МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА
ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ

На правах рукописи

Печникова Розалия Багдуевна

Электронные сообщения как источник криминалистически значимой информации в расследовании преступлений

Специальность 5.1.4 Уголовно-правовые науки

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата юридических наук

Научный руководитель:
кандидат юридических наук
Сотов А.И.

Москва – 2024

Введение

Актуальность темы диссертационного исследования. Одним из основных условий существования человеческого общества является обеспечение свободной коммуникации между ее членами. Поэтому Конституция Российской Федерации защищает права и свободы человека и гражданина, среди которых одним из важнейших названо право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (п 2. ст.23).

На момент принятия Конституции еще не было понятно, что именно те самые «иные сообщения» займут главенствующую роль в информационном обмене, но в данный момент очевидно, что это так. Речь идет об электронных сообщениях.

В настоящее время мало кто может обойтись без смартфона, почти все имеют аккаунты в социальных сетях, пользуются компьютером. К сожалению, прогресс в развитии коммуникаций служит не только благим целям, но и способствует развитию преступности, создавая новые способы и средства совершения противозаконных действий, способы связи и взаимодействия преступников между собой и с иными лицами. Речь идет не только о преступлениях в сфере компьютерной информации, а о любом противоправном деянии. Как справедливо отмечает Е.Р. Россинская, «интеграция современных информационных технологий в экономическую, социальную, управленческую и другие сферы явилась причиной того обстоятельства, что с помощью компьютерных средств и систем совершаются не только преступления в сфере компьютерной информации (гл. 28 УК РФ), но и «традиционные» преступления (например, присвоение, кража, мошенничество, фальшивомонетничество, лжепредпринимательство и др.)»[1].

Согласно результатам анкетирования, проведенного нами среди следователей, необходимость исследования переписки возникает по следующим

[1] См.: *Россинская Е.Р.* К вопросу о частной теории информационно-компьютерного обеспечения криминалистической деятельности // Известия ТулГУ. Экономические и юридические науки. 2016. Вып. 3. Ч. 2: Юридические науки. С. 109.

категориям расследуемых дел: преступления против личности – в 29,86% случаев, должностные преступления – 14,39%, хищения – 8,99%, преступления в сфере экономической деятельности – 23,38%, преступления в сфере компьютерной информации – 12,59%, преступления против общественной безопасности и общественного порядка – 6,12%, преступления против государственной власти – 7,19%, иные преступления – 6,48%.

Согласно результатам изучения надзорных производств, электронные сообщения выступали в качестве источника ориентирующей или доказательственной информации по следующим делам: ч. 1 ст. 105 – 3; п. «а» ч. 2 ст. 105 – 1; п. «к» ч. 2 ст. 105 – 1; ч. 1 ст. 109 – 2; ч. 1 ст. 110 – 4; п. «д» ч. 2 ст. 110 – 3; ч. 4 ст. 111 – 2; ч. 1 ст. 119 – 9; ч. 1 ст. 134 – 6; ч. 3 ст. 134 – 4; ч. 1 ст. 135 – 6; ч. 2 ст. 135 – 2; ч. 1 ст. 138 – 2; ч. 1 ст. 157 – 7; п. «г» ч. 3 ст. 158 – 8; ч. 1 ст. 159 – 1; ч. 2 ст. 159 – 4; ч. 3 ст. 159 – 2; ч. 1 ст. 163 – 3; ч. 1 ст. 171.2 – 5; п. «а» ч. 2 ст. 171.1 – 1; ч. 1 ст. 228.1 – 15; п. «б» ч. 2 ст. 228.1 – 12; ч. 1 ст. 272 – 1; ч. 1 ст. 327 – 1. Причем в 27,62% дел электронные сообщения выступали как основное доказательство, и в 72,38% – как ориентирующая информация (средство изобличения).

Злоумышленники планируют действия, связываются и поддерживают контакт между собой с помощью электронных сообщений. Электронные сообщения хранят в себе большое количество криминалистически важных следов преступления, которые можно и нужно использовать при расследовании, а также при доказывании.

В ходе проведенного анкетирования было выявлено, что большинство (96,69%) следователей выразило уверенность в необходимости создания рекомендаций по работе с электронной перепиской для работников следствия. Это показывает, что несмотря на повседневное использование данного вида средств сообщения, правоохранительные органы все еще испытывают недостаток в соответствующих методических материалах.

Являясь ценнейшим источником доказательственной информации, электронные сообщения одновременно требуют от следственных работников

специфических навыков, которые позволили бы их эффективно выявлять, изымать и анализировать. Однако проведенные эмпирические исследования показали наличие существенных пробелов в этой сфере у практических работников. С их стороны отмечается стремление по возможности возложить эту работу на экспертные подразделения, но при этом не учитывается, что без грамотной подготовки материалов для исследования, без корректной формулировки вопросов, без правильно налаженного поиска сообщений эксперты не смогут помочь следствию. Сложившаяся ситуация требует выработки у следственных работников методических навыков, позволяющих им правильно оценивать характер электронных сообщений и обеспечивать грамотную работу с ними, чтобы содержащаяся в них доказательственная информация не утрачивалась, а, напротив, использовалась максимально эффективно. Собственно, поэтому этот вопрос и является **актуальным**.

Степень научной разработанности темы.

Электронные сообщения прежде всего представляют из себя информацию. Основы использования информации в расследовании преступлений отражены в трудах таких уважаемых ученых, как В.Я. Колдин, Н.П. Яблоков, Р.С. Белкин, В.В. Крылов, В.А. Жбанков и др.

Вопросами определения понятия и сущности компьютерной информации, исследованием цифровых доказательств, методами поиска, получения и закрепления таких доказательств занимались такие известные специалисты, как В.Б. Вехов, А.Н. Першин, Н.Н. Федотов и др.

Вопросы криминалистического исследования компьютерной информации и электронных носителей освещались в трудах Е.Р. Россинской, А.И. Семикалентовой, В.В. Крылова, В.Б. Вехова, В.А. Мещерякова, И.В. Александрова, И.М. Комарова, М.Ш. Махтаева, А.В. Ткачева, Е.С. Крюковой, Е.И. Ян, А.Б. Смушкина, А.Н. Яковлева, А.А. Васильева, К.Е. Демина, Л.Б. Красновой и др.

Основные принципы работы компьютерных устройств, принципы функционирования сети «Интернет», основы работы с компьютерной информацией и возможности обеспечения информационной безопасности рассмотрены в работах Н.Н. Федотова, А.И. Сотова.

Актуальные проблемы, связанные с исследованием электронной информации, поднимались в работах И.М. Комарова, Т.А. Сакова, И.В. Собецкого, А.И. Усова, А.В. Мещерякова, А.Л. Осипенко, А.М. Багмета, А.Б. Смушкина, Г.П. Шамаева, И.А. Рядовского, А.В. Маилян и др.

Тактические и технические возможности собирания, изъятия и использования в расследовании электронных доказательств рассматривались в работах Е.П. Ищенко, А.И. Зазулина, С.П. Щербы, А.Е. Брусиловского, Н.А. Архиповой, А.М. Багмета, С.Ю. Скобелина, В.Ф. Васюкова, О.Г. Костюченко, А.Д. Нестерова, И.П. Пономарева, Ю.Н. Соколова, А.И. Сотова.

Особенности расследования компьютерных преступлений, преступлений с использованием информационных технологий рассматривали В.В. Крылов, М.В. Жижина, Д.В. Завьялова, А.Л. Осипенко, Н.В. Олиндер, Е.А. Гамбарова.

Тактические особенности расследования и проведения отдельных следственных действий, в том числе с использованием электронных доказательств освещались в работах Е.Е. Центрова, О.Е. Баева, А.Р. Ратинова, С.В. Баженова, В.Ф. Васюкова, Н.А. Архиповой, В.А. Образцова, Л.В. Бертовского, Н.Л. Бертовской, М.Е. Игнатьева и др.

Исследование электронных сообщений в большинстве случаев требует специальных знаний. Особенности использования специальных знаний, в том числе применительно к электронным сообщениям, рассматривались в работах по лингвистике, психологии, информационным технологиям Е.И. Галяшиной, Ф.О. Байрамовой, А.А. Воробьевой, А.В. Громовой, Т.А. Литвиновой, А.В. Гвоздева, Ю.Н. Баранова, Г.Н. Беспамятновой, С.М. Вула, А.С. Романова, О.Г. Шевелева, Е.А. Ахоховой, А.А. Журавлевой, С.Л. Коваль, А.И. Винберг, А.А. Эйсман, А.Ш. Каганова, И.Н. Подволоцкого.

Вопросы психологического исследования текста затрагивались такими авторами, как А.А. Леонтьев, А.М. Шахнарович, В.И. Батов, А.А. Журавлева, С.Л. Коваль, Е.А. Брусиловский.

Работа носит междисциплинарный характер, поэтому в ходе исследования также рассматривались работы ученых в области информационных технологий и кибернетики, физико-математических наук, логики, таких как Н. Винер, А.К. Гуц, В.Ф. Шаньгин, А.В. Галицкий, С.Д. Рябко, Д.А. Губанов, Д.А. Новиков, А.Г. Чхартитшвили, Ю.В. Ивлев, Г.В. Саенко, О.В. Тушканова. Вопросы дактилоскопического и генетического исследования биологических следов человека на устройстве, с помощью которого отправлялись электронные сообщения, рассматривались в работах И.О. Перепечиной, Э.Т. Хайруловой, Т.Ф. Моисеевой.

На монографическом уровне тематику, связанную с исследованием электронных сообщений и компьютерной информации, разрабатывали:

В.Б. Вехов («Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки», 2008); Е.Р. Россинская, А.И. Семикалентова, И.А. Рядовский («Теория информационно-компьютерного обеспечения криминалистической деятельности», 2022); И.В. Александров, И.М. Комаров, М.Ш. Махтаев, Е.С. Крюкова, Е.И. Ян и др. «Электронные носители информации в криминалистике», 2017); А.И. Сотов («Компьютерная информация под защитой. Правовое и криминалистическое обеспечение безопасности компьютерной информации», 2017) и др.

Также в процессе исследования проводился анализ иностранной литературы таких авторов, как К. Шеннон (K. Shennon), Орин С. Керр (Orin S. Kerr), С. Браун (S. Braun), М.Т. Бритц (M.T. Britz), Е. Кейзи (Casey E.), Д.Р. Хайез (D.R. Hayes), Б. Нельсон (B. Nelson), А. Филипс (A. Phillips)., С. Стюарт (C. Steuart), А. Родригез Альварез (A. Rodríguez Álvarez) и др.

Таким образом, в настоящее время сложилась обширная теоретическая и методическая база в области исследования компьютерной информации,

теоретических и тактических рекомендаций по поиску, изъятию и исследованию такой информации, особенностей расследования компьютерных преступлений и тактики проведения отдельных следственных действий с использованием электронных доказательств. Вместе с тем, несмотря на мощный вклад ученых в исследование данной области, комплексных исследований, рассматривающих именно электронные сообщения, их природу, классификацию, тактику и технические особенности изъятия и исследования, их использование для построения версий и доказывания вины не проводилось. В теории криминалистики рассматривались только отдельные вопросы по исследованию электронных сообщений, либо глобальные вопросы исследования компьютерной информации. Для устранения данного пробела было выполнено настоящее исследование.

Цель настоящего исследования состоит в разработке теоретических основ и практических рекомендаций правоохранительным органам по выявлению, исследованию и использованию криминалистически значимой информации, содержащейся в электронных сообщениях, с использованием возможностей технико-криминалистических, тактико-криминалистических и методико-криминалистических средств и методов.

В качестве средств достижения цели определен следующий комплекс **задач**:

1) раскрыть понятие электронных сообщений и отразить их криминалистическое значение;

2) выделить основания для классификации электронных сообщений для целей криминалистического исследования, выделить их криминалистически значимые характеристики;

3) разработать приемы установления местонахождения электронных средств, программного обеспечения и места хранения электронных сообщений на устройствах и носителях;

4) исследовать процесс индексированного поиска электронных сообщений;

5) рассмотреть возможности криминалистической идентификации отправителей электронных сообщений;

6) разработать тактическо-криминалистические рекомендации по изъятию и фиксации электронных сообщений;

7) выработать тактические приемы по использованию электронных сообщений в процессе допроса подозреваемого (обвиняемого);

8) раскрыть возможности судебно-экспертного исследования электронных сообщений.

Объектом диссертационного исследования являются технические, правовые и методические аспекты по применению сотрудниками правоохранительных органов криминалистических знаний в ходе исследования информации из электронных сообщений и использовании их в ходе расследования в качестве ориентирующей или доказательственной информации.

Предметом диссертационного исследования выступают закономерности и оптимальные приемы, связанные с поиском, выявлением, изъятием и анализом электронных сообщений в рамках расследования уголовного дела.

Методологическую основу исследования составил всеобщий диалектический метод познания как способ изучения явлений и процессов объективной реальности; основанные на нем общенаучные и частные научные методы. Для получения достоверных и обоснованных результатов исследования использовались методы индукции, дедукции, анализа, синтеза. С помощью этих методов были достигнуты такие задачи, как выработка понятий, криминалистических классификаций. Методы наблюдения, описания, сравнения и анализа применялись при рассмотрении исследования электронных сообщений как системы действий следователя или эксперта. Логический метод применялся для выработки алгоритма составления списка ключевых слов для индексации. Наряду с общенаучными методами использовались и частнонаучные: сравнительно-правовой метод использовался для рассмотрения законодательства и подходов к

изучению электронных сообщений в других странах; социологический - для сбора эмпирического материала путем анкетирования следователей и изучения судебных решений, материалов надзорных производств прокуратуры; информационно-кибернетический – для рассмотрения процесса индексации электронных сообщений. Также в работе были использованы специальные методы криминалистики: структурно-криминалистический для построения тактики проведения следственных действий, связанных с исследованием сообщений, и для составления рекомендаций и технико-криминалистический метод, лежащий в основе формирования рекомендаций по поиску, изъятию и фиксации электронных доказательств с использованием технико-криминалистических средств.

Нормативную основу диссертационного исследования составили: Конституция Российской Федерации; Уголовный кодекс Российской Федерации; Уголовно-процессуальный кодекс Российской Федерации; Федеральные законы «Об информации, информационных технологиях и о защите информации», «Об оперативно-розыскной деятельности», «О государственной судебно-экспертной деятельности»; международно-правовые акты; нормативные правовые документы федеральных органов государственной власти, затрагивающие исследуемую проблему[2]. Помимо указанного, в исследовании использовались межгосударственные и государственные стандарты (ГОСТ 20886-85 «Организация данных в системах обработки данных. Термины и определения»; ГОСТ *Р 53898-2013 «Системы электронного документооборота. Взаимодействие систем управления документами. Требования к электронному сообщению»;* «Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств»»).

[2] См.: Приказ МВД России, Министерства обороны РФ, ФСБ России, Федеральной службы охраны РФ, Федеральной таможенной службы, Службы внешней разведки РФ, Федеральной службы исполнения наказаний, Федеральной службы РФ по контролю за оборотом наркотиков, Следственного комитета РФ от 27.09.2013 № 776/703/509/507/1820/42/535/398/68 «Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд» // СПС «КонсультантПлюс».

Теоретическую основу диссертационного исследования составили положения, отраженные в трудах известных ученых-криминалистов. В их работах освещены вопросы изучения информации в криминалистике, информационного обеспечения криминалистической деятельности, тактические вопросы проведения следственных действий в отношении электронной информации, вопросы экспертного исследования электронной информации. В основу данного исследования легли работы по теории криминалистики В.Я. Колдина, Р.С. Белкина, Н.П. Яблокова, В.В. Крылова, В.Б. Вехова, Е.Р. Россинской, А.И. Семикалентовой, И.А. Рядовского, И.М. Комарова, И.В. Александрова, В.М. Мещерякова, А.В. Ткачева, А.И. Сотова, М.В. Жижиной, А.И. Зазулина и других авторов; работы по судебной экспертологии Е.И. Галяшиной, Ф.О. Байрамовой, А.А. Воробьевой, А.В. Громовой, Т.А. Литвиновой, А.В. Гвоздева, Ю.Н. Баранова, Г.Н. Беспамятновой, А.С. Романова, А.И. Винберга, А.А. Эйсмана, А.Ш. Каганова, И.Н. Подволоцкого, И.О. Перепечиной и других ученых; работы, затрагивающие технические аспекты: И.В. Собецкого, Н. Винера, А.К. Гуца и других авторов.

Эмпирическая база диссертационного исследования представлена:

а) обобщением результатов анкетирования сотрудников правоохранительных органов, произведенного в 2023 году, в ходе которого было опрошено 120 следователей Следственного комитета РФ и Министерства внутренних дел РФ г. Москвы, Московской, Калужской, Волгоградской, Самарской, Ярославской, Тамбовской и Ивановской областей, Республик Хакасия и Адыгея.

б) результатами обобщения следственной практики, в ходе изучения которой было проанализировано 105 надзорных производств прокуратуры Ярославской области за 2020-2023г. по уголовным делам, в которых в качестве ориентирующей или доказательственной информации фигурировали электронные сообщения;

в) результатами обобщения судебной практики, основанной на изучении 100 судебных решений по уголовным делам за 2016-2024г., в ходе расследования

которых назначались и проводились экспертизы в отношении электронных сообщений или их носителей.

Научная новизна диссертационного исследования состоит в системе новых знаний, полученных в результате комплексного подхода к работе с электронными сообщениями для следственных работников, обеспечивающей возможность наиболее эффективного использования электронных сообщений как средства доказывания.

В диссертации раскрыто понятие электронных сообщений и впервые освещены криминалистические признаки электронных сообщений, на базе которых выделены основания для классификации.

Автором разработаны методические рекомендации для работников правоохранительных органов по исследованию электронных сообщений, описаны способы установления устройств, программного обеспечения для обмена сообщениями на этих устройствах, способы поиска самой информации на устройствах, изъятия и фиксации информации, поиска относимых к расследованию сообщений путем индексации. Как результат, соискателем разработана и обоснована новая общая методика по выявлению, фиксации и использованию электронной переписки в качестве доказательства, а также разработан алгоритм составления списка ключевых слов для индексированного поиска.

Научная новизна конкретизируется в положениях, выносимых на защиту.

Основные положения, выносимые на защиту.

1. Формулировка понятия электронного сообщения, которое представляет собой ограниченный объем компьютерной информации, предназначенный для передачи от отправителя через средства электросвязи определенному количеству пользователей, характеризующийся следующими группами свойств: содержание и сопутствующая информация.

1.1. Под содержанием электронного сообщения понимается ограниченный объем компьютерной информации, который может представлять собой как

текстовую информацию, так и графическую, аудиовизуальную и иную, воспринимаемую человеком посредством компьютерных устройств.

1.2. Под сопутствующей информацией понимаются технические данные, описывающие характер сообщения и особенности его прохождения через информационно-телекоммуникационную сеть.

2. Разработана авторская классификация электронных сообщений по следующим основаниям:

– по критерию возможности непосредственного восприятия информации получателем сообщения делятся на зашифрованные и незашифрованные;

– по критерию возможности проведения индексированного поиска по ключевым словам и фразам сообщения подразделяются на индексируемые и неиндексируемые;

– в зависимости от программных средств создания и отправки сообщения могут быть созданные и отправленные (с помощью одного и того же средства; с помощью стороннего средства; программным средством без участия человека);

– по критерию достоверности, понимаемой как оценка правдивости передаваемых сведений, сообщения делятся на:

а) дезинформационные:

– образующие состав преступления (криминальные);

– ложные, но не содержащие признаков состава преступления (предкриминальные);

б) не дезинформационные (правдивые).

3. Разработан алгоритм методических рекомендаций по подбору ключевых слов для индексации с целью поиска относимой информации в массиве электронных сообщений, составляющих электронную переписку, который состоит из следующих этапов:

I. Формулировка цели;

II. Оценка имеющейся у нас информации в соответствии с расследуемым событием;

III. Сопоставление имеющейся и искомой информации;

IV. Выявление основных слов, фраз, которые могут содержаться в искомой информации;

V. Определение особенностей, которые могут быть присущи общению именно между предполагаемыми адресатами (сленг, шифр). Формирование синонимов с учетом характерных особенностей;

VI. Формирование заключительного списка ключевых слов.

4. Обоснован вывод о том, что для установления отправителя электронного сообщения потенциально идентифицирующими (отображающими) объектами могут выступать данные учетной записи (аккаунта) или адреса, с которого было отправлено сообщение; цифровые следы[3] на устройстве; признаки в самом содержании сообщения; признаки, содержащиеся в активности пользователя в сети; звучащая речь в голосовом сообщении; видеоизображения в сообщениях; биологические следы на устройстве.

Ни по одному из источников на сегодняшний момент не возможна идентификация лица в криминалистическом смысле. Установление лица, написавшего сообщение и совершившего преступление, является задачей следователя в ходе расследования и решается комплексно: использованием идентификации в алгоритме доказывания, сбором доказательств, установлением фактов с опорой на данные об идентификации пользователя в интернет-среде.

5. Разработка тактических рекомендаций по поиску, изъятию электронных сообщений и использованию их при ведении расследования. Проведенное исследование следственной и судебной практики показало, что следственные работники, понимая важность электронного сообщения как доказательства, не всегда способны самостоятельно подготовить их для надлежащего исследования и оценить в полной мере значение содержащейся в них информации. В связи с этим для повышения эффективности следственной работы требуются четкие указания,

[3] Любая криминалистически значимая компьютерная информация, т. е. сведения (сообщения, данные), находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе с помощью электромагнитных взаимодействий либо передающиеся по каналам связи посредством электромагнитных сигналов (В.Б. Вехов).

которые могли бы применяться сотрудниками, не имеющими специального образования, и позволяли решить основной круг задач, возникающих в ходе следствия.

Автором предложены тактические рекомендации по использованию следователем данных об электронных сообщениях в процессе расследования, в частности при проведении допроса.

6. Разработка тактических рекомендаций по назначению судебно-технической экспертизы. Изучение следственной практики показало, что практические работники далеко не всегда правильно понимают возможности экспертизы при исследовании электронных сообщений. Это проявляется как в ненадлежащей подготовке материалов для экспертов, так и в некорректных формулировках вопросов, которые перед ними ставятся. Для решения этой проблемы были выработаны практические указания, обоснованные современной судебно-следственной практикой, представляющие собой набор приемов и методов, направленных на подготовку объектов исследования и формулирование технически грамотных задач.

Теоретическая значимость диссертационного исследования. Автором рассмотрены теоретические вопросы понимания природы электронной информации и электронных сообщений с точки зрения криминалистики и информационных технологий, проанализированы основы изучения электронных сообщений, которые развивают положения теории криминалистической диагностики и идентификации. Сделанные выводы доказывают возможность распространения базовых положений криминалистической теории на такие новые объекты, как компьютерная информация. Также были разработаны такие теоретические положения, как понятие электронного сообщения, их классификация.

Практическая значимость диссертационного исследования. Выводы автора могут быть использованы в практической деятельности работников правоохранительных органов и юристов. Методика исследования электронных

сообщений может служить рекомендацией для следователей по работе с электронной перепиской. Материалы диссертационного исследования могут найти применение при подготовке учебных программ и учебных и методических пособий в рамках специализированных курсов, связанных с криминалистическим изучением электронных доказательств.

Также практическая значимость состоит в повышении правового и технического уровня грамотности работников правоохранительных органов, необходимого для правильного использования электронных сообщений как источника доказательственной информации.

Достоверность результатов диссертационного исследования определяется тем, что оно проведено автором самостоятельно, единолично, на основе анализа теоретических работ и нормативно-правовых актов, использованием обширной базы нормативных и доктринальных источников, как отечественных, так и иностранных; корректным применением совокупности методов, адекватных предмету, цели и задачам исследования; аргументированностью выводов и рекомендаций, их апробацией в научной и практической деятельности.

Апробация результатов исследования.

Диссертация подготовлена на кафедре криминалистики Юридического факультета Московского государственного университета имени М.В. Ломоносова.

Апробация результатов исследования осуществлялась автором в ходе:

– успешной защиты научно-квалификационной работы на тему «Электронные сообщения как источник криминалистически значимой информации в расследовании преступлений», прошедшей по окончании обучения в аспирантуре Юридического факультета МГУ имени М.В. Ломоносова;

- выступлений и докладов на конференциях и круглых столах, проводимых в том числе кафедрой криминалистики Юридического факультета МГУ имени

М.В. Ломоносова: «Использование переписки в социальных сетях в доказывании по уголовным делам» на конференции «Цифровизация: плюсы и минусы для криминалистики», г. Санкт-Петербург, Россия, 22–23 ноября 2019 г.; «Криминалистическое исследование сообщений на электронной почте, в том числе в рамках оперативно-розыскной деятельности: установление аккаунта, оператора и пользователя электронного почтового ящика» на XIV научно-практической конференции «Актуальные проблемы юридической науки и практики: взгляд молодых ученых», Федеральное государственное казенное образовательное учреждение высшего образования «Университет прокуратуры Российской Федерации», Россия, 29 апреля 2022 г.; «Электронные сообщения как источник криминалистически значимой информации в расследовании преступлений» на конференции «Ломоносов-2022»; «Криминалистические аспекты исследования доказательств в виде электронных сообщений» на XXIII ежегодной Международной научно-практической конференции «Государство и право России в современном мире» секция «Криминалистика в современном мире: проблемы теории и практики», г. Москва, Россия, 23–25 ноября 2022 г.; «Учение В.Я. Колдина об информационных полях в контексте криминалистического исследования электронных сообщений» на круглом столе «Общетеоретические проблемы криминалистики и судебной экспертизы», посвященном памяти В.Я. Колдина, МГУ, г. Москва, Россия, 20 апреля 2023 г.; выступление на заседании научно-студенческого кружка кафедры криминалистики с докладом «Электронные сообщения в криминалистике» 14 мая 2024 г.

Сформулированные автором научные положения и рекомендации были опубликованы в 10 научных статьях, четыре из которых – в ведущих рецензируемых научных изданиях, рекомендованных ВАК при Министерстве образования и науки Российской Федерации, из перечня утвержденных решением Ученого совета МГУ имени М.В. Ломоносова.

На основе результатов исследования соискателем были разработаны методические рекомендации по работе следователей с электронной перепиской.

Методические рекомендации предназначены для работников следственного комитета, следователей и дознавателей МВД РФ, но могут быть полезны экспертам-криминалистам и юристам. Они содержат комплекс предложений и указаний, способствующих внедрению в практику наиболее эффективной тактики, техники и методики исследования и использования электронной переписки в ходе расследования.

По результатам изучения контрольно-следственным отделом следственного управления Следственного комитета России по Ярославской области принято решение об использовании данных методических рекомендаций в расследовании преступлений.

Глава 1. Электронные сообщения и средства, используемые для обмена информацией

§ 1. Понятие и классификация электронных сообщений и их криминалистическое значение

Согласно общей криминалистической теории, криминалистическое изучение преступной деятельности, ее структурных элементов, их связей, и формирование на этой основе ее криминалистической характеристики невозможно без знания процесса информационного отображения события преступления во вне[4]. В современном мире практически все аспекты человеческой деятельности, в том числе преступной, так или иначе фиксируются электронными средствами. «Глобальный процесс цифровизации обусловил, с одной стороны, новые виды криминалистически значимой информации, фиксируемой на специфических компьютерных носителях, а с другой – широкое использование цифровых средств фиксации, сохранения, автоматизированной обработки и исследования доказательственной и ориентирующей информации»[5].

Учитывая ту роль, которую сейчас играет электронный информационный обмен, определение механизма данного явления, его особенностей как источника доказательственных сведений является одной из важнейших криминалистических задач и обязательным условием успешного раскрытия и расследования преступлений.

Информационный след, сформированный электронным устройством, может оставаться на нем либо быть переданным на другое устройство, создавая тем самым электронное сообщение. Такой информационный след или, как справедливо предлагает называть его Е.Р. Россинская, «цифровой след»[6], не является

[4] См.: Криминалистика: учебник / Отв. ред. Н.П. Яблоков. 3-е изд., перераб. и доп. – М.: Юристъ, 2005. – С. 53.
[5] См.: *Россинская Е.Р.* Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности // Вестник Восточно-Сибирского института МВД России. 2019. № 2 (89). С. 195.
[6] Там же. С. 199.

материальным объектом в прямом его смысле и не может восприниматься непосредственно без устройства или носителя. Это ставит вопрос о том, к какому виду следов отнести компьютерную информацию – материальным, идеальным или же к иному, новому виду.

Отвечая на данный вопрос, отдельные ученые, (В.А. Мещеряков[7], А.Б. Смушкин[8]) предлагают выделить новый вид следов – виртуальные. В.А. Мещеряков основывает такое выделение на специфических приемах и методах обнаружения, извлечения (фиксации), исследования и оценки подобных следов[9]. Однако, по мнению Е.Р. Россинской, «с позиций криминалистики "виртуальных следов" не может быть в принципе, так как описываемые следы являются материальными, поскольку зафиксированы на материальных носителях путем изменения свойств или состояния отдельных их элементов»[10]. Поддерживает данную позицию и В.Б. Вехов, который указывает, что «компьютерная информация материальна. Она всегда будет опосредована через материальный носитель, вне которого физически не может существовать. Как и некоторые другие материальные вещи, компьютерная информация может быть предметом коллективного пользования, так как доступ к ней могут одновременно иметь несколько лиц, например, при работе с информацией, содержащейся на электронной странице или сайте глобальной сети Интернет»[11]. Выражая принципиальное согласие с данной точкой зрения, мы также считаем, что информация, содержащаяся на электронном устройстве или носителе – материальна, так как не отделима от электронного носителя. «Вся компьютерная информация опосредована через материальные носители, вне которых она

[7] См.: *Мещеряков В.А.* «Виртуальные следы» под «скальпелем Оккама» // Информационная безопасность регионов. 2009. № 1 (4). С. 28–33.
[8] См.: *Смушкин А.Б.* Виртуальные следы в криминалистике // Законность. 2012. № 8. С. 43–45.
[9] См.: *Мещеряков В.А.* Указ соч. С. 29.
[10] См.: *Россинская Е.Р.* Теория информационно-компьютерного обеспечения криминалистической деятельности... С. 199.
[11] См.: *Вехов В.Б.* Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки: монография. – Волгоград: ВА МВД России, 2008. – 404 с.

существовать не может. Следовательно, она имеет материальный, но обезличенный (без жесткой персонализированной связи с лицом) характер»[12].

Суть любого электронного сообщения заключается в том, что оно представляет собой электронную информацию, имеющую определенную значимость для человека, которая представлена в виде символов, знаков, изображений, видео- и аудиозаписей и которая передается посредством информационно-телекоммуникационной сети, хранится и обрабатывается электронным устройством. Р.С. Белкин писал: «Если информационный сигнал-доказательство выступает в предметной (вещественной) форме, то обязательным элементом исследования будет последующее перекодирование этого информационного сигнала до тех пор, пока его смысловое содержание не обретет доступной для субъекта познания формы»[13]. Таким образом, восприятие сообщения получателем должно отражать в его сознании ту же информацию, которую в нее вкладывал отправитель, в противном случае сообщение будет нерасшифрованным или неверно интерпретированным.

Оценивать электронные сообщения как источник криминалистически значимой информации следует, опираясь на теорию В.Я. Колдина об информационно-логической структуре доказывания. Согласно данной теории, процесс отображения представляет собой процесс передачи сообщений в форме кода, определяемого механизмом следообразования, а след – фиксированное в окружающей среде сообщение[14]. Расследуемое событие отображается в окружающей среде в виде различных следов, каждый из которых может рассматриваться как сообщение. В результате исследования таких следов-сообщений субъект доказывания получает фактические данные об исследуемом событии. Эти фактические данные, при условии их получения в режиме процессуального доказывания, являются доказательствами и могут быть

[12] См.: Электронные носители информации в криминалистике: монография / И.В. Александров [и др.]. – М.: Юрлитинформ, 2017. – С. 28.
[13] См.: *Белкин Р.С.* Курс криминалистики: учеб. пособие для вузов. 3-е изд., доп. – М.: НОРМА, 2001. – С. 78.
[14] См.: *Колдин В.Я.* Вещественные доказательства: Информационные технологии процессуального доказывания / Под общ. ред. д. ю. н., проф. В.Я. Колдина. – М.: НОРМА, 2002. – С. 11.

использованы для установления доказательственных фактов[15]. Электронное сообщение – это информация, передаваемая в форме двоичного кода (так как механизмом следообразования в данном случае является передача информации с помощью компьютера), а след – фиксированное на электронном носителе сообщение, доступное для восприятия человеком.

Для понимания структуры электронного сообщения как источника информации его следует рассмотреть, опираясь на теорию информационных полей, которую также разработал В.Я. Колдин. В рамках данной теории предполагается последовательное выделение носителя информации, затем ее источника, а затем – информационного поля. Под носителем подразумевается материальный объект, выделенный в обстановке расследуемого события в качестве потенциального источника криминалистической информации, а под источником – выделенная в процессе криминалистического анализа система свойств носителя, измененных под воздействием расследуемого события. Информационное поле – это выделенный в составе источника поток однородной информации об обстоятельстве, подлежащем установлению в соответствии с задачами криминалистического исследования и доказывания[16].

В отношении электронных сообщений носителем является компьютер или любой другой материальный электронный носитель информации, на котором хранится электронное сообщение. Соответственно источник – само электронное сообщение в виде набора символов, изображений, звуков, адресной информации, метаданных[17] и т. д. А в качестве информационного поля будет выступать то значение информации, которое несет в себе сообщение.

Таким образом, электронные сообщения для своего правильного осмысления не требуют особого подхода в рамках криминалистической теории, и на них в полном объеме распространяются уже имеющиеся доктрины. Но, безусловно, для

---

[15] См.: *Колдин В.Я.* Вещественные доказательства. С. 11.
[16] См.: *Колдин В.Я.* Анализ информационных полей как метод декодирования криминалистической информации // Вестник криминалистики. 2012. № 4 (44). С. 14.
[17] Данные, описывающие контекст, содержание, структуру документов и управление ими – ГОСТ Р ИСО 15489-1-2007.

корректного использования электронных сообщений в процессе доказывания необходимо определить их основные черты, отличающие от других источников, т. е. выработать понятие.

Сложность в выработке определения электронного сообщения заключается в том, что с технической точки зрения такие сообщения весьма многообразны. Это может быть и SMTP (Simple Mail Transfer Protocol), используемый для передачи электронной почты в сетях TCP/IP, и SMS/MMS, используемые в сетях сотовой связи, и голосовая почта, и система мгновенного обмена сообщениями (мессенджеры), и обычная электронная почта, передаваемая по сети Интернет. Поэтому необходимо уяснить базовые признаки электронного сообщения, которые позволят выделить его из массива других источников данных.

Как указывалось выше, содержание электронного сообщения представляет собой информацию. Ю.Н. Соколов отмечает, что «электронная информация – это основной термин, и сообщения, передаваемые через единую сеть электросвязи РФ, являются информацией в электронном виде»[18]. А.И. Зазулин пишет, что «без правильного понимания природы информации невозможно проведение исследования ее значения и использования в уголовно процессуальном доказывании»[19]. По мнению В.В. Крылова, «если исходить из того, что термин “сообщение” в контексте действующих правовых норм предполагает активные волевые действия лица по передаче вовне информации, то термин “информация” может интерпретироваться и как совокупность формализованных сведений (знаний), предназначенных для передачи в качестве сообщения»[20].

Слово «информация» произошло от латинского informatio (разъяснение, изложение)[21] и означает «осведомление, сообщение». С середины XX в. оно стало общенаучным понятием, включающим «обмен сведениями между людьми,

[18] См.: *Соколов Ю.Н.* Наложение ареста на электронные сообщения, их осмотр и выемка («Российский следователь». 2020. № № 10. С. 38–41) // СПС Консультант Плюс. – С. 6.
[19] См.: *Зазулин А.И.* Правовые и методологические основы использования цифровой информации в доказывании по уголовному делу: дис. … канд. юрид. наук. – Екатеринбург, 2018. – С. 74.
[20] См.: *Крылов В.В.* Расследование преступлений в сфере информации. – М.: Городец, 1998. – С. 48.
[21] См.: *Дворецкий И.Х.* Латино-русский словарь. – М.: Русский язык, 1976. – С. 523.

