МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Институт права
(наименование института полностью)

Кафедра «Уголовное право и процесс»
(наименование)

40.03.01 Юриспруденция
(код и наименование направления подготовки, специальности)

Уголовно-правовой
(направленность (профиль)/специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (БАКАЛАВРСКАЯ РАБОТА)

на тему «Методика расследования преступлений совершенных с использованием коммуникативных сетей»

Студент Д.Д. Ледовских
(И.О. Фамилия) (личная подпись)

Руководитель С.В. Кондратюк
(ученая степень, звание, И.О. Фамилия)

Тольятти 2020

Аннотация

Тема исследования «Методика расследования преступлений совершенных с использованием коммуникативных сетей».

Данная работа посвящена исследованию методик, поиску оптимальных рекомендаций и изучению проблем расследования преступлений, совершенных с использованием коммуникативных сетей. Для полноценного исследования данной темы мы изучили действующие методики, а также разработали комплекс рекомендаций, направленных на повышение эффективности расследования и предотвращения преступлений, совершенных с помощью компьютерных технологий и средств коммуникаций.

Структурно работа состоит из введения, двух глав, первая глава самостоятельная, без разбивки на параграфы. Вторая включают четыре параграфа, заключение, список используемой литературы и используемых источников.

Введение посвящено обоснованию актуальности, выбранной для выпускной квалификационной работы темы, определению целей и задач, объекта и предмета исследования.

В первой главе раскрывается понятие и комплекс взглядов на признаки и общую характеристику уголовно-наказуемых преступлений в сфере коммуникативных сетей.

Во второй главе рассматриваются следственные ситуации, возникающие при проведении расследования преступлений, совершенных с помощью коммуникативных сетей, определяются особенности производства отдельных следственных действий, описывается их применение в случаях совершения преступлений в сфере интернет коммуникаций.

Заключение предполагает краткое подведение итогов выпускной квалификационной работы.

Оглавление

Введение

Актуальность темы исследования. В современном обществе трудно представить свою жизнь без использования достижений научного прогресса.

С каждым днем для человека открываются новые возможности упрощения своей жизни. Одним из таких достижений являются компьютерные технологии и интернет коммуникации. Но вместе с глобальной компьютеризацией, пришли и преступления в сфере интернет технологий.

Для написания выпускной квалификационной работы, мной была выбрана тема – «Методика расследования преступлений, совершенных с использованием коммуникативных сетей». Проблематика данной темы актуальна в наши дни, на это указывает как статистика совершенных преступлений в сети «Интернет», так и многие авторы, которые дискуссируют и спорят по поводу данной проблемы.

Они выделяют ее как одну из важнейших и требуемой к незамедлительному изучению и разрешению.

В представленной работе рассматриваются статистика по данным видам преступлений в Российской Федерации и в мире, также обращается внимание на способы совершения данных преступлений.

Каким образом осуществляются препятствия преступлениям в сфере коммуникативных сетей, какие организации осуществляют контроль, профилактику и предотвращение данных правонарушений.

Степень научной разработанности темы исследования. Актуальности данной темы обосновывается спорами многих выдающихся авторов-правоведов. Так как материал, который изложен в учебной литературе носит общий характер, я постараюсь сопоставить мнения ученых для более глубокого изучения данного материала. В данной работе используются статьи и нормативно правовые акты, применяемые в области исследуемой темы, а также труды ученых, таких как Ровина Е., Громов В. И.,

Чурилов С.Н., Александров И.В., Шмонин А.В., Гармаев Ю.П. и других не менее выдающихся авторов.

Так или иначе, множество исследований, посвященных вопросам методики расследования преступлений совершенных с использованием коммуникативных сетей, не решают их всесторонне, разработка концептуальных основ этого института не завершена. Отдельные вопросы остаются дискуссионными до настоящего времени. С развитием практики назрела необходимость в поиске новых подходов к их разрешению.

Предметом исследования выступает закономерность деятельности правоохранительных органов в сфере раскрытия, расследования и предупреждения совершения преступлений, совершенных с использованием средств интернет-коммуникаций.

Цель и задачи исследования. Разработка комплекса методических рекомендаций, направленных на повышение эффективности расследования и предотвращения преступлений, совершенных с помощью компьютерных технологий и средств коммуникаций. Для успешной реализации данной цели, разработан комплекс задач:

- изучение коммуникативных сетей, как средства совершения преступлений.
- изучение литературы по криминалистике, уголовному процессу, посвященной тематике предотвращения преступлений в сфере интернет-технологий.
- определение специфики тактики первоначальных следственных действий, по делам, совершенным с помощью коммуникативных сетей.
- разработка тактико-криминалистических рекомендаций по предотвращению преступлений в сфере интернет коммуникаций.

При написании работы, используются современные методы научного познания, которые используются сфере криминалистики и уголовных дисциплин в целом.

Теоретическую основу исследования составили монографическая и учебная литература в области общей теории права, теории уголовного процесса и доказательственного права, теории судебной экспертизы и криминалистики; статьи в ведущих периодических изданиях; а также диссертационные исследования, тематика которых не выходит за рамки настоящего объекта исследования.

Нормативную базу исследования составили нормативные правовые акты, регулирующие вопросы преступлений совершенных с помощью средств интернет коммуникаций, Конституция РФ, а также действующий Уголовно-процессуальный и Уголовный кодекс РФ.

Научная новизна исследования состоит в предпринятой попытке комплексного исследования уголовной ответственности за совершения преступлений с помощью коммуникативных сетей в теории уголовного права и проблем квалификации такого деяния.

Структуру работы определили цели и задачи настоящего исследования. Работа состоит из введения, двух глав, включающих четыре раздела, заключения, списка используемой литературы и используемых источников.

Глава 1 Коммуникативные сети, как средство совершения преступлений

Средства коммуникации, помимо упрощения повседневной жизни, стали служить орудиями преступлений. Преступники, понимая, что наступила эпоха компьютерного прогресса, начали приспосабливаться и искать новые способы совершения преступлений в сфере интернет коммуникаций. Согласно статистике МВД РФ «Состояние преступности в России», в январе – декабре 2019 года зарегистрировано 294,4 тысячи преступлений, совершенных с использованием информационных и телекоммуникационных технологий. Это на 68,5% больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений и их удельный вес увеличился с 8,8% в январе - декабре 2018 года до 14,5%. Почти половина таких преступлений (48,5%) относится к категориям тяжких и особо тяжких [44].

Тенденция роста преступности в данной сфере говорит о необходимости немедленного реагирования правоохранительных органов для предотвращения и предупреждения преступности. Для этого необходима разработка методик расследования преступлений, в сфере интернет коммуникаций.

Первые методические рекомендации по расследованию преступлений использовались в начале 19 века и были разработаны на основе жизненного опыта о действиях следователя, их последовательности при расследовании преступлений [4].

Для начала, требуется понять, что такое методика расследования преступлений. Общепринято понимать, что это раздел криминалистики, который исследует и разрабатывает методы, рекомендации по расследованию и предотвращению различных видов преступлений. Основа методики состоит из классификаций преступлений по определенным группам, а также характеристики всех этапов их расследования. Методика расследования

преступлений, в том числе в сфере интернет коммуникаций основывается на уголовном (определяющий само понятие преступления, состав и виды преступлений) и уголовно-процессуальном (предусматривающие средства сбора доказательств и обстоятельств уголовного дела, которые подлежат доказыванию) законодательстве.

Методика расследования различных групп и видов преступлений рассматривает три вопроса – это особенности расследования, раскрытия и предупреждения преступлений с помощью криминалистических средств.

В криминалистической методике выделяются два взаимосвязанных раздела: общие положения и методики расследования отдельных видов и групп преступлений, то есть частные методики. В них преступления отличаются между собой по составу, уголовно-правовому признаку [32].

