Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)
Юридический институт

ДОПУСТИТЬ К ЗАЩИТЕ В ГЭК
Руководитель ООП
доктор юридических наук, профессор

_____ В.А. Уткин
подпись
«_____»_____ 2021 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА МАГИСТРА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

ОСОБЕННОСТИ ВЫЯВЛЕНИЯ И РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

по направлению подготовки 40.04.01 Юриспруденция
направленность (профиль) «Российская уголовная юстиция»

Душаев Олег Олегович

Руководитель ВКР
доктор юридических наук, профессор

_____Р.Л. Ахмедшин
подпись
«18» мая 2021 г.

Автор работы
студент группы № 061984

_____ О.О. Душаев
подпись
«18» мая 2021 г.

Томск – 2021

Аннотация магистерской диссертации на тему: «Особенности выявления и расследования мошенничества в сфере компьютерной информации».

В магистерской работе рассмотрены особенности выявления и расследования мошенничества, в сфере компьютерной информации предусмотренного ст. 159.6 Уголовного кодекса РФ.

Актуальность темы исследования заключается в том, что мошенничество – один из самых распространенных видов экономических преступлений, а характер способов совершения мошенничества в Российской Федерации, в связи с расширением и усложнением механизмов хозяйственного комплекса, становится более изощренным. Несмотря на то, что норма статьи 159.6 УК РФ введена почти 9 лет назад, она не является совершенной, а поэтому существуют вопросы применения и борьбы с мошенничеством в сфере компьютерной информации.

Предметом исследования выступает: особенность криминалистической характеристики мошенничества в сфере компьютерной информации, а также информационная модель совершения мошенничества в сфере компьютерной информации, как составляющая механизма совершения преступления.

Практическая значимость исследования заключается в исследовании уголовно-правовой и криминалистической характеристики мошенничества в сфере компьютерной информации, а также способов их совершения, и разработке на их основе предложений по совершенствованию действующего законодательства в части, а также в разработке практических рекомендаций по совершенствованию расследований в данной сфере, которые могут быть использованы правоохранительными органами.

Целью работы является анализ криминалистической характеристики мошенничества в сфере компьютерной информации, а также анализ информационной модели механизма совершения данного преступления.

Объектом исследования являются общественные отношения, возникающие в процессе расследования хищений чужого имущества или

приобретения 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.

Объем основного содержания работы составил 60 страниц, было использовано 30 источников.

Структура работы отражает выполнение поставленных целей и задач. Магистерская диссертация состоит из введения, 3 глав, 7 параграфов, заключения, списка использованной литературы и нормативно-правовых актов.

Во введении магистерской диссертации отражается актуальность избранной темы исследования, устанавливаются цели и задачи исследования, предмет, объект и методы исследования, определяются теоретическая основа исследуемой тематики.

В первой главе «Природа криминалистической характеристики» рассматривается общее понятие и структура криминалистической характеристики преступления как в целом, так и в отношении мошенничества в сфере компьютерной информации.

Во второй главе «Общие положения криминалистической характеристики мошенничества в сфере компьютерной информации» рассматривается механизм совершения преступления, а также криминалистическая характеристика личности преступника, совершившего мошенничество.

В третьей главе «Информационная модель механизма совершения преступления, предусмотренного ст. 159.6 УК РФ, ее соотношение с криминалистической характеристикой мошенничества в сфере компьютерной информации» рассматривается информационная модель совершения мошенничества в сфере компьютерной информации, как составляющая механизма совершения преступления.

В заключении магистерской диссертации формулируется основные выводы исследования, определяются соответствие достигнутых результатов поставленным целям и задачам.

Содержание

Введение

Актуальность темы исследования заключается в том, что мошенничество – один из самых распространенных видов экономических преступлений, а характер способов совершения мошенничества в Российской Федерации, в связи с расширением и усложнением механизмов хозяйственного комплекса, становится более изощренным. Несмотря на то, что норма статьи 159.6 УК РФ введена почти 9 лет назад, она не является совершенной, а поэтому существуют вопросы применения и борьбы с мошенничеством в сфере компьютерной информации.

Объектом исследования являются общественные отношения, возникающие в процессе расследования хищений чужого имущества или приобретения 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.

Предметом исследования выступает: особенность криминалистической характеристики мошенничества в сфере компьютерной информации, а также информационная модель совершения мошенничества в сфере компьютерной информации, как составляющая механизма совершения преступления.

Целью работы является анализ криминалистической характеристики мошенничества в сфере компьютерной информации, а также анализ информационной модели механизма совершения данного преступления.

Для достижения данной цели были поставленные следующие задачи:

1) рассмотреть механизм совершения преступлений, предусмотренных ст. 159.6 УК РФ;

2) проанализировать личность преступника, совершившего мошенничество в сфере компьютерной информации, с криминалистической стороны.

3) рассмотреть понятие информационной модели механизма совершения преступления в криминалистической науке;

4) выявить содержание информационной модели механизма совершения мошенничества в сфере компьютерной информации;

5) соотнести понятия «информационная модель совершения мошенничества в сфере компьютерной информации» и «криминалистическая характеристика преступления».

Нормативную базу исследования составили положения Конституции Российской Федерации, нормы действующего уголовного и уголовно–процессуального законодательства, других законов и подзаконных нормативных актов, относящихся к теме магистерской диссертации.

Методологическая основа исследования, позволяющая комплексно и всесторонне изучить проблему, рассматриваемую в настоящей данной работы: общенаучный, специально–юридический, методы системного анализа и сравнительного правоведения.

Для написания настоящей магистерской работы, также, были изучены учебные пособия, учебная литература, монографическая литература, статьи ученых–криминалистов.

Структура данной работы обусловлена целью и задачами исследования и состоит из введения, трех глав, включающих семь параграфов, заключения, списка использованных источников и литературы.

Глава 1. Природа криминалистической характеристики.

1.1 Понятие криминалистической характеристики.

Успех расследования любого уголовного преступления во многом определяется способностью следователя проникнуть не только в уголовно-правовую, но и в его криминалистическую сущность. Правильно понять криминалистическую природу совершенного - ее криминалистические характеристики, следователь может только при определенных условиях. Для этого он должен иметь представление о типичных криминалистически значимых характеристиках различных видов преступлений, а также уметь целенаправленно определять необходимую криминалистическую информацию по каждому конкретному преступлению и сравнивать ее с типовыми криминалистическими характеристиками соответствующего вида преступления. соответствующие правонарушения. вид преступления. Криминалистическая характеристика преступлений - важная научно-самостоятельная понятийная категория криминалистической науки, важная как для ее общей теории (теоретические положения отдельных ее частей), так и для практической следственной деятельности, особенно методики расследования преступлений. Эту характеристику иногда называют типовой.

Типовой криминалистической характеристикой вида преступления является система научного описания криминалистически важных признаков вида, разновидности, группы преступлений, которые проявляются, прежде всего, в особенностях таких элементов, как способ, механизм и обстановка их совершения, личности их субъекта и иных свойственных для характеризуемого вида преступления элементах с раскрытием корреляционных связей и взаимозависимостей между ними, знание которых вместе с содержательной стороной описания обеспечивает успешное расследование уголовных преступлений. Эта типовая криминалистическая характеристика, в свою очередь, формируется на основе результатов научного анализа и обобщения различных криминалистических характеристик

отдельных уголовных дел по данному виду преступлений, прошедших судебное рассмотрение.

Данные о способе совершения преступления в криминалистическом понимании являются одним из важнейших элементов анализируемой структурной системы криминалистических характеристик. Способ совершения преступления, который оставляет свои следы в его последствиях, является важным источником информации о качественных аспектах преступников. Важная с криминалистической точки зрения информация о способах совершения преступления в основном носит модальный характер, а ее конкретные носители и источники, в зависимости от типа совершенного преступления, могут быть всех трех типов (субъективные, объективные и модальные).

Именно такой характер данных позволяет быстро и точнее ориентироваться в характере и особенностях совершенного преступления, его обстоятельствах, круге лиц, среди которых должны искать преступника, и предлагать наилучшие способы раскрытия преступлением.

В зависимости от того, как преступление совершено в криминалистическом смысле, целесообразно понимать объективно и субъективно обусловленную систему поведения субъекта до, во время и после преступления, оставляющую различные типы характерных следов, позволяющих с помощью криминалистических методов и средств получить представления о происшедшем, об оригинальности преступного поведения преступника, его индивидуальных персональных данных и, соответственно, для определения наиболее оптимальных методов решения задач по раскрытию уголовного преступления. Криминалистическое понимание того, как совершается преступление, в некоторой степени отличается от его уголовно-правового толкования. Для криминалистов при совершении преступлений на первый план выходят те информационные аспекты (особенности), которые являются результатом внешнего проявления закономерностей отражения основных особенностей избранного способа достижения преступных целей. В

этом контексте большую ценность представляют следы того, как преступник добился следующего: каким образом он добрался до места преступления, покинул его, преодолел различные препятствия, использовал свое служебное положение, выполнил намеченную преступную цель, какие фальшивые документы, навыки, знания и физические усилия применил, пытался (или не пытался) скрыть следы совершенного деяния.

Структура способа совершения преступления в криминалистическом и уголовном смысле - категория непостоянная. В зависимости от оригинальности виновного поведения, особенностей ситуаций, возникающих до и после совершения преступления, и других обстоятельств, она может быть трехзвенной (включая поведение субъекта до, во время и после совершения преступления) двухзвенной (в различных сочетаниях) и однозвенной (характеризуют поведение субъекта только во время самого преступного деяния). В случае умышленных преступлений данные о том, как они были совершены, обычно являются основным элементом их криминалистической характеристики, для неосторожных же преступлений в силу своеобразия волевого негативного поведения субъекта, как правило, не имеют такого значения.

Существенная криминалистическая информация также содержит данные о механизме совершения преступления, которые, в отличие от информации о способе совершения преступления, характеризуют не качественную, а последовательную технологическую сторону преступления. Уточнение последовательности правонарушений при совершении преступления позволяет, помимо прочей информации о механизме, более точно понять детали расследуемого события и на этой основе определить оптимальные способы выявления причинно-следственной связи, а также для выявления возможных местонахождений оставшихся материальных и идеальных следов.

Под механизмом совершения преступления понимается временной и динамический порядок связи между различными стадиями, обстоятельствами, факторами подготовки, совершения и сокрытия следов преступления, которые позволяют воссоздать образ процесса его совершения. Для правильного понимания механизма совершения преступления необходима криминалистическая информация всех трех типов (субъективная, объективная и модальная), а значит, от всех этих потенциальных носителей и источников. Значение данных механизма как элемента криминалистической характеристики для разных преступлений неодинаково. Для преступлений с достаточно выраженным внешним характером взаимодействия предметов, явлений, лиц, иных предметов и факторов в процессе их совершения информация о механизме обычно является важным элементом их криминалистической характеристики. В преступлениях, образ которых менее динамичен, информация о механизме может иметь второстепенное значение.

Важная криминалистическая информация обычно содержится при определении обстановки совершения преступления. Событие преступления (на всех его этапах), непосредственно предшествующая подготовка (если таковая имеется) и, соответственно, непосредственная скрытность следов деяния происходят в конкретных условиях места с его материальной ситуацией, временем, освещенности, проявлением определенные природно-климатические факторы, производственная деятельность, быт и т. д.

Под криминалистической обстановкой совершения преступления понимается система различных типов объектов, явлений и процессов, взаимодействующих до и во время совершения преступления, которые характеризуют место, время, материальные, климатические, производственные, бытовые и другие условия окружающей среды, поведенческие характеристики косвенных участников преступления, противоправные события, психологические связи между ними и другие факторы объективной реальности, определяющие возможность, условия и другие обстоятельства совершения преступления. Элементы обстановки

оставляют различные следы, которые могут быть установлены при криминалистическом анализе преступления в ходе его расследования. Модальная информация от различных носителей и источников имеет большое значение для ее понимания. Выявление и изучение криминалистической информации, особенно в начале расследования, обычно позволяет собрать основную информацию о криминальной ситуации, которая произошла до и во время события.

В частности, по таким автономным следам чаще всего можно получить следующую информацию:

- какие условия и факторы непосредственно предшествовали сопутствовавшему уголовному преступлению, каково их взаимодействие, содержание и характер воздействия на совершенное правонарушение;

- что преступник специально подготовил в связи с расследуемым происшествием и что от него не зависит;

- как фактическая ситуация, сложившаяся до и во время совершения преступления, обычно использовалась в преступных целях, в частности, при выборе метода совершения преступления;

- что в данной ситуации способствовало и предотвращало подготовку, совершение и сокрытие следов преступления и как преступник это учел;

- какие факторы необычных (нетипичных) характеристик проявились в сложившейся ситуации и какое влияние они оказали на совершение преступления;

- кто мог создать или использовать объективно сложившуюся ситуацию для совершения преступления и т. д.