человеком и машиной, машиной и машиной. С общенаучной и семиотической точки зрения информацией считается любой акт общения, выражения чувств или мыслей…»[22].

Основоположник кибернетики Н. Винер определял информацию как «обозначение содержания, полученного из внешнего мира в процессе нашего приспособления к нему и приспособления к нему наших чувств»[23]. В кибернетике также под информацией понимается «сообщение, осведомляющее кого-то о состоянии той или иной системы или воздействиях одной системы на другую систему, которые можно назвать деятельностью первой системы… Кратко можно охарактеризовать информацию как сведения о чем-нибудь»[24]. К. Шеннон определяет информацию, как «любой сигнал, который устраняет неопределенность, имеющуюся у получателя сигнала относительно свойств, которыми обладает источник сигнала»[25].

Стоит отметить, что «как правило, содержащаяся в сообщениях информация носит текстовой характер, однако во многих случаях необходимые сведения могут находиться в пересылаемых файлах формата PDF или даже JPEG, PNG (графические файлы)»[26]. Помимо указанного, сообщения могут быть представлены и в видеоформате (например, мгновенные видеосообщения в мессенджере Telegram).

Повышенная значимость информации в современном мире обусловила необходимость законодательного закрепления ее понятия. Согласно ст. 2 Федерального закона «Об информации, информационных технологиях и о защите

---

[22] См.: *Ахохова Е.А.* Семиотика и лингвистика: Конспект лекций: учеб. пособие. – Нальчик: Полиграфсервис и Т, 2007. – С. 4.
[23] См.: *Винер, Н.* Кибернетика и общество / Н. Виннер. - М. : Издательство иностранной литературы, 1958, С.31
[24] См.: *Гуц А.К.* Кибернетика: учебное пособие. – Омск: Изд-во Омск. гос. ун-та, 2014. – С. 13.
[25] См.: *Шеннон К.* Математическая теория связи // Работы по теории информации и кибернетике: сборник статей: пер. с англ. / Предисл. А. Н. Колмогорова ; под ред. Р.Л. Добрушина и О.Б. Лупанова. – М.: Издательство иностранной литературы, 1963. – С. 243–322.
[26] См.: *Сотов А.И.* Исследование электронной переписки путем индексации // Сборник материалов по результатам работы Международного научно-практического форума – круглого стола, посвященного памяти профессора кафедры криминалистики Колдина Валентина Яковлевича. – М.: Юрлитинформ, 2021 – С. 180.

информации» информацией являются «сведения (сообщения, данные) независимо от формы их представления»[27].

Информация не является однородной, у нее имеется несколько разновидностей. Объектом настоящего исследования является такая категория, как компьютерная информация. В.В. Крылов определял компьютерную информацию как «сведения, представленные в виде электрических сигналов, доступных для восприятия средствам компьютерной техники, хранящиеся на машинном носителе или передаваемые по компьютерной (информационно-телекоммуникационной) сети»[28]. Согласно ч. 1 Примечания к ст. 272 Уголовного кодекса РФ, компьютерная информация – это «сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи»[29]. Как отмечает А.И. Сотов, «данное определение является слишком широким, что позволяет признать компьютерной информацией даже сигнал, передаваемый между двумя обычными проводными телефонами»[30]. То есть под это понятие могут подпадать и другие объекты, отличные по своей природе от определяемого.

Поэтому необходимо обратиться к Постановлению Пленума ВС РФ[31], в котором уточняется понятие компьютерной информации: «Такие сведения могут находиться в запоминающем устройстве электронно-вычислительных машин и в других компьютерных устройствах (далее – компьютерные устройства) либо на любых внешних электронных носителях (дисках, в том числе жестких дисках – накопителях, флеш-картах и т. п.) в форме, доступной восприятию компьютерного устройства, и (или) передаваться по каналам электрической связи. При этом к числу

---

[27] См. пункт 1 статьи 2 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ // СПС «КонсультантПлюс».

[28] См.: *Крылов В.В.* Современная криминалистика. Правовая информатика и кибернетика. – М.: ЛексЭст, 2007. С. 99.

[29] См. часть 1 Примечания к статье 272 Уголовного кодекса Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 24.02.2021) // СПС «КонсультантПлюс».

[30] См.: *Сотов А.И.* Компьютерная информация под защитой. Правовое и криминалистическое обеспечение безопасности компьютерной информации: монография. – М.: Ru-science.com, 2017. – С. 25.

[31] См. пункт 2 Постановления Пленума ВС РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть “Интернет”» // СПС «Консультант Плюс».

компьютерных устройств могут быть отнесены любые электронные устройства, способные выполнять функции по приему, обработке, хранению и передаче информации, закодированной в форме электрических сигналов (персональные компьютеры, включая ноутбуки и планшеты, мобильные телефоны, смартфоны, а также иные электронные устройства, в том числе физические объекты, оснащенные встроенными вычислительными устройствами, средствами и технологиями для сбора и передачи информации, взаимодействия друг с другом или внешней средой без участия человека), произведенные или переделанные промышленным либо кустарным способом».

Исходя из подходов к определению информации, отличительными признаками электронного сообщения являются, с одной стороны, его информационное содержание, а с другой – электронная природа, присущая компьютерным данным.

Для понимания природы объекта исследования надо отметить, что электронное сообщение – это в первую очередь средство коммуникации. «Коммуникация – это акт отправления информации от мозга одного человека к мозгу другого человека... в этом процессе существуют отправитель, получатель и сообщение, передаваемое от первого ко второму»[32]. «Изначально люди обменивались информацией устно. Важнейший толчок развитию коммуникации дало создание письменности. По мере ее совершенствования менялась точность передачи информации текстом. Люди пытались коммуницировать при помощи предметного, пиктографического, идеографического, иероглифического, слогового, алфавитного письма. Именно алфавитом пользуется сегодня большая часть человечества»[33]. Отсюда следует, что коммуникация предполагает наличие отправителя информации и ее получателя, т. е. субъекта, который может отправленные сведения получить и понять.

---

[32] См.: *Смит П., Бэрри К., Пулфорд А.* Коммуникации стратегического маркетинга. – М.: Юнити-Дана, 2001. – С. 18.

[33] См.: *Назайкин А.Н.* Медиатекст будущего – «сенсотекст» // МедиаАльманах. 2019. № 5. С. 12−21.

Таким образом, электронное сообщение обладает такими признаками, как электронная природа, информационное содержание, наличие отправителя и получателя.

В криминалистике делались попытки определить электронное сообщение, но большинство из них были направлены не столько на описание предмета, сколько на разграничение понятий электронного сообщения и электронного документа. В.Б. Вехов предлагает понимать под электронным сообщением «информацию, переданную или полученную пользователем информационно-телекоммуникационной сети. К ним относятся так называемые сообщения “электронной почты”, “SMS”, “MMS” и др.»[34]. А.Н. Першин о понятии электронного сообщения писал следующее: «Сравнительный анализ данных определений свидетельствует о том, что электронное сообщение и электронный документ преследуют коммуникативные цели: создаются, сохраняются, обрабатываются и уничтожаются при помощи электронно-вычислительных машин и их программного обеспечения; воспринимаются человеком только благодаря электронно-вычислительной машине и программному обеспечению»[35]. Автор приводит понятие электронного документа – «документированная информация, представленная в электронной форме, т. е. в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах, подписанная электронной подписью»[36]. Основное различие электронного сообщения и документа автор видит в наличии либо отсутствии электронной подписи.

Понятие электронного сообщения отражено и в нормативных определениях. Согласно п. 10 ст. 2 ФЗ «Об информации, информационных технологиях и о защите

---

[34] См.: *Вехов В.Б., Смагоринский Б.П., Ковалев С.А.* Электронные следы в системе криминалистики // Судебная экспертиза. 2016. Вып. 2 (46). – С. 14–15.

[35] См.: *Першин А.Н.* Документированная информация: криминалистические подходы к понятию и исследованию Монография / А.Н. Першин – Москва : Проспект, 2020. Гл.4, С.11.

[36] См. п. 11.1 ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс».

информации», «электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети»[37]. По нашему мнению, данное определение довольно широко, под него могут подпадать не только электронные сообщения, но и любая передаваемая в сети Интернет информация, включая публикации, комментарии и прочее.

ГОСТ Р 53898-2013 «Системы электронного документооборота. Взаимодействие систем управления документами. Требования к электронному сообщению» определяет электронное сообщение как «файл (набор файлов), передаваемый из одной системы управления документами в другую»[38], что, на наш взгляд, также не совсем верно, поскольку не отражает информационной природы электронного сообщения.

В «Правилах оказания телематических услуг связи»[39] содержится определение телематического электронного сообщения. Оно характеризуется как «одно или несколько сообщений электросвязи, содержащих информацию, структурированную в соответствии с протоколом обмена, поддерживаемым взаимодействующими информационной системой и абонентским терминалом». В этом понятии раскрывается, что сообщения представляют собой информацию, передающуюся посредством протокола передачи данных и поддерживающуюся абонентским терминалом, представляющим собой совокупность технических и программных средств, применяемых пользователем. На наш взгляд, из всех существующих нормативных определений именно это наиболее полно отражает суть электронных сообщений для целей правоприменения. Тем не менее представляется, что приведенные выше нормативные определения упускают весьма существенный аспект, важный для правильного понимания электронного

[37] См. п. 10 ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ // СПС «КонсультантПлюс».
[38] См. п. 3.20 ГОСТ Р 53898-2013 «Системы электронного документооборота. Взаимодействие систем управления документами. Требования к электронному сообщению» // СПС «КонсультантПлюс».
[39] См. п. 2 Постановления Правительства РФ от 31.12.2021 № 2607 «Об утверждении Правил оказания телематических услуг связи» (с изменениями и дополнениями) // СПС «Гарант».

сообщения – ограниченный доступ к указанной информации (содержанию сообщения).

По смыслу вышеупомянутых определений, электронным сообщением можно также признать комментарий или публикацию, размещенные пользователем в сети Интернет. Однако комментарии и публикации, как правило, представляют собой публично размещенную информацию, доступ к которой имеют все пользователи сети или, как минимум, все зарегистрированные пользователи определенного сайта. Представляется, что как с криминалистической, так и с правоприменительной точки зрения, распространять на эти данные понятие «электронное сообщение» было бы неверно. Электронные данные, размещенные для доступа неограниченного круга пользователей (которые в полном составе заведомо не могут быть известны отправителю), следует называть объявлениями. Благодаря открытому характеру доступ к ним, их изъятие и исследование коренным образом отличается от подходов к электронным сообщениям, и в данной работе электронные объявления рассматриваться не будут.

В монографии «Электронные носители информации в криминалистике» высказывается точка зрения, что «электронные сообщения могут носить публичный, общедоступный характер (например, сообщения на интернет-форумах). Думается, что в этом случае их нельзя относить к данным переписки, которая по определению предполагает конфиденциальность»[40]. На наш взгляд, понятие электронного сообщения отграничивается от понятия электронной переписки не критерием конфиденциальности, а количественным критерием. Электронная переписка включает в себя некоторое количество взаимосвязанных электронных сообщений. То, что авторы предлагают понимать под электронным сообщением, как и говорилось выше, следует называть электронным объявлением. Электронное же сообщение имеет всегда ограниченный круг получателей. Этот круг может быть очень широким, включать множество адресов (например, в случае со спам-рассылкой тысячи адресов получателей определяются и подбираются с

[40] См.: Электронные носители информации в криминалистике. С. 131.

помощью специальных программ). Однако после получения данного сообщения оно доступно для прочтения конкретным отправителем и получателем из заранее определенного круга.

Такой признак как определенность круга получателей сообщений очень важен для изучения электронных сообщений в криминалистике. Определенность круга получателей имеет как правовое, так и криминалистическое значение. Неопределенный круг получателей позволяет характеризовать действие не как предоставление информации, а как ее распространение, что вытекает из п.8. и п.9. Федерального закона от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации", а это уже может влиять на квалификацию по таким составам как ст. 207.1, 207.2 УК РФ. С криминалистической точки зрения ограниченность круга получателей позволяет оценивать негативные последствия сообщения, направленность умысла лица на привлечение к преступному деянию нескольких субъектов или их неограниченного множества, наличие и численность организованной преступной группы и пр. Ограниченность круга лиц напрямую влияет на понимание механизма следообразования при отправке сообщения, что в свою очередь влияет на построение, выдвижение и проверку криминалистических версий, на возможности идентификации отправителей и получателей, на выбор тактики.

Существенный интерес представляют подходы к определению электронного сообщения в зарубежном законодательстве.

В типовом законе ЮНСИТРАЛ об электронной торговле, принятом Генеральной Ассамблеей ООН, понятие электронных сообщений отсутствует, однако приводится термин «сообщение данных», который означает «информацию, подготовленную, отправленную, полученную или хранимую с помощью электронных, оптических или аналогичных средств, включая электронный обмен

данными, электронную почту, телеграмму, телекс или телефакс, но не ограничиваясь ими»[41].

В Модельном законе об электронной торговле, принятом Межпарламентской Ассамблеей государств – участников СНГ, электронные сообщения определяются как «информация, подготовленная, отправленная, полученная и хранимая с помощью информационных систем, информационно-коммуникационной сети и электронных процедур»[42].

В Правилах конфиденциальности электронных коммуникаций Соединенного Королевства под электронными сообщениями понимается «любое текстовое, голосовое, звуковое или графическое сообщение, отправленное по общедоступной сети электронных коммуникаций, которое может храниться в сети или в терминальном оборудовании получателя до тех пор, пока оно не будет прочитано и включает сообщения, отправленные с использованием сервисов обмена мгновенными сообщениями»[43].

Согласно Закону США о хранящихся сообщениях, «электронные сообщения означают любую передачу знаков, сигналов, письменности, изображений, звуков, данных или разведывательных данных любого характера, передаваемых полностью или частично по проводной связи, радио, с помощью электромагнитной, фотоэлектронной или фотооптической системы»[44], не включая:

а) сообщение, переданное с помощью телеграфа или любое устное сообщение;

---

[41] См.: Типовой закон ЮНИСИТРАЛ об электронной торговле // URL: https://uncitral.un.org/ru/texts/ecommerce/modellaw/electronic_commerce (дата обращения: 20.12.2023).

[42] См. ст. 2 Модельного закона «Об электронной торговле» (принят в г. Санкт-Петербурге 25.11.2008 на 31-м пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ, Постановление № 31-12) // URL: https://docs.cntd.ru/document/902157685 (дата обращения: 15.03.2023).

[43] The Privacy and Electronic Communications (EC Directive) Regulations 2003, Regulation 2 в дополнение к Закону о защите данных 2018 года (предыдущий – 1998 года).

[44] (12) “electronic communications” means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include – (A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (as defined in section 3117 of this title); or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

б) любое сообщение, переданное через пейджинговое устройство только с тональным сигналом;

в) любое сообщение, переданное посредством устройства слежения;

г) информацию об электронном переводе денежных средств, хранящуюся финансовым учреждением в системе связи, используемой для электронного хранения и перевода денежных средств[45].

Американское законодательство трактует электронное сообщение подробнее, чем российское. С юридической точки зрения в Российской Федерации к электронным сообщениям принято относить просто информацию, переданную с помощью информационно-телекоммуникационной сети. Согласно американскому подходу, электронные сообщения, передаваемые по различным каналам связи, включая сеть Интернет, могут включать в себя текстовые, голосовые, визуальные и прочие информационные образы. Кроме того, законодательство США позволяет исключить из состава электронных сообщений аналоговые сигналы, а также некоторые сигналы технического характера. Данное упоминание очень важно с точки зрения криминалистического исследования, так как работа с электронными сообщениями должна включать в себя также и работу с изображениями, звуками, видео и прочими файлами, содержащимися в сообщении. Напротив, сигналы технического характера в качестве сообщений рассматриваться не должны.

В законодательстве США также затрагивается вопрос об ограничении доступа к информации, содержащейся в сообщении.

Закон о конфиденциальности электронных данных США[46] и Закон о противодействии терроризму США[47] защищает отправителей и получателей электронных сообщений от неправомерного доступа к их содержанию. Законодательство делит информацию, входящую в электронные сообщения (и прочие коммуникации), на два типа – сопроводительную информацию (address

[45] См.: Title 18 of the United States Code §2510 (12) Stored communications act.
[46] См.: 18 U.S. Code Chapter 119 – Wire and electronic communications interception and interception of oral communications // URL: https://www.law.cornell.edu/uscode/text/18/part-I/chapter-119 (дата обращения: 20.12.2023).
[47] См.: Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA patriot act) act of 2001 // Public law 107–56–Oct. 26, 2001.

information) и само содержание (content); защита для каждого типа регламентируется отдельно[48]. Доступ к содержанию сообщений, переданных между двумя пользователями, ограничивается как вышеуказанными законами, так и Четвертой поправкой к Конституции США[49]. Законодательные акты ограничивают доступ к содержанию электронных сообщений и для сторонних пользователей, и для правоохранительных органов. При этом понятие «сторонние пользователи» не раскрывается.

На наш взгляд, разделение информации на собственно содержание сообщения и сопроводительную информацию необходимо, так как доступ к такой информации регулируется по-разному.

Исходя из изложенного, для целей криминалистического исследования электронные сообщения можно определить как ограниченный объем компьютерной информации, предназначенный для передачи от отправителя через средства электросвязи определенному количеству пользователей, характеризующийся следующими группами свойств: содержание и сопутствующая информация.

1. Под содержанием электронного сообщения понимается ограниченный объем компьютерной информации, который может представлять собой как текстовую информацию, так и графическую, аудиовизуальную и иную, воспринимаемую человеком посредством компьютерных устройств.

2. Под сопутствующей информацией понимаются технические данные, описывающими характер сообщения и особенности его прохождения через информационно-телекоммуникационную сеть.

Приведенные в данном определении признаки информации позволяют выделить несколько криминалистически значимых типов классификации электронных сообщений.

---

[48] См.: *Orin S.* Kerr: Fourth Amendment Seizures of Computer Data // The Yale Law Journal. 2010. Vol. 119. Pp. 700–724 // URL: https://www.yalelawjournal.org/pdf/853_76rix2f4.pdf (дата обращения: 20.05.2023).

[49] См.: U.S. Constitution – Fourth Amendment // URL: https://www.law.cornell.edu/constitution/fourth_amendment (дата обращения: 25.05.2023).

Как говорилось ранее, электронное сообщение должно быть доступно для восприятия получателем. Однако в отдельных случаях, когда отправитель хочет защитить свое сообщение от постороннего доступа, он может принять меры, затрудняющие понимание смысла, содержащегося в сообщении, иными лицами, кроме получателя. В качестве таких мер выступает шифрование. Шифрование (или криптография) представляет собой преобразование информации в целях ее сокрытия[50]. Незашифрованное сообщение – это информация, свободная для восприятия человеком, причем под восприятием надо понимать именно ту информацию, которую в сообщение вложил отправитель. Зашифрованное же сообщение предполагает восприятие значимой информации получателем (т. е. уяснение того самого смысла передаваемых данных, который намеревался довести отправитель) только после его расшифровки. Расшифровка предполагает наличие на устройстве установленного специального программного обеспечения, позволяющего преобразовать сообщение и сделать его подлинное содержание доступным для восприятия после введения ключа дешифровки. Фактор шифрования, несомненно, влияет на возможности криминалистического исследования сообщений. Поэтому по данному критерию необходимо выделить сообщения:

– зашифрованные;

– незашифрованные.

В ходе криминалистического исследования электронных сообщений применяется такой инструмент, как индексация – поиск по ключевым словам. Индексируемые сообщения – это те, которые подлежат индексации, т. е. информация в них может быть найдена по заданным ключевым словам. Неиндексируемые сообщения могут быть такого формата, который исключает обработку сообщения средствами индексации, или они могут быть сокрыты с помощью специальных инструментов, исключающих возможность их поиска по

[50] См.: *Шеннон К.* Теория связи в секретных системах // Работы по теории информации и кибернетике: сборник статей: пер. с англ. / Предисл. А. Н. Колмогорова; под ред. Р.Л. Добрушина и О.Б. Лупанова. – М.: Издательство иностранной литературы, 1963. – С. 333–402.

ключевым словам. По критерию возможности поиска по ключевым словам сообщения необходимо делить на:

– индексируемые;

– неиндексируемые.

Сообщения создаются и отправляются с помощью различных программных средств информационного обмена. Как упоминалось ранее, сообщение может представлять собой не только текстовый файл, но и изображение, фотографию, аудио- и видеозапись, иные файлы и вложения. При этом программные средства для создания электронных сообщений обеспечивают формирование текстового содержания, но не позволяют создать графическое. Содержание графического формата образуется с помощью иных программных средств, но может стать частью отсылаемого электронного сообщения.

Таким образом, сообщения могут быть отправлены посредством определенных ресурсов, а создаваться при помощи иных программ. Поэтому необходимо выделить средства создания и средства отправки сообщений. В качестве первых могут выступать текстовые редакторы, фотоаппараты, графические редакторы, иные различные программы для создания видео и изображений. Так, например, обычное текстовое сообщение будет сформировано и отправлено с помощью одного и того же средства, а gif-изображение – создано с помощью одного программного обеспечения и отправлено посредством другого.

Сообщения, будучи средством коммуникации, не всегда отвечают благим целям и могут выступать инструментом совершения противоправных действий. Такие сообщения носят дезинформационный характер и используются для взлома различных систем или же для сбора персональных данных, при этом они маскируются под легальные. В.А. Образцов, Л.В. Бертовский и Н.Л. Бертовская вводят понятие криминальной фикции: «дезинформационная система, реализованная субъектом (субъектами) преступления путем создания и использования под видом подлинного искусственного (вымышленного) либо реального объекта с искусственно измененными признаками для противоправного

психологического воздействия на сознание потерпевшего, сотрудников правоохранительных органов и других лиц в расчете на введение их тем самым в состояние заблуждения, способствующее совершению ими действий, служащих интересам и планам указанного субъекта, либо принятию решения об отказе от совершения действий, невыгодных ему и/или его преступным связям»[51]. По нашему мнению, заведомо ложные сообщения, отправленные в противоправных целях, являются криминальными фикциями. Сообщения-фикции могут быть направлены на получение конфиденциальной информации и данных, таких как личные данные пользователя, паспортные данные, логин и пароль для входа в аккаунт или почтовый ящик. Они могут также отсылаться в целях распространения вредоносных программ, с целью управления системами или сбора конфиденциальных данных о компьютерной системе. Сообщения-фикции также являются распространенным инструментом совершения мошеннических действий, они могут инсценировать ситуацию, в ходе которой будет осуществлен перевод денег пользователем самостоятельно или же могут быть замаскированы под сообщения от банков, содержать ссылки и побудить пользователя ввести свои банковские данные.

Поскольку такие сообщения всегда носят заведомо ложный характер, их следует называть дезинформационными сообщениями (как часть дезинформационной системы).

Примером дезинформационных сообщений служат фишинговые сообщения. «Фишинг (от англ. phishing, от fishing – рыбная ловля, выуживание) – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Это достигается путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт,

[51] См.: *Образцов В.А., Бертовский Л.В., Бертовская Н.Л.* Фикции в криминальной, оперативно-розыскной и следственной практике: монография. – М.: Юрлитинформ, 2012. – С. 86.

внешне неотличимый от настоящего, либо на сайт с редиректом. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приемами побудить его ввести свои логин и пароль, которые он использует для доступа к определенному сайту, что позволит преступникам получить доступ к его аккаунтам и банковским счетам»[52].

Дезинформационные сообщения достаточно распространены. В ходе анализа надзорных производств прокуратуры было выявлено, что 44,76% сообщений выступали как средство совершения преступления, а 55,24% – просто несли в себе информацию, но не являлись непосредственно инструментом противоправного действия[53].

В.А. Образцов и Л.В. Бертовский, Н.Л. Бертовская лассифицируют фикции на основе учета своеобразия их системно-структурных характеристик. «С этой точки зрения криминальные фикции подразделяются на:

1) целостные системы, имманентные составам тех или иных видов преступлений;

2) подсистемы, имманентные отдельным элементам механизма какого-либо вида преступного поведения»[54]. Или, как их еще можно назвать, предкриминальные фикции.

Дезинформационные электронные сообщения следует классифицировать таким же образом. Направление одних сообщений может само по себе уже являться составом преступления, в то время как направление сообщений иного содержания может нести в себе предкриминальный характер и являться подготовкой к совершению противоправного деяния.

На этом основании можно выработать следующую классификацию сообщений:

1. дезинформационные:

---

[52] См.: *Маилян А.В.* Актуальные вопросы расследования и раскрытия кибермошенничества «Фишинг» // Философия права. 2022. № 2 (101). С. 113.

[53] См. Приложение № 3.

[54] См.: *Образцов В.А., Бертовский Л.В., Бертовская Н.Л.* Фикции в криминальной, оперативно-розыскной и следственной практике. С. 142.

1.1. образующие состав преступления (криминальные);

1.2. ложные, но не образующие признаков состава преступления (предкриминальные);

2. недезинформационные (правдивые).

§ 2. Современные электронные средства и программное обеспечение, используемые для обмена электронными сообщениями и их криминалистически значимые характеристики

Подход к исследованию электронных сообщений в значительной степени предопределяется электронными средствами и программным обеспечением, с помощью которых ведется переписка.

Как говорилось ранее, сообщения могут создаваться и отправляться как с помощью одних и тех же средств, так и с помощью сторонних. Например, в случае с отправкой изображения или анимационного изображения в формате gif для создания такого сообщения используется специальное программное обеспечение (графические редакторы).

Электронные сообщения передаются по информационно-телекоммуникационной сети и обрабатываются компьютерным средством. Такими устройствами могут быть серверы, персональные компьютеры и смартфоны. Для передачи сообщений данные устройства должны иметь возможность подключения к сети Интернет и предусматривать установку на них определенного программного обеспечения.

Основными средствами отправки электронных сообщений являются электронная почта, социальные сети и мессенджеры. Согласно результатам анкетирования, проведенного нами в ходе исследования, следователи в процессе расследования в 61,35% случаев сталкиваются с перепиской в мессенджерах, в 31,29% случаев – с электронными сообщениями, отправленными в социальных

сетях, в 7,36% случаев – с письмами на электронной почте[55]. Сообщения также могут отправляться на иных платформах, предназначенных для электронной коммуникации (веб-форумах, иных сайтах с возможностью ведения личной переписки, сайтах государственных и иных структур (где имеется форма для отправки заявлений и обращений).

Согласно результатам анализа надзорных производств прокуратуры по уголовным делам, проведенного в рамках настоящего исследования, было выявлено, что для отправки сообщений чаще всего используются следующие средства электронной коммуникации: мессенджеры Telegram, WhatsApp, социальная сеть «ВКонтакте», мессенджер на сайте «Авито». Реже применяются мессенджер Viber, социальная сеть Facebook, и в единичных случаях – сервисы электронной почты Yandex.ru, Mail.ru[56]. По делам, связанным с расследованием преступлений в сфере экономики, также могут использоваться почтовые программы (корпоративные почтовые клиенты), например Lotus или Outlook.

Несмотря на более редкое (по сравнению с мессенджерами) использование электронной почты, она все еще является важным средством интернет-коммуникации.

Описание электронной почты нашло отражение во Всемирной почтовой конвенции, участницей которой является и Российская Федерация. Согласно Конвенции, электронная почта является почтовой электронной услугой, в которой используется электронная передача назначенными операторами сообщений и информации[57].

Сегодня значение адреса электронной почты встало на один уровень с адресом места жительства или номером мобильного телефона. Появилось множество общедоступных почтовых сервисов, которые обслуживают большое количество пользователей. Именно электронная почта наиболее часто

[55] См. Приложение № 2.
[56] См. Приложение № 3.
[57] См.: Резолюция № С 42/2008 Всемирного почтового союза «Изучение о придании постоянного характера Всемирной почтовой конвенции и Соглашению о почтовых платежных услугах» (принята в г. Женеве 12.08.2008 XXIV Конгрессом Всемирного почтового союза) // СПС «Консультант Плюс».

используется для ведения корпоративной переписки, а значит, исследование отправленных через корпоративный сервис сообщений имеет существенное значение для расследования преступлений, связанных с посягательством на имущество предприятий и порядок управления в них. Однако корпоративная переписка требует самостоятельного исследования, так как обладает значительной спецификой.

Для создания электронного почтового ящика пользователю необходимо пройти процедуру регистрации на сайте почтового оператора, сгенерировать адрес или выбрать его из предложенных. Сам адрес электронной почты не несет в себе доказательственных сведений, хотя в отдельных случаях может иметь ориентирующую информацию, поскольку в самом адресе может содержаться настоящее имя отправителя, прозвище либо дата его рождения, номер телефона и прочие персональные данные.

Современные сервисы, предоставляющие услуги электронной почты, часто владеют информацией о номере телефона пользователя, его имени, фамилии и о времени и месте отправки сообщения. Эта дополнительная информация называется метаданными и может быть не менее важной для расследования, чем само содержание передаваемой информации. При этом следует иметь в виду, что такие сведения предоставляются оператору электронной почты самим абонентом и, в подавляющем большинстве случаев, не подлежат проверке на подлинность, так что установить на их основании конкретное лицо можно далеко не всегда.

Некоторые из операторов электронной почты вводят дополнительные опции для повышения конфиденциальности и безопасности в сети Интернет, поэтому зашифровывают свои данные. Одним из таких является швейцарский сервис ProtonMail. Их сервера и центр управления данными находятся в защищенном месте, в бункере, а сами сообщения подлежат шифрованию, что затрудняет их исследование при изъятии[58]. Также пользователи могут установить режим исчезающих сообщений, и тогда по истечении определенного времени письма

[58] См.: ProtonMail или что же это на самом деле? // URL: https://habr.com/ru/post/227575/ (дата обращения: 29.04.2023).

будут удаляться как у отправителя, так и у получателя. Подобных поставщиков услуг электронной почты немало, помимо ProtonMail, существуют Tutanota, Runbox.

Обслуживание пользователя сервиса электронной почты осуществляется на базе специальных программ, действующих на серверах, именуемых почтовыми агентами. Они делятся на три категории – пользовательский агент, транспортный агент и доставочный агент. Пользовательский агент отвечает за работу пользователей с сообщениями – он позволяет читать и составлять их. Далее с помощью транспортного агента письмо передается с сервера электронной почты одного оператора на сервер электронной почты другого оператора. Транспортный агент отвечает именно за отправку сообщений на сервера и между ними. После этого письмо обрабатывается с помощью доставочного агента – он помещает письмо с сервера в почтовый ящик пользователя (т. е. обеспечивает возможность доступа к полученной информации только для пользователя с определенной учетной записью).

Порядок работы почтовых агентов регулируется протоколами почтовых серверов. Эти протоколы представляют собой установленную последовательность информационных процессов, которые выполняются в зависимости от ситуаций – принять или отклонить письмо, обработать полученное сообщение, информировать отправителя, что письмо доставлено, либо прислать уведомление об ошибке. В настоящее время существуют два основных вида протоколов электронной почты – «POP3» и «IMAP». Протокол «POP3» предполагает, что письма не остаются на сервере электронной почты. Он загружает письма со всем содержимым на устройство абонента, после чего они удаляются с почтового сервера. Для расследования преступлений работа с таким протоколом имеет как плюсы, так и минусы. Удаленные с устройства письма не удастся найти на сервере оператора электронной почты. Однако если письмо не удалено, то на самом устройстве его можно просмотреть в любой момент, даже без доступа к Интернету. Протокол «IMAP», напротив, не удаляет письма с сервера. На устройство абонента

поступает только уведомление с указанием темы сообщения и, возможно, началом содержания. Доступ к письмам можно получить с любого устройства, имеющего выход в сеть Интернет. Этот протокол не загружает сообщения на устройства, для этого требуется нажать определенную команду – скачать письмо. В последнее время операторами электронной почты наиболее часто используется протокол «IMAP», так как он позволяет существенно экономить трафик. При поиске следов электронных писем следует обязательно учитывать, какой протокол используется сервером оператора электронной почты.

Но не все почтовые сервисы требуют выхода в сеть Интернет для их использования. Так, известный почтовый сервис Microsoft Outlook может работать как с помощью сети Интернет, так и с помощью локальной сети определенной компании. При этом принцип составления и доставки информации остается прежним. При передаче сообщений по локальной сети все отправления будут храниться непосредственно на локальных серверах компании (собственных или арендованных), что зачастую может затруднить их изъятие и поиск следов электронных сообщений. Особенность данной программы в том, что, кроме серверов, Outlook также хранит электронные письма на самом устройстве пользователя. Однако при переустановке операционной системы письма удаляются с устройства. Такая специфика характерна для многих почтовых программ, созданных для электронной коммуникации внутри корпораций, например, Lotus, Zimbra Desktop, Pegasus Mail и пр.

Таким образом, отличительной особенностью электронной почты как средства обмена информацией является то, что следы электронных сообщений могут быть обнаружены преимущественно на серверах поставщиков услуг электронной почты или локальных серверах компании, обеспечивающей обмен электронными сообщениями. Следы сообщений на устройстве пользователя могут быть обнаружены при использовании почтового протокола «POP3».

Другим значимым средством ведения электронной переписки являются социальные сети.

В современном мире социальные сети стали неотъемлемой частью жизни людей. В социальных сетях люди общаются как со своими друзьями и родственниками, так и с незнакомыми им людьми, состоят в сообществах по интересам, публикуют новости и фотографии и даже ведут бизнес. Явление социальных сетей глобально распространено, и случай, когда у какого-либо определенного лица нет аккаунта в социальных сетях – редкость.

Криминалистическая важность социальных сетей определяется возможностью получить в них информацию о межличностном общении, а оно, в свою очередь, задолго до появления компьютерных сетей исследовалось социологами. В социологии социальная сеть является некой структурой, в которую входит множество агентов (индивидуальных, коллективных) и отношения, которые их связывают[59].

Если подходить к характеристике социальных сетей с точки зрения информационных технологий[60], социальная сеть – ресурс, предназначенный для обеспечения взаимоотношений между людьми либо организациями в Интернете. В данном случае акцент делается на налаживании дистанционной коммуникации между людьми путем одного из возможных способов – в сети Интернет. Социальная сеть является удобным инструментом для поиска лиц, представляющих интерес для преступников, и связи с ними путем ведения переписки.

Согласно ст. 10.6 ФЗ «Об информации, информационных технологиях и о защите информации» под социальной сетью понимается «сайт и (или) страница сайта в сети “Интернет”, и (или) информационная система, и (или) программа для электронных вычислительных машин, которые предназначены и (или) используются их пользователями для предоставления и (или) распространения информации посредством созданных ими персональных страниц, на которых может распространяться реклама, направленная на привлечение внимания

[59] См.: *Губанов Д.А., Новиков Д.А., Чхартишвили А.Г.* Социальные сети: модели информационного влияния, управления и противоборства. – М.: Физматлит, 2010. – С. 4.
[60] См.: *Браун С.* «Мозаика» и «Всемирная паутина» для доступа к Internet: пер. с англ. – М.: СК Пресс, 2016. – С. 167.

потребителей, находящихся на территории Российской Федерации, и доступ к которым в течение суток составляет более пятисот тысяч пользователей сети “Интернет”»[61].

Для пользования социальной сетью, а именно ведения переписки, вступления в сообщества по интересам и совершения иных действий (публикация статуса, записи, фотографии), пользователь должен пройти процедуру регистрации на сайте социальной сети, т. е. создать аккаунт. Аккаунт – это учетная запись пользователя, с которой связана совокупность определенных возможных действий и предоставляемых ресурсов. Доступ аккаунту предоставляется на основании ввода средств аутентификации. Суть аккаунта в том, что информация, которую разместил в ней пользователь, предназначена для ознакомления с ней либо неограниченного круга лиц, либо круга, определяемого пользователем с помощью инструментов самой социальной сети. Специального согласия для каждого стороннего пользователя, желающего ознакомиться с информацией, не требуется.

