родственных или дружеских отношениях с мошенниками. Поэтому логично в таких случаях начинать поиск с ближайшего окружения поставного лица.

Обобщая вышесказанное, можно сделать вывод, что чаще всего при проведении предварительной проверки мошенничества в сфере компьютерной информации следователям (дознавателям) целесообразно проводить следующие следственные действия:

 получать объяснения от лиц, заявивших о мошенничестве;

 производить осмотр и изъятие носителей информации и документов, имеющих отношение к делу;

 производить осмотр и изъятие системных блоков, с которых было совершено мошенничество;

 назначать судебные экспертизы для изучения доказательств, а также привлекать специалистов для оказания содействия следствию;

 провести оперативно-розыскные мероприятия по поиску свидетелей или лиц, причастных к совершению мошенничества.

Частое использование правильных оперативно-розыскных мероприятий способствует поиску преступников и их дальнейшему задержанию.

В случае, если при рассмотрении сообщения о преступлении были обнаружены обстоятельства, указывающие на признаки другого преступления, подследственного иному органу предварительного расследования, то в данном случае следователю необходимо составить рапорт и передать материалы проверки сообщений соответствующему органу по подследственности.[1]

Также немаловажным фактором является то, что при производстве предварительной проверки при обнаружении признаков мошенничества в сфере компьютерной информации все полученные доказательства должны быть использованы в дальнейшем расследовании, так как некоторые из них в дальнейшем не всегда могут быть получены иными способами. Поэтому все доказательства должны быть надлежащими и процессуально верно оформленными. Во всех случаях предварительная проверка будет влиять на формирование следственных действий на следующих этапах расследования.

---

[1]Приказ Следственного комитета России «Об организации приема, регистрации и проверки сообщений о преступлении в следственных органах (следственных подразделениях) системы Следственного комитета Российской Федерации» от 11 октября 2012 г. № 72 // Российская газета. 2013. № 48.

Последствием предварительной проверки является окончательное убеждение следователя (дознавателя) в том, что вся полученная информация в достаточной мере подтверждает наличие преступного деяния и позволяет принять решение о возбуждении уголовного дела о мошенничестве в сфере компьютерной информации. При этом, все доказательства должны не просто указывать на наличие воздействия на компьютерную информацию, но и включать в себя факт хищения материальных ценностей. Только это позволит отнести противоправное деяние к мошенничеству в сфере компьютерной информации. В противном случае может быть принято решение о возбуждении уголовного дела по другим статьям или отказ в возбуждении уголовного дела.

После того, как дело было возбуждено начинаются следующие этапы расследования, которые делятся на первоначальный, последующий и заключительный.

Первоначальный этап подразумевает первичный сбор общей информации о преступлении. На данном этапе формируется доказательственная база и выдвигаются первые следственные версии.

Последующий этап включает в себя дальнейший сбор и оценку доказательств, а также установление всех элементов предмета доказывания. Данный этап позволяет составить более полную картину происшествия и упорядочить сведения, полученные в результате расследования.

Дальнейшее расследование преступления во многом зависит от информации, полученной на первоначальных этапах. Наиболее характерные следственные ситуации на начало расследования мошенничества в сфере компьютерной информации:

1. Мошенника обнаружили и задержали. В дальнейшем он полностью признал вину.

2. Мошенник прикрывает свои действия гражданско-правовой сделкой.

3. Мошенника не обнаружили и не задержали.[1]

Перечисленные выше типичные следственные ситуации являются крайне условными и могут меняться в зависимости от обстоятельств совершенного преступления.

Отдельно следует остановиться на версиях, которые выдвигаются на первоначальном этапе расследования мошенничества в сфере компьютерной информации. Существует два вида версий – общие и частные. Общие версии пытаются объяснить общие события, имеющие признаки преступления. Они делятся на следующие версии:

- преступление совершено при обстоятельствах, полученных из первичных материалов расследования;
- имеет место ложное заявление о преступлении;
- организована инсценировка преступления.

Помимо общих, существуют и частные версии, которыми объясняют отдельные стороны и элементы преступления. Они включают в себя версии о личности преступника, его целях, мотивах, способах совершения преступления и т.д.

Эффективность дальнейшего расследования на первоначальных этапах зависит от правильного подхода и верных действий со стороны следователя. Также немаловажно заранее имеет контакт с сотрудниками отдела «К» МВД, экспертами и специалистами IT-подразделений.

[1]Бердникова О. П. Особенности возбуждения уголовных дел о мошенничестве в сфере компьютерной информации и типичные следственные ситуации на первоначальном этапе расследования // Вестник Уральского юридического института МВД России. М. 2020. С.45.

3 ОСОБЕННОСТИ ТАКТИКИ ПЕРВОНАЧАЛЬНОГО И ПОСЛЕДУЮЩЕГО РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

После возбуждения уголовного дела расследование переходит к первоначальному этапу.

Исходя из анализа практики, при расследовании мошенничества в сфере компьютерной информации чаще всего используются следующие виды следственных действий:

- осмотр места происшествия;
- осмотр предметов (компьютерно-технических средств) и документов;
- обыск;
- выемка (в том числе, различных электронных носителей информации);
- допрос (потерпевшего, свидетеля, эксперта, специалиста, подозреваемого, обвиняемого);
- очная ставка;
- предъявление для опознания;
- назначение и производство экспертиз.

Рассмотрим тактические рекомендации для каждого из указанных следственных действий.

Начнем с осмотра места происшествия. Суть этого следственного действия заключается в осмотре, поиске и фиксации максимально возможного количества информации и следов, имеющих отношения к делу. Данное следственное действие чаще всего проводится на ранних этапах расследования или в рамках предварительной проверки до возбуждения уголовного дела. При необходимости он может быть проведен повторно на более поздних этапах. Но чем раньше проведен осмотр места происшествия, тем более он эффективен.

Осмотр места происшествия делится на три этапа – подготовительный, рабочий и заключительный.

Во время подготовительного этапа следователю необходимо проверить готовность технических средств, определить специалистов, обеспечить охрану места происшествияи т.д.Если следователь знает, что на объекте обыска имеются компьютерно-технические средства, подлежащие изъятию, то необходимо также подготовить соответствующую упаковку для выемки.

Перед началом следователь обязан зачитать права всех участников осмотра.

Рабочий этап осмотра места происшествия включает в себя непосредственно сам осмотр.

Перед началом проведения данного следственного действия следователю необходимо определиться со способом осмотра места происшествия. Из существует 3 вида:

 концентрический – по спирали от периферии до центра места происшествия. Применяется в случае отсутствия определенного центра происшествия и когда возможна утрата следов на периферии и нет опасения сохранности следов в центре;

 эксцентрический – наоборот от цента к периферии. Применяется в случаях, если центр происшествия определен и при подходе к нему следы на периферии не будут уничтожены или при отсутствии четких границ места происшествия;

 фронтальный – линейный осмотр от исходной границы до другой. Рекомендуется в случаях, когда границы и центр четко не определены. Поэтому следователь последовательно передвигается по осматриваемому участку.[1]

Также на рабочем этапе осмотр места происшествия делится на два вида:

 общий осмотр местности;

[1]Драпкин Л.Я. Криминалистика. М.: Проспект, 2011. С. 488.