Информация о обстановке, в которой было совершено преступление, обычно имеет решающее значение для криминалистической характеристики почти каждого преступления, поскольку она пересекается с данными о других его элементах и действует как своего рода систематизация, начинающаяся в пределах этой характеристики. Обстановка во многом определяет и

корректирует способ совершения преступления и в значительной степени влияет на характеристики и структуру его механизма.

Результаты каждой преступной деятельности содержат следы личности человека, ее осуществившего, и, в частности, сведения о некоторых его личных социально-психологических свойствах и качествах, преступном опыте, специальных знаниях, поле, возрасте, особенностях взаимоотношений с жертвой преступления и т.п. Личность преступника является объектом самостоятельного криминалистического изучения, а данные о нем — важным элементом криминалистической характеристики преступления.

В криминалистическом изучении личности преступника в настоящее время наметились два специфических направления. Первое предусматривает получение данных о личности неизвестного преступника с учетом вида, места и времени совершения деяния, предмета посягательства по оставленным им следам на месте происшествия, в памяти свидетелей и по другим источникам. Это позволяет определить направления и приемы его розыска и задержания. Второе — изучение личности задержанного подозреваемого или обвиняемого с целью криминалистической оценки личности субъекта. В этих целях целесообразно собрать сведения не только о жизненной установке, ценностных ориентациях, дефектах правосознания, особенностях антиобщественных взглядов, но главным образом и о том, какая информация о личности субъекта преступления, его связях, особенностях поведения до и во время совершения преступления поможет наладить с ним необходимый контакт, выбрать наиболее эффективную тактику общения с целью получения от него правдивых показаний, а также определить наиболее действенные способы профилактического воздействия на него.

В тех случаях, когда преступление совершается организованной преступной группой, она становится самостоятельным объектом криминалистического изучения и соответственно одним из элементов криминалистической характеристики данного преступления. При этом

изучаются особенности группы с точки зрения степени ее организованности, структуры, разветвленности, ролевых функций ее участников и др.

Информация о личностных характеристиках потерпевшего также играет важную роль в структуре криминалистической характеристики определенных видов преступлений. Криминалистическая информация об этом свойстве позволяет более подробно охарактеризовать личность преступника, мотивы совершения преступления и соответственно, помочь более точно определить круг людей, среди которых следует искать преступника, и спланировать поисковые действия, чтобы найти наиболее важные доказательства по делу. В частности, выявление и изучение криминально значимых характеристик личности и поведения жертвы (до, во время и после совершения преступления) позволяет глубже понять многие обстоятельства преступления, особенно те, которые указывают на оригинальность, направленность и мотивы преступника, его общие (типичные) и индивидуальные свойства. Это вполне объяснимо, ведь между преступником и жертвой чаще всего наблюдается определенная взаимосвязь, из-за которой преступники обычно не выбирают людей случайным образом в качестве объекта своего преступного вмешательства. Поэтому неудивительно, что в случае преступлений с участием потерпевших идентификация преступника во многом определяется цепочкой потерпевший - подозреваемый - обвиняемый. Особенно важно выявить и изучить эту взаимосвязь в начале расследования.

Поэтому для выбора наиболее подходящих методов расследования различных видов преступлений обычно используются разные криминалистические данные о личности потерпевших. Выявление характеристик потерпевших, характерных для конкретного вида преступлений, их анализ, обобщение и систематизация позволяют создать криминалистическую типологию потерпевших, которая дополнительно обогащает криминалистическую характеристику отдельных видов преступлений.

1.2 Современное состояние учения о криминалистической характеристики преступления.

Криминалистическая характеристика преступлений - сравнительно новое понятие в криминалистической науке. Тема криминалистической характеристики преступлений затрагивалась в работах А.Н. Колесниченко, Л.А. Сергеева, С.П. Митричева, П.И. Тарасова-Родионова и других ученых. Я считаю стоит рассмотреть положения, выдвигаемые учеными относительно данной категории.

Криминалистическая характеристика преступлений, как отмечают некоторые авторы, стала в последние годы базовой концепцией криминалистики как науки.[1]

Многие ученые считают, что криминалистическая характеристика - это научная абстракция, основанная на анализе следственных, экспертных, оперативно-розыскных, криминалистических и криминалистических практик.[2]

Я думаю, стоит согласиться с определением криминалистической характеристики преступлений как научной абстракции, потому что абстракция — это то, что не имеет практического применения (от латинского Abstractio - «отвлеченность, неприложенность, неприменимость»[3]). Криминалистическая характеристика преступлений, хотя и является искусственной, чисто научной концепцией, тем не менее основана на изучении конкретных преступлений и служит для успешного выявления и раскрытия определенных преступлений. И используемый термин «искусственное понятие» никоим образом не умаляет огромного значения криминалистической характеристики преступлений.

Относительно значения криминалистической характеристики преступлений можно сказать следующее.

---

[1] Образцов В.А. Криминалистическая характеристика преступлений: дискуссионные вопросы и пути их решения // Криминалистическая характеристика преступлений. С. 7.
[2] Белкин Р.С. Курс криминалистики: В 3 т. М., 1997. Т. 3. С. 317.
[3] Большой словарь иностранных слов. М., 1998. С. 11.

Подавляющее большинство ученых придерживаются мнения, что криминалистическая характеристика уголовных преступлений способствует более успешному выполнению служебных функций криминалистики, в том числе повышению уровня учебно-методической работы, проводимой следственными органами, повышению качества рекомендаций, для следственной и оперативной практики. Криминалистическая характеристика уголовных преступлений используется для разработки руководящих принципов для выявления, раскрытия определенных категорий уголовных преступлений, а также изобличения уголовных преступлений и выявления лиц, которые их совершили.

Обсудим вопрос об уровнях криминалистической характеристики преступлений. Ученые выделяют трехуровневую систему КХП:

- криминалистическая характеристика преступления как явления;
- криминалистическая характеристика вида, группы преступлений;
- криминалистическая характеристика отдельного преступления.

Если принять во внимание криминалистическую характеристику преступления в целом как явления, она будет содержать признаки, отличающие преступление от других деяний, актов человеческой деятельности, что, на мой взгляд, является не целесообразным, потому что это именно то, что другие разделы криминалистики а также смежных наук, в особенности уголовное право рассматривают более детально.

В криминалистике нет единого мнения о криминалистических характеристиках отдельных преступлений. Некоторые ученые (например, Р.С. Белкин) считают, что создание таких характеристик нецелесообразно, потому что это проблема практики, а не науки. Другие ученые считают эту характеристику необходимым звеном в системе криминалистической характеристики преступлений.

На мой взгляд, это звено необходима в системе криминалистической характеристики уголовных преступлений по двум причинам. Во-первых, хотя криминалистическая характеристика уголовных преступлений является

искусственным понятием, ее нельзя развивать без анализа отдельных уголовных дел, которые рассматриваются или уже рассматривались. Во-вторых, исходя из криминалистической характеристики раскрытого преступления, можно узнать информацию о неустановленных элементах аналогичного преступления, которое еще не раскрыто.

Характеристика вида, группы преступлений являются наиболее важными и информативными для расследования и раскрытия преступлений с научной точки зрения. Наличие такого уровня криминалистической характеристики преступлений неоспоримо.

Думаю, стоит перейти к рассмотрению элементного состава криминалистической характеристики преступлений.

На мой взгляд, не стоит касаться отдельных элементов криминалистической характеристики уголовных преступлений, а стоит рассмотреть лишь группу обстоятельств, которые, по мнению многих криминалистов, должны быть отражены в криминалистической характеристике уголовных преступлений[4]. Эти группы включают: 1) элементы реального преступления, их внешние и внутренние отношения; 2) обстановка, в которой произошло преступление; 3) криминалистические виды человеческой деятельности, имевшие место до, после и после правонарушения, которые естественно связаны с правонарушением.

На мой взгляд, основными требованиями, которые должны предъявляться к элементам криминалистической характеристики преступлений, являются теоретическая доказанность (подтвержденная практикой органов дознания и предварительного следствия); значимость тех или иных признаков для научного и практического решения задач по выявлению, раскрытию преступлений и изобличению виновных.

[4] Образцов В.А. Криминалистическая характеристика преступлений: дискуссионные вопросы и пути их решения // Криминалистическая характеристика преступлений. С. 11.

Итак, дадим определение криминалистической характеристики преступлений.

Криминалистическая характеристика преступлений — это научная категория, содержащая систему информации о типичных, криминалистически значимых признаках преступлений данного типа, знание которой позволяет находить наиболее оптимальные способы эффективного расследования и раскрытия названных преступлений и выявления преступников, причастных к данному преступлению.

1.3 Содержательные особенности криминалистической характеристики мошенничества в сфере компьютерной информации.

Криминалистическая характеристика преступлений в сфере компьютерной информации - это система криминалистически важной информации, полученная в результате специальных научных исследований, которая является основным структурным элементом методики расследования этих преступлений и способствует их раскрытию, расследованию и предупреждению.

К ее элементам, как уже говорилось выше, следует отнести такие сведения, как о:

-видовом предмете преступного посягательства;

-способе совершения преступления и механизме следообразования;

-условиях совершения преступления (месте, времени и обстановке);

-личности вероятного преступника, типичных мотивах и целях преступления;

-личности возможного потерпевшего;

-связях между этими элементами.

Содержание выявленных структурных элементов определяется спецификой уголовных правонарушений данного типа. Рассмотрим их подробнее.

Криминалистическая информация о конкретном видовом предмете преступления помогает следователю выявить и объективно оценить все признаки состава преступления, содержащиеся в исходной информации, еще на стадии возбуждения уголовного дела, представить разумные следственные версии в отношении возможного преступника. Часто именно эта информация определяет способ совершения преступления и дает представление о вероятном месте совершения преступления.

Уголовное наказание за совершение преступлений в сфере компьютерной информации предусмотрено главой 28 УК РФ. Преступными являются следующие виды деяний:

Неправомерный доступ к охраняемой законом компьютерной информации (ст. 272 УК).

Создание, использование и распространение вредоносных программ (ст. 273 УК).

Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК).

Неправомерное воздействие на критическую информационную инфраструктура Российской Федерации (ст. 274.1)

Как правило, эти преступления совершаются в совокупности с другими общественно опасными преступлениями. Это связано с тем, что, когда компьютерная информация используется как средство совершения другого преступления, она сама становится предметом общественно опасного преступления. Невозможно незаконно использовать компьютерную информацию без нарушения ее правовой защиты, то есть без выполнения хотя бы одного из перечисленных в ст. 16 Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации», а именно: утечки, хищения, утраты, искажения, подделки, уничтожения, модификации, копирования, блокирования и т.д.

Компьютерная информация - информация, зафиксированная на машинном носителе в форме, доступной восприятию ЭВМ. При этом информация – сведения (сообщения, данные) независимо от формы их содержания (статья 2 Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»). Другими словами, компьютерная информация — это информация, циркулирующая в вычислительной среде, записанная на машинном носителе в форме, доступной для компьютерного восприятия, или переданная по телекоммуникационным каналам через электромагнитные сигналы от одного компьютера к другому, от компьютера к другому периферийному устройству или к датчику управления устройствами.

С криминалистической точки зрения, компьютерную информацию условно можно подразделить по следующим основаниям.

1. По юридическому положению:

1.1. Недокументированная компьютерная информация - данные, команды и сигналы, образующиеся в процессе создания, преобразования, передачи, хранения, воспроизведения, уничтожения информации и не обладающие признаками документа.

1.2. Документированная компьютерная информация (электронный документ) — это информация о лицах, объектах, фактах, событиях, явлениях и процессах в электронно-цифровой форме, записанная на машинном носителе посредством электромагнитных взаимодействий или переданная по телекоммуникационным каналам с использованием электромагнитных сигналов с данными, позволяющими идентифицировать данные сведения.

2. По категории доступности:

Общедоступная - компьютерная информация общего пользования (с неограниченным доступом).

Охраняется законом - компьютерная информация, доступ к которой ограничен в соответствии с законодательством Российской Федерации. Этому условию соответствует информация, касающаяся различных видов тайны (государственной, служебной, коммерческой, банковской, предварительного расследования, медицинской, личной, семейной и т. д.), которая передается посредством переписки, телефонных разговоров, почтовых, телеграфных или иных сообщений, которая может быть объектом авторских и смежных прав; иметь статус персональных данных - сведений о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющих ему узнать свою личность. Эта информация всегда будет чужой для лица, которое не имеет к ней законного доступа или которому она была предоставлена с нарушением установленного порядка, с нарушением правил ее защиты.

3. По форме представления:

3.1. Электромагнитный сигнал - средство переноса компьютерной информации в пространстве и во времени с помощью электромагнитных колебаний (волн).

3.2. Упорядоченные семантические данные и команды.