Согласно п. 5.3 Правил пользования сайтом «ВКонтакте», «при регистрации на Сайте Пользователь обязан предоставить Администрации Сайта необходимую достоверную и актуальную информацию для формирования персональной страницы Пользователя, включая уникальные для каждого Пользователя логин и пароль доступа к Сайту, а также фамилию и имя. Регистрационная форма Сайта может запрашивать у Пользователя дополнительную информацию»[62].

В социальных сетях существуют следующие значимые источники криминалистической информации:

1) чаты[63];
2) участие пользователей в группах и сообществах;

[61] См. ст. 10.6 Федерального закона «Об информации, информационных технологиях и о защите информации».
[62] См.: Правила пользования сайтом «ВКонтакте» // URL: https://vk.com/terms?ysclid=lnnpsaqiy313123338 (дата обращения: 13.10.2023).
[63] Чат – сервис для общения онлайн, в режиме реального времени, переписка.

3) записи публичного доступа – электронные объявления (статусы[64], записи, публикации, комментарии);
4) иная информация (лайки, реакции и т. д.).

Доступ к аккаунту и возможность обмена информацией в социальной сети осуществляется либо через сайт, либо с помощью приложения – специального программного обеспечения, устанавливаемого на устройство, которое обеспечивает более удобный доступ ко всем ресурсам социальной сети.

У каждого пользователя социальной сети имеется техническая возможность перейти в раздел «Сообщения» со своей страницы и отправить сообщение другому пользователю. В настоящее время почти во всех социальных сетях встроена функция обмена мгновенными сообщениями. Также в них имеется возможность публикации записей, комментариев. Отличие таких публикаций от сообщений в том, что их могут просматривать все пользователи либо те, которым открыт доступ (участники группы, «друзья» пользователя). То есть автор публикации не имеет полной уверенности относительно того, кто именно будет воспринимать размещенную им информацию.

Сообщения в социальной сети формируются отправителем на сайте социальной сети и сразу отправляются на ее сервер. На устройство пользователя приходит уведомление о полученном сообщении, которое самой информации практически не содержит. Это объясняется тем, что пользователи передают сообщения между аккаунтами, принадлежащими к одной социальной сети, которая обычно поддерживается в пределах одного серверного пространства, в то время как по электронной почте возможна отправка сообщений между почтами различных провайдеров, и рабочие серверы у них тоже могут быть разными.

Таким образом, доступ к сообщениям можно получить или непосредственно с сервера сети, или через пользовательское устройство.

[64] Статус – информация, размещаемая пользователями в своей «анкете» в социальной сети, характеризующая самого обладателя аккаунта.

Получение информации о сообщениях непосредственно от операторов социальных сетей, являющихся резидентами РФ, не представляет существенных сложностей. Согласно п. 3 ст. 10 ФЗ «Об информации, информационных технологиях и о защите информации», организаторы распространения информации в сети Интернет обязаны хранить сообщения пользователей до шести месяцев с момента их передачи. Но зачастую они сохраняются намного дольше. У популярных социальных сетей с большим количеством пользователей имеется в распоряжении большое количество серверов – серверных мощностей, которые обеспечивают работу этих сетей, в том числе и хранят огромный массив сообщений. Информация с них может быть изъята на основании запроса от правоохранительных органов.

Доступ к социальной сети с помощью устройства можно осуществлять следующими способами.

Во-первых, доступ к сообщениям можно получить через вход в аккаунт с самого устройства его обладателя. Часто, при посещении сайта социальной сети с того же устройства и браузера, повторная процедура аутентификации (с введением логина и пароля) не требуется.

Если речь идет о мобильном устройстве, то доступ с устройства обладателя можно осуществить через приложение[65]. В настоящее время пользователи чаще осуществляют доступ к социальным сетям не посредством браузера, а через специальное программное обеспечение, разработанное для адаптации социальной сети к смартфонам и компьютерам. Вход в приложение может осуществляться как с запросом на введение пароля, так и без него. Если пароль не требуется, то в приложение можно войти, открыв данную программу. Данные из приложений, включая переписку, хранятся на устройстве, доступ к ним зачастую можно получить даже без выхода в сеть Интернет. При отключении устройства от сети

[65] См.: Печникова Р.Б. Криминалистическая тактика изъятия мобильных устройств для обеспечения сохранности электронной переписки» // Юридическое образование и наука. 2022. № 7. С. 16

Интернет в приложении могут оставаться все данные, которые были загружены ранее, включая сообщения.

У иных устройств информацию можно обнаружить в специальной папке – кэше браузера. Многие браузеры сохраняют некоторые файлы с посещаемых пользователем сайтов в памяти устройства. Сохраняются данные для упрощения работы компьютера, чтобы не загружать информацию с веб-сервера каждый раз, а использовать уже имеющуюся. Таким образом, если пользователь часто посещал страницу с сообщениями в социальной сети через браузер, они могли сохраниться в кэше. Для поиска файлов с сообщениями в кэше потребуется специальное программное обеспечение. Оно находится в общем доступе для всех пользователей. Данный метод, к сожалению, работает, только если пользователь заходил в социальную сеть через браузер, так как возможности восстановления сообщений в кэше приложения нет.

Во-вторых, войти в аккаунт пользователя можно с любого устройства, если у нас имеются логин и пароль пользователя, в том числе с помощью установленных приложений соответствующей сети.

В-третьих, некоторые социальные сети имеют функцию оповещения по электронной почте. Если она была подключена, то входящие сообщения пользователя полностью или частично могут дублироваться электронным письмом на его электронную почту. Чаще всего такие письма выглядят как уведомления с частичным цитированием текста сообщения. Однако содержание сообщения может и полностью отображаться в письме. Так, например, для социальной сети «ВКонтакте» можно выбрать опцию «Показывать текст сообщений» в уведомлении, и тогда полный текст сообщения будет приходить в тексте оповещения на электронную почту. Таким образом, в почтовом ящике пользователя можно попробовать найти следы сообщений из социальных сетей при условии, что это именно тот почтовый ящик, который привязан к аккаунту в социальной сети.

Наиболее распространенными социальными сетями в России являются «ВКонтакте», «Одноклассники», Facebook (принадлежит компании Meta, признанной экстремисткой организацией на территории РФ[66]). После запрета Facebook на территории РФ большинство пользователей также продолжает использовать эту социальную сеть, обходя блокировку с помощью виртуальных частных сетей (VPN). Поэтому российским правоохранительным органам не следует исключать поиск следов электронных сообщений в переписке на Facebook. Также это относится к деяниям, совершение которых относится к периоду до блокировки соответствующих сетей. Переписка может также вестись в социальных сетях для знакомств, для профессиональных сообществ (таких как LinkedIn) или же в сетях, предназначенных для продажи вещей («Авито», «Юла»).

Помимо вышеназванных социальных сетей, существуют также интернет-платформы, основной целью которых является не обмен текстовыми сообщениями, а размещение данных определенного характера – в первую очередь фотографических материалов и видео. Это, например, Instagram (также принадлежащий компании Meta, признанной экстремисткой на территории РФ), который предназначен для размещения фотографий и коротких видеозаписей; TikTok, нацеленный на публикацию коротких видео. На данных платформах также есть возможность ведения текстовой переписки, следы которой можно обнаружить в приложении на устройстве пользователя.

Иногда для ведения переписки используются совсем неожиданные средства. Так, зачастую продажа наркотиков осуществляется в чатах игровых приложений, например, приложения PokerStars. Хотя эти чаты имеют вспомогательный характер, но в силу их использования фактически становятся социальной сетью. Как отмечает В.А. Мещеряков, «в последнее время коммуникационной средой для проведения переговоров об обстоятельствах дачи/получения взяток становятся все более неожиданные компьютерные приложения, например коммуникационные сервисы компьютерных игр, миры виртуальной реальности (типа SeconfLife и т.п.),

[66] См.: Решение Тверского районного суда г. Москвы от 21.03.2022 по делу № 02-2473/2022 // СПС «Гарант».

а ставшие уже традиционными - электронная почта и интернет-мессенджеры отходят на второй план»[67]. Сложность поиска следов сообщений в таких чатах состоит в том, что они предназначены исключительно для обмена информацией во время игры и быстро удаляются как с устройства, так и с серверов компаний, выпускающих такие приложения.

Таким образом, при поиске следов сообщений, отправленных в социальной сети, они могут быть обнаружены на устройстве получателя и отправителя (как в браузере, так и в приложении социальной сети), либо на сервере компании, владеющей социальной сетью. Удаленные из аккаунта сообщения могут быть найдены в папке кэша браузера либо же в письмах с уведомлениями в почтовом ящике электронной почты. Помимо социальных сетей, предназначенных для ведения текстовой переписки, сообщения могут находиться на платформах, предназначенных для публикации фото- и видеоматериалов, игровых приложениях, сайтах знакомств, профессиональных сообществ и т. д.

Третьим инструментом обмена электронными сообщениями, который в настоящее время приобретает наибольшее значение, являются мессенджеры. Мессенджер – программа с системой мгновенного обмена сообщениями, которые позволяют с быстрой скоростью передавать как текстовые сообщения, так и файлы, включая мультимедиа, именно поэтому они так удобны и широко используются по всему миру. «Правила идентификации пользователей информационно-телекоммуникационной сети “Интернет” организатором сервиса обмена мгновенными сообщениями» определяют мессенджер как «организатор сервиса обмена мгновенными сообщениями»[68]. Основные черты мессенджеров – возможность отправки быстрых сообщений, адаптация к мобильным устройствам и связанным с ними программам, удобство обработки мультимедиафайлов, возможность сочетания различных видов электронной коммуникации. Важнейшим

[67] См.: *Мещеряков В.А.* Криминалистические особенности дачи - получения взятки с использованием электронных платежных систем // Воронежские криминалистические чтения. 2007. № 8. С. 208-217

[68] См.: Постановление Правительства РФ от 27.10.2018 № 1279 «Об утверждении Правил идентификации пользователей информационно-телекоммуникационной сети “Интернет” организатором сервиса обмена мгновенными сообщениями» // СПС «КонсультантПлюс».

свойством мессенджеров является наличие сервиса голосовой связи, отсутствующего, например, в электронной почте. Пользователи мессенджеров могут не только обмениваться сообщениями, но и разговаривать в режиме реального времени или коммуницировать при помощи сервиса видеосвязи.

Первым мессенджером был ICQ, появившийся в 1996 г. Далее возникли такие мессенджеры, как Skype и Jabber. Главным их отличием от электронной почты был так называемый статус присутствия, когда пользователи могли общаться в реальном времени и обмен сообщениями максимально приближался к реальному общению.

В 2010 г. появились такие крупные мессенджеры, как WhatsApp и Viber, а в 2011 г. Apple выпустили свой встроенный мессенджер iMessage. В 2013 г. на рынке был представлен новый мессенджер – Telegram, который в настоящее время является очень популярным средством для обмена мгновенными сообщениями.

Простота использования мессенджеров привела к тому, что люди с их помощью обмениваются огромным количеством сообщений, что делает мессенджеры важнейшим инструментом для получения криминалистически значимой информации.

Для работы мессенджера на устройство необходимо установить специальное программное обеспечение – приложение (их также называют клиентскими программами или просто клиентами). Клиентская программа взаимодействует с программой-сервером организатора обмена мгновенными сообщениями. Программа-сервер размещается на аппаратном оборудовании организатора обмена сообщениями. По сути, на этом сервере и происходит мгновенный обмен сообщениями, а клиенты обеспечивают доставку и показ сообщений пользователям на их устройствах.

Электронные сообщения, переданные посредством мессенджера, можно обнаружить:

– на устройстве, с которого осуществлялась переписка;

– в облачном хранилище данных (если мессенджер предусматривает размещение сообщений в таком хранилище);

– на сервере провайдера услуг;

– на устройстве лица, не принимавшего участие в переписке, но состоящего в той же группе (общем чате).

На самом устройстве переписка хранится в приложении-клиенте, но помимо этого она может быть также сохранена в отдельный файл. Так, небезызвестный мессенджер WhatsApp автоматически делает резервную копию всех сообщений, найти которую можно путем подключения смартфона к компьютеру. Однако функцию создания резервной копии данных пользователь может отключить в настройках устройства.

Следует учитывать, что даже получение полного доступа к устройству не всегда гарантирует доступ к электронной переписке. Некоторые мессенджеры предоставляют возможность шифрования и удаления сообщений. Так, в Telegram существует возможность создания секретного чата, сообщения из которого подлежат удалению через установленный период времени.

Использование некоторых мессенджеров, например WhatsApp, предполагает хранение переписки в облачном хранилище данных. Это определенный объем памяти на сервере, который предоставляется в пользование различными интернет-сервисам и пользователям. Современные мобильные устройства – смартфоны, имеют возможность осуществления такого хранения, благодаря чему объем сохраняемых данных уже не ограничивается аппаратными возможностями устройства. Большая часть данных с них попадает в облачное хранилище даже тогда, когда пользователь об этом не подозревает. Однако, как отмечает М.В. Жижина, «проблема получения информации из облачных хранилищ является одной из наиболее острых на сегодняшний день»[69]. Получение данных из облачных хранилищ в большинстве случаев предполагает международное сотрудничество,

[69] См.: *Жижина М.В., Завьялова Д.В.* Расследование преступлений в сфере компьютерной информации в Российской Федерации и зарубежных странах. – М.: Проспект, 2023. – С. 12.

так как сервера, на которых хранятся данные, могут быть расположены в другой стране. Это значительно усложняет и увеличивает сроки расследования. Однако в некоторых случаях, если пользователь удалил сообщения и заблокировал доступ к устройству, можно получить доступ к его облачному хранилищу и восстановить сообщения. Для этого потребуется сим-карта пользователя, специальное криминалистическое оборудование и программное обеспечение.

Большое значение при проведении расследований имеет тот факт, что в мессенджерах возможно создание общих чатов, в которых состоит более двух отправителей и получателей. В таком случае переписку можно обнаружить на устройстве стороннего пользователя, состоящего в общем чате, который не был непосредственным участником расследуемого события.

Помимо устройства и облачных хранилищ данных, электронная переписка, осуществлявшаяся посредством мессенджеров, хранится и на самих серверах организаторов обмена мгновенными сообщениями.

Итак, следы электронных сообщений могут быть обнаружены:

– на устройстве отправителя или получателя:

а) в программном обеспечении, используемом для отправки сообщений;

б) в скрытых файлах – резервных копиях или папке кэша браузера;

– на сервере поставщика услуг электронной почты; владельца социальной сети; организатора обмена мгновенными сообщениями;

– в облачном хранилище данных;

– на стороннем устройстве пользователя – участника общего чата.

Таким образом, понимание природы того инструмента, с помощью которого велась электронная переписка, является предпосылкой для ее успешного обнаружения и изъятия.

Согласно результатам проведенного в рамках исследования анкетирования работников следственного аппарата, чаще всего переписку удается обнаружить на устройстве, с которого она велась (85,07%), более редко она изымается с сервера организатора обмена сообщениями (8,96%) и обнаруживается на устройстве лица,

не принимавшего участие в переписке, но состоящего в той же группе (общем чате) (5,97%).

Глава 2. Криминалистическое исследование электронных сообщений и особенности работы с ними в процессе расследования

§ 1. Установление места нахождения электронных средств, их программного обеспечения и места хранения электронных сообщений

Установление места нахождения электронных средств, программного обеспечения и места хранения электронных сообщений можно разделить на несколько стадий:

– версионный анализ природы носителя искомой информации и его местонахождения;

– поиск носителя информации (непосредственный и удаленный);

– обнаружение электронных сообщений, имеющих отношение к расследуемому событию.

1. Версионный анализ

Собирание криминалистически значимой информации основывается на выдвижении и проверке версий. В криминалистическом и уголовно-процессуальном познании события преступления основным его инструментом соответственно является криминалистическая версия как разновидность частной гипотезы, т. е. гипотезы, примененной к нескольким фактам или отдельному социальному явлению, имевшему место в прошлом[70].

Криминалистическую версию можно определить следующим образом – это «логически построенное и основанное на фактических данных обоснованное предположительное умозаключение следователя (других субъектов познавательной деятельности по уголовному делу) о сути исследуемого деяния, отдельных его обстоятельствах и деталях и их связи между собой, требующее соответствующей проверки и направленное на выяснение истины по делу»[71]. В.Я.

[70] См.: Криминалистика: учебник / Под ред. Н.П. Яблокова. 4-е изд., перераб. и доп. – М.: Юр.Норма, НИЦ ИНФРА, 2019. – С. 120.
[71] Там же. С. 121.

Колдин под версией, в соответствии с принципами системно-деятельностного подхода, понимал элемент версионной подсистемы в составе информационной модели расследуемого события, используемый во взаимодействии с другими элементами и подсистемами данной модели для получения новой информации, формирования доказательственных систем и обоснования криминалистических решений[72]. Это положение он предлагал рассматривать как основу методологии версионного анализа.

Для точной локализации носителя электронных сообщений выдвигаются версии о природе носителя и оценивается возможность проверки версии о носителе.

По своей природе носители делятся на:

а) Компьютерные устройства (включая те, с которых было отправлено сообщение, на которых оно было получено, а также транзитное устройство)

«К числу компьютерных устройств могут быть отнесены любые электронные устройства, способные выполнять функции по приему, обработке, хранению и передаче информации, закодированной в форме электрических сигналов (персональные компьютеры, включая ноутбуки и планшеты, мобильные телефоны, смартфоны, а также иные электронные устройства, в том числе физические объекты, оснащенные встроенными вычислительными устройствами, средствами и технологиями для сбора и передачи информации, взаимодействия друг с другом или внешней средой без участия человека), произведенные или переделанные промышленным либо кустарным способом»[73].

Устройств, на которых может находиться электронная переписка, бывает два или более. Переписка происходит между двумя и более абонентами, таким образом, всегда есть устройство отправителя и устройство получателя, на которых потенциально возможно обнаружить сообщения, имеющие значения для

[72] См.: *Колдин В.Я.* Вещественные доказательства... С. 52.
[73] См. пункт 2 Постановления Пленума ВС РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть “Интернет”» // СПС «Консультант Плюс».

расследования. Однако участников переписки может быть более двух. Это справедливо как для сервисов электронной почты, когда в адресной строке указывается несколько адресатов, так и для мессенджеров, особенно при использовании так называемых групповых чатов, в которых состоит несколько участников и где сообщение одного участника делается доступным всем остальным.

При обмене электронными сообщениями информация создается на электронном устройстве одного абонента, после чего направляется на сервер оператора информационного обмена (мессенджера, электронной почты и пр.), который, в свою очередь, направляет ее получателю. Такой сервер является промежуточным (транзитным) устройством. На нем могут оставаться как информация об отправленном сообщении – логи, так и само содержание сообщения. Однако продолжительность их сохранения может сильно отличаться. Так, сообщения, отправленные в социальной сети «ВКонтакте», хранятся на сервере в течение 6 месяцев, а информация о них – до одного года[74]. Письма, отправленные по электронной почте, реже сохраняются на серверах, а вот информация об их отправке хранится значительно дольше.

б) Носители электронной информации, предназначенные для использования в составе компьютерного устройства

Информация может храниться не только на самих устройствах, но и на их элементах или отдельных носителях, которые могут быть отделены от основного предмета и не использоваться для работы, однако способность сохранять зафиксированную на них информацию у них остается. Современные компьютеры состоят из следующих элементов: устройства ввода, устройства вывода, процессор, внутренняя и внешняя память[75]. Носители информации являются материальными объектами, используемыми для записи и хранения компьютерной информации.

[74] См. ст. 15 Федерального закона от 06.07.2016 № 374-ФЗ (ред. от 29.12.2022) «О внесении изменений в Федеральный закон “О противодействии терроризму” и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности // СПС «Гарант».
[75] См.: *Сотов А.И.* Компьютерная информация под защитой. – С. 21–22.

Использование носителей позволяет экономить размеры устройств, хранить больше данных, не увеличивая величину устройства. Кроме того, это дает возможность пользователям работать с одними и теми же данными на разных устройствах. Но, одновременно, это открывает опции и для поиска и анализа данных, помимо поиска на самих устройствах. Мессенджер WhatsApp, к примеру, хранит резервные копии переписок на самом устройстве, а при отсутствии памяти они сохраняются на внешнем носителе – SD-карте. Эти карты могут храниться отдельно от устройства, с которого велась переписка, и при необходимости использоваться в стационарной компьютерной технике.

в) Электронные каналы связи

«Такие сведения могут находиться в запоминающем устройстве электронно-вычислительных машин и в других компьютерных устройствах (далее - компьютерные устройства) либо на любых внешних электронных носителях (дисках, в том числе жестких дисках - накопителях, флеш-картах и т.п.) в форме, доступной восприятию компьютерного устройства, и (или) передаваться по каналам электрической связи»[76]. Однако, электронные сообщения в каналах электрической связи находятся только в период их передачи. В данном случае в отношении них речь может идти скорее не о копировании информации с каналов связи, а о перехвате, поэтому в рамках данной работы этот вопрос не рассматривается.

г) Предметы, не являющиеся электронными устройствами

В ходе выдвижения версий допустимо предположить, что искомое сообщение вообще может существовать не в виде компьютерной информации, а в виде иного документа, на котором зафиксировано его содержание. Это может быть фотография, скриншот (снимок экрана), распечатанная на бумаге копия переписки. Например, экран смартфона или компьютера был снят с помощью фотоаппарата,

[76] См.: См. пункт 2 Постановления Пленума ВС РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть “Интернет”» // СПС «Консультант Плюс».

после чего фотография была напечатана и предоставлена следователю. Однако такая фиксация следов не является общераспространенной и обуславливается специфическими обстоятельствами, в которых действует лицо, а также его личностными характеристиками.

Выдвигая версию о том, на каких носителях может содержаться информация об электронной переписке, следователю стоит не только делать предположения о природе носителя, но и оценивать возможности проверить ту или иную версию. Так, выдвигая версию о том, что сообщения могли сохраниться на телефоне получателя или отправителя, следователь должен параллельно оценивать возможность поиска данных устройств и получения к ним доступа. Выдвигая версию о хранении сообщений на транзитном устройстве, например сервере, следователь должен оценивать возможность изъятия информации с сервера с учетом, к примеру, его местоположения (Российская Федерация или другая страна). Версия, проверить которую не представляется возможным, не позволяет получить новую информацию и, соответственно, изменить следственную ситуацию. Поэтому при составлении плана расследования их целесообразнее не учитывать.

2. Поиск носителя информации

Важнейшей характеристикой предварительного расследования преступлений является его поисково-познавательная природа. По мнению В. А. Образцова, «объектом криминалистического изучения является поисково-познавательная деятельность в уголовном процессе»[77]. Поисково-познавательная деятельность следователя, как пишут В.Д. Корма и В.А.Образцов, направлена на «мысленное реконструирование (воссоздание) юридически значимых обстоятельств и участников подготавливаемого, совершаемого или совершенного деяния с признаками преступления путем обнаружения, фиксации и исследования материальных носителей уголовно-релевантной информации, получения, анализа, проверки, оценки данной информации, преобразования ее в доказательства и

[77] См.: *Образцов В. А.* Криминалистика. Цикл лекций по новой программе курса. – М.: Юрикон, 1994. – С. 9.

использования их в целях установления истины и принятия законных, обоснованных, справедливых правовых и организационно-тактических решений в стадиях возбуждения уголовного дела и предварительного расследования»[78]. На основании выдвинутой версии о том предмете, на котором могут храниться сообщения, возможно начать его поиск.

Как уже говорилось ранее, искомое устройство может представлять собой персональный компьютер, смартфон, отдельный электронный носитель без средств ввода и вывода или же крупный сервер, состоящий из множества объектов аппаратного оборудования[79]. Начать поиск можно несколькими способами: непосредственно либо удаленно.

1. Непосредственный поиск устройства

Устройство, с которого осуществлялась переписка (или на котором она может находиться), может быть изъято в ходе осмотра места происшествия, выемки, обыска, личного обыска или осмотра трупа.

Как правило, мобильные устройства, с которых ведется переписка, участники расследуемого события имеют при себе или в местах непосредственной досягаемости. Поэтому в случае задержания подозреваемого следует незамедлительно произвести личный обыск, а также произвести обыски в местах его жизнедеятельности (учеба, работа, место жительства). Также нельзя упускать тот факт, что лицо может предпринимать попытки к уничтожению как самого устройства, так и информации, хранящейся на нем.

В ходе проведения обыска следует обращать внимание на поведение подозреваемого. Он может попытаться предупредить других соучастников либо удалить или закрыть программы на мобильном устройстве. Следовательно, рекомендуется незамедлительно изъять устройство у подозреваемого. Очень

---

[78] См.: *Корма В.Д., Образцов В.А.* К вопросу о структуре и особенностях криминалистической теории следственного познания // Сборник научных статей по материалам Всероссийской научно-практической конференции (с международным участием) «Современные проблемы отечественной криминалистики и перспективы ее развития». – Краснодар: Кубан. гос. аграр. ун-т им. И.Т. Трубилина, 2019. – С. 65.

[79] Электронная вычислительная машина – совокупность технических и программных средств для обработки информации.

важно, получив в свое распоряжение устройство, избежать блокировки экрана. В том случае, если на него установлен пароль, такая блокировка может исключить проведение исследований, особенно если речь идет о технике, выпускаемой корпорацией Apple. Необходимо немедленно потребовать у владельца устройства сообщить пароль.

Обыск следует производить с применением специальных технических средств, которые помогают обнаружить мобильные устройства. Такими устройствами являются нелинейные локаторы[80]. Они обладают уникальной способностью обнаруживать любые радиоэлектронные устройства практически в любом месте, будь то строительные конструкции, предметы интерьера и т. д. Нелинейные локаторы позволяют обнаружить устройство, находящееся как во включенном (активном) состоянии, так и в выключенном.

В наши дни существует большое количество различных моделей нелинейных локаторов – отечественных и иностранных. Они различаются в зависимости от процесса излучения, мощности и частоты этого излучения.

Работа нелинейного локатора основывается на физическом свойстве всех нелинейных компонентов радиоэлектронных устройств излучать в эфир при их облучении сверхвысокочастотными сигналами гармонические составляющие, кратные частоте облучения. При облучении подозреваемой области, гармонические частоты анализируются на наличие сигнала. При этом процесс преобразования не зависит от того, включен или выключен исследуемый объект, также несущественно функциональное назначение радиоэлектронного устройства. Благодаря этому возможно обнаружить устройство даже через стену.

На данный момент используются нелинейные локаторы, такие как «Лорнет-24», «Лорнет-36» «NR-900S», «Люкс», «ORION HGO-4000»[81]. Кроме того, возможно применение приборов по обнаружению мобильных средств связи, как

[80] См.: *Ищенко Е.П., Костюченко О.Г.* Современные технико-криминалистические средства, применяемые для обнаружения доказательств на электронных носителях информации // Вестник Восточно-Сибирского института МВД России. 2021. № 2. С. 185.
[81] См.: *Ищенко Е.П., Костюченко О.Г.* Указ. соч. С. 185.

находящихся в режиме регистрации, так и работающих в режиме приема-передачи голосового и текстового сообщений, например прибор BVS WH и др.[82]

В связи с тем, что со стороны подозреваемых возможно осуществление удаленного доступа к устройству, необходимо сразу же при обнаружении устройства помещать его в специальный чехол – «чехол Фарадея», который блокирует доступ к нему через любые каналы беспроводной связи[83]. Его перевод в специальный режим (например, режим полета), который отключает получение и передачу данных, нежелателен, поскольку может нарушить функционирование запущенных на устройстве программ. При этом, если пароль для разблокирования мобильного устройства с сенсорным экраном получить не удалось, то даже при его помещении в «чехол Фарадея» необходимо принимать меры, чтобы поддерживать экран в активном состоянии и не допустить его блокировки.

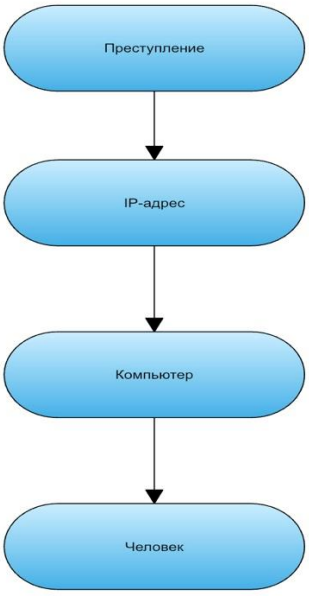
2. Удаленное обнаружение местоположения устройства

Удаленный поиск устройства осуществляется по уникальному идентифицирующему адресу устройства в сети – IP-адресу[84]. IP-адрес является уникальным идентификатором компьютера или иного устройства в сети Интернет. Получить его следователь может, направив запрос провайдеру. Также IP-адрес можно найти в метаданных сообщения, которое уже имеется в распоряжении следствия, либо получить с помощью ссылки с ложным адресом – так называемой IP-ловушки.

Н.Н. Федотов пишет[85], что цепочка доказательств, связанная с IP-адресом, выглядит следующим образом:

---

[82] См.: *Багмет А.М., Скобелин С.Ю.* Особенности применения криминалистической техники для извлечения и анализа данных мобильных устройств // Сборник материалов Международной научно-практической конференции «Совершенствование деятельности правоохранительных органов по борьбе с преступностью в современных условиях» (1–2 ноября 2013 г.). Вып. 10. – Тюмень: ТГАМЭУП, 2013. – С. 13–17.
[83] См.: *Ищенко Е.П., Костюченко О.Г.* Указ. соч. С. 184.
[84] См.: *Сидорова К.С.* Способы установления IP-адреса и сведений о нем при расследовании уголовных дел // Вестник Сибирского института бизнеса и информационных технологий. 2018. № 2. С. 88.
[85] См.: *Федотов Н.Н.* Форензика – компьютерная криминалистика. – М.: Юридический Мир, 2007. – С. 158.



Суть поиска заключается в том, что с помощью технических средств фиксируется IP-адрес, с которого осуществлялась преступная деятельность, после чего устанавливается компьютер, использованный для достижения противоправных целей. Далее уже устанавливается конкретное лицо – человек, который осуществлял деятельность с определенного компьютера.

На стадии поиска устройства значение имеет этап цепочки «IP-адрес – компьютер».

Поскольку IP-адрес является уникальным идентификатором устройства в сети, обычно в конкретный момент времени только одному устройству может быть присвоен конкретный адрес. Уникальный IP-адрес в сети присваивается устройству провайдером, обеспечивающим подключение к Интернету.

IP-адреса могут быть динамическими и статическими. Статический адрес присваивается пользователю на постоянной основе, а динамический – только на отдельный сеанс доступа в электронную компьютерную сеть. В большинстве случаев IP-адреса динамические, поэтому при установлении принадлежности адреса конкретному устройству важно как можно более точно определить время сеанса, который проводился под конкретным IP-адресом, учитывая также часовой пояс, в котором осуществляется фиксация.

Установив провайдера, через которого осуществлялся сеанс связи, необходимо направить ему официальный запрос относительно того, какому абоненту в указанный период времени был предоставлен конкретный IP-адрес не обеспечивается провайдером). Получив сведения об абоненте, уже становится возможным определить его местонахождение, например, домашний адрес, по которому и может располагаться разыскиваемое устройство. Но не стоит забывать, что IP-адрес, особенно для частных абонентов в многоквартирных домах, предоставляется Wi-Fi-роутеру, через который могут выходить в сеть через свои устройства все жильцы квартиры или даже соседи. Следовательно, существует вероятность, что разыскиваемый пользователь определенного IP-адреса даже не проживает в квартире, где размещен Wi-Fi-роутер. В этом случае придется исследовать записи (логи) подключений самого роутера и устанавливать точные данные того устройства, которое подключалось к нему в интересующий следствие момент времени.

Однако описанный выше способ не всегда может сразу привести к нужному результату, если доступ в сеть Интернет осуществлялся пользователем через подключение к локальной сети. В этой ситуации конкретный пользователь осуществляет сеанс работы через частный IP-адрес, в то время как провайдер может установить только публичный IP-адрес. Публичный адрес – глобальный, который используется для выхода в общедоступную сеть Интернет всеми абонентами локальной сети. Частные же адреса не идентифицируются в сети Интернет. В данном случае необходимо осмотреть мосты локальных сетей – сетевые устройства, используемые для подключения нескольких локальных сетей.

Также IP-адреса могут относиться к категориям multicast и broadcast, т. е. групповые и широковещательные. Эти адреса присваиваются в тех случаях, когда информация от одного источника передается не одному конкретному получателю, а сразу определенной (или неопределенной) совокупности таких получателей. В обычном случае (так называемый юникастовый трафик) получатель информационного пакета один, и именно его адрес указывается в заголовке IP-

адреса. При проходе через промежуточный узел, благодаря таблице маршрутизации, неопределенности с получателем не возникает. Но если необходимо сразу передать информацию многим абонентам, то многократное дублирование пакетов по числу получателей с перебором адресного кода для отправителя будет означать существенный рост трафика, нагрузку на передающую сеть, повышение платы от провайдера и пр. Поэтому была разработана категория IP-адреса, одновременно обозначающая целую группу получателей, чтобы доставить данные одним пакетом, без многократного дублирования. В данных случаях отправка данных осуществляется по диапазону адресов, и вычислить принявшее сообщение устройство не представляется возможным. Все устройства, которые подпадают под такой IP-адрес, становятся членами мультикастовой группы. Членство в ней динамическое: каждый абонент в любой момент может включить свое устройство в информационный поток или выключиться из него. Соответственно, идентифицировать устройство, которому предназначался определенный пакет информации, весьма сложно.

Помимо этого, особенно актуально в наши дни использование специального программного обеспечения, которое предоставляет доступ в Интернет через виртуальную частную сеть (VPN), из-за чего идентифицированный во время следствия доступ к ресурсу осуществляется с промежуточного IP-адреса, никак не связанного со злоумышленником. В таких случаях можно попробовать установить устройство (по MAC-адресу получится установить роутер, но не само устройство, через которое осуществлялся вход в сеть Интернет) по физическому идентификатору – MAC-адресу.

MAC-адрес – это уникальный идентификатор, присваиваемый каждой активной единице оборудования. Он представляет из себя шесть пар букв/цифр (шестибайтный номер), где зашифрована информация о производителе (первые три старших байта) и модели сетевого устройства. MAC-адрес также называют физическим адресом, так как он прописан в самом устройстве, а не присваивается виртуально, как IP-адрес. Код MAC-адреса содержится в сетевой карте, благодаря

которой устройство получает возможность выхода в сеть Интернет, и вносится он уже производителем.

При подключении к транслятору сетевого трафика, например к Wi-Fi-роутеру, устройство сообщает ему свой MAC-адрес. Этот MAC-адрес фиксируется в системном журнале (журнал с записями логов) роутера. Благодаря этому подключаемые устройства могут быть точно идентифицированы, а также установлены их локации и время сеансов.

В таком случае следует проверить, устройство с каким MAC-адресом было подключено к роутеру в тот период, когда через роутер осуществлялся искомый сеанс. Проверить это можно с помощью особого файла – так называемого системного журнала, который хранит информацию о действиях программного обеспечения или пользователей, подключенных к сети.

После того, как удастся установить MAC-адрес мобильного устройства, если выход в Интернет осуществляется не по сети Wi-Fi, а через оператора сотовой связи, его можно будет отслеживать в пространстве с помощью сотовых вышек. MAC-адрес не изменяется даже после замены сим-карты в устройстве. С помощью данных от оператора связи собирается следующая информация: код страны, код оператора сети, код соты и идентификатор вышки, с которой поддерживает связь искомое устройство, после чего эти данные преобразовываются в координаты.

Погрешность в таком поиске составляет примерно 150–300 метров в черте города и не более 3 километров за городом[86]. Зная данные о местонахождении устройства, с помощью которого предположительно осуществлялись неправомерные действия, уже можно планировать следственные и оперативно-розыскные мероприятия, с помощью которых можно получить устройство в распоряжение правоохранительных органов.

Что же касается установления местонахождения иных устройств, например переносных персональных компьютеров – ноутбуков, это также возможно, если

[86] См.: *Бозов А.А.* Методические рекомендации: Использование возможностей сотовой связи при раскрытии и расследовании преступлений // URL: https://alexboz.pravorub.ru/personal/30734.html?ysclid=lskn84o691724196356 (дата обращения: 10.10.2023).