 детальный, концентрирующийся на конкретных предметах.[1]

Для мошенничества в сфере компьютерной информации местом происшествия является место нахождения компьютерно-технических средств потерпевшего или место обнаружения хищения денежных средств.

Во время проведения осмотра необходимо установить:

 наличие следов, совершенного преступления;

 какие предметы могут содержать следы преступления;

 какие технические средства могли использоваться для совершения преступления;

 кто потенциально мог стать очевидцем преступления.[2]

Для мошенничества в сфере компьютерной информации наибольшее количество следов содержится в компьютерной технике, носителях информации и иногда в бумажной документации. Именно поэтому, на них в первую очередь необходимо обращать внимание. Весь процесс осмотра места происшествия необходимо фиксировать в протоколе, включая информацию о. том, где именно были обнаружены улики, их индивидуальные признаки (надписи, маркировки, наклейки, логотипы и т.д.)

Если осмотр места происшествия проходит в крупных организациях, в которых данные хранятся на сервере, то в протоколе необходимо зафиксировать место нахождение сервера. Если сервер расположен в самой организации или неподалеку, то при необходимости можно также провести его осмотр. Если сервер арендован или расположен далеко от места происшествия, то данный факт также фиксируется и указывается место нахождения компьютеров у которых имеется административный доступ, позволяющий осуществлять управление сервером. Место доступа к серверу должно быть также осмотрено следователем.

---

[1]Агафонов В. В. Криминалистика. М.: Издательство Юрайт, 2015. С. 77.
[2] Там же. С. 78.

Для осмотра места происшествия данного вида преступления необходимо привлекать специалистов и использовать их знания для изъятия и фиксации следов преступления.

Заключительный этап осмотра места происшествия включает в себя:

 повторный обзор места происшествия с целью выявления пропущенных объектов,

 упаковка изъятых предметов,

 принятие мер для сохранения доказательств, которые невозможно изъять с места происшествия

 составлениепротокола осмотра места происшествия, в котором описывают обстановку, следы, все совершенные действия следователя, указывают участников следственных действий и собираются их подписи.[1]

Следующее следственное действие, которое мы рассмотрим – обыск.

Обыск может быть проведен у субъектов, заподозренных в совершении мошенничества в сфере компьютерной информации. При этом у следователей должно быть достаточное количество доказательств, подтверждающих, что у подозреваемого может находиться похищенное имущество, орудия, предметы или документы, с помощью которых было совершено мошенничество.

Проведение обыска производится на основании постановления следователя или судебного решения.

В соответствии с п.5 ст. 182 УПК РФ: «До начала обыска следователь предлагает добровольно выдать подлежащие изъятию предметы, документы и ценности, которые могут иметь значение для уголовного дела. Если они выданы добровольно и нет оснований опасаться их сокрытия, то следователь вправе не производить обыск».[2]

При подготовке к обыску необходимо заранее изучить информацию:

---

[1]Агафонов В. В. Криминалистика. М.:Издательство Юрайт, 2015. С. 79.

 о месте обыска: характеристика здания, его схема с количеством этажей, квартир и комнат, нахождение входов и выходов, место нахождение распределительного щитка, наличие охранной кнопки;

 о лицах, находящихся в здании, наличие домашних животных и т.д.

В соответствии со ст. 170 УПК РФ при обыске должно участвовать не менее двух понятых. При этом, прибыв на место обыска следователь обязан зачитать права всех участников обыска.

В обыске участвуют лица, в помещении которых производится обыск, либо совершеннолетние члены семьи этих лиц. По требованию последнего может бытьпривлеченадвокат.

На месте следователю нужно определить последовательность действий и направление движения, например, по часовой стрелке, вдоль стены и т.д.

При обыске по преступлениям, связанным с мошенничеством в сфере компьютерной информации, в первую очередь нужно обращать внимание на компьютерно-технические средства, принтеры, наличие средств связи с телекоммуникационными или компьютерными сетями, записные книжки, блокноты, флешки, диски и другие носители информации, имеющие отношение к расследуемому делу. Не менее важным являются записи логинов и паролейсторонних пользователей,ID, коды, электронные адреса других, номера банковских счетов, банковских карт, бухгалтерских документов, чеков из банков, личные документов подозреваемого и т.д.[1]

При осмотре следователю нужно быть максимально внимательным, так как флешки могут имитировать разные предметы, например, ручки, игрушки, кулоны, брелоки и т.д. Такие предметы можно легко пропустить, поэтому самым действенным способом будет использование различных нелинейных локаторов, например, «Родник-23». Такие технические средства

[1] Введенская О.Ю. Лекции МВД: Особенности расследования преступлений в сфере компьютерной информации на первоначальном этапе / О.Ю. Введенская. Краснодар., 2016. С. 28.

предназначены для нахождения любых, даже скрытых, электронных устройств.[1]

Все совершенные следователем действия также необходимо фиксировать в протоколе обыска.

При осмотре места происшествия или обыске чаще всего производится изъятие предметов. Поэтому пред проведением любого из указанных выше следственных действий необходимо заранее продумать как правильно изъять предметы без повреждения следов. Чаще всего в чемодане следователя есть все необходимое для изъятия следов рук и небольших письменных доказательств. Но для более крупных доказательств, например, системных блоков необходимо заранее подготовить коробки, бумагу, картон и т.д.

По прибытию на место, следователю необходимо сразу же обеспечить сохранность компьютерно-технических средств для этого необходимо:

1. Запретить всем сторонним лицам, работающим на объекте обыска прикасаться к ЭВМ с любой целью.

2. Запретить всем сотрудникам отключать электроснабжение объекта.

3. Если электроснабжение на момент прибытия уже выключено, то до его восстановления нужно отключить все компьютерно-технические средства от сети.

4. Не совершать каких-либо действий с компьютерной техникой, если заранее нет уверенности в конечном результате.[2]

При осмотре и изъятии нужно обращать внимание на следующие неблагоприятные факторы:

- попытки сотрудников навредить ЭВМ;
- возможное наличие на компьютерах средства защиты, которое при несанкционированном доступе и отсутствии подтверждения через код, автоматически удаляют информацию.

---

[1]Введенская О.Ю. Лекции МВД: Особенности расследования преступлений в сфере компьютерной информации на первоначальном этапе / О.Ю. Введенская. Краснодар., 2016. С. 31.

[2] Там же. С. 33.

Для того, чтобы не допустить вредных последствий, следователю (дознавателю) необходимо соблюсти ряд рекомендаций:

1. Для того, чтобы быть уверенным в том, что информация не будет потеряна необходимо перед отключением компьютера корректно закрыть все программы.

2. Если на компьютерах установлена защита, то необходимо принять меры для получения кодов доступа (паролей, логинов, ключей и т.д.).

3. Корректно отключить питание у всех компьютерно-технических средств, находящихся на объекте.

4. Не пытаться смотреть информацию, содержащуюся на компьютерах на месте обыска (осмотра).

5. При возникновении технических трудностей обращаться за помощью к специалистам, а не к персоналу.

6. При возможности изъять все ЭВМ, находящиеся на объекте.