3.3. Файл — это поименованная область записей на машинном носителе данных (МНИ), где строго определенная информация хранится в закодированной форме с деталями, позволяющими ее идентифицировать. Как и в библиотеке, архиве или папке, расположение книги или документа организовано таким образом, чтобы они упорядочивали файлы в МНИ. Для этого ему дается определенное имя, которое, во-первых, позволяет отличить его от многих других файлов и, во-вторых, дает вам некоторое представление о категории информации, содержащейся в нем, или о человеке, который его создал. Однако это не обязательно: файлу можно дать любое условное имя, не связанное с его содержимым. К имени файла можно добавить так называемое расширение, т.е. заметка, содержащая до трех символов. Расширение отражает специфику формата файла и особенности его использования. Обычно вы можете указать имя или тип компьютерной программы, с помощью которой был создан файл, при помощи указанного расширения.

Когда файл создается или его содержимое изменяется компьютерной системой или компьютерной программой, дата и время выполнения этих действий автоматически записываются. Они берутся компьютером из показаний внутренней системы встроенного календаря и таймера (часов) и могут быть изменены пользователем «вручную». Имя, расширение, дата и время являются атрибутами файлов, исправленных в каталоге.

Каталог файлов - директорий («папка») содержит информацию о группе файлов, хранимых совместно на одном машинном носителе.

Каталог имеет имя и может быть зарегистрирован в другом каталоге (одна «папка» может быть вложена в другую). В этом случае он становится подчиненным или «поддиректорием». Вот как создается иерархическая файловая система: на каждом машинном носителе всегда есть корневой

каталог - тот, где начинают регистрироваться общие файлы («основная папка») и подкаталоги первого уровня («вложенные в нее папки») они, в свою очередь, могут регистрировать файлы и подкаталоги уровня 2 («папки», вложенные в «папки» уровня 1 и так далее.

3.4. Компьютерная программа - это объективная форма представления совокупности данных и команд, предназначенных для работы компьютеров и других компьютерных устройств с целью получения определенного результата, а также подготовленных и записанных на физический носитель материалов, полученных при ее разработке, и аудиовизуальных изображений порождаемые им. По функциональному назначению они делятся на следующие виды.

1. Системные программы:

Базовая система ввода / вывода (BIOS) — это специальная программа, записанная в интегральную схему постоянного запоминающего устройства (ПЗУ). BIOS обеспечивает автоматический запуск компьютера при включении питания и организует основной процесс ввода / вывода информации на уровне двоичного кода - машинных языков, преобразующих (кодирующих) всю информацию (сигналы, данные, команды) в логическую последовательность цифр «0» и «1». (Отсюда и такие названия, как «цифровая фотография», «цифровая подпись» и другие).

Системный загрузчик — это программа, которая тоже находится в ПЗУ. Он автоматически включается при запуске BIOS и проверяет все технические устройства в самом компьютере (интегральные схемы: ОЗУ, ЦП, кэш, жесткий диск, дисководы, динамики и т. д.) так и подключенных к нему (периферийные устройства). Если результат теста положительный, программа запускает (загружает) операционную систему с жесткого диска или другого носителя машины и передает ей управление с компьютера. Эта программа также позволяет пользователю выборочно работать с несколькими операционными системами на одном компьютере.

Операционная система (ОС) - набор взаимосвязанных программ, которые действуют как интеллектуальный посредник между оборудованием, средствами связи системы или компьютерной сети и пользователем (человеком). Он состоит из следующих программных компонентов:

- командного процессора (интерпретатора команд) - обеспечивает анализ и исполнение команд, подаваемых пользователем с пульта управления ЭВМ (клавиатуры), в том числе загружает программы в оперативную память (ОЗУ) и запускает их на исполнение;

- драйверов - программ, обеспечивающих автоматическое управление периферийным оборудованием (каждому отдельно взятому периферийному устройству соответствует свой драйвер);

- файловой системы - программ, обеспечивающих логическое размещение и хранение данных и команд на машинных носителях информации в виде логических дисков, папок (каталогов) и файлов.

1.4. Вспомогательные программы (утилиты) - для расширения возможностей операционной системы в определенных областях организации процесса автоматической обработки информации. С помощью этих программ пользователь получает набор дополнительных инструментов для контроля, мониторинга и управления компонентами ОС, а также внутренними и внешними компьютерными устройствами.

2. Прикладные программы - программы для ЭВМ, с которыми непосредственно работает пользователь для решения вычислительных и информационных задач. Они подразделяются на следующие виды:

2.1. Пакеты прикладных программ — это наборы специализированных программных средств, предназначенных для решения задач определенного класса. К ним относятся текстовые процессоры (редакторы); настольные издательские системы; электронные таблицы; графический редактор; автоматизированные рабочие места (АРМ); системы автоматизации проектирования (САПР); системы управления базами данных (СУБД); архиваторы; организаторы сетевого планирования и управления проектами;

антивирусные программы и системы; программы защиты от несанкционированного доступа; средства отладки программ; игры; программы распознавания символов; электронные переводчики; программы для обработки фото, видео и аудио; мультимедиа; программы симуляционного обучения; экспертные системы; программы управления процессами и др.);

2.2. Базы данных - объективные формы представления и организации совокупности данных (например, статей, расчетов), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ.

3. Инструментальные программы - системы программирования. Они используются для создания всех вышеуказанных программ и имеют следующую классификацию:

Трансляторы - программы, которые производят перевод исходного текста программы, написанного человеком на одном из языков программирования (Turbo C, Turbo C++, Turbo Pascal, Microsoft C, Microsoft Basic, Clipper и др.), на машинный язык кодов команд (объектный код);

Компиляторы (редакторы связей) - это программы, которые позволяют работать с библиотекой стандартных подпрограмм, выполняющих ввод и вывод данных и команд, их преобразование, математические функции, доступ к операционной системе, для которой пишется новая программа, и обработку возможных ошибок за «кулисами» во время выполнения программы и сообщение о них пользователю, остановка выполнения (прерывание) программы с помощью определенных команд и т. д. Компиляторы обеспечивают выбор определенных подпрограмм из библиотеки программ, подключают их и логически подключают к новой программе, созданной с помощью компилятора (автоматически устанавливают необходимые логические связи). Без них вновь созданная программа не будет работать в определенной операционной системе, программной среде или компьютере определенного типа. Компилятор имеет на входе набор объектных кодов исходной программы, библиотеку стандартных подпрограмм, и в результате

он создает набор кодов из этих компонентов с программой, готовой к запуску (работе), или с загрузочным модулем.

Декомпиляторы — это программы, которые выполняют функции над трансляторами. Они воспроизводят и преобразуют объектный код в исходный текст (от машинного языка до языка программирования).

Интерпретаторы — это программы, сочетающие в себе функции транслятора и компилятора. Пользователь вводит текст программы, написанной на определенном языке программирования, таком как BASIC, с клавиатуры и сразу же начинает его использовать.

Основные криминалистические особенности компьютерной информации заключаются в следующем:

- она достаточно легко и быстро переносится из одной формы объекта в другую, копируется (воспроизводится) на различных типах машинных носителей и отправляется на любое расстояние, ограниченное только радиусом действия современных средств телекоммуникации;

- при изъятии (копировании) компьютерной информации, в отличие от изъятия материального объекта (вещи), они хранятся в первоисточнике, поскольку к ним могут получить доступ одновременно несколько человек, например, при работе с информацией, содержащейся на электронном веб-сайте, доступ к которому одновременно имеют несколько пользователей.

Доступ к компьютерной информации — это любая форма доступа к компьютерной информации с использованием электронных компьютерных технологий, которая позволяет манипулировать информацией (уничтожение, блокирование, редактирование и копирование). В зависимости от расстояния между местом использования СВТ - средством совершения преступления и местоположением компьютерной информации - предметом криминального посягательства, различают удаленный и непосредственный доступ. Удаленный доступ осуществляется путем установки специального канала связи, по которому совершаются противоправные действия с компьютерной информацией и ее производными. При этом всегда используются транзитные

машинные носители данных и средства связи. Непосредственный подход заключается в необходимости поиска субъекта на месте преступления до, вовремя и после его совершения. Эти обстоятельства имеют криминалистическое значение и связаны с установлением места и способа совершения преступления, преступника и жертвы.

Для защиты информации от несанкционированного вмешательства используются различные методы защиты. Средства защиты компьютерной информации - это технические, криптографические, программные и другие средства, предназначенные для их защиты, средства, в которых они реализованы, а также средства проверки и контроля эффективности защиты информации.

Средства защиты компьютерной информации, охраняемой законом, подлежат обязательной сертификации. Деятельность юридических и физических лиц, связанная с разработкой, производством, продажей и эксплуатацией средств защиты информации, а также оказанием услуг в этой сфере, осуществляется исключительно на основании лицензии.

Уничтожение компьютерной информации заключается в ее удалении любыми способами, что делает невозможным использование информации по назначению и не зависит от возможности ее восстановления средствами и методами, доступными жертве. Одним из таких методов является стирание информации с машинного носителя - частичное уничтожение компьютерной информации с машинного носителя, которое заключается в устранении отдельных признаков, позволяющих их идентифицировать.

Блокирование компьютерной информации - это физическое воздействие на компьютерную информацию, ее машинные носители и / или программное и аппаратное обеспечение для их обработки и защиты, которое привело к временной или постоянной неспособности выполнять какие-либо операции с компьютерной информацией.

Модификация компьютерной информации означает внесение каких-либо несанкционированных изменений владельцем или владельцами.

Копирование компьютерной информации — это повторение и точное копирование компьютерной информации любым способом на машинный носитель, отличный от оригинала, с сохранением идентифицирующих его свойств.

Электронная вычислительная машина (ЭВМ) — это программируемое электронно-техническое устройство, состоящее из одного или нескольких взаимосвязанных центральных процессоров и периферийных устройств, которые управляются программами и предназначены для автоматической обработки информации в процессе решения вычислительных и / или информационных задач.

Компьютерная система (программно-технический комплекс) - совокупность компьютеров, программного обеспечения и различных технических устройств (периферийные устройства, датчики управления, исполнительные механизмы и т.д.), Предназначенные для организации и / или реализации информационных процессов.

Компьютерная сеть - два или более компьютера, соединенных между собой телекоммуникациями (электрические провода, модемы, коммутационные устройства и т. Д.).

Нарушение работы компьютера, компьютерной системы или их сети — это временное или постоянное создание помех их работе в соответствии с целью.

Обстановка, при которой совершается преступление в области компьютерной информации включает материальные, производственные и социально-психологические факторы среды, в которой совершается преступление. Она способна влиять на формирование всех остальных элементов преступной характеристики преступления данной категории, определять характеристики преступника и жертвы.

Важнейшей составляющей обстановки подготовки, совершения и сокрытия преступления в данном случае являются конкретные условия

деятельности потерпевшего (физического или юридического лица), которые делятся на объективные и субъективные.

К объективным условиям совершения преступления относятся:

- вид деятельности или род занятия потерпевшего;
- форма собственности предприятия или физического лица;
- юридическое положение и категория доступности используемой компьютерной информации;
- вид права собственности на обрабатываемую и используемую компьютерную информацию (информационные ресурсы), а также средства ее обработки;
- назначение и структура организации информационно-производственного процесса, характер потребляемых ресурсов и выпускаемой продукции;
- система учета и отчетности по документам на машинном носителе информации, ее соответствие действующему законодательству, правилам, положениям и иным нормативным документам;
- кадровое и материально-техническое обеспечение обработки компьютерной информации;
- вид используемых СВТ, связи и телекоммуникаций, их тактико-технические характеристики и соответствие категории обрабатываемых информационных ресурсов;
- погодные условия;
- наличие необходимых помещений и вспомогательного оборудования;
- наличие, техническое состояние и соответствие средств защиты информации, а также охраны объектов информатизации категории обрабатываемых информационных ресурсов;
- наличие необходимой организационно-распорядительной документации, регламентирующей порядок обработки и использования охраняемой законом компьютерной информации, ее соответствие Специальным требованиям защиты информации.

К субъективным условиям относятся такие факторы социально-психологического и организационно-управленческого характера, как:

- отступление от технологических режимов обработки информации;

- отсутствие, несовершенство или отступление от правил производства, проведения пусконаладочных, ремонтных, регламентных (техническое обслуживание) работ, эксплуатации программ для ЭВМ, баз данных и СВТ, а также учета, хранения, распределения и расходования МНИ;

- отсутствие или несоответствие средств защиты информации ее категории;

- нарушение правил работы с охраняемой законом компьютерной информацией;

- необоснованность использования СВТ в конкретных технологических процессах и операциях;

- неудовлетворительная организация производственных процессов, наличие одновременно ручных и автоматизированных этапов обработки документов;

-отсутствие должного контроля со стороны администрации за деятельностью своих работников, задействованных на чувствительных этапах обработки компьютерной информации;

- психологически неправильные межличностные взаимоотношения должностных лиц с подчиненными и другими работниками и т. д.