Общие положения методики расследования преступлений содержат в себе следующие структурные элементы, такие как, понятие и предмет криминалистической методики расследования преступлений, а также ее значение в системе криминалистики, содержание и понятие обстоятельств, которые подлежат установлению, сущность и значение криминалистической характеристики преступлений, понятие этапов расследования; задачи и общая характеристика каждого этапа [4].

Основоположником термина «частные методики» считается В.И. Громов, который в 1929 году опубликовал свое руководство для уголовного розыска под названием «Методика расследования преступлений» [10, с. 24]. Его работа послужила началом для развития криминалистики и методик расследования отдельных видов преступлений.

Каждый вид преступления имеет свои особенности расследования. Поэтому, научное обоснование этих особенностей примени тельное к отдельным видам преступлений, является основной задачей. Речь идет об общих рекомендациях, которые будут использоваться при расследованиях преступлений с учетом особенности каждого из них [66].

Поэтому, типовые структуры частных методик расследования, должны включать в себя обстоятельства, которые подлежат установлению при расследовании отдельных видов преступлений, особенности возбуждения уголовного дела, особенности тактики первоначальных и последующих следственных действий.

Для современных методик расследования отдельных видов преступления важную роль играет постоянное совершенствование, а именно разработка уголовно-видовых и криминалистическо-видовых методик расследования преступлений.

Как справедливо отмечает И.В. Александров, в своем учебнике по криминалистике: «Тесно связанная с уголовно-правовой классификацией криминалистическая классификация преступлений наиболее способствует целенаправленности, разрабатываемых с ее учетом методик расследования, в большей мере отвечающих потребностям следственной практики» [30, с. 15].

Результаты данных исследований способствуют адаптации и оптимизации методов расследования разных видов и групп преступлений. Криминалистическая классификация содержит в себе, как правило, обобщенные данные и типах совершенной преступной деятельности, включает в себя характеристику видов преступлений, таких как способы совершения преступности, место, время. Также большую роль играет определение преступного опыта преступника, особенностей его личности, а также типологических свойств потерпевших. Преступники в сфере коммуникативных сетей имеют профессиональные навыки преступной деятельности. Именно навыки преступника, его следы работы в интернете формируют его, так называемый почерк, который на ряду с особенностями сокрытия следов совершения преступлений содержит в себе «следы личности» преступника, совершившего преступление в интернете, которые в бедующем станут одними из важных улик для следователя. Общие положения методики расследования преступлений содержат в себе правовые основы методики, принципы организации расследования преступлений,

организация мероприятий по расследованию и раскрытию правонарушений, а также их криминалистическая классификация и характеристика [31].

С каждым днем, все больше поступает предложений по поводу современных методик расследования и борьбы с преступностью, в том числе в сфере интернет коммуникаций. Например, А.В. Шмонин указывал: «Необходима единая, ключевая идея, которая будет лежать в основе концепции криминалистических методик» [67, с. 4]. Он считает необходимым единый подход в формирования принципов построения частных методик и их содержания. Ю.П. Гармаев высказал свою точку зрения: «Данный императивный подход нежизнеспособным, а также, что структуры формирования криминалистических методик обязаны быть разнообразными» [7, с. 16].

Сущность методики расследования преступлений, совершенных в интернете, заключается в особенностях расследования каждого отдельного вида преступлений. Например, осмотр места совершения взрыва будет отличаться от осмотра места обнаружения тайников с наркотическими веществами. Обыск и выемка, которая проводится по уголовному делу о хищении, будет отличаться от выемки, совершенной по делу о мошенничестве или продаже наркотических средств по средствам интернет (изъятие компьютеров, банковских чеков, телефонов).

Все преступления в сфере интернет коммуникаций, имеют свою классификацию и особенности, для каждого конкретного преступления, существуют разнообразные, особенные методики расследования. Теоретические и практические навыки следователей в области методик расследования преступлений в сфере компьютерных коммуникаций играет большую роль.

Уголовное законодательство выделяет некоторые разновидности преступлений, совершенных с помощью коммуникативных сетей. Такими преступлениями могут быть незаконная продажа оружия и сбыт наркотических средств, путем создания интернет ресурсов, сайтов, а также

мошенничество в сети, создание, распространение вредоносных программ и получение неправомерного доступа к компьютерной информации. В данном разделе, можно выделить несколько преступлений в сфере интернет коммуникаций и попробовать дать им криминалистическую классификацию [19].

Неправомерный доступ к компьютерной информации выделяется в статье 272 УК РФ. Уголовное законодательство не выделяет четкого определения данного правонарушения, а лишь поясняет его последствия. Объектом данного преступления являются общественные отношения, которые обеспечивают доступ, создание и хранение компьютерной информации [55]. В части первой, статьи 272 УК РФ говорится: «Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации» [64]. Неправомерный доступ к ЭВМ или компьютерам производится, как правило, под чужим именем с использованием подмены кодов устройств, также предполагается установка незаконных прослушивающих механизмов или программ для извлечения информации. Также, одним из способов неправомерного доступа к компьютерной информации относится использование так называемых «дыр» в системе, то есть слабых мест, с помощью которых преступники могут украсть информацию, уничтожить ее в ЭВМ или компьютере.

Объективной стороной данного вида преступления является само деяние, которое заключается в неправомерном доступе к компьютерной информации, которая охраняется законом, а также последствий в виде ее извлечения, уничтожения и повреждения. Охраняемая информация может содержать в себе государственную или коммерческую тайну, а также личные персональные данные компьютерных пользователей. То есть, под неправомерным доступом к информации следует понимать ее извлечение, получение и использование без разрешения ее собственника. Последствия

данного вида правонарушений является уничтожение, блокировка, копирование и модификация информации [6].

Субъективная сторона данного преступления является виной в форме прямого или косвенного умысла. Субъектом выступает лицо, достигшее 16 лет, вменяемое [15]. Он осознает и понимает последствия, наступающие от его незаконных действий. Также существует специальный субъект, согласно ч. 3, статьи 273 УК РФ. Это лицо, совершившее преступление, квалифицирующееся по ст. 272 УК РФ, с использованием своего служебного положения. Под такими субъектами подразумеваются лица, которые, в соответствии своих должностных полномочий имеют доступ к информации, но используют ее незаконно.

По мнению компьютерных специалистов, программа, представляет собой набор команд, кодов и чисел, которые взаимодействуя между собой образуют алгоритмы и обеспечивают ее бесперебойную работу. Помимо незаконного использования компьютерной информации, существуют вредоносные программы для ЭВМ. Как раз компьютерные вирусы созданы и направлены на сбой в системных кодах, которые позволяют пробраться в систему, уничтожать файлы, совершать любые другие вредоносные действия. Конечные задачи таких задач, такие как уничтожение, блокирование, модификация информации определяют вредоносность программы. Компьютерные вирусы имеют способности воспроизведения самих себя, а также распространения и «размножения» себя в системе. Программа признается вредоносной, во-первых, если ее пользователь не ознакомлен с ее предназначением, во-вторых, если владелец компьютера не дал разрешение на ее установление [2].

Объектом данного преступления выступают общественные отношения в области обеспечения компьютерной информации. Субъект – это лицо вменяемое, которое достигло шестнадцатилетнего возраста. Наступление последствий, в том числе тяжких, будет являться квалифицирующим признаком данного вида преступлений. Так как определение тяжести

последствий происходит оценочно, следует обращать внимание на обстоятельства уголовного дела и нанесенный ущерб от компьютерного вируса или вредоносной программы [14].

При оценке следует учитывать материальный ущерб, нанесенный данным типом программ, а также нарушения работы учреждений и предприятий.

Объективной стороной выступает совершение определенного действия по созданию, распространению, использованию вредоносных программ и компьютерных вирусов, а также изменения в программах, которые приводят к уничтожению информации, ее распространению или блокированию.

Субъективная сторона может заключаться только в прямом умысле правонарушителя. То есть лицо осознает опасность своих деяний, предполагает и желает наступления тяжких последствий после его неправомерных деяний. Непосредственным объектом является неприкосновенность ЭВМ и компьютерной информации [54].