устройство подключалось к Wi-Fi-роутеру. Роутер сохраняет данные о подключавшихся к нему устройствах и их адресах, а также о локации подключаемого устройства. При отсутствии подключения к конкретному роутеру, но при включенном на устройстве Wi-Fi-модуле, возможно установить местонахождение устройства с помощью Wi-Fi-радара, но только если оно находится относительно недалеко от радара, в пределах досягаемости его датчиков. По сути, включенный Wi-Fi-модуль на устройстве автоматически раскрывает его MAC-адрес.

Установить местонахождение стационарного компьютера можно с помощью провайдера, через которого он подключается к сети Интернет. У провайдера есть полная информация о клиенте, включая физический адрес, а записи выхода в Интернет хранятся на его сервере.

3. Поиск сообщений на носителе

Когда удалось получить устройство в распоряжение следователя, можно приступать к поиску самих сообщений на нем.

Как говорилось ранее, сообщения могут храниться на внешнем носителе (диск, карта памяти) и на самом устройстве (отправителя, получателя, транзитном). В зависимости от этого поиск имеет свои особенности.

Найти сообщения, хранящиеся на дисках или картах памяти, в большинстве случаев, осуществимо самим следователем, если не возникнет трудностей с получением доступа. В противном случае (например, если контактные устройства носителя повреждены) информация может быть снята с носителя в ходе экспертного исследования (этому посвящен второй параграф третьей главы). Если же доступ к носителю имеется, то следователь может осуществить поиск, подключив его к своему персональному компьютеру. Поиск следует проводить путем просмотра, по всему носителю, а файлы, в которых хранятся сообщения, будут иметь расширение EML, EMLX – в случае с почтой, TXT – в случае с мессенджером или социальными сетями, OGG – если это аудиосообщение.

Необходимо отметить, что следователь может использовать только те программы для просмотра информации, которые не меняют содержание компьютерной информации и метаданные, иначе, полнота и достоверность может быть утрачена. Желательно, также, копировать информацию (если это позволяют технические возможности устройства следователя), прежде чем изучать ее.

Поиск электронных сообщений на устройстве обладает характерными особенностями в зависимости от того, с помощью какого сервиса они были отправлены. Наиболее популярными сервисами для отправки сообщений являются электронная почта, социальные сети и мессенджеры.

1. Электронная почта

Пересылка писем по электронной почте может быть осуществлена путем отправки непосредственно с сайта оператора электронной почты либо с использованием специального программного обеспечения – клиента электронной почты.

Сообщения, отправленные посредством программ-клиентов, могут храниться:

– на самом устройстве, на котором было составлено сообщение;

– на другом устройстве пользователя, на котором стоит клиент той же почтовой программы с тем же почтовым аккаунтом. В приложении почтового клиента может быть настроено локальное сохранение, благодаря чему переписку осуществляемую, например, с компьютера, можно обнаружить на телефоне, где установлен тот же клиент;

– на устройстве получателя сообщения;

– на оборудовании (серверах) администрации почтового сервиса.

Когда сообщение проходит свой путь, оно в первую очередь попадает на промежуточные сервера, а затем уже – в электронный почтовый ящик получателя. На промежуточных серверах не всегда сохраняется копия самого сообщения, но как правило имеется отметка в виде записи (лога) сервера о том, что письмо прошло через этот сервер.

Удаленные сообщения, отправленные с помощью клиента, также могут сохраняться на самом устройстве. Например, сообщения, отправленные с помощью клиента Microsoft Outlook, сохраняются не только в почтовом ящике, но и в файловом архиве Microsoft PST. Этот архив расположен на жестком диске устройства и хранится в папке с системными файлами Outlook.

Файлы с письмами из клиента электронной почты, установленного на персональном компьютере, сохраняются на жестком диске этого устройства в формате EML, реже в формате TXT. Существует специальное программное обеспечение – программа The Bat!, с помощью которой возможно открыть и прочитать файлы такого формата. Хранятся они, как правило, на жестком диске устройства, с которого осуществлялась отправка сообщений, в папке, одноименной с названием клиента или самого сервиса электронной почты, посредством которого было отправлено сообщение.

Письма, отправленные с помощью программы-клиента, можно найти в самой программе. При наличии облачного хранилища и при создании резервной копии они также могут сохраниться внутри резервной копии. Открыть и прочитать их будет возможно при загрузке резервной копии в устройство. Причем загрузить ее можно не только в то же самое устройство, с которого велась переписка, но и в другой подобный смартфон с такой же операционной системой. Для этого необходимо получить доступ к облачному хранилищу пользователя и выбрать загрузку резервной копии. Также просмотреть резервную копию можно при помощи специального криминалистического технического и программного обеспечения, например Cellebrite UFED.

Доступ к письмам, хранящимся в самом приложении клиента на смартфоне, возможен, когда приложение действует в режиме авторизованного пользователя. Если же не была осуществлена авторизация, необходимо попробовать восстановить доступ к аккаунту почтового сервиса. В данном случае при входе в аккаунт следует перейти к форме восстановления пароля. Чаще всего для входа в аккаунт необходима двухфакторная аутентификация, и сервис предлагает

восстановление пароля по номеру телефона. В этом случае требуется доступ к телефону, к которому привязан почтовый ящик, либо же можно использовать аппарат с дубликатом сим-карты. Сервис автоматически вышлет на номер телефона код доступа, который необходимо ввести в форму и восстановить доступ к ящику. Восстановление доступа может также осуществляться через резервную почту, приложение клиента на другом устройстве.

2. Социальные сети

Сообщения, отправленные в социальных сетях, также могут быть отправлены посредством браузера либо приложения социальной сети.

Сообщения, отправленные с помощью браузера, можно обнаружить, войдя в аккаунт пользователя, если они не были удалены. Также эти сообщения не проходят через промежуточные сервера и могут храниться только на самих серверах социальной сети, откуда их можно получить путем направления официального запроса администратору сайта.

Впрочем, получить доступ к этим сообщениям можно и без привлечения оператора социальной сети.

Современные компьютерные устройства построены так, что все исполняемые в текущий момент времени программы, в том числе для обмена сообщениями, загружаются в оперативное запоминающее устройство (далее – ОЗУ), которое способно поддерживать данные только до тех пор, пока устройство включено. На включенном устройстве исполняемые программы и их данные находятся в оперативной памяти. На неработающем устройстве данные, связанные с сетевыми сеансами, могут иметься в файлах гибернации. Файл гибернации представляет собой автоматически создаваемую копию того информационного массива, который находился в обработке перед выключением устройства.

Для того, чтобы авторизоваться в социальной сети, пользователю требуется зайти на сайт с помощью браузера. От сервера, на котором размещен сайт, устройство получает набор кода, который браузер и преобразовывает в визуальный образ. С данным образом пользователь может взаимодействовать. Пока

пользователь продолжает сеанс, происходит загрузка получаемых данных в оперативное запоминающее устройство (ОЗУ) и их обработка процессором. После прерывания сеанса или выключения устройства и обесточивания ОЗУ находящиеся в нем данные теряются, поскольку оперативная память является энергозависимой. Однако современные операционные системы для удобства пользователя, прежде чем информация удалится из ОЗУ, обеспечивают ее копирование и запись на специально выделенный участок в постоянное запоминающее устройство (ПЗУ). Оно уже способно хранить данные даже в обесточенном состоянии. Как правило, это происходит при отправлении компьютера в спящий режим или режим гибернации. Во время спящего режима вся информация из оперативной памяти переносится на жесткий диск в специальный файл гибернации и может быть впоследствии оттуда извлечена. При выходе из спящего режима данные файла гибернации снова выгружаются в оперативную память, что позволяет пользователю быстрее возобновить работу, неоконченную в ходе предыдущего сеанса. Таким образом, если перевести компьютер в спящий режим с открытыми в браузере социальными сетями, вся переписка и содержание страницы сохранятся на жесткий диск. Учитывая большое количество времени, которое пользователи проводят в социальных сетях, и особенности современных устройств, люди, как правило, не выключают компьютеры и постоянно переводят их в спящий режим. Это позволяет сделать вывод о том, что при установлении места хранения данных из социальных сетей в первую очередь следует проверять именно файл гибернации.

Существуют также файлы в текстовом формате, которые фиксируют информацию из браузера о посещенных сайтах (файлы cookies). Они хранятся на устройстве и, как правило, их достаточно несложно найти и просмотреть. Располагаются они в системных папках, относящихся к браузеру, через который осуществлялся выход в Интернет. Например, если выход в сеть осуществлялся с операционной системы Windows, через браузер Google Chrome, то искать cookies надо по следующему пути: C: \Users \Имя_пользователя \AppData \Local \Google \Chrome \User Data \Default. Сами файлы как правило и называются Cookies.

Хранятся они в текстовом формате или в расширении FILE, которое открывается либо через веб-страницу, либо через текстовый редактор. Прочитать и расшифровать такие файлы не всегда возможно обычному пользователю, в том числе следователю, поэтому тут может потребоваться назначение компьютерно-технической экспертизы. В результате следователь получит информацию о посещенных сайтах, о времени входа и выхода, о вводимых на сайте данных.

Если сообщение в социальной сети было отправлено с помощью приложения, то оно может храниться на мобильном устройстве. Для его обнаружения стоит исследовать как сами программы-приложения, так и файлы, сохраненные на устройстве. Сделать это может как сам следователь путем открытия и просмотра содержимого имеющихся на смартфоне программ, так и эксперт в ходе компьютерно-технической экспертизы, если доступ к программам, например, заблокирован.

3. Мессенджеры

Поиск переписки в мессенджере лучше всего вести через программу-приложение, доступную на полученном устройстве. Необходимо начинать поиск с просмотра истории сообщений. Для этого следует открыть нужный чат и просмотреть переписку в нем либо воспользоваться поиском по тексту переписки.

Сообщения, отправленные в чате, могут быть удалены или архивированы. Просмотреть архивированную переписку возможно, зайдя в архив чатов.

Следует учитывать, что устройство не является единственным местом, где переписку можно обнаружить. Многие современные мессенджеры, такие как WhatsApp, Telegram, хранят переписку как локально на компьютере или смартфоне, так и в облачном хранилище.

Переписка из мессенджеров может также оставаться на серверах организаторов обмена мгновенными сообщениями. Получить эту переписку можно посредством выемки серверов, однако в большинстве случаев такие организаторы и их сервера располагаются за пределами Российской Федерации. В таком случае попробовать получить данные с серверов можно путем направления международного запроса.

В последнее время популярными в России становятся азиатские мессенджеры, например WeChat. Программная архитектура этого мессенджера такова, что все данные шифруются и отправляются на серверы, расположенные в Китае, а затем конечному пользователю. Такой промежуточный перехват или сбор данных не является обычным в других коммуникационных приложениях, таких как Facebook Messenger, WhatsApp или iMessage, которые отправляют зашифрованные данные непосредственно между пользователями.

Также особенности исследования сообщений из мессенджера WeChat заключаются еще и в сложностях с наличием у судебных экспертов программного обеспечения для проведения такой судебной экспертизы. Эксперты из компании Belkasoft отмечают[87], что существуют трудности при просмотре сообщений из WeChat в последовательности, так как стикеры, видео и изображения отображаются на одном ряду с сообщениями. В данном случае поиск относимых сообщений зависит от осведомленности эксперта. Если эксперт не имеет четкого представления о контексте общения и контексте, в рамках которого был осуществлен обмен стикерами, изображениями и видеозаписями, при представлении их клиенту или суду может быть допущена ошибка, если не будет проявлена большая осторожность[88].

Данная проблема, на наш взгляд, может быть решена с помощью индексации и составления следователем подробного списка ключевых слов, о котором будет сказано в следующем параграфе.

§ 2. Поисково-познавательная деятельность при анализе электронных сообщений, относимых к расследованию, и их индексация

[87] См.: WeChat. The Forensic Aspects Of and Uses for Evidence from a Super-App // URL: https://belkasoft.com/WeChat-forensics (дата обращения: 14.10.2023).
[88] См.: WeChat. The Forensic Aspects Of and Uses for Evidence from a Super-App // URL: https://belkasoft.com/WeChat-forensics (дата обращения: 14.10.2023).

В случае с исследованием электронных сообщений поисково-познавательный процесс заключается в изучении содержания сообщений и выявлении данных, относящихся к расследуемому событию и позволяющих установить те или иные обстоятельства.

В связи с ростом объема информации, который хранится в электронных устройствах, из них может быть извлечено большое количество данных, не все из которых являются относимыми к расследуемому событию, поэтому прежде чем включать их в материалы дела, необходимо произвести предварительный отбор. Для такого отбора применяются следующие методы: 1) отсечение по временным меткам; 2) выделение по адресатам; 3) индексация.

Согласно результатам анкетирования[89], в 35,47% случаев следователи выявляют сообщения, относящиеся к расследуемому событию, путем простого просмотра переписки, пока не найдут интересующую их информацию о расследуемом событии; 16,75% – используют поиск по дате, 30,54% – поиск по ключевым словам, а 17,24% – назначают для этого экспертизу или привлекают специалиста.

Временная метка – это последовательность символов или закодированной информации, показывающая, когда было осуществлено определенное действие. Обычно они содержат дату и время (иногда с точностью до долей секунд). Такая метка, как правило, содержится в сообщении или файле. Например, в устройствах с операционной системой IOS такие метки хранятся в формате MAC Absolute Time и представляют собой количество секунд, прошедших с 00:00:00 1 января 2001 года. Эти метки, например, очень часто встречаются в базах данных различных программ-приложений, включая мессенджеры. Располагая ориентирующей информацией о том, когда было совершено преступление, либо примерным временем, когда могли быть отправлены искомые сообщения, следователь может найти необходимый объем сообщений, с наибольшей степенью вероятности относящихся к расследуемому событию.

[89] См. Приложение № 2.

Выделение по адресатам применяется в случаях, если в ходе расследования было выяснено, между какими лицами велась переписка, что позволяет выделить для исследования только несколько диалогов с конкретными абонентами. При реализации такого отграничения следует учитывать то, что пользователи в сети могут называться не своими именами, а также фальсифицировать переписку путем присвоения своему аккаунту чужого имени пользователя. В данном случае необходимо проверять номера телефона, на которые зарегистрированы аккаунты, и устанавливать лиц иными способами, описанными в параграфах выше.

При наличии большого массива сообщений решить задачу можно с помощью их индексации. При этом основой для индексированного поиска должны быть факты о расследуемом событии.

Сплошной просмотр сообщений займет много времени и может привести к срыву процессуальных сроков. Поэтому для решения этой задачи были разработаны специальные программные инструменты. На данный момент нет более эффективного средства для поиска относимых сообщений, чем индексация – поиск по ключевым словам[90]. Ключевое слово – это такое слово, которое содержится в искомом сообщении или характеризует его, благодаря чему сообщение может быть выделено и помечено как имеющее значимость для следствия.

Необходимо отметить, что индексация или индексированный поиск – термин, используемый в профессиональной среде специалистов по расследованию компьютерных инцидентов и по информационной безопасности, который подразумевает под собой поиск по совпадающим ключевым словам в массиве данных. Использование данного термина обусловлено переводом с английского языка руководств пользования[91] программным обеспечением для осуществления такого поиска.

---

[90] См. Печникова Р.Б. Indexing of electronic messages during the investigation of crimes // Евразийская адвокатура. 2023. № 3 (62). С. 101.

[91] См.: ZyLAB General Search Language Guide // ZYLAB. 2016. // URL: https://docs.zylab.com/articles/#!zylab-one-search-language-guide-publication/10824 (дата обращения: 20.05.2023).

В ходе анкетирования работников следственного аппарата, в том числе следователей-криминалистов, было выявлено, что при поиске относимых к расследуемому событию сообщений большинство следователей (35,47%)[92] ищет сообщения путем просмотра переписки, пока не найдет интересующие. Это показывает, что многие работники следствия не знакомы с понятием индексации либо знакомы, но никогда не применяли ее на практике. Также довольно небольшое количество опрошенных знакомо с каким-либо программным обеспечением, облегчающим поиск по сообщениям. Данное обстоятельство показывает, что уровень владения приемами индексации среди следственных работников достаточно низок, и одной из наиболее актуальных задач является разработка эффективной методики их применения.

Первая стадия индексированного поиска начинается с определения круга лиц, электронных почтовых адресов, переписки с которыми потенциально могут содержать нужную информацию. Затем, с помощью уже имеющихся данных, ограничивается временной промежуток, к которому может относиться переписка, содержащая искомую информацию. В ограниченной таким образом области переписки уже проводится поиск по ключевым словам.

Поиск осуществляется с помощью специального программного обеспечения. Во-первых, это коммерческие программные комплексы, предназначенные для исследования электронных устройств в целом, такие как AccessData FTK, EnCase, BelkaSoft и «Архивариус», Oxiom, BlackBag и др. В данных программах имеется возможность поиска с использованием ключевых слов, но это только одна из задач и далеко не первостепенная для данного программного обеспечения. Во-вторых, это специализированные программные комплексы, которые позволяют искать ключевые слова в больших массивах данных, и такой поиск является их основной задачей; кроме того, они обладают некоторыми аналитическими функциями, с помощью которых можно фильтровать файлы по тематикам. К таким программам относятся ZyLab, Relativity, Nuix, Ringtail и др. Они отличаются наличием больших

[92] См. Приложение № 2.

возможностей, таких как поиск в файлах различного формата, поиск похожих слов и т. д.

Поиск происходит следующим образом: оператор загружает в программу подлежащий исследованию объем сообщений, формирует список ключевых слов, задает их для поиска, после чего проверяет выданные программным инструментом результаты.

Разумеется, программное обеспечение не осуществляет примитивный поиск по сочетанию букв. Например, орфографические ошибки, незаконченные слова, синонимы и созвучные с ключевыми слова – все это будет найдено. Но такие программы способны решить далеко не все задачи. Как пишет А.И. Сотов, «важнейшим элементом успешного исследования переписки является подбор правильных ключевых слов (key-words)»[93]. Непосредственно сам список ключевых слов должен составляться человеком, в нашем случае следователем или экспертом.

Согласно анкетированию следователей, большинство из них ответили, что смогли бы сформировать поиск ключевых слов (55,93%), многие составили бы, но беспокоятся, что он будет не исчерпывающим (38,14%), а 5,93% считают, что не справились бы с этим[94]. Индексация, по мнению 51,15% опрошенных, должна проводиться в рамках экспертизы, и по ответам 48,85% опрошенных – следователями самостоятельно.

Поэтому, на наш взгляд, продумывание ключевых слов следователем должно осуществляться в соответствии со следующим алгоритмом[95]:

«1. Производится **формулировка цели**, а именно примерное представление об информации, которую мы пытаемся найти;

2. Производится **оценка имеющейся у нас информации** в соответствии с расследуемым событием;

---

[93] См.: *Сотов А.И.* Исследование электронной переписки путем индексации // Юридическое образование и наука. 2021. № 10. С. 33–36.

[94] См. Приложение № 2.

[95] См. Печникова Р.Б. Алгоритм выявления ключевых слов и составления их списка для индексации электронных сообщений в ходе расследования преступлений // Юридическое образование и наука. 2023. № 2. С. 35

3. Производится **сопоставление имеющейся и искомой информации**, определяются основные пробелы (под пробелами понимается недостаточность доказательственной информации во всем объеме информации, полученной в ходе расследования конкретного уголовного дела), которые требуется найти посредством поиска;

4. С учетом определившихся пробелов **выявляются основные слова, фразы, которые может содержать искомая информация**;

5. С учетом сторон, ведущих переписку, **определяются особенности**, которые могут быть присущи общению именно между ними (сленг, шифр). **Формируются синонимы с учетом характерных особенностей** (например, преступный сленг);

6. **Формируется заключительный список** ключевых слов»[96].

Иллюстративно данный алгоритм представлен в Приложении № 1[97]. Теперь необходимо рассмотреть все этапы подробнее.

1. **Формулировка цели.** На данном этапе формируется представление о тех фактических обстоятельствах, которые могут отражаться в переписке и которые можно использовать в ходе доказывания по делу. Этот этап помогает избежать необоснованного просмотра сообщений, не относящихся к делу, который так или иначе является нарушением тайны переписки, чего следует избегать без необходимости.

   Так, в США существует оговорка к Четвертой поправке к Конституции США, которая называется «plain view doctrine» – «теория открытого взгляда». Она разрешает сотрудникам полиции осматривать и изымать только те доказательства, которые находятся на виду (т. е. могут быть обнаружены без выполнения специальных поисковых мероприятий), либо те, непосредственно на которые направлен обыск[98]. В деле США против Кэри[99] у полиции был ордер, который предусматривал поиск, во время

[96] См.: *Печникова (Гасанова) Р.Б.* Индексация электронных сообщений, используемых в качестве доказательств при расследовании преступлений // Universum: экономика и юриспруденция. 2021. № 6 (81). С. 29.
[97] См. Приложение № 1.
[98] См.: Orin S. Указ. соч.
[99] Там же.

обыска, компьютерных файлов, содержащих имена, адреса, номера телефонов, относящиеся к распространению запрещенных веществ. В ходе обыска один из сотрудников полиции стал просматривать все файлы на компьютере и нашел снимки, на которых были изображены порнографические материалы. В ходе разбирательства суд впервые применил теорию открытого взгляда к обыску компьютера и постановил, что изыматься должны только те файлы и данные, которые имеют отношение к расследуемому событию. Ч. 1 ст. 88 УПК РФ содержит требование об относимости доказательств. Б.Т. Безлепкин[100] считает, что признаком относимости доказательств в уголовном процессе является их логическая связь с перечисленными в ст. 73 УПК обстоятельствами, подлежащими доказыванию, т. е. с предметом доказывания. Однако зачастую массив данных в переписке настолько большой, а используемые в них речевые обороты и формулировки так неоднозначны, что выявить относимые сообщения бывает довольно сложно.

В российском уголовном процессе информация на устройствах часто получается следователями в ходе осмотра вещественных доказательств (например, осмотра смартфона). Порядок такого осмотра не налагает ограничения на следователя в отношении того, какие файлы он может просматривать и какую информацию получать. На наш взгляд, сообщения, осматриваемые следователем, должны быть относимыми к расследуемому событию, по аналогии с опытом США. И именно корректная индексация электронных сообщений в ходе расследования поможет ограничить круг рассматриваемых правоохранительными органами сообщений, сузив их до относимых к конкретной искомой информации.

2. **Оценка имеющейся информации.** На этом этапе следователю стоит проанализировать всю имеющуюся информацию по делу. Особое внимание

[100] См.: *Безлепкин Б.Т.* Комментарий к Уголовно-процессуальному кодексу Российской Федерации. – М.: Проспект, 2021. – 640 с.

нужно уделить именам, адресам, номерам телефонов, прозвищам (если таковые имеются), возрасту адресатов, их образованию. Также ценным источником данных могут стать записи допроса или материалы оперативно-розыскных мероприятий, которые могут помочь установить своеобразные речевые обороты, условные выражения, слова, применяемые в живой речи лицом, переписка которого исследуется. В результате мы получаем обоснованное представление о круге проверяемых лиц, об обстоятельствах, которые могут отразиться в переписке, об интеллектуальном уровне развития участников переписки, о лексиконе, который они используют и т. д.

3. **Сопоставление имеющейся и искомой информации.** По мнению В.Я. Колдина, следственные действия «без информационно-поисковой модели искомого и четкого представления задач следственного действия, как правило, не приводят к цели, а чаще всего наносят тактический вред»[101]. Это относится и к индексации электронных сообщений в процессе расследования. Именно сравнение и сопоставление имеющейся информации с искомой определит дальнейшие задачи следователя на пути к формулировке ключевых слов. Так, например, следователь знает, что ему не достает доказательств о передаче взятки, на данной стадии он сопоставляет имеющиеся данные (свидетельские показания о том, что взятка была передана определенному лицу, документы, подтверждающие выполнение лицом определенных действий) с отсутствующими (сумма взятки, подтверждение факта ее передачи, договоренность о выполнении действий, возможность лица выполнить эти действия и т. д.), после чего он получит более четкое представление об искомой информации: ему предстоит найти сообщения, подтверждающие встречу или договоренность. Это позволит следователю выявить пробелы в массиве доказательств и понять, смогут ли сообщения, потенциально имеющиеся на устройстве, их заполнить.

[101] См.: *Колдин В.Я.* Вещественные доказательства… С. 3.

4. **Выявление основных слов и фраз.** Определившись с тем, какие доказательственные сведения следователь предполагает обнаружить в переписке, он, для начала в общих чертах, формирует список слов и фраз, которые могут содержаться в предполагаемой информации и которые обозначают интересующие следствие обстоятельства.
5. **Выявление особенностей и формулировка синонимов.** Современное программное обеспечение помогает осуществить поиск не только конкретных слов, но также и сообщений, включающих похожие слова или слова-синонимы. Однако такие программы не могут учитывать, например, весь сленг преступного мира или определенные шифры. Именно поэтому в ходе формулировки ключевых слов для следователя немаловажное значение имеет также социальная группа, к которой относятся адресаты сообщений, и даже индивидуальные особенности словарного запаса участников переписки, фразеологические обороты, которые используются или могут быть использованы ими применительно к расследуемому событию. Например, если речь идет об индексации сообщений электронной корпоративной почты, не стоит забывать о корпоративном сленге. Так, слово «взятка» на корпоративном языке часто заменяется словом «откат», «подгон», «кик-бек». Или, например, если речь идет о генеральном директоре, его могут называть «Гена». Если следователь формирует ключевые слова для индексации сообщений, связанных со сбытом наркотических веществ, то «распространение» может быть заменено такими словами, как «банчить», «банковать», сами вещества могут называться, например, марихуанна – «бошка», кокаин – «белый», героин – «Гриша» и т. п. Понимание терминологии тех групп, к которым принадлежат участники переписки, важно постольку, поскольку способствует уяснению их индивидуального лексикона. Это позволяет выдвинуть обоснованные версии, в каких словах авторы сообщений могут формулировать свои мысли.

6. **Формирование заключительного списка ключевых слов.** На этом этапе следователь, обобщив свои представления о применяемой в переписке терминологии и ее месте в расследуемом событии, составляет полный список ключевых слов с учетом всех имеющихся пробелов и особенностей.

Для выполнения задач, требующих специальных знаний, УПК РФ предусматривает возможность привлечения специалиста[102]. В ходе формулирования ключевых слов для индексации нами предлагается не пренебрегать помощью специалиста по шифрованию данных, лингвиста или, например, переводчика.

После формирования списка ключевых слов он должен быть введен в поисковую систему так, чтобы наиболее оптимальным способом выявить весь объем релевантной информации. Современные программные инструменты индексации основаны на логических операторах поиска.

Одни, например, позволяют осуществлять поиск одновременно по нескольким ключевым словам, что позволяет исключить возможные упущения, связанные с орфографическими ошибками или сокращениями, допущенными при составлении самих сообщений, а также расширить поиск за счет использования синонимов. Так, для поиска в сообщениях информации о взятке с помощью программы ZyLab, могут применяться следующие ключевые слова (с использованием языка запроса программы ZyLab: * – любое количество любых символов, OR – логическое «или», w/2 – искать следующее слово на расстоянии не больше 2 слов от первого[103]):

1. Возм. OR возме* OR откат* OR взятк* OR взяточ* OR взяток* OR подкуп* OR отплат* OR отблагодар* OR облагодет* OR озоло* OR «на лапу» OR прикорм* OR подкорм* OR «в карман*»;
2. обнал* OR налом* OR налик* OR наличны* OR конверт*;

[102] См.: ст. 58 Уголовно-процессуального кодекса Российской Федерации от 18.12.2001 № 174-ФЗ // СПС «КонсультантПлюс».
[103] См.: ZyLAB General Search Language Guide // ZYLAB. 2016. P. 118. // URL: https://docs.zylab.com/articles/#!zylab-one-search-language-guide-publication/10824 (дата обращения: 20.05.2023).

3. (моя OR моей OR мою OR наша OR нашей OR нашу OR своя OR своей OR свою) w/2 (компани* OR фирм* OR контор*);

4. «в доле» OR распил* OR навар* OR дележ*.

Поиск в программе ZyLab может также производиться с помощью логического оператора AND. Оператор AND – это логический оператор поиска, который сужает поисковый запрос. Он извлекает все файлы, содержащие все заданные слова вместе. Например, при вводе запроса «запрещенные» AND «вещества» оператором будут найдены только те файлы, которые содержат оба этих слова, что позволяет сузить круг поиска.

Оператор поиска IN позволяет искать информацию не только в самих файлах, но и в метаданных.

Бесспорным достоинством программы ZyLab является способность искать слова во вложенных файлах, включая не только текстовые, но и графические. Но в настоящее время эта программа не всегда доступна работникам следственного аппарата.

Результаты анкетирования, проведенного в рамках данного диссертационного исследования, показали, что большинство (52,07%)[104] работников правоохранительных органов не знакомы с понятием индексации электронных сообщений и не применяют его на практике. Однако есть и те, кто знаком или успешно использует данный метод в ходе расследования: 10,74% опрошенных применяют на практике, 37,19% – знакомы с данным инструментом, но не используют. Применяющие индексацию на практике работают со следующим программным обеспечением: dtSearch Desktop (21,95%), dtSearch Network (12,20%), ZyLab (9,76%), Relativity (4,88%), BelkaSoft (14,63%), «Архивариус» (36,58%).

Программное обеспечение dtSearch Desktop выполняет мгновенный поиск файлов, доступных на рабочем столе. Поиск в программе также осуществляется посредством логических операторов, однако их намного меньше, чем в ZyLab: И/ИЛИ/НЕ, поиск похожих слов, слов с другим окончанием, поиск по числам и

[104] См. Приложение № 2.

возможность комбинировать все виды поиска. Программа «Архивариус» помогает осуществлять поиск документов и сообщений в компьютере, локальной сети и съемных дисках.

При выборе программы для индексации необходимо оценить работу программы на предмет сохранения информации в том объеме, в котором она загружается для поиска и анализа. Недопустимо, чтобы программа меняла информационный массив, так как это приведет к утере ее достоверности в качестве доказательственной и криминалистически значимой информации в расследовании.

Поиск по ключевым словам в электронной переписке может осуществляться как в рамках компьютерно-технической экспертизы, так и непосредственно следователем в рамках осмотра устройства. Для этого следователю требуется установить программу, обеспечивающую индексированный поиск, на свой рабочий компьютер, подключить к нему устройство и с помощью программы выгрузить подлежащий исследованию массив сообщений в буфер для обработки, после чего провести его анализ путем индексации. Современные программы обладают достаточно удобным интерфейсом, понятным каждому, и не требуют специальных познаний, выходящих за пределы навыков обычного пользователя. Разумеется, такие действия не в каждом случае могут быть осуществлены следователем, поскольку доступ к данным на устройстве не всегда просто получить, и, если для этого потребуются специальные знания, устройство должно быть направлено на экспертизу. Найденные сообщения должны фиксироваться в протоколе осмотра или в заключении эксперта. Сами же электронные сообщения, выбранные по результатам поиска, должны быть перенесены на электронный носитель и приобщены к материалам дела.

Современное программное обеспечение для индексации действительно обладает серьезными возможностями, однако участие человека все еще является наиболее важным аспектом, так как именно человек составляет список ключевых слов. Ограничение круга искомых слов и их правильная формулировка поможет не

только сконцентрироваться на важной доказательственной информации, но и избежать нарушения прав составителя исследуемых сообщений.

§ 3. Использование идентификации в алгоритме доказывания для установления автора электронного сообщения

Идентификация лица, отправившего электронное сообщение – сложный и, пожалуй, ключевой вопрос, который встает перед следователем.

Криминалистическая идентификация – сравнительное исследование объектов, связанных с расследуемым событием, в целях разрешения вопроса об их тождестве и последующего установления характера связи с расследуемым событием единичного искомого объекта[105]. Идентифицировать объект – значит, установить его тождественность самому себе, исходя из образованных им отображений. Идентификация отправителя сообщения в криминалистическом смысле представляет собой установление факта отправки электронного сообщения конкретным лицом.

Идентификация лица – это достоверное установление тождества персональных данных неизвестного человека индивидуальным данным установленного либо разыскиваемого лица, зафиксированным в юридически значимых документах посредством установленных нормативными правилами характеристик (такими как имя, пол, возраст, прописка)[106]. То есть отправитель электронного сообщения будет являться идентифицируемым объектом, а вот идентифицирующими объектами могут становиться следы (не обязательно материальные), отображающие свойства отправителя.

Помимо криминалистической идентификации, существует понятие идентификации в интернет-среде. Под ней понимается процедура, в результате выполнения которой для субъекта идентификации выявляется его идентификатор,

---

[105] См.: *Колдин В.Я.* Судебная идентификация. – М.: ЛексЭст, 2002. – С. 74.
[106] См.: *Жванков В.А.* Человек как носитель криминалистически значимой информации. – М.: АПО, 1993.

однозначно определяющий этого субъекта в информационной системе[107]. Такая идентификация подразумевает под собой определение пользователя, отправившего сообщение, в информационной системе Интернет, но не идентифицирует отправителя сообщения в криминалистическом смысле.

В данном параграфе мы будем говорить об использовании криминалистической идентификации в алгоритме доказывания. Она, разумеется, связана с интернет-идентификацией, но эти понятия не тождественны.

Как пишет А.А. Воробьева, на сегодняшний день существуют три основные группы методов идентификации пользователя в сети Интернет: по техническим характеристикам рабочей станции пользователя, по «поведенческим характеристикам» пользователя на веб-портале, по лингвистическим или стилистическим характеристикам электронных сообщений, размещаемых пользователем[108]. На наш взгляд, к этим группам стоит добавить группу «по материальным следам», так как на устройстве или носителе могут оставаться биологические следы пользователя.

Потенциально идентифицирующими объектами могут выступать:

1) аккаунт или адрес, с которого было отправлено сообщение;
2) цифровые следы[109] на устройстве;
3) признаки в самом содержании сообщения;
4) признаки, содержащиеся в активности пользователя в сети;
5) звучащая речь в голосовом сообщении;
6) видеоизображения в сообщениях;
7) биологические следы на устройстве.

---

[107] См.: Идентификация, аутентификация и авторизация – в чем разница? // URL: https://www.kaspersky.ru/blog/identification-authentication-authorization-difference/29123/?ysclid=lv2qp0i6a1644362662 (дата обращения: 20.05.2023).

[108] См.: *Воробьева А.А.* Методика идентификации интернет-пользователя на основе стилистических и лингвистических характеристик коротких электронных сообщений: дис. … канд. наук. – СПб., 2017. – С. 8.

[109] Любая криминалистически значимая компьютерная информация, т. е. сведения (сообщения, данные), находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе с помощью электромагнитных взаимодействий либо передающиеся по каналам связи посредством электромагнитных сигналов (В.Б. Вехов).

Следует подробнее рассмотреть возможности каждого объекта отображать свойства лица и перспективы идентификации по этим объектам.

1. Аккаунт или адрес, с которого было отправлено сообщение

Отправку электронного сообщения, будь то почта, социальная сеть или мессенджер, пользователь осуществляет посредством своего аккаунта. Аккаунт – это информационное пространство, предоставленное пользователю программным ресурсом, позволяющее ему пользоваться сервисами, и доступ, к которому, осуществляется на основании ввода средств аутентификации[110]. Аутентификация – это процедура проверки данных лица, входящего в свой аккаунт в социальной сети, в свой почтовый ящик или проходящего авторизацию в мессенджере[111]. Каким образом соотносятся аутентификация и идентификация? Идентификация – это сравнительное исследование отображенных объектов с целью разрешения вопросов об их тождестве[112], что, применительно к аккаунту, интерпретируется как принадлежность аккаунта конкретному лицу. Аутентификация же является своего рода процессом подтверждения права на доступ к аккаунту[113]. Аутентификация – процедура проверки подлинности заявленного пользователя, процесса или устройства. Эта проверка позволяет достоверно убедиться, что пользователь (процесс или устройство) является именно тем, кем себя объявляет. Как правило, процедура проверки основана на том, что пользователь передает некоторую секретную информацию, известную только ему – чаще всего это пароль – или каким-либо другим способом подтверждает факт владения такой информацией[114]. Идентификация в интернет-среде и аутентификация являются взаимосвязанными процессами распознавания и проверки подлинности субъектов (пользователей). Именно от них зависит последующее решение системы, можно ли предоставить

---

[110] См.: *Smith R.E.* Authentication: from passwords to public keys // URL: https://archive.org/details/authenticationfr0000smit (дата обращения: 20.05.2023).