Субъективные факторы могут существенно повлиять на ситуацию, в которой совершается преступление рассматриваемого вида и так или иначе формировать ее.

Криминалистическая информация о личности вероятного преступника. Многие ученые идентифицируют само происхождение киберпреступности в обществе с так называемыми хакерами - пользователями компьютеров, компьютерных систем или их сетей, которые ищут способы получить несанкционированный доступ к СВТ и юридически защищенной компьютерной информации. Это имя, кажется, определяет общее

(коллективное) понятие компьютерного преступника. Эти люди обычно обладают достаточно высокими профессиональными знаниями и практическими навыками в области компьютерных технологий, новых телекоммуникационных технологий и технологий репрографической печати, криптографии и электронного документооборота.

Мотивы и цели киберпреступности различны. Их можно оформить следующим образом: корысть, месть, личные неприязненные отношения с коллегами и руководством по месту работы, желание скрыть другое преступление, хулиганские мотивы и озорство, исследовательские цели, демонстрация личных интеллектуальных способностей или превосходства.

Время совершения преступлений этой категории устанавливается только в относительно редких случаях с точностью до одного дня и очень редко часов и минут. Такая точность обычно требуется при выявлении отдельных эпизодов преступления. Время совершения этих преступлений обычно рассчитывается как разница в продолжительности, связанной с деятельностью потерпевших и / или графиком работы компьютеров, компьютерных систем, их сетей, а также конкретной компьютерной программы - средств преступления. Кроме того, согласно ч. 2 ст. 9 УК РФ временем совершения каждого преступления считается время совершения общественно опасного деяния (бездействия) независимо от времени наступления последствий.

Если преступление, связанное с компьютерной информацией, совершено с использованием новых телекоммуникационных технологий и средств связи, место совершения общественно опасного правонарушения обычно не совпадает с местом, где наступают реальные опасные последствия. Таких мест может быть несколько. Их можно удалять друг от друга на большие расстояния, например, в автомобилях, в разных учреждениях, в полевых условиях, в том числе в разных странах и на разных континентах. Последнее возможно благодаря неограниченным возможностям, мобильности и доступности современных средств связи, неотъемлемой частью которых

является компьютерная информация. Поэтому наиболее целесообразно учитывать транспортное средство, часть местности или территорию данного учреждения, организации, государства, где были совершены общественно опасные действия, независимо от места наступления уголовных последствий.

Проанализируем отдельные элементы механизма мошенничества в сфере компьютерной информации, чтобы определить их взаимное взаимодействие и влияние каждого из них на формирование криминалистических знаний о противоправной деятельности. В первую очередь требуется знание компьютерных средств. Компьютерные устройства функционируют как объекты трассировки в двух аспектах:

- как носители информации об объективной стороне преступного деяния;

- как носители информации о самом субъекте преступления.

Особенность заключается в том, что сами компьютерные средства не являются следами преступления, поскольку не имеют конкретных характеристик, но в то же время содержат следы преступления. Об этом свидетельствует анализ следственной практики, когда, например, при проведении следственных действий из компьютера изымается только его «жесткий диск» - запоминающее устройство для хранения информации. В настоящее время технические характеристики компьютерного оборудования и их наличие или отсутствие должны указывать на возможность совершения уголовного преступления (например, подключение или отсутствие подключения компьютера к телекоммуникационной сети).

Большинство ученых согласны с тем, что главной особенностью компьютерного оборудования (предназначенного для исследовательских целей) является его способность хранить информацию. Я думаю, стоит согласиться с этим, потому что это решающий фактор для формирования криминалистических знаний о киберпреступности и, в частности, о мошенничестве с компьютерной информацией.

К источникам компьютерной информации относятся системы, компоненты которых обеспечивают размещение, доступность, а также целостность сведений, составляющих информацию:

- постоянное запоминающее устройство компьютера - его внутренняя память, включающая несколько микросхем, постоянно хранящих определенную информацию;

- оперативное запоминающее устройство - оперативная память, содержащая информацию, необходимую для работы компьютера;

- сверхоперативная память (кэш) - сверхбыстродействующие микросхемы памяти, кэш-память для повышения производительности компьютера.

Существуют также внешние источники - внешняя (долговременная) память, предназначенная для длительного хранения программ и данных, которые в данный момент не используются, для чего требуется устройство, способное записывать / считывать информацию (накопитель или диск), а также хранилище. К ним относятся оптические приводы компакт-дисков (CD-R/RW, DVD R/RW); флэш-накопители (MMC Plus (Multimedia Card), SD Mini (Secure Digital), SD Micro (Secure Digital), MS Pro (Memory Stick Pro), MS Pro Duo (Memory Stick Pro Duo), CF (Compact Flash), SD (Secure Digital) и др.). Таким образом, средства накопления криминалистически значимой информации представляют собой довольно сложные объекты - компьютеры (устройства), состоящие из множества элементов, а также средства накопления, обработки и хранения информации.

Компьютерные сети также интересны для получения криминалистических знаний о типе расследуемого мошенничества. По мнению В. П. Косарева и Л. В. Еремина, компьютерная сеть — это совокупность компьютеров, между которыми можно обмениваться информацией без посредников. Такое суждение является не бесспорным, поскольку данное определение не полностью отражает техническую специфику передачи данных в сети. При передаче информации автор

ориентируется только на наличие промежуточных звеньев в сети. Различные носители информации (например, портативные жесткие диски, USB-карты и флэш-карты, лазерные компакт-диски, DVD-диски и т. д.) также можно классифицировать как промежуточные элементы при передаче информации.

Кроме того, их наличие или отсутствие определяет тип компьютерной системы, которая может включать как автономные вычислительные системы, так и их сети. Поэтому компьютерную сеть нельзя назвать системой, которая, помимо рабочих станций, не включает (технически сложные устройства, такие как компьютер, смартфон, компактный персональный компьютер или планшетный персональный компьютер, через которые пользователь (подписчик) получает доступ к ресурсам компьютерной сети) какие - либо промежуточные устройства хранения информации. Отсюда следует, что характеристики компьютерных сетей заключаются в том, что они бывают нескольких типов и по территориальному распространению делятся на сети: - локальные компьютерные сети (LAN, LAN - Local Area Network) - создаются и используются юридическими лицами, обычно на их территории или физическими лицами в отдельной административно-территориальной единице; - региональный компьютер (РБК, MAN - Metropolitan Area Network), подключающий абонентов района, города, области; - глобальный компьютер (WAN, WAN - Wide Area Network), соединяющий удаленных друг от друга на любом расстоянии абонентов. Самым распространенным, конечно же, является глобальная сеть Интернет.

Анализ материалы уголовных дел, совершенных в сфере компьютерной информации, показывает, что в 95% случаев для совершения этих преступлений использовались глобальные компьютерные сети, в 4% - региональные и только в 1% - локальные компьютерные сети. Таким образом, любая компьютерная сеть также имеет свои характерные криминалистические характеристики и, по сути, может эффективно использоваться преступниками для совершения мошенничества. Характерной особенностью компьютерных сетей как инструмента и средства совершения расследуемого мошенничества

также является то, что они также содержат следы операций, направленных на совершение уголовного преступления. Например, независимо от отправляющего и принимающего устройства электронной почты, он хранит электронные сообщения, отправленные и полученные по определенному адресу. Следователь или лицо, знающий особенности и принцип работы телекоммуникационной сети, может найти в ней значительный объем информации о преступлении. Компьютерная сеть также является средством передачи информации между участниками сети.

В процессе расследования уголовных преступлений, по которым ведется расследование, следует иметь в виду, что подготовка, написание, тестирование специальных компьютерных программ на взлом, внедрение вредоносных «троянов», шпионского ПО, поиск паролей или указание методов входа без пароля оставят виртуальные следы в памяти компьютера или другое технически сложное оборудование, используемое мошенником. При этом применяемые методы воздействия на компьютер жертвы также оставляют след в памяти ее компьютера.

Как справедливо отмечает А. Смушкин, для выявленных правонарушений могут использоваться программы разного уровня сложности: «стандартные» - настраиваются максимально просто и легко могут быть найдены в Интернете или в специальном разделе «закрытая часть Интернета»; «Настроенный» - модифицированный самим злоумышленником под свои нужды; рукописный (сделанный самим). Благодаря формированию криминалистических знаний о мошенничестве в осферебласти компьютерной информации отдельные ученые предлагают новые возможности для определения термина и механизма следообразования. Однако, на мой взгляд, к этому следует подходить с осторожностью. Так, П.В. Мочагин предлагает добавить к двум традиционным формам отражения следообразования (материально фиксированных и идеальных) и добавить еще одну - виртуальную - информационную и технико-компьютерную. Эта позиция кажется довольно спорной, поскольку специфика создания, обработки и

хранения компьютерной информации позволяет использовать для этих целей вполне материальные (компьютерно-технические) средства. Именно это обстоятельство обеспечивает возможность материально устойчивого отображения компьютерной информации на носителе данных средств.

В результате электронные сигналы (команды), передаваемые с компьютера преступника, которые передаются по телекоммуникационным сетям с целью похищения чужого имущества или получения права на чужое имущество путем ввода, удаления, блокировки, изменения, могут считаться следами компьютерного мошенничества, компьютерная информация или другое вмешательство в операции хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Эти сигналы имеют начальную и конечную точки своего движения (то есть компьютеры, между которыми они передаются) и в конечном итоге имеют материально фиксированное выражение - персональный компьютер или другое технически сложное устройство, его IP-адрес. В криминалистической литературе предлагается называть эти следы информационными или виртуальными, а в том виде, в каком их представляют ученые, они представляют собой не что иное, как материальные следы-отображения. Это связано с тем, что они имеют полностью материально закрепленное отражение на материальных носителях, благодаря чему их можно идентифицировать средствами и методами, разработанными наукой.

2.Общие положения криминалистической характеристики мошенничества в сфере компьютерной информации.

2.1 Механизм совершения мошенничества в сфере компьютерной информации.

Криминалистическая характеристика мошенничества в сфере компьютерной информации- общее описание системы криминалистически важной информации о признаках и характеристиках совершенного преступления. Криминалистическую характеристику преступлений также называют «научной абстракцией», которая состоит из знаний о признаках, их естественных взаимосвязях[5].

Криминалистическая характеристика имеет поисковое (ориентировочное) значение, которое используется статистически определенными корреляциями (вероятностными зависимостями) между его элементами, что позволяет осуществлять навигацию по предмету и направлениям поиска[6].

В.Е. Козлов высказал свое мнение по поводу определения термина «криминалистическая характеристика компьютерных преступлений». В своей работе он поясняет, что «это набор наиболее характерной криминалистической информации об особенностях и характеристиках киберпреступности, которая может служить основанием для представления версий преступления и личности преступления совершившего уголовное преступление, позволяющее правильно оценивать ситуации, возникшие при совершении уголовных преступлений, при условии использования соответствующих методов, приемов и средств» [7].

Механизм совершения преступления в криминологии точно не определен. Некоторые авторы понимают под механизмом преступления систему различных длительных действий, которые характеризуют временную и динамическую взаимосвязь отдельных этапов, обстоятельств и факторов,

[5] Драпкин Л. Я., Карагодин В. Н. Криминалистика : учебник. М., 2007. С. 349.
[6] Белкин Р. С. Криминалистическая энциклопедия. 2–е изд. доп. М., 2000. С. 103.
[7] Козлов В. Е. Теория и практика борьбы с компьютерной преступностью. М., 2002. С. 114.

оставивших след в памяти свидетелей и отраженных в материальной обстановке[8].

Н.П. Яблоков утверждает, что механизм совершения преступления — это последовательность преступленых действий при совершении преступления[9]. Механизм предполагает совмещение подготовки, совершения и сокрытия следов преступления[10].

Это положение вызывает споры в связи с тем, что существуют также неосторожные преступления, для которых характерно отсутствие подготовительной стадии. При совершении неосторожного преступления результат может определяться не только действиями правонарушителя, но и действиями других лиц, в том числе потерпевшего. Таким образом, совершение умышленного преступления отличается от неосторожного тем, что во время второго преступления потерпевший не препятствует ему, но может быть источником действий - условий для совершения преступления, которые, среди прочего, составляют основу механизма преступления.

Механизм совершения преступления – это сложная динамическая система, в соответствии с которой определяется содержание криминальной деятельности, включающая в себя следующие элементы:

1) предмет преступного посягательства;

2) способ совершения преступления;

3) орудия и средства преступления;

4) следы, механизм следообразования;

5) обстановка (место) совершения преступления («киберпространство» – применительно к преступлениям, предусмотренным ст. 159.6 УК РФ);

6) рассмотрение данных о личности преступника, совершающего преступление, предусмотренное ст. 159.6 УК РФ.