Мошенничество в сфере компьютерных коммуникаций квалифицируется по статье 159.6 Уголовного кодекса Российской Федерации. Предметом преступного посягательства для данного вида преступлений являются денежные средства пользователей сети интернет. Как и многие преступления, совершенные в сфере интернет коммуникаций, мошенничество отличается латентностью, то есть скрытностью. Таким оно является из-за сложностей, которые возникают в процессе расследования данных видов преступлений, а также из-за новых схем реализации мошеннической деятельности в интернете [26].

Считается, что если интернет сеть используется непосредственно для совершения преступления, то она будет считаться и средством, и способом его совершения. Исключения составляют случаи, когда непосредственно сеть выступает в качестве вспомогателя для противоправного деяния, то есть является средством облегчения мошеннической деятельности [12].

В отличии от других преступлений, направленных на хищение имущества, мошенничество отличается своими признаками, которые выделены в статье 159 УК РФ. В ней указано, что это совершение хищения, путем злоупотребления доверия и обмана.

Данная дефиниция дает возможность использовать специальные криминалистические методики расследования мошеннических действий, более успешно выявлять противоправные действия и искоренять их.

Непосредственным объектом мошенничества выступают любые материальные ценности, это могут быть ценные бумаги, денежные средства, автомобили, недвижимость и прочие. Как раз непосредственный объект будет влиять на выбор преступниками способа совершения преступления [3].

Совершение мошенничества состоит из трех этапов, таких как подготовительного, непосредственно совершения противоправного деяния, а также укрытия.

На первом этапе, как правило, мошенники достают информацию о своих жертвах, это могут быть минимальные данные о фамилии, имени и отчестве будущей жертвы, каким банком пользуется объект, информация о родственниках.

На втором этапе, мошенники руководствуясь полученными данными стараются втереться в доверие к жертве, например, представляются горячей линией банка, сотрудниками безопасности и просят всего лишь продиктовать номер карты, ее данные о дате истечения срока действия, а также код безопасности. Третий этап включает в себя устранение следов совершения преступления, например, смена номеров, непосредственного места положения [25].

В настоящее время, данные преступления называются Фишингом или Скамингом, целью которых является получение личных данных и паролей пользователей.

Преступления, связанные с незаконным оборотом наркотиков в сфере интернет коммуникаций, квалифицируются по статье 228 УК РФ. С

приходом глобальной компьютеризации, наряду с упрощением повседневной жизни, пришли и негативные последствия.

Преступники также пришли в данную сферу. Им стало проще искать потребителей, распространять информацию о наркотических средствах, а также осуществлять сбыт своего товара оставаясь в тени интернета [46]. Данный вид преступлений несет угрозу социальным отношениям, которые обеспечивают здоровье и благополучие населения.

Степень общественной опасности преступлений, связанных с незаконным оборотом наркотических средств зависит от способа совершения преступного деяния, места, времени, степени завершенности, а также объема наркотиков, которые были задействованы в незаконном обороте, степень вреда организму человека [29].

Непосредственным объектом данных видов преступлений выступают общественные отношения, которые обеспечивают здоровье населения и нации.

Субъективная сторона преступлений, связанных с незаконным оборотом наркотиков всегда выступает умышленной виной.

Субъектами данных правонарушений, являются физические лица, достигшие шестнадцати лет, в преступлениях, которые предполагают хищение наркотических средств и их вымогательства, возраст правонарушителя достигает четырнадцати лет.

Предметом преступления являются непосредственно наркотические, психотропные вещества [47].

Таким образом, методика расследования преступлений – это раздел криминалистики, который разрабатывает рекомендации по расследованию и предотвращению различных видов преступлений.

Существуют такие преступления, совершенные с помощью коммуникативных сетей, как незаконная продажа оружия и сбыт наркотических средств, путем создания интернет ресурсов, сайтов, а также

мошенничество в сети, создание, распространение вредоносных программ и получение неправомерного доступа к компьютерной информации.

Все преступления в сфере интернет коммуникаций, имеют свои особенности и классификацию.

Тенденция их роста в сфере компьютерных технологий, означает необходимость усовершенствования и создание новых методических указаний расследования данных преступлений.

Сущность методики расследования преступлений, совершенных в интернете, заключается в особенностях расследования каждого отдельного вида преступлений.

Например, осмотр места совершения взрыва будет отличаться от осмотра места обнаружения тайников с наркотическими веществами.

Глава 2 Особенности производства отдельных следственных действий

2.1 Следственные ситуации и планирование расследования

Следственная ситуация – это комплекс данных, которые определяют обстановку, в которой подлежит действовать следователю. Хотя данное определение не единственное в своем роде, множество ученых правоведов предлагают свое толкование следственной ситуации. Например, И.А. Копылов выделял термин, как «криминалистическую характеристику расследования конкретного преступления в определенный момент, необходимой для принятия следственных решений» [28, с. 4].

Вопрос о следственных ситуациях заставлял дискутировать авторов, выдвигать новые определения и тактические приемы следственных действий. Таким образом был создан комплекс тактических действий и рекомендаций в различных следственных ситуациях.

Классификация следственных ситуаций выделяется по отношению между участниками. Например, конфликтные и бесконфликтные. В данном случае основой в формировании классификации выступает психология, а именно психологический компонент следственной ситуации: противодействие сторон, у которых цели расследования преступления не совпадают [22].

По возможности достижения цели при расследовании преступлений бывают благоприятные и неблагоприятные для следствия. Это значит, что все следственные ситуации, должны подлежать оценке следователя на положительность или отрицательность для проведения следственных действий и достижения цели.

Сущность следственной ситуации определяется собранными по делу доказательствами, а также любой другой информацией, которая будет иметь значение для расследования преступления. Все собранные данные

представляют собой объективную картину расследования события, позволяют следователю дать всеобъемлющую оценку этим событиям и принимать решение в отношении его дальнейших следственных действий [43].

Необходимо указать, что существуют некие факторы, которые определяют следственную ситуацию. Их можно разделить на объективные и субъективные. К числу объективных можно присвоить этапы расследования, источники информации по уголовному делу (их виды и качество), а также особенности криминальной ситуации. К субъективным факторам можно отнести поведение участников следственных действий, жизненный опыт следователя или дознавателя, их мастерство, их навыки правильно анализировать ситуацию, умение обдумывать и взвешивать все свои действия [36].

При изучении следственных ситуаций следует обратить внимание не только на факторы, но и условия, которые образуют систему компонентов психологического, информационного, а также процессуального и тактического характера. К первым относится психологическое состояние следователя, его конфликт с лицами, препятствующими расследованию преступления. Противодействия расследованию определяется как умышленное совершение действий, которые направлены на препятствование установления объективных обстоятельств по уголовному делу [20].

К субъектам внутреннего противодействия, которые мешают предварительному следствию, относятся лица, которые совершили преступление. К внешнему воздействию относятся такие субъекты, как свидетели, а также работники государственных органов, в том числе и правоохранительных. Так, например, в случае с незаконным оборотом наркотиков в сфере интернет коммуникаций, целью препятствования расследования, будет служить тщательная работа преступников с вопросами о недосягаемости их интернет ресурсов и серверов, с помощью которых они осуществляют сбыт наркотических веществ [62].

К компонентам информационного характера относится осведомленность следователя о противостоящих ему лицах, об обстоятельствах уголовного дела, о местах сокрытия преступников. Чтобы привести пример, рассмотрим ситуацию. Полиция задержала преступника – закладчика. Следователь должен установить его личность, провести допрос, чтобы узнать на какой ресурс работает правонарушитель, кто является заказчиком его работы, а также должен провести изъятие средств связи, с которыми работал преступник [1].