7. При обыске не подносить металлоискатели и другие источники магнитного поля к компьютерам ближе, чем на 1 метр.[1]

Если на месте производства обыска изымаются любые носители информации, то обязательно должен участвовать специалист. При изъятии любых электронных носителей информации, владелец изымаемого имущества вправе подать ходатайство о создания копий информации с изымаемого устройства. Для этого специалист в присутствии понятых производит копирование информации на другие устройства, которые в дальнейшем останутся у собственника данной информации.

Прежде чем произвести изъятие компьютеров, ноутбуков, планшетов и других компьютерно-технических средств следователю нужно проконсультироваться со специалистом о наличии подключения к единой сети, коннекта с серверами и т.д. Это необходимо для того, чтобы после изъятия не выяснилось, что на носителях содержится не вся информация.

---

[1]Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: автореф. дис. …канд. юрид. наук. М., 2016. С. 9-10.

При наличии сервера его также стоит изъять. Все компьютеры, системные блоки, серверы изымаются в сборе и каждый упаковывается в отдельную коробку, которую заклеивают листами бумаги сопись и оттисками печати подразделения, совершившего изъятие.

При изъятии планшетов и смартфонов необходимо понимать, что на них могут содержаться следы, подтверждающие, что ими пользовалось конкретное лицо. Перед упаковкой телефон необходимо перевести в «Режим полета», обернуть в фольгу и упаковать вместес зарядным устройством.

Каждый изъятый предмет фотографируется, упаковывается в индивидуальную упаковку и описывается. Потом все эти описи прикладываются к протоколу в качестве приложения.

При необходимости изъятые предметы можно будет в дальнейшем предъявить для опознания.

Предъявление для осознания компьютерной информации имеет важно значение для установления и уточнения обстоятельств, совершенного мошенничества в сфере компьютерной информации. При этом предъявить на опознание можно как непосредственно саму компьютерную информацию, так и предметы (например, флешки, диски и другие носители информации).

Что касается компьютерной информации, то она предъявляется в виде программ, баз данных, текстовых, графических файлов и т.д.

При опознании компьютерной информации важную роль играют её индивидуальные признаки:

- содержание;
- вид;
- формат;
- носители;
- имя и размер файлов;
- даты и время их создания;
- шрифты и кегль;
- интерлиньяж (расстояние между строк);

- размер абзацных отступов;
- размер полей;
- нумерация страниц;
- назначение и выполняемые функции;
- интерфейс;
- графическое и музыкальное оформление и т.д.

Именно эти индивидуальные признаки делают информацию пригодной для опознания.[1]

Следующим следственным действием, которое мы рассмотрим является допрос.

Тактика производства допроса по делам о мошенничестве в сфере компьютерной информации зависит от специфики самого механизма совершенного преступления и негативных и позитивных факторов. К первым относится наличие определенного объема информации о преступлении, полученного из разных источников, информация о лице, с которым предстоит произвести следственное действие и т.д. К негативным факторам можно отнести промежуток времени, прошедший с момента совершения преступления и до момента производства.[2]

При подготовке к проведению допроса следует понимать, что допрашиваемые лица для данной категории дел могут быть как неопытные, так и опытные пользователи компьютерно-технических средств. Если с первыми не возникает особых сложностей, то последние в данном случае могут иметь высшее образование в области компьютерной информации и владеть профессиональной терминологией. Например, системные администраторы, программисты, специалисты по компьютерной безопасности и т.д. Именно поэтому во время допроса таких лиц следует

---

[1] Мещеряков В.А. Формирование доказательств на основе электронной цифровой информации. URL: https://cyberleninka.ru/article/n/formirovanie-dokazatelstv-na-osnove-elektronnoy-tsifrovoy-informatsii/ (дата обращения 10.03.2021)

[2] Коломинов В.В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: дис. … канд. юрид. наук. Иркутск, 2017. С. 28.

задавать уточняющие вопросы или привлечь специалиста в области вычислительной техники, как минимум для согласования формулировок вопросов.

Само присутствие специалиста не всегда является положительным фактором. Иногда наличие третьих лиц не позволяет следователю наладить психологический контакт с допрашиваемым. Преимуществами участия специалиста являются: оперативное получение разъяснений, отсутствие барьера в понимании профессиональных терминов и механизмов работы компьютерной техники, сетей и самого преступления.

К негативным факторам участия специалиста можно отнести нежелание давать показания, дача негативных показаний, отрицание вины и другие формы препятствия следствию со стороны допрашиваемого. Особенно это касается допросов подозреваемых (обвиняемых) на более поздних этапах расследования.

Поэтому следователю необходимо заранее изучить ознакомительно-ориентирующую информацию и проконсультироваться со специалистом.

Основной тактической задачей при проведении допроса на стадии предварительного расследования является выявление элементов состава преступления, места, времени, круга лиц, способа совершения и других обстоятельств значимых для следствия.[1]

При допросе потерпевшего и свидетеля чаще всего задается следующий перечень вопросов:

1. Каким образом произошло завладение информацией?

2. Проявлял ли кто-нибудь интерес к данной информации, программному обеспечению или компьютеру в организации?

3. Присутствовал ли кто-нибудь из посторонних лиц в помещении, где располагаются компьютеры?

---

[1] Смирнова И. Г. Тактические особенности производства допроса по делам о преступлениях в сфере компьютерной информации. URL: https://cyberleninka.ru/article/n/taktycheskie-osobennosti-proizvodstva-doprosa-po-delam-o-prestupleniyah-v-sfere-kompyuternoy-informatsii (дата обращения 18.04.2021).

4. Были ли сбои в работе программного обеспечения?

5. Пропадали ли носители компьютерной информации (флешки, диски, внешние жесткие диски и т.д.)?

6. Проверялись ли компьютеры на наличие вирусов и как давно была последняя проверка? Как в целом осуществляется защита компьютерной информации?

7. Как осуществляется доступ к компьютерной сети? Кто из пользователей имеет право на доступ и какие у них полномочия?

8. Кто является собственником компьютерной информации?

9. Совершал ли кто-либо необоснованных манипуляций с информацией?[1]

Так, например, согласно материалам уголовного дела № 1-345/2019подсудимая Захарова, работая в организации, оказывающей услуги мобильной связи, в рамках своих должностных обязанностей осуществляла продажу сим-карт, обрабатывала запросы клиентов, выполняла сервисные операции и обрабатывала персональные данные. Вступив в сговор с неустановленным лицом через социальную сеть Вконтакте, она неправомерно передавала ему персональные данные клиентов. А также заменяла отдельные сим-карты, путем подмены информации в лицевой карточке абонента, оформив услугу на получение другой сим-карты и смене номера абонента, осуществляла выдачу такой сим-карты. После чего вставляла выданную сим-карту в свой телефон, активировала её и принимала смс-сообщение, поступающее на этот номер с электронного кошелька, подтверждая легитимность этого перевода.[2]

1. Были ли случаи прослушивания телефонных разговоров?

---

[1]Коломинов В.В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: дис. … канд. юрид. наук. Иркутск, 2017. С. 28.

[2]Уголовное дело № 1-345/2019 по обвинению Захаровой М.А. по ч. 3 ст. 272, п. «а», «в» ч. 3 ст. 159.6 УК РФ. URL: https://sudact.ru/regular/doc/LkG0QbZcSoNb/ (дата обращения 07.03.2021).

2. Какой порядок работы с программами, как они обрабатываются и передаются?