---

[8] Сотников К. И. Общие и частные криминалистические теории : лекция. СПб, 1997. С. 5.

[9] Яблоков Н. П. Информационное отражение преступлений, их криминалистическая характеристика, ситуационные особенности преступной деятельности и ее расследования // Криминалистика: учебник. М., 2005. С. 67

[10] Яблоков Н. П. Криминалистика : учебник. М., 2011. С. 29.

Информация по каждому из вышеперечисленных элементов должна помочь следователю в соответствии со ст. 159.6 УК РФ выдвигать определенные версии события преступления и личности преступника, обычно неизвестного (признак компьютерного информационного мошенничества), для определения направления поиска информации по возбужденному уголовному делу.

Основным элементом криминалистической характеристики мошенничества по ст. 159.6 УК РФ (его определяющий признак) является способ совершения преступления.

Способ мошенничества в сфере компьютерной информации достаточно сложен, он состоит из:

– подготовки к совершению мошенничества;

– реализации самого способа совершения;

– деятельности, направленной на сокрытие следов преступления.

Степень подготовки к совершению рассматриваемого вида преступления специфична: преступники часто на стадии подготовки осуществляют деятельность, направленную на сокрытие следов преступления. Это может быть достигнуто, например, путем создания вредоносных программ, которые позволяют жертве войти в компьютер, создавая удаленный доступ к компьютеру, а также общаясь с ним на значительном расстоянии с помощью таких программ, как «Skype», «Zoom» и т. д.

В зависимости от выбранного метода преступники могут создавать веб-сайты, на которых жертва получает любую информацию, через которую они могут отправлять вредоносные программы или информацию, используемую для вовлечения жертвы в мошеннические схемы.

Существует несколько распространенных способов мошенничества в сфере компьютерной информации:

– незаконное завладение регистрационными данными учетных записей на различных интернет–ресурсах с последующей их реализацией либо дальнейшим использованием в мошеннических схемах;

– использование платежных сервисов из различных интернет-источников при выполнении платежных операций, впоследствии при сборе средств или при покупке различных товаров с использованием средств со счета жертвы (у мошенников уже есть необходимые данные о карте жертвы на момент совершения платежа-преступления);

– размещение ложной информации на специально разработанном веб-сайте с целью ввести потенциальную жертву в заблуждение относительно возможности получения крупных денежных сумм от краткосрочных инвестиций с последующим заключением виртуальных транзакций и переводом средств на банковский счет за рубежом;

– взлом электронных кошельков «Qiwi», «YandexMoney» и др. с последующим хищением денежных средств, переводом на другие счета (в том числе посредством рассылки вредоносного программного обеспечения либо ссылок на него);

– рассылка писем – «спамов», содержащих вредоносные программы, на электронную почту жертвы с различными предложениями (перевод финансов; приобретение медикаментов; выгодное инвестирование или кредитование и т.д.).

Экспертами в области IT–технологий отмечено большое количество таких писем в общем объеме электронных писем в сети Интерне – до 25–30 млн. рассылок ежегодно (примерно 50% от общего объема)[11];

– получение денег через виртуальные интернет–магазины, а также создание мошенниками сайтов–двойников известных интернет–магазинов;

– проведение электронных торгов (с несуществующими лотами) или «интернет–аукционов»;

– организация благотворительных акций через Интернет, где на счета для конкретных лиц (инвалидов, больных, нуждающихся в срочных операциях

[11] Коломинов В. В. О способе совершения мошенничества в сфере компьютерной информации / В. В. Коломинов // Человек : преступление и наказание. 2015. №3 (90). С. 147.

и т. п.) предлагается перечислять денежные суммы. С этой целью могут создаваться сайты–двойники реальных благотворительных организаций;

– хищение номеров платежных карт жертв (посредством вредоносного программного обеспечения либо сайтов–двойников).

Данный перечень не является исчерпывающим.

Существует большое количество способов, которые пытались классифицировать многие ученые, но в настоящее время в России это не увенчалось успехом. Классификация основных способов совершения компьютерного мошенничества приведена в ст. 8 Конвенции ООН ETS №. 185 (Будапешт, 23 ноября 2001 г.) «О преступности в сфере компьютерной информации», в которой приводятся два основания для классификации:

1) совершение преднамеренно и без права на это лишение другого лица его собственности путем любого ввода, изменения, удаления или блокирования компьютерных данных;

2) лишение другого лица его собственности, совершенное умышленно и без права, путем любого вмешательства в работу компьютерной системы с мошенническим или нечестным намерением получить неоправданную экономическую выгоду для него или другого лица.

Второй элемент более логичен с точки зрения средств и орудий преступления. Основными средствами и инструментами являются: компьютерная сеть, провайдер, компьютерное оборудование и т. д.

В эту категорию элементов механизма уголовного правонарушения также входят лица, выполняющие свои обязанности по совершению мошенничества в зависимости от разделения задач (разработка программ, курьерские услуги).

Еще одним элементом криминалистической характеристики являются следы преступления.

В уголовных расследованиях основной целью является сбор информации о преступлении, но из-за специфики преступления информация о

событии преступлении (компьютерная информация) является особой категорией[12].

Определение относимости компьютерной информации к доказательствам возможно только при ее воспроизведении с использованием технических средств и анализе не только ее содержания, но и ее свойств. Оценка относимости предполагает:

– вывод о том, что компьютерная информация по каким–либо признакам соотносится с предметом доказывания, как именно она с ним связана;

– какие обстоятельства устанавливает компьютерная информация;

– соответствие той или иной следственной версии.

Данное положение необходимо для формирования рассматриваемого элемента криминалистической характеристики данного вида преступлений.

В процессе определения относимости важно соблюдать целостность компьютерной информации (сохранять ее полноту и неизменность). Оценка доказательств с точки зрения их достоверности осуществляется в ходе следственных действий, при оформлении следственных версий и при принятии процессуальных решений и заключается в анализе всего процесса формирования (принятия, восприятия, закрепления, консолидации, поддержание целостности, анализ содержания и свойств) компьютерной информации[13.]

Следы преступления рассматриваемого вида преступления весьма специфичны.

---

[12] Шурухнов В. А. Свойства компьютерной информации и их учет в расследовании преступлений // Актуальные вопросы применения уголовнопроцессуального и уголовного законодательства в процессе расследования преступлений (к 90–летию со дня рождения профессора И. М. Гуткина) : сб. матер. межвуз. научн.–прак. конф. : В 2–х ч. М., 2009. С. 84–88.

[13] Протасевич А. А., Зверянская Л. П. Проблемы собирания и оценки компьютерной информации как доказательства // Современная криминалистика: проблемы, тенденции, имена (к 90–летию профессора Р. С. Белкина) : сб. матер. 53–х криминалистических чтений : в 3 ч. М., 2012. Ч. 3. С. 274–275.

Известно, что следы делятся на материальные или идеальные, но в этом случае следы остаются в памяти электронных устройств - виртуальные следы[14]. Виртуальные (цифровые) следы — это следы любых действий (включая создание, открытие, активацию, внесение изменений и удаление) в информационном пространстве компьютера и других цифровых устройств, их систем и сетей. Под виртуальными следами В. А. Мещеряков понимает «любое изменение состояния автоматизированной информационной системы, связанное с преступностью и записанное в виде компьютерной информации [15].

При расследовании преступлений, совершенных с использованием компьютерных сетей, могут использоваться их следы - информация о прохождении информации по кабельным, радио, оптическим и другим системам электромагнитной связи[16].

Электронные цифровые следы всегда создаются в результате косвенного (опосредованного) воздействия компьютерных программ, не имеют геометрической формы, цвета, запаха и других характеристик, традиционно принимаемых во внимание судебной практикой и наукой, и которые могут отражать индивидуальные характеристики преступника, совершившего преступление, предусмотренное ст. 159.6 УК РФ.

В трасологии нет группы следов, как уже упоминалось - «виртуальных» или «электронно-цифровых», и поэтому кажется актуальным, важно добавить данную группу следов в классификацию следов в зависимости от их внешнего отображения.

Возможность материально-фиксированного отображения компьютерно-технических материальных средств компьютерной информации на носителе

[14] Краснова Л. Б. Компьютерные объекты в уголовном процессе и криминалистике : автореф. дис. ... канд. юрид. наук : 12.00.09 / Л. Б. Краснова. Воронеж, 2005. С. 15–17.
[15] Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации : автореф. дис. … доктора юрид. наук : 12.00.09 / В. А. Мещеряков. Воронеж, 2001. С. 33.
[16] Волеводз А. Г. Следы преступлений, совершенных в компьютерных сетях // Российский следователь. 2002. №1. С. 4–12.

обеспечивается их использованием, с помощью которых происходит создание, обработка и хранение компьютерной информации.

Следует сказать, что в настоящее время в криминалистике не существует системы знаний о виртуальных следах как объекте исследования в этой науке, поскольку она противоречит основам криминалистической науки и теории идентификации.

Классификацию следов–отображений в сфере использования компьютерно–технических средств и их систем можно представить следующим образом[17]:

1) по характеру изменений:

– структурные файловые следы;

– внешние файловые следы.

2) по степени завершенности процесса обработки команд:

– стабильные во времени файловые следы;

– временные файловые следы.

3) по размещению:

– локальные файловые следы;

– сетевые файловые следы.

Таким образом, типичными следами по делам о мошенничестве в сфере компьютерной информации являются:

1. Традиционные следы:

1) следы человека в местах нахождения в момент совершения преступления (следы пальцев рук на клавиатуре и других компьютерно–технических средствах, внешний облик при встрече с жертвой преступления и т.п.), используемых транспортных средствах, средствах связи и т.п.

2) компьютерные следы, отображающиеся в электронной памяти при любых действиях с компьютерными устройствами, мобильными телефонами, смартфонами, планшетами и т.д.:

[17] Козлов В. Е. Теория и практика борьбы с компьютерной преступностью. М., 2002. С. 336.

– включение, выключение, различные операции с содержимым памяти компьютера отображаются, например, в журналах администрирования, журналах безопасности;

– в реестре компьютера отображаются действия с программами (установка, удаление, изменение и т.д.);

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

– последние операции с файлами отображаются в свойствах файлов[18].

Закономерности и специфика формирования компьютерных следов связаны с другими элементами криминалистических характеристик рассматриваемого деяния, такими как место совершения мошенничества в сфере компьютерной информацией.

Одна из основных особенностей места совершения преступления заключается в том, что оно влияет на весь процесс формирования изображения следа и является носителем как материальных, так и идеальных следов, а это означает, что оно имеет значительную информативность.

Компьютерная информация предусматривает необходимость ее обработки, хранения и обмена, для чего необходимо иметь компьютерное оборудование и средства обмена информацией, т.е. сети.

Для управления перемещением информации в сети была описана система Интернет-адресации, описываемая протоколом IP, на основе присвоения каждому компьютеру, подключенному к сети, уникального идентификационного номера - IP-адреса - набора из четырех десятичных чисел разделенные точками.

IP–адреса могут быть статистическими и динамическими. Размещение в сети Интернет информации, доступ к ней, внутрисетевой обмен информацией

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

осуществляется при участии специализированных организаций – провайдеров[19].

Как и в любом другом процессе, в процессе эксплуатации сети возникают определенные проблемы, которые негативно влияют на раскрытие и расследование этих видов преступлений.

Например, есть категория людей, которые отправляют сообщения через Интернет, локальные сети и т. д. сообщения, электронные письма лицам, не давшим согласия на их получение - «спамерам». Эта категория людей использует адреса электронной почты за пределами доменной зоны Российской Федерации (RU), что не позволяет своевременно получать информацию о местонахождении их IP-адресов. Есть несколько проблем. Пострадавший идет в отделение полиции по месту жительства, где необходимо проверить протокол преступления, а преступники проживают в других городах, следы преступления минимальны, так как невозможно собрать никаких данных, кроме информации от жертвы компьютер.

С одной стороны, местом, где совершается мошенничество в сфере компьютерной информацией, является сама информационно-телекоммуникационная сеть, в которой компьютерная информация вводится, удаляется, блокируется, изменяет компьютерную информацию или иным образом вмешивается в операции хранения, обработки или передачи. С другой стороны, местом совершения рассматриваемых правонарушений является местонахождение конкретного компьютера, с которого осуществляется незаконный доступ, поскольку он содержит большую часть информации, характеризующей механизм правонарушения (метод, орудия, следы и т. д.).

Таким образом, местом совершения рассматриваемого преступного деяния является местонахождение компьютерно–технических средств, с которого отправляются команды.

---

[19] Воробец И. Н. Глобальная сеть Интернет, как пространство для совершения преступлений // Экономические, правовые и прикладные аспекты преодоления кризиса в европейских странах и России : доклады междунар. науч.–практ. конф. / под ред. А. М. Кустова, Т. Ю. Прокофьевой. М., 2012. С. 71.