К компонентам процессуального и тактического характера относится само состояние производства по делу, возможность проведения того или иного следственного действия, изоляция преступников друг от друга. В этой ситуации можно привести пример. При задержании двух наркокурьеров, желательно проводить параллельные обыски в их жилищах, чтобы минимизировать риски сокрытия следов преступлений, а также обнаружения тайников, чеков и прочего.

Осуществление грамотного планирования уголовного расследования, которое основывается на полной и всесторонней проработке следственных версий – одно из важных условий успешного установления истины. Как отмечал Н.А. Селеванов: «Планирование первоначальных следственных действий, заставляет следователя использовать свои максимальные возможности для сбора доказательств, и создания информативной и материальной базы для последующего уголовного расследования» [58, с. 122]. Следовательно, можно сделать вывод о необходимости планирования расследования, а также создания его плана для каждого следственного действия. Для максимальной эффективности, данные действия следует начинать незамедлительно после возбуждения уголовного дела.

При планировании следственных действий, следователю необходимо определить каких специалистов или экспертов он будет привлекать, в каких ситуациях, а также назначить их на мероприятия, в которых они должны участвовать [34].

М.А. Евгеньев писал: «План расследования уголовного дела — это общая программа работы следователя по данному делу, вообще программа его действий на ближайшие дни в частности» [13, с. 289]. Изучая работы других правоведов в данной сфере, можем заметить, что многие усилия были применены для создания определенного комплекса мероприятий, методических рекомендаций, которые представляют собой планирование расследования. Но использование уже готовых программ расследования не берут во внимание особенности личности следователя или подозреваемого, также не учитывает многие нюансы в уголовном деле. Как справедливо отмечала Л.А. Соя-Серко: «Программа дает лишь предпосылки к деятельности следователя, а успех достигается лишь их профессиональным использованием в конкретных ситуациях» [60, с. 46].

При планировании следственных действий, следователь обязан основываться на трех принципах. Это принцип индивидуальности, динамичности, а также принцип использования следственного опыта и рекомендаций. Он должен стремиться к тому, чтобы решение вопросов по уголовному делу, было обеспечено всевозможными целесообразными способами [24].

В плане расследования по делам преступлений в сфере интернет коммуникаций, необходимо отразить такие вопросы: с какого следственного действия необходимо начинать расследование, чтобы не утратить доказательства, когда лучше всего будет осуществить задержание преступника, как установить лица, причастных к преступлению, раскрыть их связи с преступными группировками, выяснить причины совершения преступлений.

Необходимо выяснить, кто из подозреваемых будет допрошен первым, дабы исключить возможность их влияния на других участников уголовного судопроизводства. Когда, в какой последовательности и у кого должны быть произведены обыски и выемки, следует поднять вопрос о назначении компьютерной технической экспертизы, какие технические средства

необходимо изъять. В последнюю очередь проанализировать все обстоятельства, полученную информацию. К примеру, если у следователя стоит вопрос об обнаружении создателей сайтов по незаконной продаже наркотических средств, он должен найти курьеров этого сайта, произвести контрольную закупку, задержать сообщников, изъять у них информационные носители, на которых может находится информация, а также переписка со злоумышленниками [18].

Таким образом, следственная ситуация – это комплекс данных, которые определяют обстановку, в которой подлежит действовать следователю. Сущность следственной ситуации определяется собранными по делу доказательствами, а также любой другой информацией, которая будет иметь значение для расследования преступления. План расследования – это так называемый скелет будущей работы работника правоохранительной структуры, она не может быть универсальной, так как личность каждого преступника индивидуальна. Следователь, основываясь на конкретной следственной ситуации, вносит в расследование свой жизненный опыт, методические наработки.

2.2 Осмотр места происшествия по делам о преступлениях, совершенных в интернете

Следственный осмотр места происшествия – это следственное действие, которое заключается в исследовании места преступления, с целью исследования, изъятия и фиксирования улик, следов преступления, а также обнаружения обстоятельств, которые имеют значение для уголовного дела [51].

Целью осмотра места происшествия, является получение следователем доказательств, которые будут способствовать расследованию преступления. Существует два вида источников сбора доказательств – это люди и вещи, найденные на месте совершенного преступного деяния. К первому источнику

относятся подозреваемые, свидетели, потерпевшие, которые могут дать информацию следователю по обстоятельствам совершенного преступления. Ко второму – материальные носители информации, то есть вещи, найденные на месте осмотра. В данном случае, роль будет играть множество факторов – это и место нахождение найденных вещей, их форма, предназначение и другие признаки, отражающие обстоятельства совершения преступного деяния.

Существует несколько видов осмотров, которые отличаются в зависимости от объектов, которые ему подлежат. Это может быть осмотр предметов, документов, места преступления (помещения, здания). Также осмотр бывает первичный и вторичный (повторный). Второй производиться в случаях, если первоначальный осмотр проводился в неблагоприятных условиях, что может повлиять на установлении объективной истины. В таких условиях, следователь мог не обнаружить предметы и следы преступления, подлежащие изъятию, не определил существенные обстоятельства для дела, не привлекал лица, которые играют роль в расследовании преступления [5].

Согласно части 2, статьи 177 УПК РФ, осмотр следов и предметов преступления производится на месте производства следственного действия [63]. Но бывают случаи, когда для данных действий требуется большое количество времени или осмотр на месте затруднен. В таких случаях, согласно части 3, статьи 177 УПК РФ, предметы изымаются, упаковываются и опечатываются, а также должны быть описаны в протоколе осмотра места происшествия. Сафаргалиева О.Н. отмечала: «Основываясь на данных, полученных при осмотре места происшествия, следователь делает выводы и выдвигает версии о способах совершения преступления, о месте нахождении преступников, а также документов и предметов, которые могут содержать себе информацию о правонарушении и стать доказательствами в уголовном судопроизводстве» [57, с. 3].

Осмотр места происшествия должен быть своевременным и основываться на таких положениях, как объективность, полнота,

методичность и последовательность. Осмотр следует производить незамедлительно, как только появляется такая необходимость, это объясняется тем, что объекты осмотра могут быть уничтожены лицами, заинтересованными в сокрытии преступления, что приведет к необъективности и неэффективности производства осмотра места происшествия [37].

Полнота осмотра заключается в выявлении, фиксации доказательств, которые могут способствовать расследованию уголовного дела. Полнота может достигаться только при условии, что все предметы, обстоятельства и объекты не останутся незамеченными следователем.

Активность осмотра заключается в заинтересованности и целеустремленности следователя в расследовании дела. Он должен принимать все возможные меры для обнаружения и изъятия следов преступлений, а также определения и изобличения преступника.

Методичность и последовательность осмотра места происшествия, основывается на использовании для него самых эффективных для определенных объектов способов и методов фиксации и изъятия, а также порядок действий следователя, которыми он руководствуется [23].

Необходимо заметить, что все следственные действия с преступлениями, совершенными в интернете, следует проводить опираясь на уголовно – процессуальный кодекс, учитывая нюансы и особенности данных видов преступлений. Одним из важных критериев проведения следственных действий по данным видам правонарушений является правильно подобранный следователем план расследования. Первым таким действием является осмотр места происшествия.

Для начала, следователь должен определить круг лиц, которые будут участвовать в данном следственном действии. Помимо него, на месте происшествия должны присутствовать криминалист – специалист, который специализируется на преступлениях данной категории, специалист компьютерных технологий, специалист по средствам связи и сетевым

технологиям, а также оперативные сотрудники и эксперт – фотограф, который будет проводить фото и видеофиксацию места происшествия [48].

Целью осмотра места происшествия, будет являться поиск ЭВМ и компьютерной информации, которые могут служить орудием преступления и использоваться для совершения преступной деятельности. Все описание предметов преступления, а именно технических средств, последовательность действий специалистов, следователя и экспертов, должны фиксироваться с помощью видеофиксации. Если при осмотре, специалисты используют различные технические устройства для поиска компьютерной техники или информации, то необходимо делать об этом отметку в протоколе осмотра места происшествия, указывать название техники, марку, лицензию, номер завода [50].