Данный перечень вопросов не является полным, так как может меняться в зависимости от обстоятельств конкретного дела или допрашиваемых лиц.

Например, при допросе сотрудников, обеспечивающих информационную безопасность, следует выяснить:

- какие специальные технические средства для защиты информации они используют;
- какой порядок получения доступов у пользователей компьютерной сети в рабочее и внерабочее время;
- порядок изменения и присвоения паролей пользователей;
- порядок идентификации пользователей компьютерной сети.

При допросе сотрудников, отвечающих за техническое обслуживание компьютерных средств нужно выяснить:

- перечень и технические характеристики вычислительной техники, установленной в организации;
- перечень защитных технических средств;
- периодичность проведения ремонтных и профилактических работ;
- сведения о произошедших в последнее время выхода их строя аппаратуры.

При допросе начальников вычислительного центра или руководителей организаций нужно выяснить:

- организационную структуру вычислительного центра или IT-службы;
- сертифицированы ли технические устройства вычислительной техники и программы, использующиеся на предприятии;
- действуют ли правила эксплуатации ЭВМ и какой порядок осуществления контроля за соблюдением этих правил;

 какие сотрудники были в последнее время уволены и по каким причинам;

 были ли ранее случаи незаконного проникновения в помещения, в которых установлена компьютерная техника;

 были ли случаи несанкционированного доступа к компьютерной информации.[1]

Отдельно стоит обратить внимание, что при допросе системных администраторов и прочих IT-специалистов, работающих в организации нельзя забывать о том факте, что они могут быть причастны к совершенному преступлению. Поэтому к такому исходу событий нужно быть также готовым и предусмотреть это при составлении вопросов.

При наличии противоречий в показаниях разных лиц, можно использовать очную ставку.

Как мы ранее уже не раз отмечали, к допросу можно привлечь специалистов. При этом, его участие не ограничивается содействием в проведении определенных следственных действий. Следователь всегда может допросить специалиста. Ведь именно специалисты могут разъяснить сложные и непонятные следствиювопросы, касающиеся особенностей функционирования локальных сетей, работы разных программ, технические и программные аспекты работы компьютерных средств и т.д. Также специалисты могут помочь с объяснением профессиональных терминов и жаргонных понятий, характерных для программистов, хакеров и т.д.

Помимо специалистов, можно допросить также и экспертов. Допрос эксперта производится для разъяснения данного им заключения. Например, для компьютерных экспертиз в ходе допроса эксперта необходимо раскрыть сущность отдельных технических терминов, содержащихся в заключении.

---

[1] Смирнова И. Г. Тактические особенности производства допроса по делам о преступлениях в сфере компьютерной информации. URL: https://cyberleninka.ru/article/n/taktycheskie-osobennosti-proizvodstva-doprosa-po-delam-o-prestupleniyah-v-sfere-kompyuternoy-informatsii (дата обращения 18.04.2021).

Отдельно подробнее стоит остановиться на применении специальных познаний и порядке назначения экспертиз.

Ранеев работе мы уже не раз отмечали, что расследование мошенничества в сфере компьютерной информации имеет свои особенности, требующие специальных знаний в области компьютерных наук и техники.

В последние годы прогресс в сфере компьютерной информации набирает обороты. Поэтому невозможно от следователя или дознавателя требовать безоговорочной компетентности во всех вопросах, которые могут возникнуть в процессе расследования. Как справедливо отмечал в свое время В. Сперанский, что «юрист не обладает и не может обладать всеобъемлющими сведениями» в знаниях его имеются настолько существенные пробелы, что для того, чтобы выполнить свое назначение, он должен прибегать к содействию специалистов из тех областей науки, которые ему неизвестны, а порою и недостаточны, специализация и прогресс техники наших дней уже не позволяют представителю одной отрасли знания быть компетентным в другой. Именно поэтому недопустимо лишать их возможности обратиться за помощью к компетентным специалистам или экспертам».[1]

Круг лиц, обладающих специальными знаниями достаточно широк. Это могут быть сотрудники специальных экспертно-криминалистических подразделений полиции, представители контролирующих органов, системные-администраторы, IT-специалисты, программисты, инженеры и другие специалисты предприятий, сотрудники научно-исследовательских институтов и иные лица, имеющие специальную подготовку.[2]

Использовать специальные знания на предварительном и первоначальных этапах можно двумя способами:

---

[1]Смолькова И. В. Великие и выдающиеся, знаменитые и известные личности об уголовном судопроизводстве. М.: Юрлитинформ, 2012.С. 288-289.

[2] Головин А. Ю. Теория и практика классификационных исследований в криминалистической науке / А.Ю. Головин. Тула, 2000. С. 194.

 Консультация - привлечение специалиста для получения объяснения по узкопрофессиональным вопросам, в которых следователь некомпетентен. Справки и консультации специалист может предоставлять как в устной, так и в письменной форме.

 Участие в следственных действиях. Ранее мы уже приводили примеры участия специалиста при допросе и осмотре места происшествия.

Если роль специалиста – содействие в составлении правильной формулировки вопросов, фокусирование внимания на обстоятельствах, связанных с обнаружением и закреплением доказательства,дача разъяснений, касающихся их компетенций и оказание другой помощи следствию и суду,то эксперт более самостоятелен и к нему предъявляются более высокие требования. В отличие от исследований специалиста, экспертизы назначаются по решению суда, следователя или иного полномочного органа. Сущность судебной экспертизы заключается в разностороннем анализе экспертом, конкретных предметов и ответом на поставленные следователем вопросы.

Следователь сам вправе принять решение о привлечении специалистов и назначении экспертизы.

При подготовке к производству экспертизы следователю нужно:

 определиться с видом экспертизы;

 выбрать какие объекты будут исследоваться;

 четко сформулировать вопросы эксперту;

 определиться со временем производства экспертизы;

 выбрать экспертное учреждение;

 подготовить постановление о производстве экспертизы и ознакомить с ним владельца объекта исследования;

 направить данное постановление в экспертное учреждение.

В рамках расследования мошенничества в сфере компьютерной информации могут использоваться любые виды экспертиз, в том числе традиционные криминалистические, экспертизы веществ и материалов,

экономические, инженерно-технические и другие экспертизы, но чаще всего назначаются судебные компьютерно-технические экспертизы.[1]

Судебная компьютерно-техническая экспертиза делится на несколько видов:

- аппаратно-компьютерная экспертиза - проводится для исследования и особенностей эксплуатации аппаратных средств компьютерной техники, например, физических электронных носителей информации;
- программно-компьютерная экспертиза – проводится при исследовании особенностей создания и использования программного обеспечения;
- информационно-компьютерная экспертиза (данных) – основной вид компьютерно-технической экспертизы, который выявляет, анализирует и оценивает информацию, находящуюся на компьютерном носителе информации;
- компьютерно-сетевая экспертиза – исследует факты и обстоятельства, связанные с использованием сетевых и телекоммуникационных технологий.[2]

Отдельно стоит отметить, что при предоставлении объектов на исследование нужно соблюсти порядок изъятия, хранения и предоставления предметов для исследования.

После того как объект выбран, следователю нужно сформулировать вопросы эксперту. При этом перечень вопросов может меняться в зависимости от конкретного дела. Но есть ряд типичных вопросов, задаваемых эксперту при назначении судебной компьютерно-технической экспертизы:

- какой марки (модели) предоставленное компьютерное устройство?