[111] Там же.

[112] См.: *Колдин В.Я.* Судебная идентификация. С. 21.

[113] См.: *Толчёнова М.* Идентификация, аутентификация, авторизация: чем они различаются // https://skillbox.ru/media/code/identifikatsiya-autentifikatsiya-avtorizatsiya-chem-oni-razlichayutsya/?ysclid=lslnhvbgrx165365124 (дата обращения: 20.05.2023).

[114] См.: *Шаньгин В.Ф.* Защита компьютерной информации. Эффективные методы и средства. – М: ДМК Пресс, 2010. – С. 173.

доступ к ресурсам системы конкретному пользователю или процессу[115]. Для подтверждения своей подлинности субъект может предъявлять системе разные сущности. В зависимости от них процессы аутентификации могут быть разделены на следующие категории:

– *на основе знания чего-либо.* Примерами могут служить пароль, персональный идентификационный код PIN (Personal Identification Number), а также секретные и открытые ключи, знание которых демонстрируется в протоколах по типу «запрос-ответ»;

– *на основе обладания чем-либо.* Обычно это магнитные карты, смарт-карты, сертификаты и устройства;

– *на основе каких-либо неотъемлемых характеристик.* Эта категория включает методы, базирующиеся на проверке биометрических характеристик пользователя (голос, радужная оболочка и сетчатка глаза, отпечатки пальцев, геометрия ладони и др.). В данной категории не используются криптографические методы и средства. Аутентификация на основе биометрических характеристик применяется для контроля доступа в помещения или к какой-либо технике[116].

Может ли пользователь, прошедший аутентификацию и вошедший в свой (или не свой) аккаунт или почтовый ящик, быть идентифицирован? Для этого стоит подробнее рассмотреть устройство современных сервисов для обмена сообщениями и регистрации в них. В социальных сетях, электронной почте и мессенджерах она устроена по-разному.

Для регистрации в социальной сети пользователю следует пройти определенную процедуру, указав персональные данные, нпример, заполнить небольшую анкету: имя, фамилию, возраст, номер телефона или адрес электронной почты – указывать обязательно; место жительства, некоторые данные о месте работы или учебы, круг интересов – не обязательно. Обязательные данные не подлежат проверке и могут быть указаны фиктивными. Однако в настоящее время

[115] См.: *Шаньгин В.Ф.* Указ. соч. С. 173.

[116] См.: *Галицкий А.В., Рябко С.Д., Шаньгин В.Ф.* Защита информации в сети – анализ технологий и синтез решений. – М.: ДМК Пресс, 2004. – С. 51.

ведутся попытки идентифицировать пользователей, регистрирующихся в социальных сетях. Так, социальная сеть «ВКонтакте» запрашивает у пользователей авторизацию через портал «Госуслуги», пока не принудительно, но в дальнейшем это, скорее всего, станет обязательным условием регистрации. Также сейчас во всех крупных социальных сетях (таких как «ВКонтакте», Facebook, «Одноклассники») при регистрации недостаточно адреса электронной почты, к аккаунту необходимо привязать номер мобильного телефона и подтвердить его. То есть условием аутентификации владельца аккаунта является наличие у него телефона с номером, к которому этот аккаунт привязан.

При создании электронного почтового ящика персональные данные вводить не обязательно, достаточно указать имя и сгенерировать уникальный адрес. Но в настоящее время основные публичные почтовые сервисы (Google, Mail.ru) начинают требовать привязки телефонного номера к почтовому аккаунту. Как правило, номер выступает дополнительным средством защиты почтового ящика, поскольку на него оператор почты направляет уведомление о неудачных попытках войти в почту или присылает на него одноразовый пароль, если пользователь его забыл.

При авторизации в мессенджере пользователь в первую очередь должен ввести и подтвердить свой номер телефона. Больше от него ничего не требуется, он может также указать свое имя пользователя, которое не является постоянным и может меняться по его желанию.

Таким образом, минимальные требования к указанию информации о себе и только начальные попытки идентификации по паспорту не дают возможности достоверно идентифицировать личность владельца аккаунта. Основной источник относительно объективных данных – номер мобильной связи.

Не стоит также забывать о том, что для входа в аккаунт, почту, мессенджер сейчас у большинства сервисов используется двухфакторная аутентификация, особенно если вход осуществляется с нового устройства. Помимо ввода данных и пароля, пользователю на телефон приходит уникальный код, который он должен

ввести для подтверждения входа в аккаунт. Это говорит нам о том, что войти в чужой аккаунт не так-то просто, и для этого как минимум потребуется доступ к телефону его владельца.

Номер, к которому привязан аккаунт, может быть виден в его настройках, особенно если речь идет о мессенджерах. Установить лицо с помощью номера, на который зарегистрирован мессенджер или аккаунт, можно путем направления запроса оператору сотовой сети.

Однако такой вариант далеко не всегда может привести к желаемому результату. Во-первых, автор сообщений может не быть тем лицом, с которым имеется договор у оператора (например, в случае приобретения «анонимной» сим-карты, использования украденного устройства), а во-вторых – преступники могут применять так называемые подменные номера (caller ID или идентификатор абонента) – это функция телефона, которая отображает информацию о абоненте, совершающем звонок, на устройстве получателя вызова[117].

Если же мобильный номер принадлежит не тому лицу, на кого зарегистрирован аккаунт, целесообразно отследить физическое местонахождение соответствующего устройства при помощи биллинга. В общем случае биллинговой системой называют аппаратно-программный комплекс, осуществляющий учет объема потребляемых абонентами услуг, расчет и списание денежных средств в соответствии с тарифами организации[118]. Необходимо проанализировать, каким образом пополнялась купленная сим-карта, какие СМС приходили на нее. Возможно, она пополнялась через уличный терминал, размещенный под камерами, и в этот момент у ее владельца был включен личный мобильный телефон, либо она пополнялась с личного электронного кошелька, что также выведет следствие на установление личности. Это даст в распоряжение следствия признаки внешности лица, пользовавшегося устройством, с которого проводились действия в аккаунте.

---

[117] См.: *Waluyo A., Setiyo M.T., Mahfud A.Z.* Digital Forensic Analysis on Caller ID Spoofing Attack // 2022 7th International Workshop on Big Data and Information Security (IWBIS). 2022. 01-03 October.

[118] См.: *Галаган Т.А., Казаков З.А.* Разработка информационной системы «Служба биллинга» // Вестник Амурского государственного университета. Серия: Естественные и экономические науки. 2013. № 63. С. 27.

Однако его еще нельзя отождествлять с автором электронного сообщения, хотя такую версию выдвинуть можно.

Еще более сложной является ситуация с «подменными номерами». В сети Интернет существует большое количество сайтов, на которых можно «арендовать» мобильный номер на короткое время. Как правило, такой номер при звонке на него будет несуществующим, а при попытке узнать, кому он принадлежит, окажется, что он ни на кого не зарегистрирован. Для покупки и использования такого номера человек создает аккаунт на сервисе, занимающимся продажей таких номеров, и привязывает к нему свою банковскую карту. Если человек использовал такой номер для регистрации в мессенджере, следует направить запрос на сервис, предоставляющий аренду номеров. Такие сервисы, как правило, выдают все имеющиеся у них данные по запросу правоохранительных органов. Наиболее популярные из них: onlinesim.io, 365sms.org.

Если же установить номер телефона не представляется возможным (например, он не указан в настройках), идентифицировать владельца аккаунта можно путем направления запроса. Например, информацию о пользователе мессенджера, а также о материалах аккаунта можно получить посредством запроса к руководству мессенджера. Федеральным законом «Об информации, информационных технологиях и о защите информации»[119] определены обязанности организатора распространения информации в сети Интернет. «Организатором распространения информации в сети Интернет является лицо, осуществляющее деятельность по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети Интернет»[120]. В свою очередь, мессенджер можно определить как средство обмена

[119] См.: Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (ред. от 03.04.2020) // СПС «КонсультантПлюс».
[120] См. ст. 10.1 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (ред. от 03.04.2020) // СПС «КонсультантПлюс».

мгновенными сообщениями. Таким образом, администраторы мессенджера, осуществляющие его функционирование и поддержку, соответствуют определению «организатора распространения информации». Согласно закону[121], организатор распространения информации в сети Интернет обязан хранить на территории Российской Федерации:

1) информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей сети Интернет и информацию об этих пользователях в течение одного года с момента окончания осуществления таких действий;

2) текстовые сообщения пользователей сети Интернет, голосовую информацию, изображения, звуки, видео, иные электронные сообщения пользователей сети Интернет до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки.

Организатор распространения информации в сети Интернет также обязан предоставлять указанную информацию уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, в случаях, установленных федеральными законами.

Соответствующий запрос следователя должен содержать требование раскрыть данные аккаунта, а именно: номер телефона, указанный и подтвержденный при регистрации, имя, ID, логин, электронный адрес.

Что касается электронной почты, можно также попытаться установить владельца электронного почтового ящика путем направления официального запроса. Чтобы установить оператора, следует обратить внимание на то, что в адресе пишется после знака @, чаще всего это и будет названием сервиса, который предоставляет услуги электронной почты.

[121]См. п. 3 ст. 10.1 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (ред. от 03.04.2020) // СПС «КонсультантПлюс».

Запрос оператору почты должен содержать требование предоставить регистрационные данные, данные об активности электронного почтового ящика, IP-адреса авторизации, абонентский номер активации. IP-адрес представляет особенный интерес, поскольку позволит установить устройство, через которое осуществлялся доступ, а оно, в свою очередь, может дать прямую связь с пользователем. Также при проверке электронного адреса стоит направить запрос в социальные сети и проверить, не зарегистрирован ли адрес в социальных сетях. Если это так, то зачастую определить личность владельца по его странице достаточно легко.

Из изложенного видно, что сам по себе аккаунт не позволяет произвести идентификацию автора сообщений, однако его исследование может дать ценные идентифицирующие признаки.

2. Цифровые следы[122] на устройстве

К цифровым следам на устройстве относятся записи (логи), папки кэша браузера, данные об отправке сообщения (время и т. д.).

Записи событий информационной системы (логи) – это организованные в виде файлов, базы данных или массива в оперативной памяти совокупности записей о событиях, зафиксированных информационной системой[123].

Такие записи ведутся автоматически, участие человека заключается в настройке режима ведения записей (какие события включаются в журнал, а какие нет). Предназначение логов заключается в протоколировании операций, выполняемых на компьютере. Такое протоколирование и его анализ позволяют определить ошибки системы в целом или конкретного сервиса, сайта, собрать статистику посещений сайта и пр. Логи бывают разные, в зависимости от программного обеспечения: основной файл лога, лог загрузки системы, логи веб-сервера, логи сервера баз данных, логи почтового сервера, логи планировщика

[122] «Цифровой след – это информационный след, сформированный электронным устройством, может оставаться на нем, либо быть переданным на другое устройство, создавая тем самым электронное сообщение». См.: *Россинская Е.Р.* Теория информационно-компьютерного обеспечения криминалистической деятельности… С. 195.
[123] См.: *Федотов Н.Н.* Указ. соч. С. 158.

задач. Но нас интересуют в большей степени логи почтового сервера и логи веб-сервера[124]. Первые хранят в себе записи о всех отправленных и полученных сообщениях, а вторые – данные об обращениях к серверу.

На любом персональном компьютере логи хранятся в специальных папках, которые можно найти в системных файлах. Папка называется logs или logFiles, доступ к ней не ограничен, а сами файлы с логами не требуют специального программного обеспечения и зачастую открываются с помощью обычных текстовых редакторов, реже требуется специальное программное обеспечение.

На смартфонах также хранятся логи, однако получить их немного сложнее. На смартфонах с операционной системой Android необходимо подключить его к компьютеру с установленным на нем программным обеспечением Android Studio. Что касается смартфонов с операционной системой iOS, необходимо непосредственно на самом смартфоне установить программу xCode, с помощью которой можно открыть и прочитать логи.

Логи, которые не хранятся непосредственно на устройстве (т. е. логи выходов определенного устройства в сеть, на определенные сайты, время выхода) можно запросить у провайдера. Понять, к какому провайдеру надо обращаться, можно, расшифровав IP-адрес пользователя. За каждым провайдером закрепляется определенный диапазон адресов. Информация о том, каким провайдером был выдан адрес содержится в самом адресе.

Особое значение имеют логи программ, через которые с устройства осуществляется доступ к интернет-ресурсам (браузеров). В логах браузера содержится доменное имя посещенного пользователем сайта, дата и время посещения, тип запроса, к которому обратился пользователь и количество переданной информации. Так, в логах будет виден факт подключения устройства к социальной сети, выход пользователя в мессенджер или подключения к серверу электронной почты. По типу запроса и количеству переданной информации будет понятно, что пользователь заходил в аккаунт или отправлял сообщение.

[124] Файлы, в которых хранится информация о взаимодействии с сервером почты или сервером сайта.

Исследование логов, как правило, требует специальных знаний и должно проводиться в рамках компьютерно-технической экспертизы. Следователям необходимо иметь общее представление об исследовании и интерпретации логов для успешного осмотра устройства. Вопрос необходимости специальных знаний для исследования логов порождает также вопрос о доказательственном значении данных, полученных без их привлечения. Так, например, Н.Н. Федотов убежден, что интерпретация логов во всех случаях требует специальных знаний[125].

По нашему мнению, логи являются достаточно стабильным доказательством и могут быть интерпретированы следователем в ходе осмотра устройства, если их использование ограничится ориентирующими сведениями. Однако для использования логов в доказывании необходимо направлять их на компьютерно-техническую экспертизу. Именно получение экспертного заключения по результатам компьютерно-технической экспертизы может наделить логи доказательственной силой и процессуальным статусом.

Помимо логов, информацию о сетевом подключении можно также получить, просмотрев кэш программы, с помощью которой осуществлялся выход в Интернет. Процесс кэширования представляет из себя автоматическое копирование некоторых данных из программ и приложений. Кэш-данные находятся в системной папке браузера, с которого осуществлялась деятельности в сети. Получить данные кэша можно с любого персонального компьютера или смартфона. В них также может содержаться информация о подключении устройства к социальной сети, почте или мессенджеру и об отправке сообщения.

Если факт подключения или отправки с исследуемого устройства установлен, необходимо сопоставить эти сеансы выхода с моментом размещения сообщения, который обычно бывает отражен в самом сообщении (в мессенджерах и социальных сетях – под сообщением, в электронной почте – в информации об отправленном письме). Тем самым у следователя появляются основания полагать, что если во время, к которому относится проверяемое сообщение, на устройстве

[125] См.: *Федотов Н.Н.* Указ. соч. С. 139.

осуществлялся сеанс с тем самым сервисом, в котором сообщение было составлено, то с высокой степенью вероятности оно было составлено именно на этом устройстве. Таким образом, благодаря данным из логов и кэша можно идентифицировать устройство, с которого осуществлялась отправка сообщения, однако данный признак не позволяет произвести полноценную идентификацию отправителя.

3. Признаки в самом содержании сообщения

К признакам, содержащимся в самом сообщении, в первую очередь относятся лингвистические и стилистические характеристики. «Каждый человек имеет свой стиль письма, который составляет уникальный "отпечаток" – набор характеристик, позволяющих его идентифицировать»[126].

Под лингвистической идентификацией понимается процесс установления пользователя, являющегося автором сообщений, по совокупности общих и частных признаков текста, составляющих авторский стиль[127].

Под интернет-пользователем ученые лингвисты предлагают понимать физическое лицо, которое своими действиями с ресурсами интернет-портала обнаруживает некоторые признаки (характеристики пользователя), определяющиеся техническими средствами, которые он использует для доступа в Интернет, или стилистическими либо лингвистическими особенностями его письменной речи[128]. Мы с данным высказыванием не согласны, поскольку по смыслу определения можно понять, что лингвистическая идентификация позволяет установить конкретное лицо, использовавшее устройство в момент отправки сообщения. В криминалистическом смысле это невозможно. Исследование текстовых сообщений дает возможность установить пользователя

[126] См.: *Воробьева А.А*. Указ. соч. – С. 9.
[127] См.: *Романов А.С.* Методика и программный комплекс для идентификации автора неизвестного текста: автореф. дис. … канд. тех. наук: 05.13.18. – Томск, 2010. – С. 26.
[128] См.: *Воробьева А.А., Гвоздев А.В.* Идентификация анонимных пользователей Интернет порталов на основании технических и лингвистических характеристик пользователя // Научно-технический вестник механики и оптики. 2014. № 1 (89). С. 139–144.

интернет-среды как совокупность характеристик личности, составляющей сообщения, но никак не идентифицировать конкретное физическое лицо.

Лингвистическая идентификация начала развиваться еще в XIX в., когда появилась потребность в определении авторов литературных текстов. Исследованием данного вопроса занимался литературовед Н.А. Морозов, который представил свой метод «отличения плагиатов от истинных произведений того или другого известного автора и для определения их эпохи»[129]. Достоверность результатов, полученных с помощью его метода, зависела напрямую от объема анализируемого текста: чем больше слов, тем более пригоден был текст для сравнения. В остальном многие исследования в те времена были направлены на установление авторства по почерку. Так, первые попытки рассмотрения содержания письма для идентификации авторства в криминалистике делал Ганс Гросс, который требовал изучать не только форму, но и содержание письма[130].

Современные потребности в лингвистической идентификации связаны как раз с установлением автора короткого электронного сообщения. Как отмечает Т.П. Соколова, «в современной фиксированной речи произошли изменения, связанные со свойствами нового носителя информации, с проявлением закона речевой экономии, который в интернет-среде выражается в сокращении количества печатных символов»[131].

А.С. Романов пишет, что за более чем 120-летнюю историю развития данного вопроса отечественными и зарубежными исследователями было предложено множество методов определения автора текста, начиная от простого подсчета количества определенных слов в сравниваемых текстах и заканчивая разработками в области искусственного интеллекта. Главной проблемой традиционных работ по данной тематике является использование при проведении экспериментов текстов объемом более 30000–40000 символов и большого количества обучающих

---

[129] См.: *Морозов Н.А.* Лингвистические спектры // Известия АН ОРЯС. 1915. Т. 20, кн. 4. С. 93−134.

[130] См.: *Гросс Г.* Руководство для судебных следователей как система криминалистики. – М., 2002. – С. 280.

[131] См.: *Соколова Т.П.* Проблемы методического обеспечения судебной авторoведческой экспертизы // Теория и практика судебной экспертизы в современных условиях: материалы VII Международной научно-практической конференции. – М.: РГ-Пресс, 2019. С. 4–7.

примеров (от 5 до 100 и более). Нерешенной задачей является идентификация авторства коротких текстов[132].

Как отмечает А.А. Воробьева, в настоящее время существует два основных подхода в лингвистической идентификации пользователей: профильный подход и подход с обучением на примерах. При профильном подходе все тексты одного пользователя объединяются в один, далее рассчитываются значения различных идентификационных признаков, т. е. пользователь представляется как один вектор значений. В подходе с обучением на примерах пользователь представляется как набор его текстов, где каждый текст является вектором со значениями идентификационных признаков и обучающим примером[133]. Первый подход более полезен, когда доступно небольшое количество текстов пользователя и они сами по себе короткие. Второй подход используется в случае, когда потенциальных авторов текста большое количество, так как при нем по примерам комбинируются различные группы признаков.

Как правило, для проведения лингвистической идентификации используется один сайт (социальная сеть, блог). Но современные научные исследования предлагают рассматривать несколько источников текстовой информации для идентификации автора[134]. Ученые отмечают, что сбор текстовой информации из нескольких источников имеет ряд преимуществ:

1. Может существенно повлиять на ход расследования преступления в сети Интернет. Так, например, у пользователя может существовать аккаунт в социальной сети, содержащий идентифицирующую его информацию, но не причастный ни к какой криминальной активности, и не содержащий идентифицирующих данных аккаунт в другой социальной сети, при помощи которого было совершено преступление. В этом случае при помощи

[132] См.: *Романов А.С., Шелупанов А.А., Бондарчук С.С.* Обобщенная методика идентификации автора неизвестного текста // Доклады ТУСУРа. 2010. № 1 (21), ч. 1. С. 108.
[133] См.: *Воробьева А.А.* Указ. соч. С. 35.
[134] См.: Межсайтовая лингвистическая идентификация интернет-пользователей / А.А. Воробьева [и др.] // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18, № 3. С. 448.

лингвистической идентификации можно связать данные аккаунты и доказать, что оба они принадлежат одному лицу и далее предпринимать соответствующие меры;

2. Позволяет существенно увеличить объем текстовой информации для одного пользователя, тем самым решая проблему малой длины сообщений и улучшая точность идентификации[135].

Мы с данной позицией согласны. В настоящее время многие пользователи имеют больше одного аккаунта в социальных сетях, больше одного номера телефона, на которые зарегистрированы в мессенджерах, и несколько адресов электронной почты. Зачастую различные аккаунты используются для осуществления разной деятельности (например, работа и личная жизнь), но также с помощью них могут совершаться и противоправные действия. На наш взгляд, следователю и эксперту необходимо проверять (в ходе осмотра, допроса, иных следственных действий), не принадлежат ли подозреваемому (обвиняемому) иные аккаунты, адреса, телефонные номера, так как в положительном случае это поможет улучшить результативность лингвистической идентификации.

С развитием искусственного интеллекта и нейросетей представляется, что в обозримом будущем программы, разработанные на основе нейросетей, могли бы решать задачи установления авторства сообщения на основании сравнения текстов исследуемых сообщений и иных текстов, найденных у подозреваемого, авторство которых он не отрицает. Зарубежные ученые уже занимаются проблемой построения минимальной по размеру нейронной сети для определения авторства[136]. В работах российского ученого О.Г. Шевелева рассматривается использование нейронных сетей для идентификации авторов литературных произведений[137].

Возможности исследования текста довольно широки и продолжают развиваться. Каждый день совершенствуются уже имеющиеся и появляются новые

---

[135] Там же.

[136] См.: *Waugh S., Adams A., Tweedie F.J.* Computational stylistics using Artificial Neural Networks // Literary and Linguistic Computing. 2000. Vol. 15, No. 2. Pp. 187–198.

[137] См.: *Шевелев О.Г.* Разработка и исследование алгоритмов сравнения стилей текстовых произведений: дис. ... канд. техн. наук: 05.13.18. Томск, 2006. –176 с.; *Шевелев О.Г., Петраков А.В.* Классификация текстов с помощью деревьев решений и сетей прямого распространения // Вестник Томского государственного университетата. 2006. № 290. С. 300–307.

способы лингвистической идентификации автора электронного сообщения. Несмотря на то, что лингвистическая идентификация не является идентификацией в криминалистическом смысле, она позволяет определить пользователя сети Интернет (но не конкретное лицо), отправившего сообщение, что наделяет следователя ориентирующей информацией и, разумеется, является важной составляющей расследования. Вопросы лингвистической идентификации, установления авторства текста решаются экспертом в ходе лингвистической, психолого-лингвистической и автороведческой экспертиз, о которых подробнее написано во втором параграфе третьей главы настоящего исследования.

4. Признаки, содержащиеся в активности пользователя в сети

На веб-сервисах могут содержаться следующие источники криминалистически значимой информации:

1) чаты[138];
2) участие пользователей в группах и сообществах;
3) действия пользователей, направленные на публичное распространение информации;
4) иная информация (статусы[139], записи и т. д.).

Вышеназванная информация может служить ориентирующей в рамках расследования уголовного дела, прежде всего она позволит сопоставить психологические черты пользователя социальной сети и автора проверяемого сообщения. То есть речь идет о сопоставлении признаков личности. Еще в XIX в. основоположник науки криминалистики Ганс Гросс говорил, что в расследовании преступлений «величайшее усилие стоит прилагать именно к выяснению собственно личности обвиняемого»[140]. Криминалистическое изучение личности – это установление криминалистически значимой информации о преступнике, жертве преступления, а также обвиняемом, потерпевшем и других участниках процесса расследования, включающей в себя сведения о присущих им

[138] Чат – сервис для общения онлайн, в режиме реального времени, переписка.
[139] Статус – короткая фраза, размещаемая пользователями в своей «анкете» в социальной сети.
[140] См.: *Гросс Г.* Указ. соч. С. 280.

анатомических, биологических, психологических и социальных свойствах, которые необходимы для идентификации личности, решения тактических задач и установления фактической картины события преступления в процессе его раскрытия и расследования, а также использования в целях осуществления криминалистической профилактики[141].

На наш взгляд, социальные сети могут быть использованы для составления криминалистической характеристики личности. Может быть составлен даже психологический портрет лица, определен его тип личности, образ жизни, предпочтения и интересы в определенных сферах жизни. Эксперимент в данной области проводили ученые-криминалисты Н.В. Олиндер и Е.А. Гамбарова, в ходе которого было выявлено, что на поиск информации о личности в сети Интернет, в том числе в социальных сетях, уходит около 2,5–3 часов. За это время можно составить довольно существенную характеристику личности[142]. Также одним из крупнейших исследователей в этой области является Майкл Козински, который утверждает, что исследование информации из социальных сетей позволяет нам сформировать некую модель личности пользователя сети. Данные из социальных сетей показывают действительно реальные факты, уровень жизни и социальную позицию человека в обществе[143].

Данные о личности, ставшие известными во время следственных действий или сбора характеризующего материала, можно сопоставить с данными о личности из социальных сетей. Это, конечно, не идентифицирует отправителя, но позволит выдвинуть приоритетные версии относительно выбора потенциального автора сообщений из нескольких подозреваемых, основываясь на их персональных качествах.

---

[141] См.: Криминалистика: учебник / Под ред. Н.П. Яблокова. 2019. – С. 752.

[142] См.: *Олиндер Н.В., Гамбарова Е.А.* Проблемные вопросы поиска и восприятия информации о человеке в сети Интернет и ее использование при расследовании преступлений // Юридический вестник Самарского университета. 2016. Т. 2, № 4. С. 58.

[143] См.: *Kosinski M., Stillwell D., Youyou W.* Computer-based personality judgments are more accurate than those made by humans // Proceedings of the national Academy of Sciences of the United States of America (PNAS). 2015. Vol. 112, No. 4. Pp. 1036–1040.

См: Do Facebook status updates reflect subjective well-being? / P. Liu [et al.] // Cyberpsychology, behavior, and social networking. 2015. Vol. 18, No. 7. Pp. 373–379.

Еще одним перспективным направлением является методика идентификации интернет-пользователя на основе анализа «клавиатурного почерка» или поведения пользователя на веб-портале. В ходе такого исследования «анализируются действия, производимые пользователем на веб-странице, либо динамика набора сообщений на клавиатуре»[144]. Процесс работы пользователя на клавиатуре представляется как «совокупность характеристики подсознательных процессов мышления при использовании устройства ввода (наборе текста), составляющей процессов мышления и механические и эргономические параметры и характеристики устройства ввода (клавиатуры), влияющие на процесс набора текста»[145]. При таком анализе учитываются временные характеристики, такие как длительность нажатия клавиш на устройстве ввода, длительность пауз между нажатиями клавиш, индивидуальные особенности работы (количество ошибок, использование специальных клавиш).

Перспективы установления отправителя сообщения на основе признаков, содержащихся в активности пользователя в сети, пока крайне расплывчаты и не позволяют провести криминалистическую идентификацию лица. Однако такие признаки должны собираться и анализироваться как следователем, так и в ходе экспертной деятельности, поскольку результаты подобных исследований могут стать ценной ориентирующей информацией для следствия.

5. Звучащая речь в голосовом сообщении

В последние годы большую популярность набрали голосовые сообщения в мессенджерах. Голосовое сообщение – это файл, содержащий в себе аудиоинформацию. Человек записывает свою речь, которая сохраняется в виде файла, и этот файл является вложением для сообщения его собеседнику.

Е.И. Галяшина отмечала, что удобство цифровой звукозаписи в наши дни вполне очевидно – малые размеры устройств, качество записи. Однако, несмотря на преимущества, возникают сложности с приобщением таких записей в качестве

---

[144] См.: *Воробьева А.А.* Указ. соч. С. 8.

[145] См.: *Никитин В.В.* Существующие системы аутентификации и идентификации пользователей: основные проблемы и направления их модернизации // Вестник Московского университета МВД России. 2014. № 2.

доказательств: как процессуальные, так и экспертные[146]. При проведении таких экспертиз следствие и суд интересуют вопросы установления подлинности фонограммы и идентификации конкретного диктора по фонограммам устной речи[147]. Е.И. Галяшина отмечает, что традиционные экспертные методики исследования фонограмм на предмет идентификации диктора малоприменимы к современной цифровой звукозаписывающей технике и средствам мобильной связи. В данной ситуации необходимо проведение комплекса научных исследований по совершенствованию используемых на практике экспертных методик идентификации диктора, с учетом особенностей цифровых фонограмм как объектов экспертного исследования, полученных в разных условиях на разных технических средствах[148].

В речеведении было разработано такое понятие, как «голосовой отпечаток». Голосовой отпечаток – это один из ключевых факторов в анализе речи, который включает в себя индивидуально отличительные паттерны голосовых характеристик говорящих[149]. Это некая уникальная для человека запись, что-то вроде отпечатка пальца. Она не основывается непосредственно на самой речи человека (конкретных словах, фразах), а характеризует голос в целом. Технологии создания и анализа таких голосовых отпечатков основаны на некоторых опорных точках в речи, например, особенных переходах между звуками. Учитываются физические характеристики: кроме высоты, скорости разговора конкретного человека, к сведению принимаются даже физиологические особенности его звукового тракта, горла, глотки, даже носа.

Изучение голосовых отпечатков входит в сферу исследований голосовой биометрии. Она предполагает сравнение голоса проверяемого лица с записями других голосов. Идентификация по голосу делится на текстозависимую и

---

[146] См.: *Галяшина Е.И.* К вопросу о достоверности криминалистической идентификации личности по цифровым фонограммам устной речи // Известия Тульского государственного университета. Экономические и юридические науки. 2016. № 3-2. С. 19.

[147] См.: *Галяшина Е.И.* Актуальные проблемы экспертизы цифровых фонограмм // Теорія та практика судовой експертизи і кримі: Зборник научных трудов. Выпуск 8. Харюв: Право, 2008. С. 248–257.

[148] *См.: Галяшина Е.И.* К вопросу о достоверности криминалистической идентификации личности… С. 22.

[149] См.: *Kersta L.G.* Voiceprint Identification // Nature. 1962. Vol. 196. Pp. 1253–1257.

текстонезависимую. Соответственно текстозависимая учитывает слова, которые произнесены человеком, а текстонезависимая – осуществляется по спонтанной речи человека, т. е. не важно, что именно человек говорит[150].

Методологическую основу фоноскопического идентификационного исследования речи составляют положения криминалистической идентификации и диагностики[151]. Возможность идентификации объектов лингвистического исследования при производстве фоноскопических экспертиз связана с наличием у них идентификационных признаков. Идентификационным признаком является специально выделенное для целей идентификации свойство объекта, обладающее качественной определенностью (т. е. способностью отличать данный объект от других ему подобных) и относительной устойчивостью (т. е. относительной неизменностью в течение длительного времени)[152].

При исследовании голосового сообщения, т. е. звучащей речи человека мы можем говорить об идентификации автора голосовой записи, так как такие исследования действительно дают возможность установить тождественность лица, исходя из оставленных им отображений в виде «голосового отпечатка». Тем не менее современные технологии неоднозначны, и рассуждать о том, что в 100% случаев лицо, кому принадлежит голос на записи, является отправителем сообщения, мы не можем. Таким образом, фоноскопическая идентификация устанавливает именно диктора голосовой записи, но не отправителя конкретного сообщения. Проводится она экспертом в рамках фоноскопической экспертизы, возможности которой рассмотрены во втором параграфе третьей главы настоящего исследования.

6. Видеоизображения в сообщениях

---

[150] См.: *Гасанова Р.Б. (Печникова Р.Б.)* Идентификационное значение голосовых сообщений при расследовании преступлений // Научная школа уголовного процесса и криминалистики Санкт-Петербургского государственного университета: материалы конференций 2020–2021 годов; сборник статей / кол. авторов; под. ред. Н.П. Кирилловой, С.П. Кушниренко, Н.Г. Стойко (отв. ред.), В.Ю. Низамова (отв. ред.). – М.: РУСАЙНС, 2021. С. 86.

[151] См.: *Галяшина Е.И.* Прикладные основы фоноскопической экспертизы // Теория и практика судебной экспертизы: сборник монографий. – СПб.: Питер, 2003. С. 93.

[152] См.: *Баранов Ю.Н.* Теоретические основы применения лингвистических знаний в криминалистике при производстве фоноскопических и автороведческих экспертиз: дис. … канд. юрид. наук: 12.00.09. – М.: РГБ, 2005. С. 29.

В данном случае речь идет о популярных в последнее время видеосообщениях или, как принято их называть, – «кружочках». Они представляют из себя короткие видеоособщения, которые пользователи могут записывать и отправлять друг другу сразу в мессенджере. Такие сообщения появились и стали популярны в мессенджере Telegram, но быстро набрали популярность и стали распространяться и в других сервисах, например в социальной сети «ВКонтакте».

Идентификация личности по видеоизображениям – довольно перспективное направление. «Преимущества видеоизображений переоценить невозможно, поскольку они позволяют расширить область изучения внешности человека за счет исследования не только статически запечатленного образа, но и признаков двигательного характера, включаемых экспертом в идентификационный комплекс»[153].

Современные исследования идентификации личности на видеозаписи основываются на методике портретного исследования. «В основном портретные экспертизы проводятся с целью идентификации человека по признакам внешности, отобразившимся на фотографиях и других носителях изображений, по результатам которых устанавливается тождество изображенных на фотографиях лиц, или же наоборот, устанавливается их различие»[154].

«Несмотря на то, что портретная идентификация по динамическим признакам находится еще в стадии становления, анализ и сравнение параметров амплитуды движений головы, рук и ног все чаще позволяет установить достаточный для решения идентификационных задач объем уникальных динамических характеристик для каждого человека»[155]. С.Д. Долгинов отмечал, что «извлеченная из мобильных устройств и смартфонов информация о внешнем облике человека подлежит последующей портретной идентификации, сложность проведения которой обусловлена ограниченным объемом информации о признаках

[153] См.: *Подволоцкий И.Н.* Современные криминалистические тенденции идентификации человека по видеоизображенниям // Вестник Академии экономической безопасности МВД России. 2015. № 2. С. 55.
[154] См.: *Зинин А.М.* Криминалистическая идентификация человека по признакам внешности: учебное пособие для вузов / А. М. Зинин [и др.] ; под редакцией А. М. Зинина. — 2-е изд. — Электрон. дан. — Москва: Юрайт, 2022.
[155] См.: *Подволоцкий И.Н.* Указ. соч. С. 55.

внешности человека, запечатленных на видеоизображениях»[156]. На наш взгляд, с распространением мгновенных видеосообщений данная проблема может минимизироваться в связи с особенностями таких сообщений.

Видеосообщения действительно обладают очень широким идентификационным потенциалом, так как характеризуются следующими криминалистически значимыми чертами:

1) такие сообщения как правило записываются на переднюю камеру устройства;

2) в большинстве случаев на видео человек снимает свое лицо вблизи;

3) видеоизображение сопровождается звуком, как правило человек что-то рассказывает;

4) основной смысл сообщения – сопровождение аудиорассказа видеоизображением реакции и эмоций рассказчика. Поэтому такие видеозаписи как правило отражают мимику лица.

Видеосообщения позволяют идентифицировать составившее их лицо как по голосу, так и по признакам внешности. Исследование видеосообщений производится в рамках экспертной деятельности, которой посвящен второй параграф третьей главы данного исследования.