Вся вспомогательная техника должна быть проверена экспертами с помощью специальных программных устройств, в присутствии понятых, на предмет отсутствия в них вредоносного программного обеспечения. Следует аккуратно обращаться с обнаруженной на месте преступления техникой. Уничтожение или искажение информации, которая находятся на ней, может привести не только ее непосредственное использование, но также кратковременное выключение, разрыв в соединении с интернетом либо локальной сетью. Если, на момент проведения следственного действия, некоторая техника находится в выключенном состоянии, включать ее не допускается, пока специалист не проведет ее осмотр [40].

Особое внимание следует уделать описанию в протоколе осмотра места происшествия ключевых данных. В нем должны быть указаны специфика расположения компьютерной техники, расположение средств питания технических средств, наличие или отсутствие локальных соединений компьютеров, соединения их ЭВМ с другим оборудованием, которое может находиться вне территории осмотра места происшествия, на что могут указать соединительные провода, наличие охраны компьютерных средств от несанкционированного доступа, указать другие средства связи, которые

находятся в помещении вместе с исследуемыми компьютерами. Такими средствами могут являться телефоны, ксероксы, факсы [9].

Следователю необходимо указывать и описывать в протоколе осмотра места происшествия такие вещественные доказательства, как найденные вредоносные программы в компьютерной технике и их носители, программы для компьютерных технических средств, которые приводят к несанкционированному доступу пользователя к различным сферам предоставления услуг, электронные записи, переписки, адреса сайтов, через которые осуществлялась преступная деятельность, специфические следы преступления.

К специфическим следам относятся показания устройств, которые производят регистрационные действия, следы взлома, уничтожения или повреждения информации, данные, оставленные преступником в интернете, такие как его электронная подпись. Следователю вместе с экспертами необходимо проверить наличие отпечатков пальцев на компьютерной клавиатуре, мониторе, системном блоке, соединительной цепи проводов, на розетках, рубильниках и на любом другом оборудовании. Никулина О.А. указывала: «Специалисты могут также обнаружить следы изоляционных материалов, которые использовались для взлома или уничтожения компьютерной техники, соединительные капли канифоли для припайки проводов, а также наличие в устройстве посторонних предметов и устройств» [48, с. 69].

Расследуя преступления, совершенные в сфере интернет коммуникаций, например, по продаже наркотических средств, следователю необходимо производить обыск жилого помещения на предмет нахождения в нем любой информации, помимо компьютерной техники. К такой информации относятся чеки, банковские выписки, записки, пароли, данные к виртуальным аккаунтам злоумышленников. Такие вещи, как правило, преступники могут хранить в тайниках, на что следователю также следует обращать внимание. Оперативным сотрудникам следует производить личный

досмотр подозреваемого, обращать внимание на потайные карманы, пошивы воротника, в которых злоумышленник мог спрятать наркотические средства [8].

Таким образом, осмотр места происшествия – это одно из основных первоначальных следственных действий, с помощью которого следователь устанавливает обстоятельства совершенного преступления, исследует доказательства преступного деяния. Осмотр места происшествия должен быть своевременным и основываться на таких положениях, как объективность, полнота, методичность и последовательность. В зависимости от того, насколько грамотно и своевременно были произведены первоначальные следственные действия, зависит успех дальнейшего расследования преступления.

2.3 Особенности осмотра и выемки средств коммуникаций

Обыск и выемка – являются одним из способов собирания доказательств по уголовному делу. Они описываются в статьях 182 и 183 Уголовно-процессуального кодекса Российской Федерации. Согласно данным статьям, можно сделать вывод, что обыск – это следственное действие, при котором проводится обследование помещений или лиц, с целью обнаружить предметы, которые будут использованы в качестве доказательств в уголовном деле. Выемка – это также следственное действие, которое направлено на изъятие конкретных предметов или документов, если точно установлено у кого и где они находятся [35].

Обыск и выемка отличаются между собой по способам и порядку проведения следственных действий, у них разная цель и основания. Например, при обыске, предметы, которые подлежат изъятию, окончательно неизвестны и их следует отыскать. При проведении выемки, точно известно где и у кого находятся подлежащие изъятию объекты. Результатами этих двух схожих следственных действий, является доказательная база, которая

формируется при изъятии документов и предметов. Обыск и выемка похожие друг на друга действия, но имеющие свои особенности. Следовательно, отнесение их в одну главу Уголовно-процессуального кодекса Российской Федерации – является правильным [11].

Согласно ч. 1, статьи 182 УПК РФ, следователь, имея достаточные основания полагать, что у какого-либо лица, в каком-либо месте находятся орудия преступлений, технические устройства, которые являлись средством совершения преступления, а также документы или ценности, нахождение которых будет иметь значение в расследовании уголовного дела, производится обыск и изъятие. Исходя из этого, для производства обыска, можно не обладать информацией о месте нахождения предмета или документа, который подлежит изъятию.

Согласно статье 182 УПК РФ, основанием является наличие достаточных оснований полагать, что разыскиваемый объект находиться в определенном месте. Такие данные могут быть получены от свидетелей, потерпевших, соучастников преступления, подозреваемых, а также в результате проведения следственно – оперативных мероприятий [42].

Обыск может быть проведен у подозреваемых, обвиняемых, а также лиц, которые выступают в уголовном судопроизводстве в качестве свидетелей. Проведение данного следственного действия, возможно только на основании судебного решения, согласно статье 165 УПК РФ. Однако существуют исключения. Одним из таких является производство следственных действий, которые не терпят отлагательств. Обыск может осуществляться при наличии данных о том, что предметы, подлежащие изъятию могут быть уничтожены или перепрятаны заинтересованными лицами. Для проведения обыска без судебного разрешения, следователь, не позднее 24 часов после начала проведения следственных действий, обязан уведомить суд об его производстве и месте производства, а также приложить к уведомлению копию постановления производства и протокола следственного действия.

У обыска существуют некие особенности, например: личный обыск ограничивает у граждан право на личную неприкосновенность ст. 23 Конституции РФ, также он должен проводиться лицами одного пола с обыскиваемым, в присутствии понятых [41].

Выемка, по своим задачам и целям очень схожа с обыском, она имеет похожую процедуру следственного действия, на нее распространяются практические рекомендации для производства обыска. Сущность данного следственного действия заключается в изъятии объектов и предметов, которые имеют значение в уголовном деле. Выемка производиться без соответствующего разрешения суда, за исключением случаев выемки объектов, содержащих государственную тайну, в присутствии двух понятых, при отказе добровольно выдать предметы, которые подлежат выемки, данное следственное действие производится в принудительном порядке.

При рассмотрении преступлений, совершенных с помощью интернет коммуникаций, обыск и выемка носят поисковый характер. Задачами данных следственных действий являются нахождение и изъятие носителей информации, ЭВМ, средств коммуникации, данных, необходимых для входа на различные электронные ресурсы, пароли и коды доступа к данным ресурсам.

Илюшин Д.А. дал определение электронного носителя: «Это техническое средство, которое используется для хранения, обработки и воспроизведения информации» [16, с. 78]. На изъятых электронных носителях, могут быть найдены: программное обеспечение, которое использовалось для взлома или неправомерного доступа к компьютеру, или электронных ресурсов, вредоносные программы, информация о незаконных банковских исчислениях и операциях, счета обманутых пострадавших.

Следователь также может обнаружить информацию о совершенном преступлении, информацию, которая находится в закрытом доступе, например, содержащую государственную тайну, экстремистские материалы и

другая информация, которая будет играть роль в доказывании по уголовному делу [52].

Современная компьютеризация несет в себе неблагоприятные последствия для следователей. Тенденция маленьких съемных носителей затрудняют и минимизируют их нахождение. При таких размерах, электронные накопители можно спрятать абсолютно куда угодно, а использовать средства для их поиска нецелесообразно. Напрямую это связано с особенностями таких носителей, любое электромагнитное воздействие могут повредить электронные накопители и уничтожить на них информацию [61].