---

[1] Звезда И.И. К вопросу о назначении судебной экспертизы при расследовании мошенничества в сфере компьютерной информации / И.И. Звезда // Известия Тульского государственного университета. Экономические и юридические науки Тула, 2018. С. 10.

[2] Введенская О.Ю. Лекции МВД: Особенности расследования преступлений в сфере компьютерной информации на первоначальном этапе / О.Ю. Введенская. Краснодар., 2016. С. 27.

- какие технические характеристики у данного устройства?
- какое функциональное предназначение данного компьютерного средства?
- исправно ли данное устройство?
- связана ли неисправность с нарушением правил эксплуатации аппаратного средства?
- данное средство является носителем информации?
- какие программы установлены на данном устройстве?
- через какого провайдера настроено подключение устройств к сети «интернет»?
- какая программа использовалась для работы в сети «интернет»?
- какие почтовые программы используются на компьютерно-техническом средстве?
- есть ли среди установленных программ, по, позволяющее копировать, блокировать, изменять и удалять информацию?
- есть ли в памяти компьютерно-технических средств следы несанкционированного доступа к информации?
- каким образом и когда было произведено несанкционированное использование или подключение к устройству?
- какие периферийные устройства были подключены к данному устройству?
- можно ли восстановить поврежденный файл на носителе, установленном в компьютере?
- какой вид установленного программного обеспечения (общесистемный, прикладной и т.д.)?
- какие реквизиты разработчика данного программного обеспечения?
- установлено ли на жестком диске программное обеспечение, позволяющее решить конкретные задачи?
- установлены ли системы защиты данного устройства?
- когда последний раз данное устройство использовалось?

- какой алгоритм работы данного программного обеспечения?
- были ли внесены какие-либо изменения в программное обеспечение и как это повлияло на функционал?
- есть на данных жестких дисках фрагменты программ, указывающие на полное или частичное копирование?
- какой формат данных, содержащихся на представленном образце (текстовый, графический и др.)?
- с помощью каких программ данные могут обрабатываться?
- какое содержание в данных, загруженных на данный электронный носитель информации и имеет ли она отношение к обстоятельствам расследуемого дела?
- какой аппаратный адрес имеют сетевые карты, находящееся в компьютере, представленном на исследование?
- содержатся ли на электронных носителях информации следы или готовые к распространению вредоносные программы, которые могут менять, добавлять, удалять, копировать информацию, нарушать функционирование компьютерных средств и сети?
- когда и кем были созданы установленные файлы?

Для правильной формулировки вопросов следователь может обратиться за помощью к специалисту.

После того, как все необходимые приготовления завершены и вопросы сформулированы, постановление о назначении экспертизы со всеми материалами дела передаются эксперту. Он знакомится с ними ипроверяет целостность предоставленных объектов. На этой стадии эксперт может отказаться от производства экспертизы. Связано это может быть с несоответствием компетенции эксперта или отсутствием остаточного количества объектов исследования.

По результатам проведенного исследования эксперт предоставляет заключение, в котором сформулированы выводы по поставленным вопросам.

Законодательством установлена форма заключения эксперта. В соответствии со ст. 204 УПК РФ в заключении обязательно должны указываться:

1. Дата, время и место производства судебной экспертизы;
2. Основания производства судебной экспертизы;
3. Должностное лицо, назначившее судебную экспертизу;
4. Сведения об экспертном учреждении, а также фамилия, имя и отчество эксперта, его образование, специальность, стаж работы, ученая степень и (или) ученое звание, занимаемая должность;
5. Сведения о предупреждении эксперта об ответственности за дачу заведомо ложного заключения;
6. Вопросы, поставленные перед экспертом;
7. Объекты исследований и материалы, представленные для производства судебной экспертизы;
8. Данные о лицах, присутствовавших при производстве судебной экспертизы;
9. Содержание и результаты исследований с указанием примененных методик;
10. Выводы по поставленным перед экспертом вопросам и их обоснование.

После того, как следователь ознакамливается заключением, топри необходимости он может провести допрос эксперта в рамках результатов егоисследования. В соответствии со ст. 205 УПК РФ: «Эксперт не может быть допрошен по поводу сведений, ставших ему известными в связи с производством судебной экспертизы, если они не относятся к предмету данной судебной экспертизы».

Чтобы заключение эксперта приобрело статус доказательства его необходимо проверить на допустимость, достоверность и относимость.

Если есть какие-либо сомнения, то следователь может обратиться за разъяснениями к специалистам и при необходимости назначить ещё одну экспертизу у другого эксперта.

После того, как указанные выше следственные действия в рамках первоначального этапа и первичный сбор общей информации о преступлении завершены, то процесс расследования переходит к последующему этапу.

Последующий этап включает в себя дальнейший сбор и оценку доказательств, а также установление всех предметов доказывания. Данный этап позволяет составить более полную картину происшествия и упорядочить сведения, полученные в результате расследования.

Ни в теории, ни в практике нет четких разграничений проведения следственных мероприятий на различных этапах. Поэтому следователь может использовать тот же самый набор процессуальных инструментов, что и на первоначальном этапе расследования.

В рамках последующего этапа мы рассмотрим особенности проведения допроса подозреваемого (обвиняемого) и проведение следственного эксперимента.

Следственный эксперимент может быть проведен как в рамках первоначального, так и в рамках последующего этапа расследования. Но, как показывает анализ судебной практики, данное следственное действие проводится применяется преимущественно на последующем этапе расследования.

Следственный эксперимент позволяет установить возможность совершения преступления, выявить особенности протекания механизмов преступного события, наличие специальных знаний и т.д.

На практике при расследовании мошенничества в сфере компьютерной информации проводятся следующие следственные эксперименты:

 проверка возможности проникновения в помещение (через двери, окна, с отключением и без отключения сигнализации);

 проверка возможности подключения компьютеров и получения доступа к компьютерной информации;

 проверка возможности проникновения в закрытые зоны с помощью подбора кодов и id;

 проверка возможности подключения к компьютерной сети и перехвата данных;

 проверка по установлению времени, необходимого для подключения и отключения к компьютерной сети;

 проверка по установлению времени, необходимого для внесения изменений в компьютерную информацию и копирование данных.

 проверка возможности совершения определенных операций с компьютерной информацией и т.д.

При проведении следственного эксперимента важно воссоздать условия в которых было совершено само преступление. В данном случае речь идет о проведении эксперимента на той же территории, в том же помещении и использовании тех же предметов и объектов.

Для того, чтобы получить максимальный объем информации и закрепить полученных результаты расследования, необходимо провести допрос подозреваемого (обвиняемого).Перед допросом, как правило, следователю нужно подготовиться в достаточно сжатые сроки. Во-первых, следователю необходимо подготовить доказательства, указывающие на причастность к преступлению подозреваемого (обвиняемого), во-вторых, максимально разузнать о личности преступника.

Перед допросом обязательно зачитываются права подозреваемого (обвиняемого).

Если речь идет только об обвиняемом, то допрос можно начать с вопроса о том, признает ли он себя виновным в предъявленном обвинении.