7. Биологические следы на устройстве

Немаловажную роль в идентификации лица, отправившего сообщение, все еще играют биологические следы. Их исследование может проводиться в рамках классических экспертиз, например, дактилоскопической экспертизы отпечатков пальцев или ДНК-экспертизы следов на устройстве.

Дактилоскопия как метод идентификации появился еще в глубокой древности, оттиски пальцев рук были найдены в древнем Китае и Индии. Пальцевые отпечатки для борьбы с преступностью впервые были использованы в середине XIX в. Уильямом Гершелем в Индии и впоследствии Генри Фолдсом в Англии.

[156] См.: *Долгинов С.Д.* Цифровые видеоизображения в криминалистической идентификации // Ex jure. 2022. № 3. С. 116–127.

Дактилоскопическая идентификация начала развиваться в России в начале XX в. Теоретические основы дактилоскопии были заложены в работах В.И. Лебедева «Искусство раскрытия преступлений. Дактилоскопия» (1912 г.), С.Н. Трегубова «Основы уголовной техники» (1915 г.), П.С. Семеновского «Дактилоскопия как метод регистрации» (1923 г.), а также впоследствии в работах таких ученых, как Б.М. Комаринец, Л.Г. Эджубов, С.А. Литинский, Г.Л. Грановский, А.А. Адрианов, С.И. Поташник и др.

В настоящее время дактилоскопия имеет большое значение для криминалистики, так как во время совершения преступления почти всегда имеются прикосновения, и по ним можно идентифицировать человека. Для отправки сообщения человеку также необходимо нажимать на клавиатуру персонального компьютера или экран смартфона, на которых он оставляет отпечатки.

«Дактилоскопический метод является одним из наиболее эффективных методов идентификации человека. На протяжении многих десятков лет данный метод активно применяется в практической деятельности правоохранительными органами многих государств и по праву считается одним из самых разработанных и надежных методов идентификации человека»[157].

Помимо самого папиллярного узора, человек оставляет на устройстве свои биологические следы, благодаря которым может стать возможной генетическая идентификация. Генетическая идентификация – это установление тождества биологических объектов посредством анализа ДНК или детерминируемых ею структур[158]. Идентифицирующими объектами при таком исследовании могут служить различные объекты биологического происхождения: подкожный жир, кожный эпителий, слюна или даже кровь, которые при различных обстоятельствах потенциально могут быть оставлены на устройстве. Как отмечает И.О. Перепечина,

[157] См.: *Хайруллова Э.Т., Шадрина Е.С.* Современное состояние дактилоскопической регистрации // Ученые записки казанского юридического института МВД России. 2019. Т. 4, № 2 (8). С. 92.
[158] См: *Перепечина И.О.* Генетическая идентификация личности // Криминалистика: учебник / Под ред. д-ра юрид. наук, проф. И.М. Комарова. Гл. 14. – М.: Юрлитинформ, 2023. С. 230.

«современные методы анализа ДНК позволяют обеспечивать исключительно высокую степень достоверности идентификации»[159].

Идентификация лица по биологическим следам человека – задача эксперта. Подробное рассмотрение экспертиз, объектами которых являются такие следы на устройстве, дается во втором параграфе третьей главы настоящего исследования.

Необходимо учитывать, что следы, оставленные на устройстве, дают возможность установить связь лица и устройства, однако не дают оснований признать идентифицированное таким образом лицо как автора отправленного сообщения.

Все рассмотренные потенциально идентифицирующие объекты могут стать основой для определения пользователя сети Интернет или конкретного устройства. Современные исследования во всех описанных сферах обладают большими перспективами. Благодаря ним мы действительно можем установить пользователя аккаунта, обладателя голоса, лицо на видеоизображении, лицо, прикасавшееся к устройству. Тем не менее, при всей ценности такой информации, на ее основании нельзя выполнить достоверную идентификацию лица, отправившего конкретное сообщение, а только выдвинуть относительно обоснованные версии о его характеристиках.

Таким образом, ни по одному из источников на сегодняшний момент не возможна идентификация лица в криминалистическом смысле. Установление лица, написавшего сообщение и совершившего преступление, является задачей следователя в ходе расследования и решается комплексно: использованием идентификации в алгоритме доказывания, сбором доказательств, установлением фактов с опорой на данные об идентификации пользователя в интернет-среде.

§ 4. Тактико-криминалистические особенности изъятия и фиксации электронных сообщений

[159] Там же. С. 239.

В ФЗ «Об информации, информационных технологиях и о защите информации» дано следующее определение электронного сообщения: «Электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети»[160]. Как отмечалось ранее, мы считаем, что электронное сообщение является частью электронной переписки.

При этом не подвергается сомнению, что действия правоохранительных органов по получению электронной переписки связаны с ограничением ч. 2 ст. 23 Конституции РФ, установившей право граждан на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, что допускается только на основании судебного решения.

Согласно ФЗ «О связи», «тайна связи» определена как тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи[161]. Электросвязь – любые излучение, передача или прием знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам[162].

В ст. 13 УПК РФ установлено, что ограничение тайны переписки допускается только на основании решения суда. Согласно ст. 8 ФЗ «Об оперативно-розыскной деятельности», проведение оперативно-розыскных мероприятий (включая получение компьютерной информации), которые ограничивают тайну переписки, допускается на основании судебного решения и при наличии определенных обстоятельств. Эти нормы говорят о том, что перечень действий по ограничению тайны связи носит закрытый характер и не предполагает расширительного толкования.

---

[160] См. п. 10 ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.
[161] См. ч. 1 с. 63 Федерального закона «О связи» от 07.07.2003 № 126-ФЗ // СПС «КонсультантПлюс».
[162] См. п. 35 ст. 2 Федерального закона «О связи» от 07.07.2003 № 126-ФЗ.

Содержание ст. 64 Закона «О связи» закрепляет обязанности операторов связи и ограничение прав пользователей услугами связи при проведении оперативно-розыскных мероприятий, мероприятий по обеспечению безопасности Российской Федерации и осуществлении следственных действий. Часть 1.1 этой статьи обязывает операторов связи предоставлять органам, осуществляющим оперативно-розыскную деятельность, два конкретных вида информации:

1) о пользователях услугами связи;

2) об оказанных им услугах связи, обязанность предоставление которой оператором связи не обуславливается наличием судебного разрешения.

Правила взаимодействия операторов связи с органами ОРД установлены в Постановлении Правительства РФ от 27.08.2005 № 538. Взаимодействие с органами следствия регулируется процессуальным законодательством. Данные, которые может предоставить провайдер следственным органам, содержат персональные данные лица, пользовавшегося услугами связи, и информацию о соединениях, получение которой регламентировано ст. 186.1 УПК РФ «Получение информации о соединениях между абонентами и (или) абонентскими устройствами». Данная статья предполагает обязательное наличие судебного решения.

Ст. 23 Конституции РФ предусматривает право граждан на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, а также право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Хотя в этой статье прямо не указано, что гражданин имеет право на тайну электронных сообщений, очевидно, что электронные сообщения подпадают под понятие «иные сообщения». Таким образом, изъятие электронной переписки у оператора обмена сообщениями также возможно при наличии судебного решения, независимо от того, делается ли это в рамках ОРД или в рамках предварительного расследования.

Однако ограничения, установленные для получения сообщений от операторов связи, уже не распространяются на сообщения, находящиеся на

абонентских устройствах. В Определении[163] Конституционный суд счел возможным чтение следователями переписки с телефонов, планшетов и компьютеров без соответствующего разрешения суда. В указанном определении Конституционного суда сказано, что проведение осмотра и экспертизы информации, находящейся в электронной памяти абонентских устройств, изъятых при производстве следственных действий, не предполагает вынесения об этом специального судебного решения.

Конституционный суд отметил, что «проведение осмотра и экспертизы с целью получения имеющей значение для уголовного дела информации, находящейся в электронной памяти абонентских устройств, изъятых при производстве следственных действий в установленном законом порядке, не предполагает вынесения об этом специального судебного решения. Лица же, полагающие, что проведение соответствующих следственных действий и принимаемые при этом процессуальные решения способны причинить ущерб их конституционным правам, в том числе праву на тайну переписки, почтовых, телеграфных и иных сообщений, могут оспорить данные процессуальные решения и следственные действия в суд в порядке, предусмотренном статьей 125 УПК РФ».

А.Н. Яковлев, касательно сообщений на электронной почте, пишет, что, если такое сообщение, а именно электронная информация, находится на устройстве лица, эта информация не должна охраняться тайной связи. Как только такая информация попадает в процесс отправки или пересылки, она автоматически охраняется тайной связи. После доставки на устройство адресата данные опять перестают быть охраняемыми. Следовательно, как отмечает автор, возможно «получать информацию в порядке ст. 86 УПК РФ в ходе следственных действий... Решения суда при этом также не требуется»[164].

---

[163] См.: Определение Конституционного Суда РФ от 25.01.2018 № 189-О «Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Д.А. на нарушение его конституционных прав статьями 176,177 и 195 УПК РФ» // СПС «КонсультантПлюс».

[164] См.: *Яковлев А.Н.* Правовой статус цифровой информации, извлекаемой из компьютерных и мобильных устройств: «электронная почта» // Вестник Воронежского института МВД России. 2014. № 4. С. 46.

Таким образом, как учеными, так и судебной практикой признается, что осмотр устройства и извлечение из него данных в ходе этого осмотра не требует решения суда. Однако, чтобы не возникало никаких вопросов, требуется четкая регламентация этого следственного действия. Получение данных из электронного устройства подразумевает под собой обнаружение и изъятие этих данных. Закрепление и фиксация производится специфическим способом, который осуществляется по специфическим правилам. Оно обладает признаками самостоятельного следственного действия и требует нормативного закрепления.

Ст. 164.1 УПК РФ регламентирует особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий. Электронные носители должны изыматься с участием специалиста, и при возможности информация с носителей должна копироваться, за исключением той, копирование которой может повлечь ее утрату или изменение.

Данные правила полностью применимы и к получению электронных сообщений, независимо от способа их передачи (электронная почта, мессенджеры, социальные сети). Как отмечалось ранее, электронное сообщение это – особый вид электронной связи, с помощью которого информация передается в электрической, цифровой форме с применением ЭВМ, программного обеспечения, провайдера (предоставляющего услуги сети)[165]. Если правовая защита сообщений электронной почты и мессенджеров очевидна, то отнесение к этой категории сообщений в социальной сети вызывает некоторые сложности, однако, согласно ч. 2 ст. 23 Конституции России, все имеют ряд следующих неотъемлемых прав: право на тайну переписки; право телефонных переговоров; право телеграфных, почтовых и иных сообщений[166]. Смысл толкования законов должны определять именно права и интересы граждан. Поэтому любое ограничение одного из этих прав может быть осуществлено только на основе судебного решения.

---

[165] См.: *Иванов А.Н., Силантьев Д.Н.* Выемка электронной почты в сети Интернет // URL: http://www.crime-research.org/library/Removing.html (дата обращения: 23.11.2023).

[166] См.: Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2023) // СПС «Консультант Плюс».

С точки зрения криминалистической тактики можно выделить изъятие электронной переписки, сопряженное с ***физическим изъятием*** электронного устройства, и изъятие самой переписки ***без получения доступа к устройству, с которого отправлялось сообщение.*** Изъятие переписки, сопряженное с физическим изъятием, производится в ходе выемки и осмотра устройства. Изъятие без получения доступа к устройству может производиться в ходе выемки и осмотра сервера, направления официального запроса организатору обмена сообщениями или в ходе таких ОРМ, как снятие информации с технических каналов связи, получение компьютерной информации. Все они имеют определенные тактические особенности.

В ходе изучения материалов надзорных производств прокуратуры было выявлено, что сообщения в ходе расследования чаще всего получаются при осмотре устройства (45,71%), а также путем приобщения в ходе допроса (17,14%), обыска и выемки (15,24%), в рамках компьютерно-технической экспертизы (13,33%) и путем запроса компании организатору обмена сообщениями (8,57%).

Согласно результатам проведенного нами анкетирования, чаще всего переписку удается обнаружить на устройстве, с которого она велась (85,07%), более редко она изымается с сервера организатора обмена сообщениями (8,96%) и обнаруживается на устройстве лица, не принимавшего участие в переписке, но состоящего в той же группе (общем чате) (5,97%). Изъятие электронной переписки осуществляется путем выемки (40,86%), осмотра (25%), запроса (9,62%), получения информации от допрашиваемого (12,02%), в ходе оперативно-розыскных мероприятий (12,5%).

В случае, если доступ к устройству, на котором хранится переписка, заблокирован, 13,43% опрошенных направляют запрос оператору обмена сообщениями для истребования переписки; 42,29% пытаются узнать пароль в ходе проведения запроса; 37,31% направляют устройство на экспертизу; 6,97%

используют собственные навыки и специальное программное обеспечение для получения доступа к переписке[167].

Как видно на практике, наиболее предпочтительным способом является изъятие переписки непосредственно с устройства, которое может осуществляться в ходе осмотра или экспертизы. Получение данных от оператора обмена сообщениями применяется существенно реже, что можно объяснить значительной сложностью взаимодействия, а также использованием сервисов, принадлежащих зарубежным операторам.

Исследование переписки с изъятием устройства

Как отмечает Н.А. Архипова, «проведение осмотра электронных сообщений – это необходимое действие, которое позволяет следователю определиться с объемом тех электронных сообщений, которые имеют значение для уголовного дела. Однако на изучение содержания всех сообщений может потребоваться продолжительное время, привлечение соответствующих специалистов и иных участников, поэтому данное следственное действие будет осуществлено недостаточно эффективно»[168]. Таким образом, она указывает, что при проведении выемки и осмотра электронных сообщений необходимо осуществить предварительный осмотр, а позже, в соответствии с ч. 3 ст. 177 УПК РФ, можно произвести подробный осмотр[169].

При физическом изъятии устройства не стоит забывать о возможности удаленного доступа к нему. Именно поэтому необходимо сразу же при обнаружении устройства помещать его в специальный чехол – «чехол Фарадея», который блокирует доступ к устройству и о котором говорилось ранее.

После этого устройство может являться предметом осмотра и быть приобщено в качестве вещественного доказательства, если на нем хранится важная информация. Осмотр такого устройства, как отмечалось выше, производится

[167] См. Приложение № 2.
[168] См.: *Архипова Н.А.* Тактика осмотра и выемки электронных сообщений, передаваемых по сетям электросвязи // Закон и право. 2018. № 6. С. 134.
[169] Там же.

следователем в качестве отдельного следственного действия, а вся информация с устройства фиксируется как в протоколе, так и на электронном носителе.

Как отмечает А.Б. Смушкин «в первую очередь определяется возможность включения телефона (реакция на кнопку питания, иные кнопки, датчик отпечатка пальца и др.). Следующий шаг - выявление факта установки защиты и ограничения доступа к смартфону посторонних лиц (пароль, цифровой код, графический ключ, доступ по отпечатку пальца, доступ после сканирования лица пользователя или сетчатки его глаза). При отсутствии пароля или иных мер защиты производится подробный осмотр хранящейся на телефоне информации»[170].

Другим важным подготовительным действием к осмотру места совершения компьютерного преступления или средств компьютерной техники выступает обеспечение участия понятых. В криминалистической литературе справедливо отмечается, что понятые должны обладать познаниями в области компьютерной техники и технологий[171].

Осмотр мобильных и компьютерных устройств отличается от иных видов осмотра тем, что компьютерная информация, содержащаяся в мобильном устройстве, не всегда может восприниматься человеком непосредственно органами чувств, следовательно, и осмотреть ее можно с помощью технических и программных средств. Осмотр компьютерных устройств, в том числе мобильных, – это зачастую не столько осмотр как таковой, а, скорее, техническое исследование, требующее определенных знаний.

Поэтому в некоторых случаях следователю необходимо отправлять устройство на компьютерно-техническую экспертизу. Думается, что осмотр устройства должен проводиться в тех случаях, когда доступ к интересующей информации возможен с применением обычного пользовательского программного обеспечения, например, в случае, если лицо добровольно предоставило доступ к

[170] См.: *Смушкин А.Б.* Криминалистическое исследование мобильных устройств // Электронное приложение к российскому юридическому журналу №2. 2020. С.48-52.
[171] См.: *Комиссаров В., Гаврилов М., Иванов А.* Обыск с извлечением компьютерной информации // Законность. 1999. № 3.

переписке на его устройстве. Так, согласно Приговору № 1-93/2017 от 17 марта 2017 г. по делу № 1-93/2017, «у Горбенко был изъят сотовый телефон, в котором была установлена программа "..." для переписки через Интернет. Горбенко разблокировал телефон и добровольно предоставил переписку в данной программе»[172]. Если это невозможно (например, доступ к устройству ограничен паролем или требуется поиск и исследование удаленных сообщений), то нужно направлять устройство на экспертизу.

В ходе осмотра следователь ведет протокол, в котором отражает весь его ход. При осмотре присутствуют понятые, которые наблюдают за действиями следователя и подписывают протокол. Ст. 164.1 УПК РФ также закрепляет обязательное участие специалиста при изъятии или копировании информации с электронных носителей. Н.А. Архипова отмечает, что «с учетом специфики проведения данного следственного действия специалистом может выступать работник организации, занимающийся распространением информации в сети Интернет, который поможет произвести копирование на материальный носитель»[173]. Данная позиция представляется верной, так как вышеуказанные работники обладают пониманием специфики копируемой информации.

Как отмечает В.Ф. Васюков, «в описательной части протокола осмотра указываются тип устройства, его модель, идентификационная информация, внешние атрибуты и особенности конструкции корпуса. После внешнего осмотра устройства без извлечения носителей информации (модуля(ей) SIM, карты памяти) в протоколе указывается путь к электронным сообщениям, например: "меню – значок «сообщения» – перечень сообщений – входящее сообщение от абонента с номером 8111111111, сохраненного под именем «Иван». После этого в протоколе указываются время получения/отправления сообщения, его дословное

[172] См.: Приговор Комсомольского районного суда г. Тольятти (Самарская область) № 1-93/2017 от 17 марта 2017 г. по делу № 1-93/2017 // URL: https://sudact.ru/regular/doc/tvlXejt5ag6u/?regular-case_doc=&regular-lawchunkinfo=&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=&regular-court=&regular-judge=&_=1713701172091&snippet_pos=12720#snippet (дата обращения: 20.01.2023).

[173] См.: *Архипова Н.А.* Указ. соч. С. 134.

содержание”»[174]. Мы согласны с таким планом отражения информации в протоколе, однако нужно добавить, что сначала следователю необходимо описать устройство и его технические характеристики, после чего разблокировать устройство, при наличии такой технической возможности, и описать, какие программы-приложения открыты на момент начала осмотра. Почти на всех компьютерных устройствах, как мобильных, так и стационарных, имеются специальные команды, позволяющие вывести список исполняемых программ (например, для компьютерной техники под ОС Windows это сочетание клавиш Alt+Tab). Следователь должен фиксировать все сообщения, которые он при этом видит в соответствующих программах-приложениях.

Осмотр может также сопровождаться снимками экрана. Снимок экрана на мобильном устройстве как правило выполняется путем нажатия комбинации клавиш: на iPhone это включение + увеличение громкости, на Android – питание + уменьшение громкости. Снимки экрана сохраняются в определенную папку на устройстве, на котором они были сделаны, оттуда их можно передать на собственное устройство и распечатать. На персональных компьютерах снимок экрана можно сделать также комбинацией клавиш: на Windows клавиши Win + PrtSc, на iOs – клавиши Shift + Command + 3. Снимки экрана впоследствии печатаются и прилагаются к протоколу осмотра. Если следователь стремится к минимальному внесению изменений в работу электронного устройства, он может делать снимки экрана с помощью имеющегося у него фотоаппарата.

В результате следователь получает доказательство, которое он может предоставить в суде – протокол осмотра устройства. Благодаря ему электронные сообщения, содержащие криминалистически значимую информацию, приобретают должное процессуальное оформление.

При осмотре персонального компьютера – ноутбука или десктопа – следователь включает устройство (или выводит из спящего режима), и также

---

[174] См.: *Васюков В.Ф.* Некоторые вопросы проведения следственных действий, направленных на обнаружение, фиксацию и изъятие электронных сообщений, переданных посредством мобильных абонентских устройств сотовой связи // Российский следователь. 2016. № 23. С. 15–18.

фиксирует происходящие в нем информационные процессы и имеющиеся данные. Сначала он заносит в протокол, какие программы и файлы открыты на момент осмотра, далее осматривает содержимое папок, неоткрытых программ (приложений мессенджеров, социальных сетей и иных) и файлов.

При осмотре устройства перед следователем зачастую встает вопрос об анализе большого количества сообщений, в том числе не относящихся к расследуемому событию. Собственный практический опыт позволяет сделать определенные выводы о том, по какому пути идет практика при расследовании преступлений, совершаемых с помощью мессенджеров. Так, в ходе расследования деяния, предусмотренного ст. 228.1 УК РФ «Незаконное приобретение, хранение, перевозка, изготовление, переработка наркотических средств, психотропных веществ или их аналогов, а также незаконные приобретение, хранение, перевозка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества», было установлено, что трое граждан распространяли рекламу и осуществляли продажу наркотических веществ с помощью мессенджера WhatsApp. Реклама осуществлялась с помощью массовой рассылки с предложением приобрести наркотики потенциальным покупателям. Диалог с покупателем также велся в WhatsApp. Обвиняемые получали деньги и прятали наркотическое вещество в определенном месте – тайнике, делали так называемую закладку, после чего объясняли ее местонахождение и путь к ней покупателю.

В ходе расследования у них были изъяты мобильные телефоны и получен доступ ко всем перепискам в мессенджере WhatsApp. Информация из сообщений была изъята в рамках осмотра телефона как вещественного доказательства. В процессе осмотра в протокол заносились все диалоги в WhatsApp, переписывалось каждое сообщение и описывались фотографии, поскольку на пересылаемом фото могли быть обозначены пути к тайнику. Такая практика, на наш взгляд, не может считаться оптимальным подходом. Действительно, любые сообщения, имеющие значение для доказывания, надо заносить в протокол, но

далеко не все сообщения на устройстве действительно имеют значение для доказывания. Занесение каждого сообщения в протокол осмотра – трудоемкая и слишком времязатратная процедура. Кроме того, это приводит к появлению в материалах дела большого количества бумаг, которые не только не имеют доказательственного значения, но и вообще не относятся к исследуемому событию.

Несмотря на информатизацию и цифровизацию жизни общества, отечественный процесс все еще остается бумажным и будет таковым в ближайшие годы. Поэтому, в целях процессуальной экономии, в материалы дела надо помещать только те данные, включая электронные сообщения, которые действительно относятся к предмету доказывания.

Исследование переписки без изъятия устройства

Изъятие электронной переписки возможно также ***без прямого доступа к устройству***, например, через оператора сервиса обмена сообщениями, либо путем изъятия его электронного оборудования (снятия с него электронных копий), либо путем направления запроса.

Выемка информации с сервера оператора связи осуществляется в случаях, когда невозможно получить доступ к самому устройству и снять переписку непосредственно с него.

Для этого следователь направляет в суд ходатайство о получении разрешения на выемку у оператора связи в порядке ст. 165 УПК РФ, с приложением материалов, обосновывающих ходатайство и подтверждающих необходимость изъятия сведений.

После получения решения суда, дальнейшие действия следователя зависят от того, где территориально находится офис администрации оператора обмена сообщениями, электронной почты или организатора обмена мгновенными сообщениями. Если он находится в том же городе/местности, где работает следователь, то он выносит постановление о производстве выемки и производит ее лично. Если главный офис оператора обмена сообщениями находится не в том же городе, где находится следователь, и у него нет возможности съездить самому, то

он направляет в местный следственный отдел поручение о производстве выемки, к которому прилагает решение суда. Следователь (лично или по поручению) ознакамливает представителей администрации с постановлением/поручением и решением суда. Чаще всего целесообразно предупредить оператора о предстоящей выемке, чтобы они могли подготовить нужные следствию данные. Однако, если есть понимание, что оператор не настроен сотрудничать со следствием, лучше использовать эффект внезапности. Выемка производится в порядке ст. 183 УПК РФ, оформляется протоколом.

Согласно п. 5 ст. 183 УПК РФ, до начала выемки следователь предлагает выдать предметы и документы, подлежащие изъятию, а в случае отказа производит выемку принудительно. Как правило, администрация социальной сети выдает нужные сведения самостоятельно (они копируются с серверов на электронный носитель (флеш-карта, диск) либо печатаются на бумаге). Если же следователь производит выемку принудительно (в редких случаях), то он должен руководствоваться ст. 164.1 УПК РФ, которая закрепляет особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий. Так, она предусматривает участие специалиста и порядок копирования информации с помощью технических средств. Согласно этой статье, если изъятие самого устройства невозможно (а зачастую это именно так, ведь аппаратное обеспечение сервера социальной сети очень объемное), то специалист или следователь в ходе производства следственного действия вправе осуществить копирование информации, содержащейся на электронном носителе информации. Однако, на наш взгляд, осуществить копирование всего содержимого сервера невозможно, так как для этого потребуется очень большой носитель. Для копирования информации необходимо ограничить область изымаемых данных. Область может быть выделена по дате и (или) по адресатам, например, «сообщения, отправленные пользователем А пользователю Б с 23:00 15.02.2022 по 16:00 20.02.2022». Дату и адресатов следователь может узнать в ходе следственных действий или оперативно-

розыскных мероприятиях. Если эти данные не известны, возможно провести индексированный поиск по данным и скопировать уже непосредственно те сообщения, которые имеют отношение к расследованию. Но для этого специалисту в ходе производства выемки необходимо подключить собственное оборудование с предустановленным на нем программным обеспечением для индексированного поиска. Такой поиск возможен в том числе и на сервере.

В протоколе следственного действия должны быть указаны технические средства, примененные при осуществлении копирования информации, порядок их применения, электронные носители информации, к которым эти средства были применены, и полученные результаты. Также в протоколе указывается, какая область изымаемых сообщений была скопирована и как она была ограничена – путем датирования, индексации и т. д. К протоколу прилагаются электронные носители информации, содержащие данные, скопированные в ходе производства следственного действия.

После производства выемки следователю необходимо в рамках отдельного следственного действия осмотреть полученный носитель с информацией. В протоколе осмотра он указывает что было изъято в ходе выемки - сам носитель (что бывает редко) или информация была скопирована на носитель специалиста. Если была снята копия, то в протокол заносятся технические устройства, с помощью которых осуществлялось копирование, и осматривается носитель, на который была скопирована информация. В ходе осмотра следователь фиксирует в протоколе установленные фрагменты, с указанием того, между кем велась переписка, сам текст сообщения и пояснение к нему в случае, если содержание каких-либо сообщений не до конца ясно (например, в сообщении содержатся смайлы). Электронный носитель приобщается в качестве вещественного доказательства к материалам дела. Если переписка была выдана на бумаге, она также прилагается к протоколу осмотра.

Как видно, выемка связана с существенными трудностями, поэтому, если это возможно, гораздо проще получить переписку путем ***истребования,*** т. е. ***направления официального запроса*** организатору обмена сообщениями.

Так, согласно материалам, имеющимся в Апелляционном постановлении Верховного суда Чувашской республики по делу № 22-2095[175], в ходе расследования были изъяты электронные письма с сервера сервиса электронной почты, для сравнения их с письмами, хранящимися в электронном почтовом ящике на устройстве Иванова П.А. Согласно Приговору Кировского районного суда г. Красноярска № 1-242/2018 от 9 июля 2018 г. по делу № 1-242/2018[176], у администрации сайта «znakomstva.ru» была истребована переписка, в результате изучения которой установлено 7 пользователей, которым пользователь «antonio3326» отправлял изображение порнографического характера с участием несовершеннолетнего лица.

Запрос на истребование переписки должен содержать требование о предоставлении информации и описание требуемых данных: сведения об адресатах, с которыми велась переписка, саму переписку, вложения с конкретным адресатом, IP-адрес, с которого выходил абонент запрашиваемого почтового ящика. Запрос, направляемый организатору сервиса информационного обмена, должен также содержать краткое описание (фабулу) дела, в рамках которого он направляется, и требование предоставить информацию, такую как данные аккаунта, IP-адреса выхода в сеть, номер телефона, привязанный к аккаунту и область запрашиваемых сообщений (например, дату).

Обычно российские компании, осуществляющие деятельность в сфере обмена сообщениями, предоставляют всю нужную информацию в ответ на запрос

---

[175] См.: Апелляционное постановление Верховного Суда Чувашской Республики № 22-2095/2018 от 20 сентября 2018 г. по делу № 22-2095/2018 // URL: https://sudact.ru/regular/doc/G7XjNyFHR5Lq/?regular-txt=&regular-case_doc=&regular-lawchunkinfo=&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=&regular-court=&regular-judge=&_=1713701692989&snippet_pos=1058#snippet (дата обращения: 20.01.2023).

[176] См.: Приговор Кировского районного суда г. Красноярска (Красноярский край) № 1-242/2018 от 9 июля 2018 г. по делу № 1-242/2018 // URL: https://sudact.ru/regular/doc/LxeUj9ESahoP/?regular-txt=&regular-case_doc=&regular-lawchunkinfo=&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=&regular-court=&regular-judge=&_=1713701978587&snippet_pos=7748#snippet (дата обращения: 20.01.2023).

правоохранительных органов. Однако чаще всего российские пользователи используют иностранные сервисы.

Огромное количество граждан России используют для создания электронной почты такие сервисы как Gmail (Google), Yahoo!mail, сотрудничество с которыми затруднено.

Позиция оператора Google заключается в том, что для раскрытия информации местным правоохранительным огранам им потребуется распоряжение суда и ордер на обыск: «Четвертая поправка к Конституции США и закон США "О защите информации, передаваемой с помощью электронных систем связи" (ECPA) ограничивают возможность государства принуждать поставщиков услуг к раскрытию информации пользователей. Сотрудники правоохранительных органов обязаны по меньшей мере сделать следующее»:

1) получить решение суда, которое обязывает их раскрыть данные, не являющиеся контентом, например, содержание полей «От кого», «Кому», «Копия», «Скрытая копия», «Дата отправки» в случае сообщений электронной почты;

2) получить ордер (разрешение) на обыск, который обязывает их предоставить содержание переписки, например, электронные письма, документы и фотографии.

Что касается запросов от государственных органов за пределами США, Google готовы сотрудничать и предоставлять данные, если это не противоречит вышеназванному закону США «О защите информации, передаваемой с помощью электронных систем связи» (ECPA); законодательству страны, органы которой направили запрос; международным нормам, а именно принципам свободы самовыражения и конфиденциальности (одобрены Комитетом министров ЕС)[177] и правилам Google.

[177] См.: Global network initiative [сайт]. Международные принципы свободы выражения и конфиденциальности в сети закреплены в Глобальной сетевой инициативе (Global Network Initiative). Защита и развитие свободы выражения мнений и неприкосновенности частной жизни в информационно-коммуникационных технологиях // URL: https://globalnetworkinitiative.org/ (дата обращения: 20.01.2023).

Согласно Международным принципам свободы выражения и конфиденциальности в сети[178], «право на неприкосновенность частной жизни не может быть ограничено правительством, исключением могут быть только определенные обстоятельства в рамках международных стандартов. Такие ограничения должны соответствовать преследуемой цели. Компании-участники указанных Принципов обязуются применять средства защиты персональных данных во всех странах, где они ведут свою деятельность, в целях работы над защитой права пользователей на неприкосновенность частной жизни, а также уважать права пользователей на неприкосновенность частной жизни и защищать их». Разумеется, этот документ не является международным договором в строгом смысле этого слова, однако он обязателен для всех компаний, подписавших его. Среди ведущих операторов электронной почты, которые поддерживают данный документ, числятся Google, Microsoft.

Такие правила говорят о том, что для раскрытия информации о пользователе правоохранительные органы должны предоставить в запросе довольно веские основания. Раскрывать данные или нет – всегда будет оставаться вопросом на усмотрение компании. Разумеется, большинство известных сервисов, предоставляющих услуги электронной почты на международном уровне, являются участниками этой Глобальной сетевой инициативы.

Мессенджерами, которыми привыкли пользоваться современные российские пользователи, также владеют иностранные компании. Однако и с ними возможно сотрудничество и истребование данных.

«Обмен информацией о компьютерных инцидентах с уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, осуществляется Национальным координационным центром по

[178] См.: Декларация о свободе обмена информацией в интернете (принята Комитетом Министров Совета Европы от 28.05.2003 на 840-м заседании заместителей Министров) // СПС «КонсультантПлюс».

компьютерным инцидентам, за исключением случаев, когда обмен субъекта критической информационной инфраструктуры такой информацией напрямую с иностранной (международной) организацией предусмотрен международным договором Российской Федерации»[179].

С.П. Щерба приводит следующий алгоритм действия при необходимости получения данных от иностранных поставщиков услуг в сфере информационно-компьютерных технологий:

1. Первым делом необходимо направить запрос о сохранении интересующих данных, так как сроки хранения коммуникаций в разных странах могут существенно отличаться и быть непродолжительными. Такой запрос направляется провайдеру, по каналам правоохранительного сотрудничества.

Так, например, руководство мессенджера WhatsApp[180] со своей стороны предлагает[181] предпринять меры в интересах правоохранительных органов по сохранению данных аккаунтов в течение 90 дней в связи с официальным следствием по уголовному делу в случае, если к ним поступит имеющий законную силу запрос на сохранение этих данных. Существует возможность безотлагательно подать подобный запрос, используя онлайн-систему для запросов от правоохранительных органов. Применение этой системы возможно и в случаях, требующих немедленного раскрытия информации, под которыми руководство мессенджера понимает неминуемую опасность для ребенка, смертельную опасность или риск причинения тяжкого вреда здоровью любого лица.

---

[179] См.: п. 11 Приложения № 1 Приказа ФСБ России от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения» // СПС «Гарант».

[180] Мессенджер WhatsApp принадлежит Meta. Деятельность компании Meta Platforms Inc. на территории РФ запрещена.

[181] См.: WhatsApp: официальный сайт. Информация для правоохранительных органов // URL: https://faq.whatsapp.com/26000050 (дата обращения: 12.01.2023).

2. Далее необходимо направить запрос о предоставлении данных об абоненте и используемом им оборудовании;

3. При необходимости получения данных о соединениях между абонентами и абонентскими устройствами запрос направляется в компетентные органы соответствующего государства в порядке ст. 453 УПК РФ.

4. При необходимости получения данных о содержании сообщений (контенте), включая предусмотренные ч. 7 ст. 185 УПК РФ осмотр и выемку электронных сообщений или иных передаваемых по сетям электросвязи сообщений, запрос о правовой помощи направляется в компетентные органы иностранного государства в порядке ст. 453 УПК РФ с приложением соответствующего постановления российского суда или его заверенной копии. Необходимо учитывать, что понятие контента может различаться в зависимости от страны. В США, например, к таковому отнесены также данные геолокации и аватары.

5. При необходимости проведения оперативно-розыскных мероприятий, связанных с получением информации об абонентских соединениях или о содержании сообщений (контроль сообщений, прослушивание переговоров, снятие информации с технических каналов связи, получение компьютерной информации) в компетентные органы иностранного государства может быть направлен запрос об оказании содействия в их проведении, в особенности если в иностранном государстве ведется параллельное производство по тем же фактам. Однако большинство стран требуют обращения за проведением подобных мероприятий исключительно в рамках процедуры правовой помощи, а не правоохранительного содействия[182].

С.П. Щерба также отмечает, что при составлении международного «запроса о сохранении или предоставлении электронных доказательств необходимо обеспечивать его максимальную конкретизацию, в частности, приводя точные

[182] См.: Собирание электронных доказательств по уголовным делам на территории России и зарубежных стран: опыт и проблемы / Под общ. и науч. ред. С.П. Щербы. – М.: Проспект, 2022. – С. 82–87.

данные о времени доступа к информационному ресурсу в сети Интернет, вплоть до секунды, сведения о часовом поясе, об IP-адресе посещенного ресурса (внешнего сайта), название протокола или номер порта, по которому происходило соединение, без которых исполнение запроса зарубежными партнерами может оказаться невозможным»[183].