Также высказываются следующие точки зрения касательно места совершения преступления:

1) рабочее место – место обработки информации – предмета преступного посягательства;

2) место постоянного хранения или резервирования информации – сервер или стример;

3) место использования технических средств для неправомерного доступа к компьютерной информации, находящейся в другом месте;

4) место подготовки преступления (разработки вирусов, программ взлома, подбора паролей);

5) место непосредственного использования информации (копирование, распространение, искажение), полученной в результате неправомерного доступа к данным, содержащимся на персональном компьютере[20].

Некоторые авторы предлагают использовать термин «киберпространство» как место преступления для компьютерной информации. В состав киберпространства должны входить:

– отдельные помещения, в которых размещены автоматизированные информационно–вычислительные системы с соответствующим техническим комплексом обеспечения ее деятельности (системы связи, электропитания, заземления и т.п.);

– средства автоматизированной обработки информации (вычислительные машины и их системы);

– каналы телекоммуникаций и передачи данных (также звуковые волны и электромагнитные поля);

– машинные носители информации, обеспечивающие хранение информации в виде, пригодном для ее автоматизированной обработки;

[20] Протасевич А. А., Зверянская Л. П. Указ. соч. С. 45–47.

– информация, представленная в виде, пригодном для ее автоматизированной обработки (данные в соответствующих форматах, управляющие программы и т.п.)[21].

Специфика типичных признаков места происшествия обусловлена его двойственным объектом. Преступление считается оконченным с момента, когда виновный получает денежную сумму (чужое имущество) и приобретает законное право распоряжаться этими деньгами (имуществом). Принимая это во внимание, помимо телекоммуникационной сети местом совершения мошенничества является место, где «обналичиваются» полученные в результате мошенничества средства.

Последний элемент механизма кибермошенничества - субъект преступления - личность преступника - будет рассмотрен в следующей части этой главы.

[21] Мещеряков В. А. Указ. соч. С. 15–16.

2.2 Криминалистическая характеристика личности преступника, совершившего мошенничество в сфере компьютерной информации.

Одним из основных элементов сложной динамической системы механизма мошенничества, предусмотренного ст. 159.6 УК РФ, является субъект преступной деятельности, типичная информация о личности которого имеет важное криминалистическое значение[22].

«Криминальная» личность характеризуется набором биологических, физических, социальных характеристик, информация о которых отображается в процессе ее деятельности в виде материальных и идеальных следов. Личностные черты и качества человека, совершающего мошенничество в киберпространстве, естественным образом формируются под влиянием различных условий социальной среды и относительно стабильны.

Субъект мошенничества в сфере компьютерной информацией имеет компьютерное оборудование, подключенное к компьютерной сети, характеристики которого влияют, во-первых, на выбор способа совершения мошенничества или злоупотребления доверием со стороны преступников и во-вторых, напрямую зависят от квалификации человека, его реализующего.

Анализ следственной и судебной практики показывает, что в большинстве случаев (95%) субъектами преступной деятельности рассматриваемого вида являются лица мужского пола в возрасте, варьирующемся от 18 до 35 лет[23]. В последние годы возрастает число мошенничеств рассматриваемого вида, совершаемых женщинами, что объясняется профессиональной ориентацией отдельных должностей и специальностей на автоматизированные компьютерные системы (секретарь, экономист, бухгалтер и т.д.), которые чаще занимают женщины.

---

[22] Белкин Р. С. Проблемы, тенденции, перспективы. От теории к практике. М., 1988. С. 178.
[23] Данные судебной статистики // Официальный сайт Судебного департамента при Верховном Суде Российской Федерации. URL : http://www.cdep.ru/index.php?id=79 (дата посещения: 09.04.2021 г.).

Большинство преступников имеет высшее или неоконченное высшее техническое образование (53,7%), а также другое высшее либо неоконченное высшее образование (19,2%).

Предлагается классификация субъектов мошенничества в сфере компьютерной информации в зависимости от уровня знания, владения и умения пользоваться компьютерно–техническими средствами[24]. Согласно данному основанию классификации следует различать:

1) профессиональных субъектов преступной деятельности – так называемых «хакеров», «компьютерных злоумышленников», являющихся программистами высшего класса (IT–специалистами):

а) работающих с уже реализованными программами;

б) придумывающих, создающих уникальные программы самостоятельно;

2) непрофессиональных субъектов преступной деятельности (могут иметь специальное образование или относятся к «самоучкам»):

а) «продвинутые» пользователи, которые могут создавать несложные компьютерные программы, сайты;

б) уверенные пользователи, которые знают, как работают компьютерные системы, могут сами устанавливать компьютерные программы.

Классификация также может быть основана на количественном составе мошенников в сфере компьютерной информацией, в связи с чем выделяются три категории мошенничества, указанные в ст. 159.6 УК РФ: одно лицо, группа лиц по предварительному сговору или организованная преступная группа (преступное сообщество).

В 43% случаев мошеннические действия, составляющие объективную сторону преступления, предусмотренного ст. 159.6 УК РФ, были совершены группой лиц при их соучастии (в том числе организованными преступными группами).

[24] Пучкова И. М. Психологические аспекты профессиональной подготовки пользователей ЭВМ : автореф. …канд. психол. наук : 19.00.03 / И. М. Пучкова. М., 1995. С. 14.

Специфика компьютерного информационного мошенничества, совершаемого группой людей, заключается в том, что организаторы этих групп не только используют навыки высококвалифицированных IT-специалистов (программистов), но и сами могут обладать знаниями и опытом и навыками обращения с компьютерной техникой.

Компьютерные инструменты с высокими техническими характеристиками необходимы для совершения компьютерного мошенничества в сфере компьютерной информации, так как важно обеспечить высокую скорость обмена информацией при совершении этих преступлений, чтобы избежать различных способов регистрации их действий. Более профессиональные пользователи, рассматривая возможность модификации компьютерного оборудования, закупают расходные материалы в торговых предприятиях, модифицируют их, тем самым достигая более значительных технических возможностей. Это сделано для увеличения скорости обработки информации дл проникновения в системы и компьютерную технику лиц, в отношении которых осуществляется преступная деятельность.

Личность преступников – мошенников в сфере компьютерной информации отличается следующими особыми характеристиками:

1) такие лица четко и профессионально формулируют задачи, однако отличаются хаотическим бытовым поведением;

2) имеют весьма развитое формально–логическое мышление;

3) стараются говорить четко, точно и однозначно, регулярно переспрашивают, используя уточняющие вопросы;

4) говорят, преимущественно, на компьютерном жаргоне, который малопонятен непрофессионалам.

Преступники отличаются разным уровнем образования и социальным статусом. Они подразделяются на две большие категории:

1) лица, находящиеся с потерпевшим в деловых или трудовых отношениях (сотрудники организаций, злоупотребляющие своим служебным положением);

2) лица, не имеющие деловых связей с потерпевшим (лица, обладающие большими познаниями в сфере современных компьютерных технологий и руководствующиеся в основном корыстными мотивами).

Некоторые авторы включают личность потерпевшего в механизм преступления, а другие нет, но этот элемент криминалистической характеристики нельзя игнорировать.

Поэтому следует начинать поиск жертвы преступления со стороны лица, совершившего мошенничество. По этой причине преступники могут осуществлять деятельность, не связанную с обработкой компьютерной информации (например, отслеживание определенных лиц в учреждениях, приобретение различных баз данных операторов мобильной связи и т. д.).

Наиболее распространенный способ найти жертву, используемый в сфере мошенничества компьютерной информации, — это спонтанный выбор путем рассылки различных предложений, которые могут содержать вредоносное ПО. Например, типичным методом здесь является блокировка программного обеспечения компьютеров пользователей Интернета, в результате чего на экране компьютера пользователя появляется окно («баннер») с информацией о том, какие действия необходимо предпринять для разблокировки компьютера. Баннер содержит информацию о том, что пользователь посетил запрещенные сайты, поэтому он должен заплатить за это штраф, добавив на баланс конкретный номер телефона одного из мобильных операторов, после чего он получает специальный код, который разблокирует компьютерное программное обеспечение[25].

Вышеупомянутый метод называется «Спам» (от англ. слова «SPAM» – «Self Promotion and Marketing») - анонимная массовая рассылка электронных сообщений рекламного или иного характера, которые ранее не запрашивались

[25] Чекунов И. Г. Квалификация мошенничеств, связанных с блокированием программного обеспечения компьютеров пользователей сети Интернет / И. Г. Чекунов // Российский следователь. 2012. №5. С. 31–32

получателем сообщения. Для отправки почты обычно используются интернет-сервисы, что обеспечивает ее низкую стоимость и анонимность[26].

Лица, совершающие уголовные преступления по ст. 159.6 УК РФ, действуя без соучастников (т.е. в одиночку), совершает самые примитивные виды компьютерного мошенничества, которые, как правило, не требуют значительных финансовых и ресурсных затрат (покупка пиратских программ или поиск и скачивание их в Интернете и т.п.).

Таким образом, типовые черты личности преступника в делах о мошенничестве в сфере компьютерной информацией позволяют лицам, расследующим уголовные преступления в ходе расследования, не только определить круг подозреваемых в совершении уголовных преступлений, но и разработать потенциальные модели их поведения, предположить, какими будут следующие шаги выстроить алгоритм следственных действий в процессе расследования преступления и сбора доказательств для передачи в суд.

[26] Семенов Г. В. Криминалистическая классификация способов совершения мошенничества в системе сотовой связи // ИНФОРМОСТ–Средства связи. М., 2001. №3 (16). С. 37–45.

3. Информационная модель механизма совершения преступления, предусмотренного ст. 159.6 УК РФ, её соотношение с криминалистической характеристической мошенничества в сфере компьютерной информации.

3.1 Понятие информационной модели механизма совершения преступления в криминалистике.

В криминалистической, как и в других науках, часто нет четко сформулированных определений некоторых терминов. Таким образом, существует несколько аспектов определения термина «информационная модель механизма совершения преступления».

В конце 80-х гг. началось формирование типовых информационных моделей уголовных правонарушений, позволяющих получать информацию о личностях преступников и других обстоятельствах совершенных уголовных правонарушений на основе выявленных статистических зависимостей между их элементами[27].

Разработка типовой информационной модели преступной деятельности - новый этап в развитии криминологической науки, в соответствии с которым возникает ситуация появления качественно нового источника актуальной криминалистической информации (анализ структуры преступной деятельности) в сравнение с традиционными источниками криминалистической информации.

В 1989 г. впервые была интерпретирована концепция «Типовой информационной модели». Таким образом, авторы понимали типовую информационную модель как «информационную систему, построенную на основе статистической обработки уголовных дел определенной категории, отражающую логические связи между элементами события преступления, используемую для составления типовых версий и создания методологии для расследование определенной категории преступлений[28].

---

[27] Видонов Л. Г. Криминалистические характеристики убийств и системы типовых версий о лицах, совершивших убийство без очевидцев. Горький, 1978.

[28] Типовые модели и алгоритмы криминалистического исследования / под ред. В. Я. Колдина. М., 1989.

Информационная модель формируется в соответствии с требованиями, которые обеспечивают ее функциональность и практическую эффективность:

1) действие определяющих факторов способствует закономерности и достаточности информационных связей между элементами преступления. Не каждое преступление похоже на любое другое, поэтому обнаруживать поиск связи между элементами преступлений нецелесообразно, а судить о них одним конкретным методом - неправильно.

Предлагается выделить информативные для расследования звенья на уровне подгрупп по преступлениям, присвоенных с учетом выбора преступления, характера местности, объектов, на которые направлены преступления, места (обстановки) преступления.

2) информационная модель - комплексная система преступления, которая содержит элементы - мотив, цель, программу. При отсутствии элементов целостная система не создается и невозможно получить полную информацию о естественных связях между ее элементами.

3) типовая информационная модель с выделенными в ней элементами должна находиться в тесной связи с характеристиками личности преступника и способами его преступной деятельности.

Рассмотрим данное достаточно сложное требование на примере кражи со взломом. Выявление высокой информативной значимости элементов деятельности преступника предопределило способы:

– взлом путем отжима или открывания замка техническими средствами;

– выбивание двери;

– взлом окна, проникновение через открытые окна или дверь;

– совершение кражи лицом, находящимся в гостях;

– этаж квартиры, время суток;

– выбор похищенных ценностей.

Нет такой тесной связи между типами преступного поведения, которые являются плохо прогнозируемыми системами (для преступлений,

совершенных в состоянии аффекта по неосторожности). Поэтому создание типовой информационной модели здесь нецелесообразно[29].

4) по окончании формирования информационной модели преступления должна быть выявлена совокупная характеристика преступника и существенные для расследования обстоятельства.

5) информационные модели механизмов преступления предопределяют предоставление полной информации о подозреваемом, а также о других обстоятельствах расследуемого события. Это требование реализуется после выполнения всех вышеперечисленных требований.