В процессе допроса лица дают показания: подозреваемые рассказывают об обстоятельствах, которые стали причинами задержания и других известным обстоятельствам дела, а обвиняемые рассказывают о

предъявленном обвинении, собранных доказательствах и других обстоятельствах преступления.

При допросе подозреваемого бывает так, что допрашиваемый слишком растерян из-за неожиданного задержания и готов дать показания или, наоборот, он может быть возмущен и агрессивен, в таком случае он будет отрицать свою причастность к преступлению.

В первом случае складывается бесконфликтная ситуация, которая позволяет получить информацию в полном объеме, путем постановки следователем наводящих вопросов.

Проверить правдивость описанных обстоятельств, следователь может путем постановки контрольных вопросов. Для этого следователь может:

 побуждать допрашиваемого к отказу от противодействия и введения следствия в заблуждение;

 создавать впечатление о безнадежности таких попыток;

 использовать сомнения допрашиваемого в целесообразности придерживаться выбранной линии поведения;

 внезапно предъявить уличающие доказательства и т.д.

В случае, если подозреваемый отказывается от дачи показаний или отрицает причастность к преступлению, то складывается конфликтная ситуация.

В данном случае следователь может применить следующие приемы:

 объяснить значение чистосердечного признания;

 отметить несоответствие показаний с материалами дела;

 задавать уточняющие вопросы;

 продемонстрировать вещественные доказательства, изъятое с места происшествия;

 назвать подозреваемому иные средства установления его причастности к содеянному: продемонстрировать соответствующие поисковые приборы, разъяснить возможности экспертиз и т.д.

 создать у допрашиваемого преувеличенное представление о степени своей осведомленности, сформировать впечатление, что следователю не известны только некоторые второстепенные обстоятельства.[1]

Если подозреваемый утверждает, что на момент совершения преступления он находился в другом месте, то необходимо безотлагательно провести допрос тех лиц, которые могли бы подтвердить алиби подозреваемого.

Эффективен способ, при котором постепенно предъявляются доказательства, причастности подозреваемого к конкретному делу. Порядок их предъявления может быть разным, но чаще всего начинают от менее важных до более веских. Но это сработает только в случае, если все доказательства достоверные, в противном случае подобный прием может усугубить ситуацию.

Также неправильное и поспешное предъявление доказательств может снизить их эффективность и натолкнуть допрашиваемого на выдвижение ложных объяснений. Поэтому следователю нужно заранее предвидеть такой исход событий при подготовке тактики допроса.

Если доказательств недостаточно, то следователь может воспользоваться противоречиями и оговорами допрашиваемого.

При допросе нескольких подозреваемых по делам о групповых преступлениях целесообразно использовать психологические феномены межличностного взаимодействия: разнонаправленные интересы членов группы, соперничество, антагонизм, нарушенную согласованность групповых позиций, а также стремление отдельных членов группы приуменьшить свою роль в совершении преступления.[2]

[1.] Рычкалова Л.А. Проблемы тактики допроса подозреваемого и обвиняемого. URL: https://cyberleninka.ru/article/n/problemy-taktiki-doprosa-podozrevaemogo-i-obvinyaemogo (дата обращения 10.05.2021).

[2]Рычкалова Л.А. Проблемы тактики допроса подозреваемого и обвиняемого. URL: https://cyberleninka.ru/article/n/problemy-taktiki-doprosa-podozrevaemogo-i-obvinyaemogo (дата обращения 10.05.2021).

При допросе обвиняемого можно воспользоватьсятакими же приемами. Но обвиняемый – наиболее информированный и сложный источник информации. Поэтому при допросе нужно обязательно учитывать его психологическое состояние: подавленность, депрессия, страх и т.д.

Эффективным будет применение психологического воздействия на обвиняемого. В зависимости от ситуации можно использовать следующие приемы воздействия:

- активизировать положительные качества допрашиваемого;
- разъяснить правовые последствия деятельного раскаяния и активной помощи в раскрытии преступления.

Допрос группы лиц, обвиняемых в преступлении будет зависеть от их места иерархии и связи с другими членами группы. Например, наличие родственных связей, страх по отношению к вышестоящим членам группы и т.д.

Если подозреваемый, (обвиняемый) идет на контакт, то необходимо узнать подробности о мошеннической схеме, изменениях, внесенных в программу, какое вредоносное программное обеспечение он использовал, действовал ли он один или в сговоре с другими лицами, куда передавалась полученная информация и другие обстоятельства, имеющие значение при расследовании мошенничества в сфере компьютерной информации.

Как мы уже ранее отмечали, присутствие специалистов на допросе подозреваемых или обвиняемых чаще всего негативно влияет на результаты допроса и не позволяет следователю наладить психологический контакт с допрашиваемым. Поэтому в данном случае лучше просто ограничится помощью с формулированием вопросов.

Порядок окончания последующего этапа расследования регламентируется ст. 215 УПК РФ: «Признав, что все следственные действия по уголовному делу произведены, а собранные доказательства достаточны для составления обвинительного заключения».

Но существует мнение, что окончание следственных действий происходит в рамках заключительного этапа, который включает в себя ознакомление обвиняемого со всеми материалами дела и разъяснения его прав.[1]

Подводя итог, важно отметить, что не существует четкого разделения следственных действий на первоначальный и последующий этапы. Следователь может использовать любой законный инструмент для получения информации о преступлении независимо от этапа расследования.

Расследование мошенничества в сфере компьютерной информации имеет свои особенности, которые обуславливаются механизмом совершенного преступления и субъектами его совершившими. Поэтому для того, чтобы достигнуть желаемого результата необходимо заранее тщательно готовиться к производству каждого следственного действия, используя различные приемы и помощь специалистов.

[1]Лобунец Е.С. Назначение и содержание этапов расследования преступлений. М.: Юрлитинформ, 2015. С. 27-28.

ЗАКЛЮЧЕНИЕ

На основании исследования по теме: «Методика расследования мошенничества в сфере компьютерной информации», можно сделать следующие выводы:

1. Мошенничество в сфере компьютерной информации имеет особенности, влияющие на разработку методических рекомендаций расследования. С одной стороны, это связано с самим понятием «мошенничества», как хищения чужого имущества или приобретение на него права, а с другой – подобного рода преступления происходят в виртуальной среде, путем ввода, удаления, изменения и другого вмешательства в данные. Именно этот факт является главным при разработке криминалистической характеристики мошенничества в сфере компьютерной информации.

2. Криминалистическая характеристика – это сложная структура, которая состоит из следующих элементов: способ совершения преступления, особенности следовой информации, особенности обстановки совершения преступления (место совершения преступления, время совершения преступления и др.), личностная характеристика преступника, особенности непосредственного предмета преступного посягательства.

Из-за сложной специфики, начать расследование мошенничества в сфере компьютерной информации не просто. Для этого следователю нужно иметь специфические знания и умения. Но благодаря тесной взаимосвязи элементов криминалистической характеристики для следствия появляется ориентир, который не просто дает толчок в расследовании, но и позволяет выдвигать типичные следственные версии и направлять поиск в нужное русло.

3. Предпосылкой любого расследования является стадия возбуждения уголовного дела. Эта стадия подразумевает следующий алгоритм действий: приём, регистрацию, проверку сообщений о преступлении и принятие решения об отказе или о возбуждении уголовного дела.