Разумеется, результаты и возможности такого сотрудничества напрямую зависят от страны, действующих международных договоров и самой компании, предоставляющей услуги обмена сообщениями.

Например, подход оператора WhatsApp заключается в том[184], что раскрыть данные аккаунта они могут только в соответствии с их Условиями предоставления услуг и применимыми законами, в том числе Stored Communications Act[185] (Законом о сохраненных сообщениях), 18-й свод законов США, разделы 2701–2712, согласно которому: «Для раскрытия основной информации пользователя, включая имя, начало предоставления услуг, время последнего использования приложения, электронный адрес и IP-адрес, требуется имеющий законную силу судебный запрос в рамках официального уголовного расследования».

Для раскрытия определенных записей и другой информации аккаунта (не включающей в себя содержимого материалов), такой как номера абонентов, заблокировавших пользователя и заблокированные им, в дополнение к основной информации абонента, указанной выше, также требуется судебный ордер, выданный на основании § 2703(d) 18-го раздела Кодекса США, который гласит, что ордер может быть выдан любым судом, в компетенции которого находится рассмотрение данного вопроса, однако только в том случае, если правительственный орган предоставит конкретные и поддающиеся изложению факты, свидетельствующие о наличии разумных оснований полагать, что

[183] Там же. С. 87–88.
[184] См.: WhatsApp: официальный сайт. Информация для правоохранительных органов.
[185] См.: Stored Communications Act: Reform of the Electronic Communications Privacy Act (ECPA) / Congressional research service. 2015 // URL: https://fas.org/sgp/crs/misc/R44036.pdf (дата обращения: 12.01.2020).

запрашиваемая информация имеет отношение к текущему уголовному расследованию[186].

Для раскрытия сохраненных материалов любого аккаунта требуется ордер на обыск и достаточные для него основания. Администрация WhatsApp не хранит сообщения и журналы действий более 30 дней.

Что касается требований к иностранным судебным приказам, то WhatsApp раскрывают данные аккаунтов также только в соответствии с их условиями предоставления услуг и применимым законодательством. Кроме того, они рассматривают эти запросы на предмет соответствия международным стандартам, включая права человека, надлежащие правовые процедуры и принцип верховенства закона, для раскрытия данных аккаунта может потребоваться запрос об оказании взаимной правовой помощи или судебное решение.

Однако далеко не все мессенджеры готовы сотрудничать с правоохранительными органами и спокойно раскрывать информацию, а некоторые даже не смогут предоставить никакие данные. К таким относится, например, мессенджер Signal. У него нет оператора в общепринятом смысле, а его разработкой занимается некоммерческий фонд Signal Technology Foundation. Все сообщения, отправленные в это мессенджере, подвергаются E2E шифрованию, т. е. шифрованию «из конца в конец». В данном случае только общающиеся между собой пользователи могут читать сообщения, что исключает доступ к ним операторов связи, провайдеров и любых иных лиц.

Также не все сервисы электронной почты смогут предоставить информацию в ответ на запросы правоохранительных органов. К ним относятся, например, сервисы электронной почты Tutanota или ProtonMail. Суть работы таких сервисов заключается в кодировании передаваемых сообщений, и третья сторона (включая сам сервис) не может получить к ним доступ. В таком случае вряд ли получится истребовать информацию у оператора сервиса. Для получения доступа к переписке

[186] См.: 18 U.S. Code § 2703 – Required disclosure of customer communications or records // URL: https://www.law.cornell.edu/uscode/text/18/2703 (дата обращения: 10.10.2023).

с использованием этих сервисов необходимы такие приемы, как взлом электронного почтового ящика и подбор ключей шифрования к письмам.

Взлом электронного ящика не относится к законным источникам получения доказательственной информации в рамках расследования. Но, если сервис, предоставляющий услуги электронной почты, не сотрудничает с правоохранительными органами, единственным способом собрать какие-либо данные о владельце может служить взлом[187] аккаунта. Иногда такие данные могут быть важными не только для удачного расследования, но и для спасения чьей-то жизни. Письма, хранящиеся в электронном почтовом ящике, могут указать на владельца и даже на его местонахождение. Поэтому, на наш взгляд, такой несанкционированный доступ должен иметь место, разумеется, при достаточных основаниях полагать, что он даст доступ к действительно важной информации и при наличии судебного решения. Очевидно, что такой взлом, как и использование вредоносных программ, должен проводиться исключительно в рамках оперативно-розыскного мероприятия – получение компьютерной информации и при наличии мотивированного решения судьи[188].

[187] В данном случае под взломом понимается доступ к электронной информации без разрешения владельца аккаунта и оператора.

[188] См., например, Определение Конституционного Суда РФ от 20.03.2007 № 178-О-О «Об отказе в принятии к рассмотрению жалобы гражданина Донского Александра Павловича на нарушение его конституционных прав пунктами 4 и 6 части первой и частью третьей статьи 6 Федерального закона “Об оперативно-розыскной деятельности” и статьями 13, 89 и 186 Уголовно-процессуального кодекса Российской Федерации».

Глава 3. Использование электронных сообщений в расследовании преступлений.

§ 1. Использование данных об электронных сообщениях в процессе допроса подозреваемого (обвиняемого)

Вопросы использования цифровых доказательств при допросе рассматривались в некоторых работах, например: Е.К. Антонович «Использование цифровых технологий при допросе свидетелей на досудебных стадиях уголовного судопроизводства (сравнительно-правовой анализ законодательства Российской Федерации и законодательства некоторых иностранных государств)»; И.П. Пономарев «Цифровое алиби и его проверка»; А.В. Платенкин «Особенности использования электронных доказательств при проведении допроса подозреваемого»; Н.А. Иванов «Применение специальных познаний при проверке “цифрового алиби”».

Как отмечает Е.К. Антонович, «при всем многообразии подходов значение информационных технологий при собирании, проверке и оценке показаний свидетеля можно рассматривать по следующим основным направлениям: как средство фиксации следственного действия, как способ установления фактических обстоятельств, имеющих значение для дела, как средство обеспечения производства следственного действия и как средство передачи информации»[189]. Действительно, цифровизация поспособствовала увеличению возможностей следователя при сборе показаний как у свидетеля, так и у подозреваемого, обвиняемого. Но в данном параграфе для нас имеет значение именно использование цифровых технологий при допросе как способ установления фактических обстоятельств. Доказанный факт того, что подозреваемый или обвиняемый в момент совершения преступления работал на компьютере не в месте

[189] См.: *Антонович Е.К.* «Использование цифровых технологий при допросе свидетелей на досудебных стадиях уголовного судопроизводства (сравнительно-правовой анализ законодательства Российской Федерации и законодательства некоторых иностранных государств)» С. 1 // СПС «Консультант Плюс».

совершения преступления, за рубежом получило условное название «цифрового алиби» (digital alibi)[190]. По мнению Н.А. Иванова, «факт “цифрового алиби” будет доказан лишь в том случае, когда показания подозреваемого о том, что в момент совершения преступления он работал со средствами компьютерной техники, совпадут с данными, которые будут получены в результате проведения компьютерно-технической экспертизы»[191].

И.П. Пономарев отмечает, что «в обоснование заявляемого алиби все чаще ссылаются на то, что в момент совершения преступления они осуществляли взаимодействие с какими-либо электронными системами (работали с персональным компьютером, пользовались мобильным телефоном, попадали в поле зрения систем видеонаблюдения, авторизовались в системах контроля доступа в помещение и т. д.), находящимися в другом месте»[192]. В настоящее время технические средства играют такую большую роль в жизни людей, что, действительно, многие подтверждают те или иные факты использованием технического устройства, в том числе отправкой электронных сообщений. Поэтому мы согласны с позицией И.П. Пономарева, который также отмечает, что необходимо учитывать следующее: «…2) основным источником формирования доказательств, подтверждающих либо опровергающих цифровое алиби, выступает информация, находящаяся в цифровой форме на машинных носителях; 3) данная информация благодаря своей природе легко может быть создана, изменена (модифицирована) и уничтожена, в том числе и в целях ее фальсификации для последующего обеспечения доказательств ложного алиби»[193]. Следователю, при проведении допроса стоит учитывать, что, с одной стороны, информацию из цифровых источников, в том числе электронных сообщений, легко проверить (так

---

[190] См.: *Иванов Н.А.* Применение специальных познаний при проверке «цифрового алиби» // URL: https://wiselawyer.ru/poleznoe/15880-primenenie-specialnykh-poznanij-proverke-cifrovogo-alibi?ysclid=lu8uhw6n54525886018 (дата обращения: 10.10.2023).
[191] См.: *Иванов Н.А.* Применение специальных познаний при проверке «цифрового алиби».
[192] См.: *Пономарев И.П.* Цифровое алиби и его проверка» // Вестник Воронежского государственного университета. 2011. № 2 (11). С. 440.
[193] Там же.

как там, как правило, указывается дата, время, место отправки – так называемые метаданные), но с другой – такую информацию довольно легко фальсифицировать.

Л.Б. Краснова справедливо отмечает, что «техническая проверка такого алиби является весьма трудной задачей, т. к. достаточно просто отследить владельца цифрового устройства, однако сложно доказать, какой конкретно человек использовал это устройство в конкретный момент времени. Однако правильно проведенный допрос лица, заявившего о наличии у него “цифрового алиби”, может разрешить эти вопросы»[194].

В ходе анализа электронной переписки в процессе расследования следователь получает определенный объем информации, которую можно использовать при проведении дальнейших следственных действий. Весьма эффективным является использование данных из электронных сообщений при допросе[195].

Информация из электронных сообщений, которую следует использовать в процессе допроса, может быть следующей:

1. Метаданные (дополнительная, сопутствующая информация о сообщении):
   1.1. Дата и время отправки;
   1.2. С какого аккаунта / номера телефона / адреса / под каким никнеймом было отправлено сообщение;
   1.3. Адресат, которому предназначалось сообщение (лицо, на которое был зарегистрирован мобильный номер, обладатель аккаунта в социальной сети, почтового ящика или его никнейм);
   1.4. Данные об устройстве и выходе в сеть (IP-адрес, MAC-адрес).
2. Информация, содержащаяся в самом сообщении:
   2.1. Информация о том, что расследуемое деяние имело место;
   2.2. Информация о месте и времени совершения расследуемого деяния

[194] См.: *Краснова Л.Б.* Компьютерные объекты в уголовном процессе и криминалистике: учебное пособие / Науч. ред. В.А. Мещеряков. – Воронеж: Изд-во Воронеж. гос. ун-та, 2006. – С. 114.
[195] См.: Печникова Р.Б. Использование данных об электронных сообщениях в процессе допроса подозреваемого (обвиняемого) // Евразийский юридический журнал. 2023. № 7 (182). С. 354

2.3. Информация о лицах, причастных к деянию или обладающих релевантной информацией о нем;

2.4. Информация об обстановке расследуемого события.

Типовые ситуации допроса подозреваемого (обвиняемого) обуславливаются объемом имеющихся в распоряжении у следователя доказательств. Именно поэтому определение того, какая именно имеется информация у следователя, должно быть его первым шагом в подготовке к допросу, так как понимание характера имеющейся информации позволит определить и выстроить тактику допроса. Как отмечает А.В. Платенкин, «особое значение для допроса лица, заявившего “цифровое алиби”, имеет его подготовительный этап»[196]. Следственные ситуации, возникающие при допросе с использованием электронных сообщений, можно разделить в зависимости от того, что следователь считает более существенным источником доказательственных данных – сами сообщения или сведения, которые он рассчитывает получить в ходе допроса с их помощью. Соответственно, информацию из сообщений можно разделить на:

– недостаточную, которую необходимо восполнить путем допроса;

– достаточную, которую необходимо дополнительно подтвердить в процессе допроса.

В первой ситуации следователю рекомендуется использовать такие приемы, позволяющие выяснить нужную информацию у допрашиваемого:

1) *прием косвенного вопроса.* Следователю необходимо начать вести с подозреваемым беседу, в ходе которой характер поставленных вопросов не должен позволить допрашиваемому понять, что следователь осведомлен о содержании его переписки, но вопросы должны касаться именно тех обстоятельств, которые в ней освещаются. При этом вопросы должны касаться как обстоятельств, которые известны из переписки, так и тех, которые в ней не приведены. Сопоставление полученных показаний по тем обстоятельствам, которые могут быть проверены,

[196] См.: *Платенкин А.В.* Особенности использования электронных доказательств при проведении допроса подозреваемого // World science. 2016. Vol. 4, № 5 (9). С. 9.

может дать основание для вывода о достоверности показаний по другим вопросам и оценить тем самым искренность допрашиваемого. Однако этот прием не будет очень эффективным в тех случаях, когда допрашиваемый догадывается о наличии его переписки у следователя, например, когда у него изъято мобильное устройство;

2) *внезапный вопрос или внезапное предъявление доказательств.* После беседы следователю необходимо внезапно задать конкретный вопрос, чтобы у допрашиваемого не было времени подготовиться. Например, лицо рассказывает о круге общения, знакомых, в том числе о потерпевшем. Следует неожиданно спросить: «А почему же Вы тогда ему написали?». Суть данного приема заключается в использовании психологического шока, который может возникнуть у допрашиваемого из-за того, что фактическая осведомленность следователя оказалась существенно выше, чем он предполагал. После этого желательно продолжать «психологическую атаку», быстро задавая все новые и новые вопросы, а также используя стимулирующие приемы, побуждающие допрашиваемого отвечать скорее. В результате можно будет добиться показаний по тем вопросам, которые в переписке отсутствовали. При этом данный прием также может оказаться неэффективным в том случае, если допрашиваемый догадывается о том, что следователь мог ознакомиться с его перепиской.

М.Е. Игнатьев под тактическим приемом фактора внезапности предлагает понимать предпринятые следователем действия (бездействие), явившиеся неожиданностью для того, кому они адресованы[197]. Он также отмечает, что использование фактора внезапности – это мощный тактический прием в достижении поставленных следователем целей. Внезапное предъявление доказательства применительно к электронному сообщению заключается в том, что следователь должен неожиданно предъявить допрашиваемому изобличающие его доказательства, например, показать текст сообщений.

[197] См.: *Игнатьев М.Е.* Фактор внезапности, его процессуальное и криминалистическое значение для расследования преступлений. – М.: Юрлитинформ, 2004. – С. 22.

Психологические и мыслительные механизмы ложных показаний значительно сложнее, чем правдивых. Поэтому при неожиданных высказываниях или действиях следователя лгать становится намного сложнее. Допрашиваемому необходимо так дополнить и скорректировать свои показания, чтобы привести их в соответствие с внезапно полученной от следователя информацией. Это сложный процесс, требующий умственных и психологических усилий. В условиях ограниченного времени и сильного волнения попытки решить такую задачу могут привести к психологической фрустрации и надлому. Этой ситуацией можно воспользоваться, чтобы добиться правдивых показаний;

3) *опережающий вопрос.* В данном случае следователю необходимо сформулировать вопросы, используя сведения, полученные из переписки, чтобы создать у допрашиваемого преувеличенное представление об осведомленности следователя и склонить его к сотрудничеству к даче показаний, убедив, что у правоохранительных органов достаточно оснований для его изобличения. Возможно, следует уточнить какую-либо специфическую деталь или обстоятельство, чтобы у допрашиваемого создалось впечатление, что все остальное уже известно. Сюда хорошо применим аргумент о двухфакторной аутентификации. Если следователю известно, что для входа в аккаунт, с которого велась переписка, установлена двухфакторная аутентификация, можно использовать это как веский аргумент в пользу того, что именно подозреваемый писал сообщения с данного аккаунта, учитывая, что только он мог иметь доступ к телефону, а значит, только он мог войти в аккаунт.

Во второй ситуации у следователя достаточно информации, которую необходимо только подтвердить в процессе допроса. Но наличие у негодостаточной совокупности уличающих доказательств еще не означает, что с их помощью можно во всех случаях получить от допрашиваемого правдивые показания. Следователю необходимо тактически правильно распорядиться имеющимся объемом доказательственной переписки, чтобы подтвердить факты в расследуемом событии.

Тактические действия следователя зависят от того, какую задачу при допросе он ставит перед собой – проверка достоверности показаний или изменение установки допрашиваемого на дачу ложных показаний. В первом случае нет необходимости предъявлять переписку, нужно только фиксировать показания, а потом сравнить их с данными переписки, оценить совпадения и противоречия, определить их доказательственное значение. Второй случай требует использования специальных тактических приемов.

Например, полезным может стать *прием детализации показаний*. Это классический способ проверки алиби при допросе подозреваемого, однако при наличии у следователя электронной переписки детализация становится более доступным и актуальным приемом. Метаданные, такие как время отправки, время выхода в сеть, адреса, помогут следователю проверить детальный рассказ подозреваемого и уличить его во лжи в случае нахождения неточностей в рассказе.

Также полезным будет *прием предъявления логической цепочки доказательств*. Начинать следует с сообщений, содержащих простые факты и постепенно переходить к изобличающим. Но в некоторых случаях рекомендуется предъявить всю переписку сразу, чтобы подозреваемый оценил ситуацию и понял, что нет смысла скрывать вину.

С тем, какие именно использовать приемы при допросе, следователю необходимо определиться еще на стадии подготовки. Она должна также включать в себя оценку ситуации и психологического состояния допрашиваемого, продумывание перечня вопросов и способа демонстрации сообщений (на электронном устройстве, в распечатанном виде и пр.).

Е.Е. Центров отмечает, что «для криминалистов очень важно … принимать во внимание зависимость поведения людей от их определенных личностных особенностей и тех ситуаций, в которых они оказываются в связи с совершенным преступлением и проводимым расследованием»[198]. Такие психические и

[198] См.: *Центров Е.Е.* Руководство по следственной тактике: монография / Е.Е. Центров. – Москва : Норма : ИНФРА-М, 2024,С.86.

личностные особенности подозреваемого могут прослеживаться в его переписке, сообщениях, поведении в сети Интернет. «Орудия, средства преступления, способ совершения преступления подбираются виновным на основе его жизненного опыта, профессиональных, преступных навыков Он действует в криминальной ситуации так, как привык действовать, как действовал в аналогичных ситуациях раньше. Для преступника независимо от того, совершает он преступление один или в группе, или даже если преступление совершает группа лиц, характерен определенный почерк, определенная совокупность способов совершения преступления»[199]. Так, мы можем узнать качества, навыки и особенности лица по его жизни и поведению в сети Интернет и связать их с его способом совершения преступления. Активность в социальных сетях может свидетельствовать о навыках, психологическом складе, отношению к определенным людям и объектам и пр. А это уже позволяет делать выводы о мотивации, заинтересованности в определенных событиях и готовности к совершению определенных действий.

Применительно к использованию информации из электронных сообщений в допросе необходимо выделить и рассмотреть следующие ситуации:

1) допрашиваемый отрицает авторство сообщений;

2) допрашиваемый вел переписку за другое лицо.

В обоих случаях следователю необходимо тщательно подготовиться к допросу. Ему нужно по возможности иметь распечатанные выдержки переписки для внезапного ее предъявления допрашиваемому. Более эффективным будет также иметь на руках результаты лингвистической или психолого-лингвистической экспертизы.

Также в ходе подготовки к такому допросу следователю рекомендуется получить консультацию специалиста, чтобы грамотно сформулировать вопросы для допроса. Необходимо учитывать, что допрашиваемый может быть хорошо

[199] См.: *Центров Е.Е.* Расследование преступлений: учет и преодоление современных тенденций, присущих криминальной среде // Вестник Московского университета. Сер. 11 Право. 2014. № 4. С. 75.

подкован в области информационных технологий и использовать сложную техническую информацию, чтобы запутать следователя.

Опираясь на информацию, полученную из электронных сообщений, следователь может использовать приемы психологического воздействия, например, создание на основе информации из переписки преувеличенного впечатления у допрашиваемого лица об объеме осведомленности следователя (например, опережающий вопрос).

Необходимо также отметить, что предъявление электронной переписки в ходе допроса также подлежит обязательной фиксации в протоколе. Согласно ч. 3 ст. 190 УПК РФ, «если в ходе допроса допрашиваемому лицу предъявлялись вещественные доказательства и документы, оглашались протоколы других следственных действий и воспроизводились материалы аудио- и (или) видеозаписи, киносъемки следственных действий, то об этом делается соответствующая запись в протоколе допроса»[200]. Следователю необходимо записывать в протоколе то, как и какие фрагменты электронной переписки были предъявлены подозреваемому и как он их пояснил. Обязательно указать то, в какой форме переписка была продемонстрирована. Если это была электронная форма, нужно указать носитель (приобщенный к материалам дела) и устройство, с которого она была показана, если же это была распечатанная на бумаге переписка, то она также должна быть приобщена к материалам уголовного дела.

§ 2. Судебно-экспертное исследование электронных сообщений.

Судебно-экспертное исследование играет важную роль для использования электронной переписки в качестве доказательства.

Вопросы судебно-экспертного исследования электронных доказательств, в том числе электронных сообщений, рассматривались Е.Р. Россинской в работах «Теория информационно-компьютерного обеспечения криминалистической

[200] См. ч. 3 ст. 190 Уголовно-процессуального кодекса РФ // СПС «КонсультантПлюс».

деятельности», «Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе», коллективом авторов кафедры криминалистики МГУ им. М.В. Ломоносова в монографии «Электронные носители информации в криминалистике»; вопросы лингвистических знаний в криминалистике и автороведческих экспертиз изучались в трудах таких авторов, как Е.И. Галяшина, Ф.О. Байрамова, Ю.Н. Баранов, А.В. Громова, Т.В. Назарова. Вопросам, связанным с экспертизой материальных следов на устройствах, генетической идентификации личности и ДНК-анализа, посвящены работы И.О. Перепечиной и других авторов.

Как отмечал В.Я. Колдин, «важный аспект расследования в этих случаях состоит в том, что собирание и исследование доказательств не может быть осуществлено без использования специальных познаний в области *современных информационных технологий*»[201]. Поэтому при разработке данной части исследования автору необходимо было обращаться к публикациям ученых в смежных областях, таких как информационные технологии и информационная безопасность. К таким исследованиям относятся следующие: «Форензика-компьютерная криминалистика» Н.Н. Федотова, «Методика идентификации интернет-пользователя на основе стилистических и лингвистических характеристик коротких электронных сообщений» А.А. Воробьевой, «Структура программного комплекса для исследования подходов к идентификации авторства текстов» А.С. Романова.

По мнению Е.Р. Россинской, процессы цифровизации в раскрытии и расследовании преступлений проявляются через широкое использование цифровых средств фиксации, сохранения, автоматизированной обработки и исследования доказательственной и ориентирующей информации, а также через новые виды криминалистически значимой информации, фиксируемой на компьютерных носителях[202]. Мы с данным высказыванием согласны и считаем, что

[201] См.: *Колдин В.Я.* Вещественные доказательства… С. 690.
[202] См.: *Россинская Е.Р.* Теория информационно-компьютерного обеспечения криминалистической деятельности: монография. – М.: Проспект, 2022. – С. 15.

процессы цифровизации в расследовании обязывают следователя обладать познаниями в области информационных технологий и техническими средствами. Е.Р. Россинская и И.А. Рядовский также отмечают, что «предварительное исследование, предшествующее назначению судебной экспертизы, возможно провести в рамках осмотра предметов с привлечением специалиста, с использованием многофункциональных возможностей универсальных криминалистических комплексов с высоким уровнем автоматизации»[203]. Действительно, наличие познаний и навыков работы с цифровыми устройствами у следователя неоспоримо, однако этого может быть недостаточно. Без помощи эксперта электронную переписку можно утратить, не получить доступ к ней или неправильно истолковать. Это поднимает проблему разграничения задач следователя, эксперта и специалиста в работе с такими доказательствами, как электронные сообщения.

Основная процессуальная форма использования специальных знаний в исследовании электронной переписки – это судебная экспертиза. Однако участие специалиста в сборе доказательств также необходимо и прямо предусмотрено УПК РФ[204]. Как пишет В.Я. Колдин, «именно экспертные исследования обеспечивают получение результатов, имеющих наибольшее доказательственное значение при исследовании аппаратных средств, программного обеспечения и компьютерной информации. В этих условиях первоочередными задачами следователя являются поиск, фиксация, изъятие с помощью специалистов и представление эксперту необходимых материальных объектов – носителей компьютерной информации»[205]. Наша позиция совпадает с высказыванием В.Я. Колдина, действительно, основными задачами следователя должны являться правильный сбор, фиксация и хранение электронных сообщений (на устройстве или вне его) для дальнейшего

[203] См.: *Россинская Е.Р., Рядовский И.А.* Тактика и технология производства невербальных следственных действий по делам о компьютерных преступлениях: теория и практика // Киберпространство. 2021. Т. 74, № 9 (178). С. 106.
[204] См.: Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // СПС «КонсультантПлюс».
[205] См.: *Колдин В.Я.* Вещественные доказательства… С. 690.

предоставления в качестве материала для исследования в ходе судебно-экспертных исследований.

В процессе исследования нами было проанализировано 100 судебных решений по уголовным делам, в расследовании которых в качестве доказательств использовались электронные сообщения[206]. В результате данного анализа было выявлено, что по 50% дел в отношении электронной переписки назначается судебная компьютерно-техническая экспертиза, в 37% – экспертизы речи и текста (22% – лингвистическая экспертиза,4% – автороведческая, 11% – психолого-лингвистическая), в 8% – фоноскопическая экспертиза голосовых сообщений, в 3% – экспертизы видеоматериала (2% – портретная экспертиза видеозаписей, 1% – видеотехническая экспертиза), в 2% дел – молекулярно-генетическая экспертиза следов на устройстве.

Таким образом, в процессе расследования дел, в ходе которого происходит исследование электронных сообщений, назначаются следующие виды экспертиз (в порядке убывания по частоте назначения):

1) компьютерно-техническая;

2) автороведческая и лингвистическая;

3) психолого-лингвистическая;

4) фоноскопическая;

5) экспертизы видеозаписей;

6) экспертизы материальных следов.

Рассмотрим каждую из них подробнее.

1. Компьютерно-техническая экспертиза

«Судебные компьютерно-технические экспертизы (СКТЭ) производятся в целях определения статуса объекта как компьютерного средства, выявления и изучения его роли в расследуемом преступлении, а также получения доступа к информации на носителях данных с последующим всесторонним ее исследованием. Общим предметом СКТЭ являются факты и обстоятельства,

[206] См. Приложение № 4.

устанавливаемые на основе исследования закономерностей разработки и эксплуатации компьютерных средств, обеспечивающих реализацию информационных процессов, которые зафиксированы в материалах уголовного дела»[207]. Согласно результатам анкетирования, 82,76% следователей предпочитают самостоятельно осматривать устройство, и 17,24% назначают экспертизу или привлекают специалиста[208]. На наш взгляд, важность экспертных исследований недооценена. Специальные знания необходимы для исследования компьютерных средств, и назначение компьютерно-технической экспертизы в ходе расследования очень часто необходимо. Разумеется, это не исключает важности для следователя обладать навыками работы с компьютерной информацией.

Изучение компьютерной информации, начавшееся в рамках экспертных исследований, быстро показало, что для адекватного решения практических задач, возникающих в ходе расследования, только экспертных исследований недостаточно. Проблематика компьютерной информации вышла за пределы экспертного исследования и стала предметом изучения криминалистической техники[209]. Поэтому для грамотного расследования преступления нельзя возлагать все надежды не только на эксперта, следователю также необходимо прилагать усилия. Важно не только предоставить правильные образцы для исследования, но и выстроить верное взаимодействие с экспертом, которое заключается в первую очередь в правильной постановке вопросов на его разрешение. Также, как отмечает М.В. Жижина, «следователь должен быть максимально “экономным” при подготовке объектов к проведению экспертизы». Необходимо быть максимально внимательным к «качеству, количеству и подготовленности таких объектов»[210].

Н.Н. Федотов[211] полагает, что для формулировки вопросов для СКТЭ всегда следует привлекать специалиста. Это может быть специально приглашенный

---

[207] См.: *Россинская Е.Р.* Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе. – М: Норма, 2006. – С. 218.
[208] См. Приложение № 2.
[209] См.: *Ткачев А.В.* Исследование компьютерной информации в криминалистике // Эксперт-криминалист. 2012. № 4. С. 5–8.
[210] См.: *Жижина М.В., Завьялова Д.В.* Указ. соч. С. 51.
[211] См.: *Федотов Н.Н.* Указ. соч. С. 132.

эксперт или неофициальная консультация. В крайнем случае, сам специалист, которому предстоит проводить КТЭ, поможет следователю верно поставить вопросы. Полезным будет предварительно проконсультироваться с экспертом для определения корректных формулировок и правильной постановки вопросов, учитывая характер носителя, предоставляемого для исследования, его состояние и обстоятельства получения.

Получив в свое распоряжение устройство с хранящейся на ней электронной информацией или ее образом, следователь должен решить, какие вопросы он может вынести на разрешение эксперта. Это могут быть: извлечение всех сообщений, включая удаленные; проведение индексированного поиска по ключевым словам; поиск метаданных; поиск информации и получение к ней доступа. Неприемлемо выносить на разрешение эксперта вопросы о правомерности доступа к компьютерной информации, об оценке содержания найденной информации, переписки, о наличии признаков преступления в тексте сообщений.

Вопросы, выносимые на разрешение эксперта при назначении компьютерно-технической экспертизы, должны быть направлены на установление конкретных обстоятельств расследуемого события, соответствовать уровню подготовки и инструментальному оснащению экспертов экспертного учреждения, должны соответствовать представляемым на исследование вещественным доказательствам[212], т. е. устройствам или носителям.

При назначении компьютерно-технической экспертизы мы предлагаем выносить на разрешение эксперта следующие вопросы (разумеется, с учетом информации о расследуемом событии и с опорой на типовые вопросы[213]):

1. Каково целевое назначение представленного носителя информации?

2. Каков вид (тип, модель, марка) представленного носителя информации?

---

[212] См.: *Саенко Г.В., Тушканова О.В.* Компьютерная экспертиза. Исследование компьютерной информации. – М.: ЭКЦ МВД России, 2010. – С. 199.

[213] Там же.

3. Доступен ли для чтения представленный носитель информации с использованием пользовательских программных средств? Если нет, то каковы причины отсутствия доступа к носителю информации?

4. Какие сведения о собственнике (пользователе) компьютерной системы (в т. ч. имена, пароли, права доступа и пр.) имеются на носителе?

5. Имеются ли признаки функционирования данного компьютерного средства в составе локальной вычислительной сети? Каково содержание установленных сетевых компонентов?

6. Имеются ли признаки работы представленного компьютерного средства в сети Интернет?

7. Имеется ли на носителе информация в виде сообщений, и если да, то каков их формат?

8. Находилась ли на носителе информация, которая была удалена? Если да, то какая именно?

9. Содержится ли на данном носителе информация, имеющая ключевые слова, предоставленные следователем?

10. Установлены ли на носителе программы (приложения) для мгновенного обмена сообщениями (мессенджеры)? Если да, возможен ли к ним доступ?

11. Имеются ли метаданные сообщения?

12. Были ли сообщения когда-то удалены?

13. Можно ли определить, было ли сообщение отправлено в общем чате или в приватном?

14. Можно ли определить, было ли оно прочитано?

Правильный подход к компьютерно-технической экспертизе начинается еще до ее назначения, при изъятии компьютерной информации. Ст. 164.1 УПК РФ закрепляет особенности изъятия электронных носителей информации и копирования этой информации. Электронные носители информации подлежат изъятию с обязательным участием специалиста, следователю также дается право

осуществить копирование информации, содержащейся на носителе. «Если специалист указывает на недопустимость копирования информации вследствие высокой вероятности изменения или утраты доказательственной информации, следует произвести выемку устройства целиком»[214].

Перед выемкой необходимо позаботиться о том, чтобы у специалиста был носитель с достаточным объемом памяти, или же следователю нужно взять с собой специальный носитель для сообщений, если их можно будет выгрузить сразу.

В большинстве случаев представляется целесообразным копировать информацию, чтобы при дальнейшем ее изучении следователем или экспертом оригинал носителя не мог быть поврежден, и информация не была безвозвратно утрачена. Как отмечает Н.Н. Федотов[215], исследовать в ходе компьютерно-технической экспертизы оригинал носителя нежелательно. Сохранность информации может гарантировать только оставленный оригинал. По нему впоследствии возможно будет провести повторную или дополнительную экспертизу. Поэтому экспертное исследование не самого устройства, а снятого с него криминалистического образа надежнее, быстрее, а оригинал устройства будет освобожден для проведения трасологических, биологических и иных экспертиз.

Доказательственным значением после копирования будут также обладать и лог-файлы. Так, И.В. Собецкий в своей статье «О доказательственном значении лог-файлов»[216] поднимает полемику на тему их доказательственной силы. По мнению многих интернет-пользователей, эта сила утрачивается после их изъятия с компьютера потерпевшего, так как после изъятия данные файлы могут быть изменены, но И.В. Собецкий с данной точкой зрения не согласен. Изъятие лог-файлов не умаляет их доказательственного значения. Так, согласно п. 4 ст. 235 УПК РФ, при рассмотрении ходатайства об исключении доказательства, заявленного стороной защиты на том основании, что доказательство было получено с

---

[214] См.: Электронные носители информации в криминалистике. С. 184.
[215] См.: *Федотов Н.Н.* Указ. соч. С. 418.
[216] См.: *Собецкий И.В.* О доказательственном значении лог-файлов // URL: http://www.bnti.ru/showart.asp?aid=806&lvl=01.02.01.&ysclid=liythp76wi586757589 (дата обращения: 10.10.2023).

нарушением требований настоящего Кодекса, бремя опровержения доводов, представленных стороной защиты, лежит на прокуроре. В остальных случаях бремя доказывания лежит на стороне, заявившей ходатайство. В случае с заявлением о том, что логи были подделаны, бремя доказывания будет лежать на стороне, заявившей ходатайство. По мнению И.В. Собецкого, опираясь на действующее законодательство, несложно сделать вывод о том, что оспорить доказательственное значение лог-файлов, снятых с компьютера потерпевшего, не удастся, если они изъяты по всем нормам уголовно-процессуального права, с участием специалиста и компетентных понятых, которые способны понять происходящее действие.

Однако И.В. Собецкий отмечает, что бывают случаи, когда копирование лог-файлов и иной информации будет не всегда целесообразным. Это могут быть случаи, связанные с информационными атаками на корпоративные серверы, когда логи скомпрометированного компьютера были изменены. Однако, если такие атаки были неудачными, логи можно изъять, скопировать и использовать в качестве доказательства. «Если специалист указывает на недопустимость копирования информации вследствие высокой вероятности изменения или утраты доказательственной информации, следует произвести выемку устройства целиком»[217].

Экспертное исследование происходит в несколько этапов. Первый этап – идентификация объекта исследования. Эксперт фотографирует упаковку и вскрывает ее, извлекает поступившее на экспертизу устройство, которое указано в постановлении о назначении экспертизы. Само устройство эксперт фотографирует (с линейкой) и описывает. Описание зависит непосредственно от самого устройства. Как правило, фиксируются размерные характеристики, маркировочные обозначения (производитель, серийный номер, модель), а также

[217] См.: Электронные носители информации в криминалистике. С. 171.

индивидуализирующие особенности – внешние повреждения и дефекты, которые имеются на устройстве[218].

Также эксперт устанавливает, имеются ли внутри мобильного устройства карты памяти или SIM-карты. Для большинства современных электронных средств не требуется изъятие аккумулятора для установления наличия сим-карты, поскольку ее отсутствие видно на экране самого устройства. Следователь не выключает устройство вплоть до попадания его на экспертизу, в некоторых случаях необходимо даже постоянное поддержание активности телефона. В случае с более старыми моделями целесообразнее удалить аккумулятор из устройства. Рекомендуется убирать его в чехол Фарадея, а экспертизу производить в экранированной комнате или хотя бы в комнате с наличием глушащих сигналы связи устройств.

Следующим этапом является подготовка оборудования к проведению исследования[219]. Эксперт изучает документацию и руководство пользователя об исследуемой модели устройства, подбирает соответствующее программное[220] и техническое обеспечение.