Следуя за развитием технологий, следователи сами начинают использовать новые способы обнаружения киберпреступников, широких баз данных, а также средств фиксации информации. Как известно, правонарушители оставляют так называемый «электронный след» работы в интернете. Использую данную зацепку, следователь может обнаружить преступника.

Так, по делу о распространении наркотических средств в интернете, следователь, используя телефон посредника – курьера, обнаружил электронный адрес злоумышленника и переписку в сети. Далее, он делает запрос провайдеру, с указанием телефонного номера, электронного адреса, а также самого сообщения преступника. Провайдер проверяет информацию и выдает справку для следователя, с указанием электронного IP-адреса и физического адреса, непосредственно из которого осуществляется выход в интернет. Получив всю необходимую информацию, следователь обращается в суд с ходатайством о производстве обыска на адресе злоумышленника.

Если есть информация, что информация находится на нескольких компьютерах, целесообразно проводить параллельный обыск на нескольких адресах, для этого все участники следственного действия должны быть проинформированы и проинструктированы об особенностях расследуемого

преступления, материалах, которые требуется изъять, а также о правильном обращении с компьютерной техникой [21].

Особенностями последующих следственных действий будут являться несколько критериев, а именно: следователю будет необходимо участие экспертов по компьютерной технике, работа с компьютерами должна быть осторожной. Следователю необходимо помнить об осторожной транспортировке компьютерных носителей. Для этого, как правило, следователи используют металлические коробки, чтобы на электронные носители не повлияли электромагнитные излучения. Вся полученная информация будет использоваться в качестве доказательств по уголовному делу.

Таким образом, можно подвести итог. Обыск и выемка компьютерных средств – один из способов собирания доказательств по уголовному делу. Задачами данных следственных действий являются нахождение и изъятие носителей информации, ЭВМ, средств коммуникации, данных, необходимых для входа на различные электронные ресурсы, пароли и коды доступа к данным ресурсам. Зачастую, правонарушители оставляют так называемый «электронный след» работы в интернете. Например, получив мобильный телефон подозреваемого, следователь делает запрос сотовому оператору о звонках, узнает куда чаще всего звонил злоумышленник, что может привести к соучастникам совершения преступления. Если известен IP-адрес, правоохранительные органы, путем запроса провайдеру, могут установить место, откуда злоумышленники осуществляют противоправную деятельность.

2.4 Назначение и оценка результатов судебной компьютерно-технической экспертизы

Судебная компьютерно-техническая экспертиза – исследования проводимые в целях установления и изучения роли компьютерной техники в расследуемом преступлении. Такая экспертиза назначается с целью поиска доказательств по уголовному делу. Судебная компьютерно-техническая экспертиза имеет ряд свойственных для нее признаков, которые отличают ее от других подобных способов изучения и извлечения информации для уголовного дела, например: для проведения данного вида экспертизы, требуется тщательная подготовка материалов для проведения изучения компьютерной информации, при ее проведении, следует использовать специальные методы и способы извлечения нужных данных.

Подготовку и производство исследования компьютерной техники и компьютерных носителей информации, обязан проводить эксперт по информационным технологиям, его заключение будет выступать в роли доказательства по уголовному делу [33]. Результатом проведения компьютерно-технических исследований, будет являться информация, изъятая из компьютерных носителей, то есть заключение эксперта. Данная информация будет выступать лишь основой, изучая которую, следователь должен оценить полученные данные. Вместе с другими доказательствами по уголовному делу, он оценивает совместимость и допустимость данных доводов [45].

Судебная компьютерно-техническая экспертиза подразделяется на несколько видов. Первым видом является аппаратно-компьютерная экспертиза, проведение которой определяет марку компьютера, его тип, возможности, а также его назначение. Именно благодаря этой экспертизе, следователь может сделать вывод о том, в какой сфере использовался компьютер, а также определить техническое состояние данного устройства [53].

Предметом этого вида экспертизы выступают обстоятельства, которые устанавливаются на основе закономерности эксплуатации компьютерных устройств. Существует несколько задач, которые решает аппаратно-компьютерная экспертиза, например: определение технического состояния компьютеров, определение обстоятельств использования данных устройств, восстановление хронологической последовательности их использования и эксплуатации.

Программно-компьютерная экспертиза – это такой вид экспертизы, задачей которой является выявление и изучение определенных обстоятельств, относящихся к уголовному делу. Данная экспертиза, как правило, назначается в уголовных делах, расследующих незаконное внедрение посторонних компьютерных программ и файлов, и включает в себя несколько подпунктов: экспертиза веб-сайтов, программного обеспечения, исследование системной безопасности и защиты, а также экспертиза баз данных. В своей работе, Елена Россинская указывает: «Предметом являются закономерности разработки и использования программного обеспечения компьютерной системы, представленной на исследование в целях установления истины по уголовному делу» [56, с. 122].

Самой часто проводимой экспертизой, является информационно-компьютерная, которая служит для исследования информационной составляющей компьютеров. Целями данного вида экспертизы выступают анализ информации, ее оценка, а также изучение влияния посторонних программ на компьютерные устройства [59]. Данный вид исследования изучает информацию, созданную пользователем и программами. Информационно-компьютерная экспертиза определяет способы записывания данных на информационном носителе, их свойства и параметры, а также сущность информации, техническое состояние и воздействие на нее, путем копирования или попытками внедрения или уничтожения.

Компьютерно-сетевая экспертиза назначается для проверки функционирования корпоративных сетей и компьютеров, которые

подключены к информационным ресурсам. Корпоративные сети используются, как правило, в государственных организациях, экспертиза которых требует специальных знаний и умений. Подобного рода исследования позволяют определить были ли попытки внедрения в сеть предприятия, какие сторонние программы используются на устройствах организации, а также позволяют установить попытки неправомерного доступа к компьютерной информации данных устройств [49].

Основными задачами данного вида экспертиз, являются диагностика компьютерной информации и технических устройств, изучение алгоритма работы компьютеров, установление влияния на них стороннего программного обеспечения. Устанавливается вредоносность программ, которые воздействуют на сеть, их возможности, а также определения источника внедрения вирусов и стороннего вмешательства в корпоративные сети.

Заключение эксперта является одним из видов доказательств по уголовному делу, оно оформляется в письменном виде с указанием выводов лица, которое обладает специальными навыками в области компьютерных технологий и отвечает на вопросы, которые были поставлены следователем [65]. Заключение подлежит оценке с точки зрения допустимости, относимости и достоверности.

С точки зрения относимости, эксперт устанавливает наличие или отсутствие связи с конкретным уголовным делом. Об этом, как правило, указывается в тексте данного заключения. Например, указание на постановление о проведении компьютерно-технической экспертизы, которое вынес следователь.

Допустимость заключения эксперта устанавливает соответствие этого заключения требованиям законодательства, в том числе и уголовно-процессуального кодекса. В данном случае необходимо корректно ставить вопросы эксперту, устанавливать процедуру получения объектов для экспертного исследования, а также правильность оформления выводов в его

заключении. Исходя из этого, экспертиза проводится экспертно-криминалистическими отделами органов внутренних дел, но в случаях отсутствия специальных программных средств, следователи могут обращаться к негосударственным экспертным учреждениям, если те обладают специальными знаниями и навыками [49].

Достоверность заключения эксперта. В данном случае оценке подлежит вещественные доказательства, их пригодность и достаточность для проведения исследований для того, чтобы дать заключение. К примеру, при постановке вопроса следователем о пригодности модема для выхода в интернет, эксперту для проверки необходимо передать этот модем.