6) информация, следуемая из информационной модели, должна быть правильно оценена и использована.

7) наличие информационной модели не означает стереотипность при расследовании преступления следователем.

Итак, с учетом сказанного, рассмотрев содержание и требования информационной модели преступности, можно сказать, что она означает систему описания преступных характеристик конкретного вида преступлений, которая определяет характеристики преступлений группы, личности типового субъекта, механизма преступления и другие обстоятельства[30].

Указанная система также отражает логические связи между элементами преступной деятельности и имеет значение при построении типовых следственных версий и формировании методологии расследования рассматриваемой (определенной) категории уголовных правонарушений.

Информационная модель — это своего рода «научная абстракция», с помощью которой можно описать типичные криминальные черты и процессы преступления. Описание представляет собой общую информацию об

---

[29] А. И. Баянов. Криминалистическая характеристика преступления : назначение, содержание / Баянов А. И. // Современные проблемы уголовного права и уголовного процесса. Красноярск, 2003. Том 2. С. 205–206.

[30] Давыдов В. О. Информационная модель преступления как инструмент формирования криминалистической методики расследования (на примере исследования статистических зависимостей между элементами преступлений экстремистской направленности) // Известия ТулГУ. Экономические и юридические науки. 2012. №1–2. С. 170.

участниках преступления, их действиях, ситуации, в которой было совершено преступление, и направлено на оптимизацию процесса расследования.

Информационная модель преследует несколько целей:

1) познавательная цель – формулирование нового знания об исследуемом объекте;

2) объяснительная цель – объяснение происходящих в процессе преступного деяния изменений;

3) инструментальная цель – моделирование и мысленное экспериментирование – определение реакции на то или иное воздействие элементов между собой и факторов внешней среды;

4) прогностическая цель – прогнозирование динамики связанных с развитием информационных технологий изменений в исследуемом объекте.

Типичные следственные версии, основанные на информационной модели, служат только в качестве руководства в расследовании, поскольку они имеют только вероятностные знания о преступлении и преступнике.

Информационная модель и следственная версия работают со стандартным способом совершения преступления. Если метод нетипичный, следователи должны использовать эвристические способности, опыт, интуиция и архивные файлы, описывающие расследования редких преступлений, должны использоваться в качестве вспомогательного материала.

Информационная модель, формирование которой является одной из актуальных проблем теоретической криминалистики, имеет своими основными функциями следующие:

1) служит основой для формирования методов расследования конкретного вида преступлений. Таким образом, считается, что информационная модель отражает структуру преступной деятельности в криминалистической системе.

Тип методики уголовного расследования определяется типом преступления через картину следов, а тип и информационная структура такой

картины в конечном итоге определяют выбор средств (тактических, технических и т. д.) для его анализа.

Задача первой функции информационной модели - обеспечить составление модели искомого лица и обстоятельств исследуемого события на основе информации, полученной в процессе проектирования типовых следственных ситуаций.

2) представляет собой методическую основу практических расследований. Суть: следователю предоставляется информация, которая помогает спланировать следственные и оперативно-розыскные мероприятия в областях, где вероятно, можно найти больше источников криминалистической информации.

Информационная модель преступления часто отождествляется с криминалистической характеристикой преступления. В следующем параграфе дипломной работы будет рассмотрена информационная модель механизма совершения мошенничества в компьютерной сфере во взаимосвязи с криминалистической характеристикой преступления.

Для чего же нужны информационные модели?

Во–первых, их создание и изучение способствует проверке и получению новой информации;

Во–вторых, с их помощью исследуются и объясняются связи между фактами и явлениями, между механизмом совершенного преступления и последствиями, которые наступили после совершения преступления;

В–третьих, изучение информационных моделей может раскрыть следователю ситуацию взаимосвязи между собой участников преступления (как прямых участников, так и косвенных).

3.2 Информационная модель механизма совершения мошенничества в сфере компьютерной информации в соотношении с криминалистической характеристикой рассматриваемого преступления.

Криминалистическая характеристика мошенничества в сфере компьютерной информации - общее описание системы криминалистически важной информации о признаках и характеристиках совершенного преступления. Криминалистическую характеристику преступлений также называют «научной абстракцией», которая состоит из знаний о признаках, их естественных взаимосвязях[31].

Криминалистическая характеристика имеет поисковое (ориентировочное) значение, которое используется статистически определенными корреляциями (вероятностными зависимостями) между его элементами, что позволяет осуществлять навигацию по предмету и направлениям поиска[32].

Наряду с криминалистической характеристикой существует еще такая категория, как механизм преступления. Механизм преступления — это структурный элемент криминалистической характеристики преступления, который важен для понимания закономерностей процесса совершения преступления, обусловленных различными факторами криминальной ситуации. Выше уже указывалось, что механизм уголовного правонарушения считается независимым институтом, соответствующим категории «криминалистическая характеристика».

Существует мнение, что криминалистическую характеристику мошенничества в сфере компьютерной информацией не следует рассматривать изолированно от механизма преступления.

Механизм совершения мошенничества по ст. 159.6 Уголовного кодекса Российской Федерации представляет собой сложное образование, весьма специфичное среди других криминалистических компонентов. Специфика

[31] Драпкин Л. Я., Карагодин В. Н. Криминалистика : учебник. М., 2007. С. 349.
[32] Белкин Р. С. Криминалистическая энциклопедия. 2–е изд. доп. М., 2000. С. 103.

здесь зависит от характера взаимоотношений между элементами механизма, а также от их взаимосвязей.

Модель механизма преступления – важный элемент, поэтому в основу разработки модели механизма совершения мошенничества, предусмотренного ст. 159.6 УК РФ, положены слова Р.С. Белкина, отметивший: «Информация о механизме совершения преступления и сопутствующих ему обстоятельствах с того момента, как механизм начинает складываться и дополняться на протяжении всего его действия, является неизбежной, а сам процесс получения информации является естественным"[33].

Идея компьютерного информационного мошенничества (как и любого другого преступления) создается путем анализа первичной информации, собранной следователем, где она служит основой для создания мысленной модели объектов и процессов, связанных с событием.

Посредством криминалистического моделирования (оно бывает материальное и мысленное) возможно решать также и задачи по расследованию мошенничеств в сфере компьютерной информации. Модель строится здесь, предварительно пройдя несколько этапов:

1. Формирование и получение информационной модели;

2. Исследование полученной информационной модели посредством применения методов анализа, синтеза и т.д.;

3. Оценка результатов;

4. Формулирование выводов посредством интерпретации оцененных результатов.

Информационная модель механизма компьютерного информационного мошенничества создается с использованием следующих инструментов: следственных и процессуальных действий, содержание которых способствует получению представления о характеристиках и качествах расследуемого преступления. Таким образом, информационная модель в данном случае

[33] Белкин Р. С. Курс криминалистики. В 3 т. Т. 1 : Общая теория криминалистики. М., 1997. С. 118.

отражает качественные и количественные характеристики преступления, «заполняет» существующие пробелы в интерпретации известных фактов преступления, помогает ускорить поиск недостающих (дополнительных) доказательств и способствует раскрытию и расследованию мошенничества в сфеое компьютерной информации.

Информационная модель механизма совершения мошенничества по ст. 159.6 Уголовного кодекса Российской Федерации весьма специфична. Поэтому ее особенности следует учитывать при подготовке научных положений и практических советов, а также при расследовании указанных преступлений. Все элементы механизма совершения мошенничества в сфере компьютерной информации взаимодействуют между собой, что связано с тем, что в зависимости от профессиональной квалификации преступных субъектов, предусмотренных ст. 159.6 УК РФ зависит от выбора способа совершения кибермошенничества, а также орудий, средств, обстановки. Это означает, что чем более квалифицированными являются киберпреступники, тем изощреннее их методы и средства совершения преступлений, предусмотренных ст. 159.6 УК РФ и наоборот.

Информационная модель должна включать следственные тактические действия, направленные на поиск информации, которая могла бы скрыть следы компьютерного информационного мошенничества. Определенные обстоятельства совершенного преступления (именно скрытые) часто остаются невыявленными для оцениваемой категории преступлений, лица, совершившие эти преступления, остаются неустановленными. Такая ситуация приводит к тому, что подобные преступления будут происходить и в будущем[34].

[34] Косынкин А. А. Некоторые аспекты преодоления противодействия расследованию преступлений в сфере компьютерной информации на стадии предварительного расследования / А. А. Косынкин // Российский следователь. 2012. №2. С. 2–3.

Сокрытие следов от мошенничества в сфере компьютерной информации может происходить следующими способами (связанными с компьютерной информацией и оборудованием):

1) фальсификация программных продуктов;

2) маскировка программных продуктов;

3) маскировка местонахождения преступника;

4) восстановление нормальной работоспособности компьютерного устройства;

5) сокрытие присутствия в операционной системе (сокрытие присутствия процессов, файлов и т.д.);

6) противодействие расследованию, уклонение от участия в расследовании.

Эти методы важны для разработки информационной модели механизма компьютерного мошенничества, поскольку их необходимо учитывать при подготовке научных положений и разработок, основанных на практических рекомендациях по расследованию данных преступлений, а именно, при расследовании уголовных дел о преступлениях, предусмотренных ст. 159.6 УК РФ.

Особенности формирования криминалистических знаний о расследовании мошенничества согласно ст. 159.6 УК РФ, их основные источники и характеристика предопределяют создание информационной модели механизма совершения рассматриваемого преступления.

Используя созданную и действующую при расследовании мошенничества в сфере компьютерной информации информационную модель, следователь оптимизирует весь процесс расследования и поиска доказательств по уголовным делам о преступлениях, предусмотренных ст. 159.6 УК РФ.

Говоря о взаимосвязи между информационной моделью и криминалистическими характеристиками, в этих обстоятельствах было высказано множество точек зрения.

Например, Н. П. Яблоков говорит, что «знания о преступлениях, накопленные теорией криминалистики, предстают в виде типовых моделей преступлений (криминалистических характеристик преступлений). Однако знания о преступлении, полученные в процессе практического расследования, имеют форму индивидуальной модели расследуемого преступления и его индивидуальных криминалистических характеристик» [35].

Автор отождествляет термины «типовая модель преступления» и «криминалистическая характеристика преступления», использует их как синонимы. Такой же точки зрения придерживается О.А. Берзин: «Криминалистическая характеристика преступлений стала типичной мысленной моделью преступной деятельности» [36].

Высказывается мнение о разделении этих понятий авторами, которые считают следующее. Информационная модель не должна заменять формы чувственного и рационального познания, поскольку она касается форм, внешних по отношению к субъекту познания - выражения того, что человек знает с помощью компьютера. Таким образом, если прилагательное «информационный» используется для объяснения использования компьютерных инструментов в деятельности следователя, это исключает использование статистического метода расследования.

В.Я. Колдин указал на практическую важность статистической информационной модели, основанной на выявленных статистических закономерностях между элементами преступности. По его мнению, такая информационная модель позволяет получить информацию о личности преступника и других обстоятельствах преступления[37].

Авторы, которые выступают «против» отождествления криминалистической характеристики и информационной модели

---

[35] Криминалистика : учебник / под ред. Н.П. Яблокова. 4–е изд., перераб. и доп. М., С. 102.
[36] Берзинь О. А. Криминалистические подходы к моделированию преступной деятельности / О. А. Берзинь // Журнал Высшей школы экономики. 2011. №4. С.136.
[37] Криминалистика : информационные технологии доказывания : учебник для вузов / под ред. В. Я. Колдина. М., 2007. С. 74.

высказываются, что «информация о личности преступника» – это только сведения, без связи их с информационными технологиями, следовательно, данное основание лишь запутывает изложенную мысль В. Я. Колдина[38].

Действительно, нецелесообразно отождествлять информационную модель для механизма компьютерного мошенничества с криминалистическими характеристиками. Анализ изученных источников литературы и практических материалов позволил провести следующие исследования.

Известно, что для установления криминалистической характеристики преступлений определенного вида необходимо обобщить значительный круг преступлений, уже расследованных следователями и оцененных судами соответствующей категории (в нашем случае преступления, предусмотренные статьей 159.6 УК РФ). Индивидуальная криминалистическая характеристика мошенничества в сфере компьютерной информации составлялась в процессе анализа конкретного дела на основе выделения информации о субъекте, объекте, месте и механизме совершения преступления. Такое индивидуальное свойство является своего рода промежуточным элементом научного исследования, не имеющим самостоятельного значения.

Рассмотрев несколько уголовных дел, каждое из которых имеет свою криминалистическую характеристику, следователь уже имеет набор этих характеристик, на основе которых следователь создает обобщенную типовую (информационную) модель преступлений определенного вида.

В этом и заключается разница между информационной моделью механизма преступления и его криминалистической характеристикой. Хотя существует закономерность соответствия между структурами этих понятий, они имеют существенное различия.