Для правильного принятия решения следователями проводится предварительная проверка. Это необязательная процедура, но, как показывает практика, в делах о мошенничестве в сфере компьютерной информации она достаточно распространена.

Важным моментом её проведения является оперативное проведение проверочных мероприятий для собора максимального количества информации и быстрого принятия решения. В лучшем случае при правильных и оперативных действиях следователя можно раскрыть преступление «по горячим следам».

Для мошенничества в сфере компьютерной информации наиболее часто используемыми проверочными действиями являются: получение объяснений, осмотр места происшествия, истребование необходимых материалов и проведение оперативно-розыскных действий.

4. Расследование любого преступления происходит поэтапно. После возбуждения уголовного дела наступает первоначальный и последующие этапы расследования. В рамках первого, формируется основной пласт доказательственной базы. На последующем этапе сведения, полученные ранее упорядочиваются, и картина преступления полностью складывается.

Для любого этапа могут использоваться любые предусмотренные законом следственные действия.Чаще всего производятся: осмотр места происшествия, обыски; выемки; допросы; назначение экспертизы и т.д. Отдельно хотелось бы остановиться на роли экспертов и специалистов в расследовании рассматриваемого вида преступлений. Из-за сложной специфики расследования данной категории дел и низкой компетентности следователей в вопросах, связанных с компьютерной информацией, очень часто приходится привлекать лиц, обладающих специальными знаниями.

Подводя итог можно сделать вывод, что мошенничество в сфере компьютерной информации это преступление с высоким уровнем латентности. Потерпевшие не всегда знают, что стали жертвой преступления или же не видят причин для обращения в правоохранительные органы.

На наш взгляд основными проблемами расследования мошенничества в сфере компьютернойинформацииявляются:

1. Низкая квалификация следователей и дознавателей в области компьютерных технологий.

2. Слабая научная база из-за недостаточного количества внимания со стороны ученых к изучению проблем мошенничества в сфере компьютерной информации. Данная тенденция с каждым годом меняется, но в любом случае, в силу своей новизны, эта сфера остается одной из самых слабоизученных.

3. Недостаточное количество практики расследования некоторых видов мошенничества в сфере компьютерной информации. По большей части это связано с быстрым появлением новых способов интернет-мошенничества и с высокой латентностью.

4. Относительно низкий уровень раскрываемости мошенничества в сфере компьютерной информации. Данный пункт является следствием всех вышеперечисленных проблем.

На данный момент следствие использует весь спектр следственных действий для раскрытия мошенничеств в сети Интернет. Но не избавившись от всех вышеперечисленных проблем невозможно повысить раскрываемость.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

РАЗДЕЛ I НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ И ИНЫЕ ОФИЦИАЛЬНЫЕ АКТЫ

1. Уголовный Кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // СЗ РФ. 1996. № 25. Ст. 2347.
2. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ // СЗ РФ.2001. № 249. Ст. 4921.
3. Федеральный закон «Об информации, информационных технологиях и защите информации» от 27 июля 2006 г. № 149-ФЗ // СЗ РФ. 2006. № 31 (часть I) ст. 3448.
4. Приказ Следственного комитета России «Об организации приема, регистрации и проверки сообщений о преступлении в следственных органах (следственных подразделениях) системы Следственного комитета Российской Федерации» от 11 октября 2012 г. № 72 // Российская газета. 2013. № 48.
5. Статистические данные о состоянии преступности в России за январь-декабрь 2019 года. Официальный сайт Министерства Внутренних Дел. URL: https://xn--b1aew.xn--p1ai/reports/item/19412450/ (дата обращения 12.02.2021).
6. Статистические данные о состоянии преступности в России за январь-декабрь 2020 года. Официальный сайт Министерства Внутренних Дел. URL: https://xn--b1aew.xn--p1ai/reports/item/22678184/ (дата обращения 12.02.2021).

РАЗДЕЛ II ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. Аверьянова, Т.В. Криминалистика: Учебник для вузов / Т.В. Аверьянова, Р.С. Белкин. М.: Издательство НОРМА, 2002. 960 с.
2. Агафонов, В. В. Криминалистика / В. В. Агафонов, А. Г. Филиппов. М.: Издательство Юрайт, 2015. 184 с.

3. Аносов, А.В. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий. / А.В. Аносов, Гаврилин Ю. В., Васильченко Д. А. и др. М.: Академия управления МВД России, 2019. 208 с.

4. Белицкий, В.Ю. Распространенные виды мошенничеств в сети интернет

5. / В.Ю. Белицкий. // Актуальные проблемы современности. Барнаул. 2020. №2(28). С 31-36.

6. Белкин, Р.С., Понятие, ставшее «криминалистическим пережитком» / Р.С. Белкин. // Российское законодательство и юридические науки в современных условиях; состояние, проблемы, перспективы. М., 2000. С. 11−12.

7. Бердникова, О. П. Особенности возбуждения уголовных дел о мошенничестве в сфере компьютерной информации и типичные следственные ситуации на первоначальном этапе расследования / О.П. Бердникова // Вестник Уральского юридического института МВД России. М. 2020. С.46-49.

8. Бессонов, С.А. К вопросу о структуре и природе криминалистической характеристики преступлений / С. А. Бессонов // Вестник Поволжского института управления. Саратов, 2014. № 4(43). С. 54.

9. Введенская, О.Ю. Лекции МВД: Особенности расследования преступлений в сфере компьютерной информации на первоначальном этапе / О.Ю. Введенская. Краснодар., 2016. 125 с.

10. Вехов, В.Б. Компьютерные преступления. Способы совершения, методики расследования / В.Б. Вехов. М.: Право и закон, 1996. С. 182.

11. Вехов, В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и сведений. Волгоград, 2008. 408 с.

12. Гаврилин, Ю.В. Расследование неправомерного доступа к компьютерной информации / Ю.В. Гаврилин, А.В. Пушкин, Н.Г. Шурухнов и д.р. М.: ЮИ МВД РФ, 2004. С. 320.

13. Гаврилин, Ю.В. Особенности следообразования при совершении мошенничеств в сфере компьютерной информации / Ю.В. Гаврилин, В.В. Шипилов. // Российский следователь. 2013. №23. С. 2-6.

14. Головин, А. Ю. Теория и практика классификационных исследований в криминалистической науке / А.Ю. Головин. Тула, 2000. 196 с.

15. Драпкин, Л.Я. Криминалистика / Л.Я Драпкин, В.Н Карагодин. М.: Проспект, 2011. 768 с.

16. Дударчик, Я.Ю. Анализ взглядов на криминалистическую характеристику преступлений / Я.Ю. Дударчик // Вестник Академии МВД. Краснодар, 2017. № 2. С. 45-48.

17. Звезда, И.И. К вопросу о назначении судебной экспертизы при расследовании мошенничества в сфере компьютерной информации / И.И. Звезда // Известия Тульского государственного университета. Экономические и юридические науки Тула, 2018. С 10.

18. Зигура, Н.А. Компьютерная информация как вид доказательств в уголовном процессе России: дис. ... д-ра юрид. наук / Зигура Н.А. Челябинск. 2010. 234 с.

19. Козлов, В.Е. Теория и практика борьбы с компьютерной преступностью / В.Е. Козлов. М.: Горячая линия – Телеком, 2002. 336 с.