Таким образом, судебная компьютерно-техническая экспертиза – исследования проводимые в целях установления и изучения роли компьютерной техники в расследуемом преступлении. Такая экспертиза назначается с целью поиска доказательств по уголовному делу. Ввиду особенностей преступлений, совершенных с помощью средств коммуникаций, производство и подготовку данного вида исследований должен проводить эксперт, обладающий специальными навыками и знаниями. Оценка заключения эксперта — это сложный процесс, требующий от следователя, прокурора и суда обширных знаний в области исследуемого события. Критерии оценки заключения эксперта будут служить основой его эффективного анализа исследуемых объектов, следовательно, признания полученных доказательств обоснованными и допустимыми.

Заключение

Проведенное исследование позволило прийти к следующим выводам:

1. Тенденция роста преступности в сфере коммуникативных сетей, говорит о необходимости усовершенствования и создания новых методических указаний расследования данных преступлений. Сущность методики расследования преступлений, совершенных в интернете, заключается в особенностях расследования каждого отдельного вида преступлений.

2. Следственная ситуация – это комплекс данных, которые определяют обстановку, в которой подлежит действовать следователю. Сущность следственной ситуации определяется собранными по делу доказательствами, а также любой другой информацией, которая будет иметь значение для расследования преступления. План расследования – это так называемый скелет будущей работы работника правоохранительной структуры, она не может быть универсальной, так как личность каждого преступника индивидуальна. Следователь, основываясь на конкретной следственной ситуации, вносит в расследование свой жизненный опыт, методические наработки.

3. Исходя из краткой характеристики преступлений в сфере компьютерных технологий установлено, что это общественно-опасные деяния, которые нарушают право собственности, причиняют ущерб имуществу, здоровью потерпевшего и совершаются, в основном, по корыстным мотивам.

4. Обыск и выемка компьютерных средств – один из способов собирания доказательств по уголовному делу. Задачами данных следственных действий являются нахождение и изъятие носителей информации, ЭВМ, средств коммуникации, данных, необходимых для входа на различные электронные ресурсы, пароли и коды доступа к данным ресурсам. Зачастую, правонарушители оставляют так называемый

«электронный след» работы в интернете. К примеру, зная IP-адрес, правоохранительные органы, путем запроса провайдеру, могут установить место, откуда злоумышленники осуществляют противоправную деятельность.

5. Судебная компьютерно-техническая экспертиза – исследования проводимые в целях установления и изучения роли компьютерной техники в расследуемом преступлении. Такая экспертиза назначается с целью поиска доказательств по уголовному делу. Основными задачами данного вида экспертиз, являются диагностика компьютерной информации и технических устройств, изучение алгоритма работы компьютеров, установление влияния на них стороннего программного обеспечения. Ввиду особенностей преступлений, совершенных с помощью средств коммуникаций, производство и подготовку данного вида исследований должен проводить эксперт, обладающий специальными навыками и знаниями.

6. Заключение эксперта является одним из видов доказательств по уголовному делу, оно оформляется в письменном виде с указанием выводов лица, которое обладает специальными навыками в области компьютерных технологий и отвечает на вопросы, которые были поставлены следователем. Оценка заключения эксперта — это сложный процесс, требующий от дознавателя, прокурора и суда обширных знаний в области исследуемого события. Критерии оценки заключения эксперта будут служить основой его эффективного анализа исследуемых объектов, следовательно, признания полученных доказательств обоснованными и допустимыми.

7. Таким образом, разработка новых методик расследования преступлений, будет способствовать уголовно-правовому регулированию ответственности за совершение преступлений в сфере коммуникативных сетей, а также приведет к повышению качества работы правоохранительных органов.

Список используемой литературы и используемых источников

1. Альборов М.З. Особенности расследования преступлений, связанных с распространением синтетических наркотических средств в информационной сети. // Научные вести. Белгород. 2018. С. 4-9.

2. Андреев Д.А., Котрахов В.В., Остапенко А.Г. Компьютерные вирусы: классификация и статистический анализ. // Информация и безопасность. Воронеж: Воронежский государственный технический университет. 2010. С. 295-296.

3. Атаманов Р.С. Некоторые вопросы расследования мошенничества в сети интернет. // Актуальные проблемы российского права. Москва: МГЮА. 2010. С. 201-205.

4. Баршев Я. Основания уголовного судопроизводства с применением к российскому уголовному судопроизводству. С.-Пб., 1841. 326с.

5. Брянская Е.В. Понятие и виды доказательств в уголовном судопроизводстве. // Сибирский юридический вестник. Иркутск. 2013. С. 86-92.

6. Воробьёв В.В. Особенности объекта преступления в составе ст. 272 УК РФ (неправомерный доступ к компьютерной информации). // Вестник коми республиканской академии государственной службы и управления. Сыктывкар: Коми республиканская академия государственной службы и управления. 2014. С. 51-56.

7. Гармаев Ю.П. Криминалистическая методика в эпоху информационного общества: статья в сборнике трудов конференции // Криминалистика как наука и учебная дисциплина: история, настоящее и перспективы развития. – Уфа : Башкирский государственный университет, 2017. С. 12-21.

8. Гортинский А.В. Некоторые рекомендации по проведению следственных действий при расследовании преступлений, совершенных с

использованием печатающих средств персональных компьютеров // Вопросы квалификации и расследования преступлений в сфере экономики. Саратов : СЮИ МВД России. 2009. С. 182-187.

9. Гортинский А.В. Особенности получения информации из электронных документов. // Информационная безопасность и компьютерные технологии в деятельности правоохранительных органов. Саратов: СЮИ МВД России. 2010. С. 107-112.

10. Громов В.И. Методика расследования преступлений / В.И. Громов. – М., 1929. 130 с.

11. Губарев В.В. Обыск и его основные отличия от выемки. // Ачинск: Сибирский институт бизнеса, управления и психологии. 2017. С. 341-344.

12. Дремлюга Р.И. Интернет-преступность. Владивосток, 2008. С. 34-35.

13. Евгеньев М.А. Методика и техника расследования преступлений. Учеб. пособие. Киев, 1940. С. 418.

14. Евдокимов К.Н. К Вопросу об объекте преступления при создании, использовании и распространении вредоносных программ для ЭВМ (ст. 273 УК РФ). // Сибирский юридический вестник. Иркутск: Иркутский государственный университет. 2009. С. 39-34.

15. Евдокимов К.Н. Субъективная сторона неправомерного доступа к компьютерной информации. // Вестник академии генеральной прокуратуры российской федерации. Москва: Академия Генеральной прокуратуры Российской Федерации. 2009. С. 53-58.

16. Илюшин Д.А. Особенности тактики производства обыска при расследовании преступлений в сфере предоставления услуг «Интернет» // 17. Вестник Муниципального института права и экономики (МИПЭ). 2004. № 1. С. 77-86.

18. Илюшин Д.А. Планирование расследования преступлений в сфере предоставления услуг в сети "интернет". Москва: Редакция журнала «Законность». 2007. С. 33-34.

19. Казанцева Д.Б., Бричкова М.Н. Проблема квалификации преступлений, совершённых в сети интернет. // Сборники конференций ниц социосфера. – Пенза: Пензенский государственный университет, 2014. С. 175-179.

20. Карагодин В.Н. Преодоление противодействия предварительному расследованию. Свердловск, 1992. 388 С.

21. Клевцов В.В. Проблемные аспекты изъятия электронных носителей информации при расследовании распространения «дизайнерских» наркотиков с использованием сети интернет // Рос. следователь. 2015. № 6. С. 195-197.

22. Князьков А.С. Классификации следственных ситуаций // Вестник томского государственного университета. Право. Томск: Национальный исследовательский Томский государственный университет. 2013. С. 36-47.

23. Ковтуненко А.Б. Особенности криминалистической тактики осмотра места происшествия. // Актуальные проблемы деятельности подразделений УИС. Воронеж. 2012. С. 538-542.

24. Козловский П.В. Планирование расследования преступлений. // Вестник волгоградской академии МВД России. Волгоград. 2019. С. 90-97.