[38] Большакова В. Н. Разграничение криминалистических понятий : модель преступления, поисковый портрет преступника, криминалистическая характеристика преступлений / В. Н. Большакова // Пробелы в российском законодательстве. 2014. №3. С. 208.

По сравнению с криминалистической характеристикой преступления, информационная модель механизма преступления (включая компьютерное мошенничество) характеризуется более высоким уровнем формализации, что значительно упрощает проводимые с ней эксперименты.

Таким образом, криминалистическая характеристика преступления выступает как замкнутая информационная система, содержащая достоверные сведения, представленные в вербальной форме. Информационная модель, в свою очередь, представляет собой систему, содержащую надежные и вероятностные знания, представленные в вербальной и графической форме в виде символов, таких как изображение и т. д.

Заключение

В процессе написания магистерской диссертации была достигнута ее цель. Так, была рассмотрена криминалистическая характеристика преступления в целом, а также предусмотренного ст. 159.6 УК РФ. Рассмотрен механизм совершения преступления, информационная модель механизма совершения преступления, личность лица, совершающего мошенничество в сфере компьютерной информации. Цель была достигнута посредством выполнения задач, поставленных во введении:

1) рассмотрен механизм совершения преступлений, предусмотренный ст. 159.6 УК РФ;

2) проанализирована личность преступника, совершившего мошенничество в сфере компьютерной информации, с криминалистической стороны.

3) рассмотрено понятие информационной модели механизма совершения преступления в криминалистической науке;

4) выявлено содержание информационной модели механизма совершения мошенничества в сфере компьютерной информации;

5) соотнесено понятия «информационная модель совершения мошенничества в сфере компьютерной информации» и «криминалистическая характеристика преступления».

Анализируя выявленную информацию в ходе написания магистерской работы, можно сделать некоторые выводы.

Механизм преступления – это часть криминалистической характеристики, которая закрепляет анализ элементов, входящих в нее. Механизм преступления включает в себя следующие элементы:

1) предмет преступного посягательства;

2) способ совершения преступления;

3) орудия и средства преступления;

4) следы;

5) место совершения преступления («киберпространство»);

6) личность преступника, совершающего преступление, предусмотренное ст. 159.6 УК РФ.

Некоторые авторы включают сюда также личность потерпевшего, в процессе написания магистерской работы личность потерпевшего была рассмотрена в главе 2, параграф 2.

Так, в отношении наиболее распространенных мошеннических схем при использовании сетевых ресурсов в сфере компьютерной информации нельзя озвучить все способы мошенничества, сведя их к одному классификационному основанию, поэтому существует большое количество классификаций способов, что предопределяет необходимость выделения одной общеизвестной и обще используемой классификации. Последняя будет дополняться со временем новыми видами, так как ежегодно появляются новые способы мошенничества в сфере компьютерной информации.

Криминалистической характеристики любого из преступлений не может существовать без связи между элементами механизма совершения рассматриваемого преступления. Каждый из элементов детально анализируется в ходе изучения судебно–следственной практики и положений науки. Указанное помогает в подготовке научных положений и разрабатываемых на их основе практических рекомендаций расследования данного вида преступной деятельности.

Криминалистическая характеристика мошенничества в сфере компьютерной информации представляет собой обобщенное описание системы криминалистически значимой информации о признаках и свойствах преступления, предусмотренного ст. 159.6 УК РФ, и позволяет служить основанием для выдвижения типичных версий о событии преступления и личности преступника, определения направления поиска и познания лица, ведущего расследование.

Список используемой литературы и нормативных актов:

1. Конституция Российской Федерации : принята всенар. голосованием от 12 дек. 1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020 : (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6–ФКЗ, от 30.12.2008 № 7–ФКЗ, от 05.02.2014 № 2–ФКЗ, от 21.07.2014 № 11–ФКЗ, от 14.03.2020 № 1–ФКЗ) // КонсультантПлюс: справ. правовая система. – Версия Проф. – Электрон. дан. – М., 2021. – Доступ из локальной сети Науч. б–ки Том. гос. ун–та.

2. Уголовно–процессуальный кодекс Российской Федерации : Федеральный закон от 18 дек. 2001 г. № 174–ФЗ : (ред. от 24 февр. 2021 г.) // КонсультантПлюс : справ. правовая система. – Версия Проф. – Электрон. дан. – М., 2021. Доступ из локальной сети Науч. б–ки Том. гос. ун–та.

3. Уголовный кодекс Российской Федерации [Электронный ресурс] : Федеральный закон от 13 июня 1996 г. № 63–ФЗ : (ред. от 24 февр. 2021 г.) // КонсультантПлюс : справ. правовая система. – Версия Проф. – Электрон. дан. – М., 2021. Доступ из локальной сети Науч. б–ки Том. гос. ун–та.

4. Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // КонсультантПлюс: справ. правовая система. – Версия Проф. – Электрон. дан. – М., 2021. – Доступ из локальной сети Науч. б–ки Том. гос. ун–та.

5. Азаров В. К. Практика расследования мошенничества / В. К. Азаров // Вестник криминалиста. – 2011. – № 6. – С. 28–31.

6. Ахмедшин Р. Л. Изучение личности преступника в методике расследования преступления // Р. Л. Ахмедшин. – Томск : Изд–во Том. гос. ун–та, 2000. – 138 с.

7. Ахмедшин Р. Л. Криминалистическая характеристика личности преступника // Р. Л. Ахмедшин. – Томск : Изд–во Том. гос. ун–та, 2005. – 210 с.

8. Архипов А.В. Квалификация мошенничества по уголовному законодательству России. Монография. - М.: Юрлитинформ. 2020. - 232 с.

9. Баев О. Я. И все же: реальность или иллюзия (еще раз о криминалистической характеристике преступлений) / О. Я. Баев // Вестник криминалистики. – М., 2002. – Вып 1 (3). – С. 20.

10. Белкин А. Р. Курс криминалистики. Общая часть / В. М. Богданов, Э. И. Бордиловский и др. – М. : Юрист, 2004. – 642 с.

11. Белкин Р. С. Криминалистика : проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики / Р. С. Белкин. – М. : Инфра–М–НОРМА, 2001. – 240 с.

12. Белкин Р. С. Криминалистическая энциклопедия. – 2–е изд., доп. – М., 2000. – 215 с.

13. Безверхов А.Г., Григорян Г.Р. Корыстные преступления против собственности в условиях цифровой трансформации // Российская Юстиция. - 2021. - № 1. - С. 16-17.

14. Безверхов А.Г. Цифровая экономика и уголовный закон // Уголовное право: стратегия развития в XXI веке: материалы XVIII Международной научно-практической конференции. - М.: РГ-Пресс, - 2021. - С. 474-479.

15. Белкин Р. С. Курс советской криминалистики. Ч. II. Частные криминалистические теории. – М. : Академия МВД СССР, 1978. – 410 с.

16. Бегишев И.Р. Преступления в сфере обращения цифровой информации / И.Р. Бегишев, И.И. Бикеев - Казань: Изд-во «Познание» Казанского инновационного университета, 2020. - 300 с.

17. Большаков Н.А., Гаврилин Ю. В. Арендованное компьютерное оборудование и программное обеспечение как орудия и средства совершения преступлений в сфере компьютерной информации. E-SCIO. - Сар. - 2019. - С. 384-388.

18. Васильев А. Н., Яблоков Н. П. Предмет, система и теоретические основы криминалистики / А. Н. Васильев, Н. П. Яблоков. – М., 1984. – 144 с.

19. Возгрин И.А. Общие положения методики расследования отдельных видов преступлений / И. А. Возгрин. – Л., 1976. – 80 с.

20. Волеводз А. Г. Следы преступлений, совершенных в компьютерных сетях / А. Г. Волеводз // Российский следователь. – 2002. – № 1. – С. 4–12.

21. 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.

22. Григорян Г.Р. Социально-экономические и информационно-технологические основания криминализации мошенничества в сфере компьютерной информации // Юридический вестник Самарского университета. - 2019. - Т. 5. - № 3. - С. 141-146.

23. Карпович О. Г. Финансовое мошенничество. Актуальные проблемы / О. Г. Карпович // Юридический мир. – 2010. – № 7. – С. 34–37.

24. Князьков А. С. Криминалистическая характеристика преступления в контексте его способа и механизма / А. С. Князьков // Вестник Томского гос. ун–та. – 2011. – №1. – с. 51 – 64.

25. Князьков А. С. О критериях значимости криминалистической характеристики преступления / А. С. Князьков // Вестник Томского гос. ун–та. – 2007. – № 304. – С. 122–128.

26. Коломинов В. В. О способе совершения мошенничества в сфере компьютерной информации / В. В. Коломинов // Человек : преступление и наказание. – 2015. – №3 (90). – С. 145–149.

27. Кули-Заде Т.А. Проблемы квалификации мошенничества в сфере компьютерной информации // Российская юстиция. - 2019. - № 4. - С. 21-23.

28. Криминалистика : учебник / под ред. А. Г. Филиппова (отв. ред.), А. Ф. Волынского. – М. : Проспект, 2011. – 688 с.

29. Криминалистика : учебник / под ред. Н. П. Яблокова. 3–е изд., перераб. и доп. – М. : Юристъ, 2005. – 781 с.

30. Лопашенко Н.А. Законодательная реформа мошенничества: вынужденные вопросы и вынужденные ответы // Всероссийский криминологический журнал. - 2015. - Т. 9. - № 3. - С. 504-513.

31. Лопашенко Н.А. Компьютерное мошенничество - новое слово в понимании хищения или ошибка законодателя? // Пермский юридический альманах. - 2019. - № 2. - С. 598-609.

32. Методика расследования отдельных видов мошенничества : учеб. пособие / Л. Е. Чистова [и др.]; под ред. А. Г. Филиппова. – М. : МосУ МВД России, 2014. – 53 с.

33. Мусьял И.А. Дифференцированные виды мошенничества: теоретические и практические проблемы: дис. канд. юрид. наук: 12.00.08 / Мусьял Ирина Александровна. - Курск, 2018. - 13 с.

34.

35. Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации : дис. … д–ра. юрид. наук : 12.00.09 / В. А. Мещеряков. – Воронеж, 2001. – 387 с.

36. Образцов В. А. Криминалистика: курс лекций / В. А. Образцов. – М. : Право и закон, 1996. – 447 с.

37. Осипенко А.Л., Соловьев В.С. Киберугрозы в отношении несовершеннолетних и особенности противодействия им с применением информационных технологий // Общество и право. - № 3. - 2019. - С. 23-31.

38. Преступления в сфере компьютерной информации: квалификация и доказывание : учеб. пособие / под ред. Ю.В. Гаврилина. – М. : ЮИ МВД РФ, 2003. – 234 с.

39. Пучкова И. М. Психологические аспекты профессиональной подготовки пользователей ЭВМ : автореф. …канд. психол. наук : 12.00.09 / И. М. Пучкова. – М., 1995. – 19 с.

40. Россинская Е. Р Уголовный процесс и криминалистика на рубеже веков / Е. Р. Россинская, А. И. Усов. – М. : Академия управления МВД России, 2000. – 416 с.

41. Типовые модели и алгоритмы криминалистического исследования / под ред. В. Я. Колдина. – М. : МГУ, 1989. – 184 с.

42. Серебренникова А.В., Лебедев М.В. Уголовное право в эпоху цифровых технологий. Изд. Проспект. - М. 2020. - № 4. - С. 65-69.

43. Харитонов А.Н., Никульченкова Е.В. Квалификация мошенничества в сфере компьютерной информации // Российская юстиция. - 2019. - № 11. - С. 35-38.

44. Хисамова З.И. Об уголовной ответственности за хищения, совершенные с использованием IT-технологий: анализ изменений законодательства и правоприменительной практики // Российский следователь. - 2018. - № 9. - С. 43-47.

45. Хромова Н.М. Возраст уголовной ответственности несовершеннолетних // Журнал российского права. - 2018. - № 4(256). - С. 96109.

46. Фролов М.Д. Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации: дис. ... канд. юрид. наук: 12.00.08 / Фролов Михаил Дмитриевич. - М., 2018. - 90 с.

47. Чупрова А.Ю. Уголовно- правовые механизмы регулирования отношений в сфере электронной коммерции: дисс. ...д-ра юрид.наук: 12.00.08 / Чупрова Антонина Юрьевна. - М., 2015. - 17 с.

48. Чекунов И. Г. Квалификация мошенничеств, связанных с блокированием программного обеспечения компьютеров пользователей сети Интернет / И. Г. Чекунов // Российский следователь. – 2012. – № 5. – С. 31–32.

49. Челышева О. В. Гносеологические основы отечественной криминалистики (теоретико–прикладное исследование) : автореф. Дис д–ра юрид. наук. – СПб., 2003. – 40 с.