20. Колесниченко, А.Н. Научные и правовые основы расследования отдельных видов преступлений: автореф. дис. ... д-ра юрид. наук / А.Н. Колесниченко. Харьков, 1967. 27 с.

21. Коломинов, В.В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: дис. … канд. юрид. наук / В.В. Коломинов. Иркутск, 2017. 93 с.

22. Комарова, А.А. Интернет-мошенничество: проблемы детерминации и предупреждения: монография. / А.А. Комарова. М.: Юрлитинформ, 2013. 179 с.

23. Конин, В.В. Тактико-криминалистическое обеспечение предварительной проверки заявлений и сообщений в рамках стадии возбуждения уголовного дела / В.В. Конин // Криминалистика: вчера, сегодня, завтра. Иркутск, 2020. №2 (14) С.116-130

24. Коновалов, С.И. Теоретико-методологические проблемы криминалистики: / С.И. Коновалов. Ростов-на-Дону: РЮИ МВД России, 2001. 85 с.

25. Корнакова, С.В. Процессуальный статус прокурора в стадии возбуждения уголовного дела / С.В. Корнакова, А.В. Чубыкин. М.: Юрлитинформ, 2015. 200 с.

26. Лавров, В.П. Криминалистика / В.П. Лавров. М.: Норма, 1999. 181 с.

27. Лавров, В.П. Криминалистическая характеристика преступления / В.П. Лавров, А.Ф. Волынский. М., 2009. С. 30.

28. Лобунец, Е.С. Назначение и содержание этапов расследования преступлений / Е.С. Лобунец. М.: Юрлитинформ, 2015. 160 с.

29. Лубин, А.Ф. Методология криминалистического исследования механизма преступной деятельности: дис. … канд. юрид. наук / А.Ф. Лубин. Новгород, 1997. 337 с.

30. Менце, Т. Кибербезопасность систем промышленной автоматизации в 2019 году. URL: https://ics.kaspersky.ru/media/Kaspersky-ARC-ICS-2019-Trend-Report-Ru.pdf (дата обращения 27.01.2021).

31. Мещеряков, В.А. Формирование доказательств на основе электронной цифровой информации. URL: https://cyberleninka.ru/article/n/formirovanie-dokazatelstv-na-osnove-elektronnoy-tsifrovoy-informatsii/ (дата обращения 10.03.2021).

32. Мещеряков, В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. / В.А. Мещеряков. Воронеж, 2012. 150 с.

33. Пантелеев, И.Ф. Методика расследования преступлений / И.Ф. Пантелеев. М., 1975. 592 с.

34. Протасевич, А.А. Криминалистическая характеристика компьютерных преступлений / А.А. Протасевич, Л.П. Зверянская // Российский следователь. 2013. № 11. С. 115.

35. Рычкалова, Л.А. Проблемы тактики допроса подозреваемого и обвиняемого. URL: https://cyberleninka.ru/article/n/problemy-taktiki-doprosa-podozrevaemogo-i-obvinyaemogo (дата обращения 10.05.2021).

36. Самойлов, А.В. Современное состояние учения о криминалистической характеристике преступлений / А. В. Самойлов // Российский следователь. М., 2010. № 22. С. 5.

37. Сергеев, Л.А. Расследование и предупреждение преступлений совершаемых при производстве строительных работ: автореф. дис. ... канд. юрид. наук. М., 1966. 234 с.

38. Смирнова, И. Г. Тактические особенности производства допроса по делам

о преступлениях в сфере компьютерной информации. URL: https://cyberleninka.ru/article/n/takticheskie-osobennosti-proizvodstva-doprosa-po-delam-o-prestupleniyah-v-sfere-kompyuternoy-informatsii (дата обращения 18.04.2021).

39. Смолькова, И. В. Великие и выдающиеся, знаменитые и известные личности об уголовном судопроизводстве / И. В. Смолькова. М.: Юрлитинформ, 2012. 688 с.

40. Старичков, М.В. Понятие «Компьютерная информация» в российском уголовном праве. URL: https://cyberleninka.ru/article/n/ponyatie-kompyuternaya-informatsiya-v-rossiyskom-ugolovnom-prave/viewer (дата обращения 30.04.2021).

41. Старичков, М.В. Способ совершения как элемент криминалистической характеристики мошенничества в сфере компьютерной информации / М.В. Старичков // Криминалистика: вчера, сегодня, завтра. 2018. № 4. С. 177-179.

42. Степанов-Егиянц, В.Г. Понятие «компьютерная информация» с точки зрения её уголовно-

правовой защиты. URL: https://cyberleninka.ru/article/n/ponyatie-kompyuternaya-informatsiya-s-tochki-zreniya-ugolovno-pravovoy-zaschity.

43. Уткин, М.С. Некоторые вопросы общей методики расследования преступлений / М.С. Уткин. Омск: Омская высш. шк. милиции, 1986. С. 26.

44. Чистов, Л.Е. Методика расследования отдельных видов мошенничества: учеб. Пособие / Л.Е. Чистова, А. Г. Филиппов и др. М.: МосУ МВД России, 2014. С. 41.

45. Шаров, А.В. Методика проведения доследственной проверки материалов, содержащих признаки мошенничества, при отчуждении квартир, находящихся в собственности граждан / А.В. Шаров // Вестник криминалистики. М., 2002. С. 62.

46. Шевченко, Е.С. Тактика производства следственных действий при расследовании киберпреступлений: автореф. дис. …канд. юрид. наук: 12.00.12 / Е.С. Шевченко. М., 2016. 249 с.

47. Яблоков, Н.П. Информационные основы расследования и криминалисти ческая характеристика преступлений / Н.П Яблоков, Л.Д., Самыгин. М.: Бек, 1995 С. 45.

48. Статистические данные Hi-Tech Crime Trends за 2020 – 2021 год. URL: https://www.group-ib.ru/blog/trends20_21 (дата обращения 27.01.2021).

49. Сайт производителя MOBILedit оборудования для цифровой криминалистики URL: https://www.mobiledit.com/forensic-express (дата обращения 18.03.2021).

РАЗДЕЛ III ПОСТАНОВЛЕНИЯ ВЫСШИХ СУДЕБНЫХ ИНСТАНЦИЙ И МАТЕРИАЛЫ ЮРИДИЧЕСКОЙ ПРАКТИКИ

1. Уголовное дело № 1-345/2019 по обвинению Захаровой М.А. по ч. 3 ст. 272, п. «а», «в» ч. 3 ст. 159.6 УК РФ. URL: https://sudact.ru/regular/doc/LkG0QbZcSoNb/ (дата обращения 07.03.2021).

2. Уголовное дело № 1- 588/18 по обвинению Редозубов А.Г. по ч. 2 ст. 159.6, ч. 2 ст. 273 УК РФ URL: https://sudact.ru/regular/doc/o3PSlcynw8Lv/ (дата обращения 10.03.2021).

3. Уголовное дело № 1-277/2020 по обвинению Мишланова Д. Е. по .3 ст.30, п.«б» ч.3 ст.159.6 УК РФ, / Архив Советского районного суда г. Владивостока. URL: https:// sudact.ru/regular/doc/4AyuDmz7J9oX/ (дата обращения 18.03.2021).