25. Козодаева О.Н., Обыденнова А.С. Способы совершения мошенничества с использованием банковских карт. // Ученые записки тамбовского отделения РОСМУ. Тамбов: Тамбовское региональное отделение Общероссийской общественной организации «Российский союз молодых ученых». 2019. С. 52-58.

26. Комаров А.А. Специфика мошенничества в интернете. // Современное право. Москва : Издательство «Новый индекс». 2009. С. 91-92.

27. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ) // Собрание законодательства РФ, 04.08.2014, N 31, ст. 4398.

28. Копылов И.А. Следственная ситуация и тактическое решение. Волгоград, 1988. 19 с.

29. Корчагин О.Н., Чирков Д.К., Литвиненко А.С. Синтетические наркотики в России как реальная угроза национальной безопасности. // Актуальные проблемы экономики и права. Казань : Татарский центр образования "Таглимат". 2015. С. 245-253.

30. Криминалистика. В 5 т. Том 5. Методика расследования преступлений: учебник для вузов / И.В. Александров [и др.]; под общей редакцией И.В. Александрова. – Москва : Юрайт, 2020. 242с.

31. Криминалистика: учебник // под ред. И.Ф. Пантелеева, Н.А. Селиванова. – М. : Юрид. лит., 1988. 672 с.

32. Криминалистика: Учебник. Изд. 2-е, испр. и доп. // Под ред. доктора юридических наук, профессора Е.П. Ищенко - М. : Юридическая фирма «КОНТРАКТ», «ИНФРА-М», 2006. 748 с.

33. Кузнецов А.А., Муленков Д.В., Соколов А.Б. Назначение судебной компьютерной экспертизы. // Воронежский институт Министерства внутренних дел Российской Федерации. Воронеж. 2019. № 1. С. 37-43.

34. Кузьмин С.В. Планирование расследования преступлений: различные подходы и описания. // Вестник московского университета МВД России. Москва: Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя. 2008. С. 111-115.

35. Лавренко С.Ю. Понятие, характеристика, значение обыска и выемки для расследования преступлений против собственности на

современном этапе. // Молодость. Интеллект. Инициатива. Витебск : ВГУ имени П.М. Машерова. 2018. С. 294-295.

36. Лакомская М.Ю. Мыслительная деятельность следователя как средство разрешения проблемной ситуации расследования преступлений. // Проблемы правоохранительной деятельности. Белгород: Белгородский юридический институт Министерства внутренних дел Российской Федерации им. И.Д. Путилина. 2017. С. 141-146.

37. Лебедев Н.Ю. Некоторые проблемные аспекты проведения осмотра места происшествия. // Правовые проблемы укрепления Российской государственности. Томск. 2009. С. 216-217.

40. Ленков О.В Производство осмотра места происшествия по делам о неправомерном доступе к компьютерной информации. // Научные исследования. Иваново. 2018. С. 54-58.

41. Ложков И.А. Личный обыск: понятие, криминалистическая и процессуальная сущность. // Гражданин и право. 2008. № 2. С. 92-96.

42. Лупинская П.А. Уголовно-процессуальное право Российской Федерации: Учебник // П.А. Лупинской. – М. : ДизайнПолиграфСервис. 2006. 550 с.

43. Луценко О.А., Ткаченко В.З. Следственная ситуация. Понятие, сущность, значение для расследования преступления. // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. Ростов-на-Дону: Фонд поддержки образования и науки в Ростовской области. 2015. С. 113-117.

44. Министерство Внутренних Дел Российской Федерации. Состояние преступности в России. // ФКУ «Главный информационно-аналитический центр». 2019. 66 с.

45. Муленков Д.В. Особенности назначения судебно-компьютерных экспертиз. // Восточно-Сибирский институт Министерства внутренних дел Российской Федерации. Иркутск. 2015. С. 154-161.

46. Мухина А.Д. Незаконный оборот наркотиков с использованием ресурсов сети "интернет": риски и пути решения. // Юридическая техника. Нижний Новгород: Нижегородская академия Министерства внутренних дел Российской Федерации. 2019. С. 738-739.

47. Николаев К.Д. Объект и предмет преступлений, связанных с незаконным оборотом наркотиков. // Вестник воронежского института МВД России. Воронеж: Воронежский институт Министерства внутренних дел Российской Федерации. 2009. С. 42-46.

48. Никулина О.А. Особенности тактики производства осмотра места происшествия по делам о преступлениях в сфере компьютерной информации. // Вестник Воронежского института ФСИН России. Воронеж. 2015. С. 68-71.

49. Омарова М.М. Теоретические аспекты проведения судебной компьютерно-технической экспертизы. // Аллея науки. Издательский центр «Quantum». 2017. №7. С. 296-299.

50. Пашкова Е.В. Тактика проведения осмотра места происшествия и особенности применение технических средств. Курск: Курский государственный университет. 2019. С. 220-225.

51. Поздеева А.А. Тактика осмотра места преступления: сущность и основные проблемы. // XIII Державинские чтения в республике Мордовия. Саранск. 2017. С. 341-344.

52. Попова А.Р. Современные возможности по исследованию информации, содержащейся на различных электронных носителях. // Государственный институт экономики, финансов, права и технологий. Гатчина. 2019. С. 462-465.

53. Потапов С.А., Потапова И.С. Использование экспертиз при расследовании и раскрытии преступлений, совершенных с применением сотовых телефонов. // Социально-экономические явления и процессы. Тамбовский государственный университет имени Г.Р. Державина. Тамбов. 2016. С. 155-161.

54. Репьева Е.О. О Некоторых проблемах определения непосредственного объекта ст. 273 УК РФ. // Вестник науки. Тольятти: Индивидуальный предприниматель Рассказова Любовь Федоровна. 2019. С. 136-138.

55. Ровина Е.Е. Неправомерный доступ к компьютерной информации: понятие и пути противодействия. // Современный ученый. – Иркутск : Восточно-Сибирский институт МВД России, 2019. С. 333-335.

56. Россинская Е.Р., Усов А.И. Судебная компьютерно-техническая экспертиза // Право и закон. М., 2001. 414 с.

57. Сафаргалиева О.Н. Осмотр места происшествия и установление личности преступника по материальным следам преступления. Томск. 1990. 17 с.

58. Селиванов Н.А. Советская криминалистика: система понятий. М., Юрид лит., 1982. 152 с.

59. Семикаленова А.И. Цифровые следы: назначение и производство экспертиз. // МГЮА имени О.Е. Кутафина. Москва. 2019. № 5. С. 115-120.

60. Соя-Серко Л.А. Програмирование и творчество в деятельности следователя. В кн.: Проблемы предварительного следствия в уголовном судопроизводстве. М., 1980.

61. Старичков М.В. Вопросы использования носителей компьютерной информации в качестве доказательств // Известия Тульского государственного университета. Экономические и юридические науки. 2014. № 2-2. С. 120.

62. Тимошенко Н.А., Ушакова К.С. Сокрытие преступления в структуре преступной деятельности. Пенза: «Наука и Просвещение». 2017. С. 249-252.

63. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 07.04.2020) (с изм. и доп., вступ. в силу с 12.04.2020) // Собрание законодательства РФ, 24.12.2001, N 52, ст. 4921.

64. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 07.04.2020) (с изм. и доп., вступ. в силу с 12.04.2020) // Собрание законодательства РФ, 17.06.1996, N 25, ст. 2954.

65. Хомутов С.В. О некоторых особенностях оценки заключения эксперта следователем и судом. // Ростовский юридический институт Министерства внутренних дел Российской Федерации. Ростов-на-Дону. 2018. № 4. С. 183-186.

66. Чурилов, С.Н. Методика расследования преступлений: общие положения // С. Н. Чурилов. - М. : Юстицинформ, 2009. 310 с.

67. Шмонин А.В. Методология криминалистической методики: Монография. – М. : Юрлитинформ, 2010. 416 с.