Экспертиза должна начинаться с копирования информации. Как говорилось ранее, копирование информации осуществляется специалистом в ходе следственных действий, направленных на изъятие компьютерной информации, или экспертом в ходе компьютерно-технической экспертизы в целях создания им копии, которую он сможет всесторонне и полноценно исследовать без риска утраты. В методике проведения компьютерно-технической экспертизы также указывается на необходимость проведения побитового копирования информации с машинных носителей[221].

Самым полным и безопасным копированием является создание криминалистического образа. Оно способно обеспечить полную сохранность

---

[218] См.: *Саенко Г.В., Тушканова О.В.* Указ. соч. С. 190.
[219] Там же. С. 191.
[220] Драйвер – компьютерное программное обеспечение, с помощью которого другое программное обеспечение (операционная система) получает доступ к аппаратному обеспечению некоторого устройства.
[221] См.: *Саенко Г.В., Тушканова О.В.* Указ. соч. С. 192.

данных, доступ к данным, в случае если они зашифрованы или защищены паролем, а также в некоторых случаях способны восстановить удаленную информацию.

Снятие криминалистического образа – это полное копирование всей информации, включая не только файлы, несущие в себе информацию (переписки, фотографии и т. д.), но и системные файлы устройства. Следовательно, криминалистический образ устройства идентично копирует носитель, позволяя эксперту использовать его в целях проведения полной и всесторонней экспертизы.

Техника, предназначенная для снятия криминалистического образа, т. е. извлечения данных из устройства, шагнула далеко вперед. Она позволяет не только копировать и восстанавливать любые данные из устройства, но и получать доступ к нему без специального пароля, защищающего операционную систему от стороннего пользователя. Разработкой и продажей таких программно-аппаратных комплексов занимается израильская компания Cellebrite. Новейшим ее достижением явилась разработка комплекса Universal Forensic Extraction Device (далее – UFED) для взлома и копирования данных с любых мобильных телефонов. Аналогичные инструменты для криминалистической экспертизы делает российская компания «Элкомсофт».

Вышеназванные инструменты больше подходят для работы с мобильной техникой. Для работы с информацией на персональном компьютере, съемном носителе или ноутбуке используются блокираторы. Это программы или устройства, не позволяющие записать что-либо на исследуемый накопитель, благодаря чему возможно безопасное подключение исследуемых жестких дисков к компьютеру. Они исключают возможность случайного изменения данных на них. Необходимость применения таких средств происходит как из требований процессуального законодательства (например, ст. 164.1 УПК РФ), так и из различных рекомендаций методического и иного характера, а также из стандартов (например, СТО БР ИББС-1.3-2016)[222].

[222] См.: Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Сбор и анализ технических данных при реагировании на инциденты информационной

Аппаратные блокираторы представляют из себя устройство, которое подключается к персональному компьютеру или ноутбуку, а программные являются программным обеспечением, устанавливаемым на компьютер.

Некоторые аппаратные блокираторы, например, WiebeTECH Forensic UltraDock V5 способны не только производить блокировку информации на жестких дисках, но также «эмулировать», т. е. имитировать функционирование всей системы персонального компьютера без искажения данных на диске-источнике. Благодаря такой эмуляции на другом устройстве (например, на компьютере следователя или эксперта) может функционировать программа, которая функционировала на исследуемом устройстве. Блокиратор с возможностью эмуляции подключается к устройству и запускает функционирование всей системы устройства, с которого был снят образ для эмуляции.

Снятие криминалистической копии устройства позволяет извлечь все данные из памяти мобильных устройств, в том числе и электронные сообщения, которые были отправлены с помощью мессенджера, приложения социальной сети или электронной почты.

Снятие данных с устройства может происходить на различных уровнях[223].

Самый нижний уровень предполагает ручное извлечение данных, которое происходит за счет устройств ввода и вывода[224]. Извлечение предполагает либо непосредственный осмотр содержимого устройства следователем или экспертом, либо подключение исследуемого носителя к устройству следователя или эксперта и копирование, и просмотр данных без использования специальных программных средств, т. е. с применением стандартных инструментов работы операционной системы. Такой метод является наиболее простым, но позволяет извлечь далеко не всю информацию, в частности, не дает восстановить удаленные данные.

безопасности при осуществлении переводов денежных средств» СТО БР ИББС-1.3-2016» (принят и введен в действие Приказом Банка России от 30.11.2016 № ОД-4234) // СПС «КонсультантПлюс».

[223] См.: Производство судебной компьютерно-технической экспертизы. Часть V. Актуальные задачи исследования компьютерной информации: методическое пособие / Под ред. А.И. Усова. – М.: ЭКОМ, 2011. – 270 с.

[224] Устройства ввода-вывода – компонент ЭВМ, предоставляющий компьютеру возможность взаимодействия с внешним миром.

Следующий уровень – извлечение данных на физическом уровне.

При физическом извлечении устройство подключается к устройству эксперта, на которой установлено специальное программное обеспечение. С помощью него производится копирование данных, находящихся на дисках[225] устройства. В рамках этого уровня по битам копируется буквально вся внутренняя память компьютерного устройства, включая удаленные данные. На данном уровне используется специальное программное обеспечение, которое решает множество криминалистических задач, таких как извлечение и декодирование данных из мобильных устройств различных моделей, восстановление удаленных данных, возможность дешифрования баз данных, комплексного анализа и составления отчетов. Снятие криминалистического образа относится к физическому уровню.

Существует также логический уровень.

Логический уровень предполагает подробное копирование данных, однако без физического доступа к устройству. На данном уровне эксперт работает при помощи API-методов, которые предполагают взаимодействие программ и операционных систем без физического контакта. На логическом уровне выполняется снятие данных, например, из облачных хранилищ. Копирование на логическом уровне возможно при наличии удаленного подключения к исследуемому носителю.

Следующий уровень – извлечение данных из интегральной схемы памяти или «Chip-off»[226]. Чип памяти из мобильного устройства вручную извлекается специалистом, после чего помещается либо в идентичное мобильное устройство, либо в специальную аппаратуру – адаптер для микросхем памяти. После этого информация с чипа считывается через устройство, в которое он был помещен. Суть метода состоит в том, что чип попадает в идентичное устройство, благодаря чему

[225] Логический диск – часть долговременной памяти компьютера. С точки зрения операционной системы каждый логический диск воспринимается как отдельное запоминающее устройство, хотя физически это один и тот же хранитель данных.

[226] См.: *Жижина М.В.* Извлечение данных с мобильных телефонов: проблемы на практике // Уголовный процесс. 2024. № 3. Март // URL: https://e.ugpr.ru/1071993?ysclid=lv2jzy6cfg597645352&fromId2=true&from=id2 (дата обращения: 14.04.2024).

становится возможным включить его, просмотреть, и скопировать всю нужную информацию. Используется данный метод тогда, когда из устройства оригинала не получается стандартными методами считать информацию, например при наличии шифра или пароля. При извлечении чипа извлекаются именно микросхемы, содержащие необходимую информацию.

Стоит отметить, что такое извлечение требует определенных навыков специалиста и является довольно сложным. Данный метод возможно использовать при исследовании более старых моделей телефонов или, например, флеш-накопителей, поскольку у новых моделей микросхемы шифровки данных и самих данных не разделимы. Но эксперту рекомендуется быть предельно осторожным и при возможности предварительно проверить метод на таком-же устройстве.

Однако этот уровень не является последним, возможно еще извлечение данных на микроуровне. В рамках такого метода вышеназванная интегральная микросхема анализируется с помощью электронного микроскопа.

Таким образом, становится возможным снятие данных с устройства даже в том случае, если они находятся под серьезной защитой. Chip-off или анализ под микроскопом позволяют решить проблему пароля, так как в данных случаях информация по сути считывается с самого физического носителя, без устройства как такового, что позволяет снять ее на уровне нулей и единиц, а затем снова преобразовать в воспринимаемый человеком вид. Однако в данном случае пароль должен храниться на устройстве в отдельном чипе, а информация не должна шифроваться полностью.

Применение этой технологии имеет значительные ограничения. Есть основания полагать, что выпаивание микросхемы методом Chip-off из айфонов (смартфонов марки Apple) невозможно из-за конструктивных особенностей данных смартфонов. Данный вопрос рассмотрен в руководстве по безопасности смартфонов Apple[227].

[227] См.: Безопасность платформы Apple. Май 2022 г. // URL: https://help.apple.com/pdf/security/ru_RU/apple-platform-security-guide-rs.pdf (дата обращения: 14.04.2024).

«Уникальный ключ мобильной операционной системы iOS, зафиксированный в процессоре на стадии изготовления микросхемы памяти, не позволяет проводить дешифрование данных в процессе экспертного исследования через какие бы то ни было считыватели в отсутствие подлинного пароля пользователя. Таким образом, использование метода Chip-off в целях извлечения информации из отдельных моделей телефонов iPhone в рамках судебной экспертизы является априори безрезультатным»[228]. Это подтверждается и судебной практикой. Так, согласно определениям[229] кассационных судов общей юрисдикции, гражданам, чьи мобильные телефоны Apple iPhone подлежали изъятию и экспертизе, возвращали их в разобранном состоянии, с демонтированными чипами. Восстановлению устройства не подлежали. Несмотря на то, что ФЗ «О государственной судебно-экспертной деятельности» закрепляет, что «повреждение вещественных доказательств и документов, произведенное с разрешения органа или лица, назначивших судебную экспертизу, не влечет за собой возмещения ущерба их собственнику государственным судебно-экспертным учреждением или экспертом»[230], экспертам необходимо более обоснованно подходить к выбору методики исследования.

В последнее время все большее распространение получает хранение больших объемов компьютерной информации в так называемых облачных хранилищах данных, расположенных на удаленных сетевых серверах, что необходимо учитывать при поиске криминалистически значимой информации[231]. Облачное хранилище – это онлайн-хранилище, которое находится на распределенных в сети серверах и предоставляет место для пользования клиентам. Такое хранение обеспечивают различные сервисы, такие как социальные сети, почта, мессенджеры.

---

[228] См.: *Жижина М.В.* Указ. соч.

[229] См.: Определение Седьмого кассационного суда общей юрисдикции от 19.04.2022 №№ 88-5860/2022, 2-6379/2021 // URL: http://7kas.sudrf.ru/modules.php?name=sud_delo&srv_num=1&H_date=19.04.2022 (дата обращения: 14.04.2024); Определение Восьмого кассационного суда общей юрисдикции от 24.06.2022 № 88-11303/2022 // URL: http://8kas.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=24390969&case_uid=80db1ca9-aea3-4653-b066-32df8e53fc40&delo_id=2800001&new=2800001 (дата обращения: 14.04.2024).

[230] См. ст. 10 Федерального закона от 31.05.2001 № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» // СПС «Консультант Плюс».

[231] См.: Электронные носители информации в криминалистике. С. 43.

По этой причине объектом экспертного исследования могут стать не данные с носителя, а информация, скопированная из удаленного хранилища.

Так, возможно восстановить удаленную переписку из облачного хранилища, имея доступ к SIM-карте и специальное программное обеспечение. Например, с помощью того же устройства Cellebrite UFED возможно клонирование идентификатора SIM-карты, что позволит получить доступ к использованию номера телефона лица, на которого зарегистрирован аккаунт в мессенджере, социальной сети или электронный почтовый ящик.

«Для получения информации из облачных хранилищ существует программа «Мобильный Криминалист» – технико-криминалистическая экспертная программа, сделавшая возможным извлечение данных из облачного хранилища с помощью модуля Oxygen Forensic Extractor for Clouds[232]. Указанный модуль может подключаться к облачному хранилищу, используя только данные учетной записи: адрес электронной почты и пароль. Как только соединение установлено, Oxygen Forensic Extractor for Clouds начинает извлечение данных. Сильной стороной модуля является не только извлечение данных, но и их представление в удобном для анализа виде и наличие различных инструментов для анализа, что позволяет специалисту экономить очень много времени»[233].

В качестве отдельной области экспертного исследования можно указать поиск и расшифровку лог-файлов. Такие файлы записываются компьютером автоматически и не воспринимаются человеком. Для того чтобы расшифровать их, чаще всего необходимы специальные знания. Н.Н. Федотов предполагает, что «логи, как правило, не являются непосредственным источником доказательств, но опосредованным. Вместо самих логов в качестве доказательств используются: заключение эксперта, заключение специалиста, а также показания изучавших логи

[232] См.: *Нестеров А.Д.* Получение информации из облачных хранилищ при расследовании инцидентов в сфере информационной безопасности // Advances In law studies. 2015. № 22. // URL: http://sci-article.ru/stat.php?i=1433879423 (дата обращения: 14.05.2023).
[233] См.: *Тушканова О.В.* Терминологический справочник судебной компьютерной экспертизы: справочное пособие. – М.: ЭКЦ МВД России, 2005. – С. 56.

свидетелей специалиста, эксперта, понятых»[234]. Мы согласны с данной позицией, так как очевидно, что предоставить в суде распечатку лог-записей, интерпретировать и понять их участникам процесса будет довольно сложно.

Наконец, отдельной формой экспертного исследования может быть индексация электронных сообщений, о которой рассказывалось ранее. Индексацию может проводить как следователь, если он обладает должными навыками и имеет необходимое программное обеспечение, так и эксперт, в случае если следователь решил поручить это ему.

Согласно проведенному среди работников следственного аппарата анкетированию, 48,85% опрошенных считает, что проведение индексированного поиска лучше осуществлять следователю самостоятельно, а 51,15% полагают, что это лучше доверить эксперту.

Однако, на наш взгляд, индексацию лучше в большинстве случаев доверить эксперту, так как специальные знания и навыки позволят ему не упустить нужной информации в ходе поиска. Разумеется, что для осуществления такого поиска следователь должен составить и предоставить эксперту исчерпывающий список ключевых слов.

При назначении экспертизы с целью проведения индексации следователю рекомендуется поставить перед экспертом следующие вопросы:

– Найдены ли на носителе/устройстве сообщения, содержащие заданные ключевые слова, с учетом их релевантности заданным словам?

– Какое количество сообщение было найдено по заданным ключевым словам?

– Каково содержание сообщений, содержащее заданные ключевые слова, с учетом их релевантности?

На устройстве среднестатистического пользователя сети Интернет хранится огромное количество электронных сообщений. Их может обнаружить эксперт, в том числе и восстановить удаленные. Поэтому, на наш взгляд, следователю всегда

[234] См.: *Федотов Н.Н.* Указ. соч. С. 202.

необходимо включать индексацию в список задач, ставящихся перед экспертом, и всегда предоставлять ему грамотно составленный список ключевых слов. Эксперту же необходимо будет передать следователю отдельно найденную относимую переписку, а также всю остальную найденную переписку (на носителе), чтобы следователь при необходимости мог сам произвести повторный индексированный поиск.

Итак, для того чтобы правильно назначить компьютерно-техническую экспертизу необходимо:

1) организовать правильное изъятие электронного носителя, в соответствии с требованиями УПК РФ, чтобы избежать потери информации;

2) учитывая большой объем электронной переписки на устройствах современных пользователей, следователю рекомендуется всегда составлять и предоставлять в распоряжение эксперта список ключевых слов для индексированного поиска относимой переписки, а также ставить вопрос об индексации. Эксперту при составлении заключения рекомендуется прилагать к заключению сообщения, которые он нашел по ключевым словам и счел относимыми;

3) все вопросы, так или иначе связанные с электронной перепиской и при этом требующие наличия специальных знаний, рекомендуется выносить на разрешение эксперта: индексация, исследование и расшифровка лог-файлов.

2. Лингвистическая и автороведческая экспертизы

Важную роль в исследовании электронных сообщений играют экспертизы продуктов речевой деятельности. Экспертизы текста и речи основываются на разносторонней экспертной деятельности, которая включает в себя знания эксперта не только в области лингвистики, но и криминалистики и иных отраслей знания и жизни. Также немаловажную роль в исследовании речи играют и технические достижения.

Лингвистическая экспертиза – процессуально регламентированное исследование продуктов речевой деятельности[235]. Эта экспертиза используется довольно часто, и ее результаты занимают важное место среди массива доказательственной базы в суде.

«Как судебно-экспертное исследование речевых произведений лингвистическая экспертиза представляет собой процессуальное действие, состоящее из проведения исследования содержательно-смысловой и формально-языковой стороны устного или письменного текста»[236].

Объектами лингвистической экспертизы могут, как пишет Е.И. Галяшина, выступать только «продукты речевой деятельности (устной или письменной), обладающие свойствами текста, произведенные в конкретно-определенной коммуникативной ситуации и зафиксированные на материальном носителе»[237]. Таким образом, объектами лингвистической экспертизы могут быть как текстовые сообщения, так и аудио-, видеосообщения, которые содержат в себе продукты речевой деятельности.

«Существенными свойствами для установления факта негодности (непригодности) продукта речевой деятельности для проведения судебной лингвистической экспертизы является фрагментарность, несвязность, отрывистость, частичность, невнятность, компилятивность речевого продукта, т. е. несоответствие представляемого на экспертизу материала критериям текста, определяющим его структурированность, связность, целостность, завершенность, семантическую определенность и т. д.»[238].

---

[235] См.: Приказ Минюста России от 27.12.2012 № 237 «Об утверждении Перечня родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России, и Перечня экспертных специальностей, по которым представляется право самостоятельного производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Минюста России» // СПС «Гарант».

[236] См.: *Галяшина Е.И.* Судебная лингвистическая экспертиза и пределы допустимости использования методов лингвистической науки // Вестник Московского университета МВД России. 2018. № 4. С. 31.

[237] См.: *Галяшина Е.И.* Разграничение деятельности судебного эксперта-лингвиста и лингвиста-аналитика: компетенции, методы и технологии // Acta Linguistica Petropolitana. Труды института лингвистических исследований. 2019. Vol. 15.1. P. 113.

[238] Там же.

С помощью лингвистической экспертизы электронной переписки можно установить, все ли сообщения принадлежат одному лицу или в ведении переписки с одной стороны, вероятно, участвовала группа лиц, установить ориентирующую информацию о личностных характеристиках автора сообщений – пол, возраст, язык, национальную и религиозную принадлежность, установить психическое состояние, в котором находился автор текста при его написании, подтвердить или опровергнуть содержание в тексте призывов к экстремизму, развратным действиям, насилию. Такая экспертиза решает задачи определения направленности информации, содержащейся в тексте (клевета, оскорбление, возбуждение ненависти и вражды и т. д.).

Судебно-лингвистическая экспертиза имеет следующий порядок проведения:

1. Эксперт получает постановление или определение о назначении экспертизы, а также материалы, которые необходимо исследовать, в нашем случае это тексты интернет-коммуникаций (публикации, комментарии, статусы и т. д.);

2. Анализирует вопросы, которые ставятся перед ним, касающиеся исключительно лингвистической экспертизы;

3. Затем, эксперт изучает предоставленные ему материалы. Данный этап является самым трудоемким. На нем эксперт прочитывает тексты, изучает природу происхождения каждого слова, символа, прослушивает аудио- и видеозаписи, если это является необходимым для более четкого определения факта совершения противоправного деяния.

4. На завершающем этапе эксперт дает заключение о проделанной работе, отвечает на поставленные перед ним вопросы[239].

Результативность лингвистической экспертизы зависит от правильно поставленных следователем вопросов. На разрешение эксперта следует ставить вопросы о наличии определенных речевых особенностей и о том, на что они могут

[239] См.: *Пучкова Д.В.* Особенности проведения лингвистической экспертизы текстов интернет-коммуникаций // Международный журнал гуманитарных и естественных наук. 2020. Вып. 1-12 (50). С. 112–113.

указывать. Иные вопросы недопустимы, поскольку выходят за пределы компетенции эксперта. Так, например, в ходе защиты Егора Жукова по делу о публичном призыве к осуществлению экстремисткой деятельности[240], его адвокат предоставил в судебном заседании результаты лингвистической экспертизы. На разрешение эксперта он поставил вопрос «Имеются ли с позиции лингвистической квалификации в предоставленных видеозаписях призывы к осуществлению незаконной деятельности?». Данный вопрос поставлен некорректно, так как позиция лингвистической квалификации позволяет судить о содержании языковых выражений, давать интерпретацию высказываниям в случае возникновения сомнений, характеризовать высказывания по цели речевого акта. Лингвистические методы не позволяют извлечь из содержания текста указания на незаконность действий, которые текст описывает. Правовая квалификация действий не относится к сфере компетенции лингвистического эксперта[241].

Поэтому необходимо четко понимать компетенцию и возможности эксперта-лингвиста, для того чтобы поставить правомерные вопросы на его разрешение и получить в результате заключение, которое будет служить допустимым доказательством в суде.

Судебная автороведческая экспертиза – традиционный род криминалистических экспертиз, предметом которого являются фактические данные, установление которых осуществляется экспертом на основе изучения письменных документов с использованием специальных знаний в области судебного автороведения[242]. Автороведческая экспертиза назначается для разрешения идентификационных, диагностических, ситуационных задач[243]. Данный вид экспертизы может решить проблему установления автора сообщений,

---

[240] См.: Суд признал виновным фигуранта «дела 27 июля» Егора Жукова // URL: https://www.rbc.ru/rbcfreenews/5dea00d49a794767a9bc4b20?ysclid=lmixefzae0103196460 (дата обращения: 27.02.2023); См. ст. 280 Уголовного кодекса Российской Федерации от 13.06.1996 № 63-ФЗ // СПС «КонсультантПлюс».

[241] См.: Постановление Пленума Верховного суда России от 21.12.2010 № 28 «О судебной экспертизе по уголовным делам» // СПС «КонсультантПлюс».

[242] Судебная автороведческая экспертиза // URL: http://www.sudexpert.ru/possib/author.php (дата обращения: 12.11.2023).

[243] См.: *Баев О.Я.* Тактика следственных действий. – М.: Юрлитинформ, 2013. С. 366.

имеющих криминалистическую значимость, или решить диагностические задачи и сузить круг потенциальных авторов. Развитие интернет-технологий провоцирует и улучшение инструментария автороведческих экспертиз. Так, Т.В. Назарова и А.В. Громова отмечают, что совершенствование данной экспертной области необходимо на постоянной основе: «как показывает практика, динамичное развитие функциональных возможностей создания и обработки текстов, связанное прежде всего с развитием технологий интернет-коммуникации, требует совершенствования инструментария автороведческих экспертиз»[244]. По мнению этих авторов, «задачи, которые решает эксперт, можно разделить на две большие группы:

1) идентификационные задачи, связанные с определением автора текста путем проведения раздельного и сравнительного анализа признаков, проявившихся в спорном тексте и текстах – образцах письменной речи подозреваемого лица;

2) диагностические задачи, связанные с определением половозрастных, индивидуально-личностных характеристик, уровня коммуникативной компетенции, речевой культуры, сферы профессиональной деятельности автора текста»[245].

А.В. Громова и Т.А. Литвинова уточняют задачи, которые могут быть решены в ходе идентификации:

«1. Кто из замкнутого круга лиц (небольшого, как правило 2–3 человека) является автором криминалистически значимого текста (в зарубежной литературе – closed-set problem)?

2. Является ли данное лицо, сравнительные образцы текстов которого представлены эксперту, автором криминалистически значимого текста (verification problem)»[246]?

---

[244] См.: *Назарова Т.В., Громова А.В.* Объекты и задачи лингвистических и автороведческих экспертиз, проводимых в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации // Судебная экспертиза Беларуси. 2016. № 1 (2). С. 43–46.

[245] Там же.

[246] См.: *Громова А.В., Литвинова Т.А.* Компьютерные технологии в судебной автороведческой экспертизе: проблемы и перспективы использования // Вестник Волгоградского государственного университета. 2020. № 1. С. 78.

На протяжении последних 15 лет специалисты в области информационных технологий (computer scientists) активно разрабатывают методы идентификации и диагностирования личности по тексту (преимущественно на материале английского языка). Как правило, исследователи ставят задачу диагностировать пол и возраст, реже – некоторые психологические характеристики автора, однако такие работы не направлены специально на решение задач экспертной практики[247].

На современном этапе основной проблемой, стоящей перед экспертами, является как раз экспертиза коротких электронных сообщений. Проблема обуславливается недостаточностью текста для проведения экспертизы, ведь многие исследования описывают методику установления авторства текста, применимую от определенного количества символов или слов. Как отмечает А.А. Воробьева, «существенный вклад в проблематику данной области внесли работы Морозова Н.А., Маркова А.А., Фоменко В.П., Хмелева Д.В., Романова А.С., Лебедева И.В. Однако представленные в них методы разработаны для сообщений более 20000 символов, что существенно превышает среднюю длину сообщений в Интернете. Также в них не учитывается неравномерное распределение количества сообщений по пользователям»[248]. А.С. Романов полагает, что «задача идентификации авторства коротких текстов возникает чаще… Это связано, прежде всего, с широким распространением программ для обмена сообщениями в сети Интернет…»[249].

На наш взгляд, следователю необходимо изымать и предоставлять на экспертизу не только отдельные сообщения, но и всю переписку в ее взаимосвязи. Это позволит как увеличить количество пригодного для экспертизы текста, так и связать информацию из коротких электронных сообщений с контекстом расследуемого события.

А.В. Громова и Т.А. Литвинова рассматривают анализируемый в ходе авторoведческой экспертизы текст как некий интеллектуальный след, продукт

---

[247] См.: *Громова А.В., Литвинова Т.А.* Указ. соч. С. 78.
[248] См.: *Воробьева А.А.* Указ. соч. С. 9.
[249] См.: *Романов А.С.* Указ. соч. С. 81.

целенаправленной деятельности, выступающий носителем информации, в том числе и о личности автора[250]. В речеведении были разработаны такие понятия, как «языковая личность», «речевой портрет» и «обликовая характеристика личности». Языковая личность – это совокупность коммуникативных способностей и характеристик, а также отличительных черт, обнаруживающихся в коммуникативном поведении человека[251]. Понятие «языковая личность» тесно связано с понятием «речевого портрета». Речевой портрет – это совокупность языковых личностных характеристик лица[252]. Е.И. Галяшина и Е.Р. Россинская под обликовой характеристикой личности понимают как некоторые признаки внешнего облика человека, так и эмоциональное состояние говорящего в момент речепорождения (тревожность, волнение, страх), психофизиологическое состояние (патологии речи)[253]. Именно речевой портрет выводит нас на обликовую характеристику личности. Исследователи в области речеведческих экспертиз утверждают, что в рамках «обликовой характеристики личности» можно выяснить половозрастные характеристики, социо-биографические (этническую и территориальную принадлежность, регион длительного проживания, уровень образования, профессию или род занятий), особенности физиологического и психофизиологического состояния[254].

Сопоставляя обликовую характеристику личности, установленную на основании изученных сообщений, с характеристиками конкретного лица, можно делать относительно обоснованные предположения о том, может ли оно являться их автором. Сейчас это делает человек, однако уже на современном уровне развития техники решение этой задачи может быть автоматизировано.

На данный момент в России существуют программы, предназначенные непосредственно для проведения исследований в области идентификации автора и

---

[250] См.: *Громова А.В., Литвинова Т.А.* Указ. соч. С. 80.
[251] См.: *Беспамятнова Г.Н.* Языковая личность телевизионного ведущего: дис. ... канд. филол. наук: 10.02.04. – Воронеж, 1994. – С. 217.
[252] Там же.
[253] См.: *Россинская Е.Р., Галяшина Е.И.* Настольная книга судьи. Судебная экспертиза. – М., 2010. – С. 314.
[254] См.: *Байрамова Ф.О.* Исследование акцента в интерферированной русской речи: на материале русской речи азербайджанцев: автореф. дис. ... канд. филол. наук: 10.02.01, 10.02.21. – М., 2012. – С. 20.

криминалстического изучения письменной речи, такие как «Автор» и автоматизированное рабочее место «Лексика»[255], «Штампомер»[256], «Лингвоанализатор»[257], «Атрибутор»[258], «СМАЛТ»[259]. А.С. Романов провел исследования по разработке алгоритмического и программного обеспечения для идентификации автора письменной речи «Авторовед». «Оно позволяет производить полный цикл обработки текстов, исследований влияния характеристик текста, вида классификатора и его параметров на точность идентификации автора неизвестного текста, идентифицировать автора из множества возможных претендентов с помощью искусственных нейронных сетей и машины опорных векторов, проводить анализ потенциально заимствованного текста, подтверждать или опровергать авторство текста»[260].

3. Психолого-лингвистическая экспертиза

Впервые это направление получило развитие в 1920-е гг., когда были предприняты первые попытки создать судебно-психологическую экспертизу документов. Теоретической основой методов судебно-психологических экспертиз были многочисленные экспериментальные исследования психологии свидетельских показаний, психологии обвиняемого, психологии участников судебного процесса и др. Основой судебно-психологической экспертизы того времени являлся исключительно анализ содержания документов[261].

В настоящее время комплексная психолого-лингвистическая экспертиза набирает актуальность в связи с исследованием печатных текстов в сети Интернет «по делам коррупционной направленности; по делам, связанным с оскорблением

---

[255] См.: *Комиссаров А.Ю.* Криминалистическое исследование письменной речи с использованием ЭВМ: дис … канд. юрид. наук: 12.00.09. – М., 2001.
[256] См.: Штампомер – описание работы программы // URL: http://www.shtampomer.narod.ru/manual.htlm (дата обращения: 20.05.2023).
[257] См.: *Хмелев Д.В.* Распознавание автора текста с использованием цепей А.А. Маркова // Вестник МГУ. Сер.9. Филология. 2000. № 2.
[258] См.: Атрибутор // URL: http://www.textology.ru/web.htm (дата обращения: 20.05.2023).
[259] См.: Компьютерная обработка текстов при помощи ИС «СМАЛТ» / А.А. Рогов [и др.] // Проблемы развития гуманитарной науки на Северо-западе России: опыт, традиции, инновации: Материалы научной конференции. – Петрозаводск, 2004. Т. 1.
[260] См.: *Романов А.С.* Указ. соч. С. 12.
[261] См.: *Леонтьев А.А., Шахнарович А.М., Батов В.И.* Речь в криминалистике и судебной психологии. – М., 1977. – С. 24.

чувств верующих; информационных материалов, предназначенных для детей; по материалам оперативных и следственных действий с целью установления влияния на содержание показаний; опросов (допросов) несовершеннолетних потерпевших по делам о преступлениях против половой неприкосновенности и половой свободы личности; экспертиза текстов религиозного характера»[262].

В рамках психолого-лингвистической экспертизы рассматривается речь людей в контексте их смыслового содержания, подтекста, психологической направленности. Она заключается в комплексном исследовании текста сообщения как экспертом-лингвистом, так и психологом. Данный вид экспертизы направлен на то, чтобы установить психологическое состояние лица на момент написания сообщения, его так называемый посыл или намерение и, в некоторых случаях, возможное восприятие текста сообщения его получателем.

Данная экспертиза отличается от лингвистической тем, что, помимо смыслового содержания и контекста сообщения, в ходе нее также анализируется психологическая направленность написанного. Например, при анализе переписок с несовершеннолетними на сексуальную тематику психолого-лингвистическая экспертиза позволяет установить не только смысловое содержание и коммуникативные намерения, но и выявить признаки оказания психологического давления на несовершеннолетнего – что имеет важность для квалификации развратных действий.

С точки зрения психологии, в исследовании письменной речи выделялось два аспекта: психолингвистический и психологический[263]. При психолингвистическом исследовании текста устанавливаются те навыковые свойства личности, которые налагают психологическое ограничение на отбор и организацию языковых средств высказывания (текста). При психологическом анализе устанавливают те

[262] См.: *Секераж Т.Н., Кузнецов В.О.* Комплексная судебная психолого-лингвистическая экспертиза: формы, виды, перспективы развития // URL: https://www.lingvisticheskaja-ekspertiza.com/post/2018/12/27/-d0-9a-d0-9e-d0-9c-d0-9f-d0-9b-d0-95-d0-9a-d0-a1-d0-9d-d0-90-d0-af-d0-a1-d0-a3-d0-94-d0?ysclid=lv5g816y24592296841 (дата обращения: 20.05.2023).

[263] См.: *Вул С.М.* Об использовании признаков письменной речи в криминалистической экспертизе письма: автореф. дис. ... канд. юрид. наук. – Харьков, 1975.

навыковые свойства личности, которые влияют на организацию неязыковых, тематических, понятийно-смысловых структур текста.

Одно и то же сообщение может выражаться и быть понято в совершенно разных смыслах. Изучение только лишь лингвистической стороны текста не всегда позволяет отразить все смыслы написанного, поэтому возникает необходимость и в анализе психологом.

Лингвистический анализ сообщения отвечает на вопросы о том, что именно выражено в тексте переписки, какое у написанного значение и какими методами оно выражено. Психологическая методика экспертизы отвечает на вопросы о том, какая у автора была субъективная направленность, установки, определяет психологическую и социальную направленность текста. Как само написание сообщения человеком является комплексной деятельностью (выбор лингвистических средств для составления текста сообщения и вклад психологического значения в написанное), так и исследование сообщений должно производиться комплексно. Благодаря комплексному исследованию становится возможным дать ответы на вопросы «почему» и «с какой целью» что-то говорится в тексте. Это именуется социально-психологической направленностью текста.

«Компетенцию лингвиста и психолога в рамках комплексного исследования можно разграничить следующим образом: филолог-лингвист устанавливает, что конкретно сказано (показано), какой компонент значения выражен и какими языковыми средствами; психолог, на основе описания сказанного (показанного), верифицированного лингвистом, устанавливает направленность материала с точки зрения формируемых у адресата социальных установок»[264].

Важно отметить, что при исследовании электронной переписки в рамках психолого-лингвистической экспертизы нельзя предоставлять на анализ отдельные сообщения без контекста. Исследоваться должна последовательная переписка за определенный период, а не выдернутые из общего смысла всей коммуникации

[264] См.: Семантические исследования в судебной лингвистической экспертизе: методическое пособие / А.М. Плотникова [др.]; под ред. проф. С.А. Смирновой. – М.: ФБУ РФЦСЭ при Минюсте России, 2018. – С. 17.

сообщения. На наш взгляд, в распоряжение эксперта целесообразно предоставлять именно электронную версию переписки, так как распечатанная на бумаге переписка может не отражать всей полноты смысла (на ней могут отсутствовать вложения, время, ссылки, смайлы, в том числе цветные). При назначении такой экспертизы следователю (или компьютерно-техническому специалисту) необходимо перенести (скопировать) переписку на электронный носитель, такой как съемный диск или флеш-накопитель. Данный носитель должен быть доступен для подключения и изучения на компьютере эксперта с использованием стандартного программного обеспечения.

Довольно актуальным вопросом, связанным с понимаем смысла электронной переписки, является использование в тексте особых графических изображений (эмотиконов), выражающих эмоциональную окраску написанного – текстовые знаки (скобки и т. д.), смайлы, гифки и стикеры. Экспертам, как лингвистам, так и психологам, необходимо учитывать их при анализе смыслового содержания текста сообщения.

В пособии РФЦСЭ «Семантические исследования в судебной лингвистической экспертизе»[265] выделяются функции смайлов:

– информирования адресата о том, как собеседник должен видеть, понимать состояние автора сообщения;

– текстового знака, который добавляет и меняет значение текста;

– коммуникативного знака, который может использоваться с разными целями (например, информировать о том, что сообщение получено, понято собеседником);

– выражения отношения адресата к изложенной адресантом информации;

– выражения иронии;

– нивелирования значения, выраженного вербальными знаками;

– манипулирования ходом диалога и т. д

Е.И. Галяшина предлагает дополнить их следующими функциями:

– интонации;

[265] См.: Семантические исследования в судебной лингвистической экспертизе. – С. 17–19.

– знака препинания;

– фатическая[266];

– усиления воздействующего эффекта вербального компонента текста;

– смыслового дополнения, приращения смысла вербальной составляющей текста;

– имитации и/или маскировки эмоционального состояния автора сообщения;

– «провокации» (побуждения) адресата на определенную реакцию;

– воздействия на эмоциональное состояние реципиента и т. д.[267]

Нельзя с ней не согласиться, однако, на наш взгляд, функции смайлов и иных эмотиконов могут быть гораздо шире, и никогда нельзя заранее предугадать точный перечень того, что они будут обозначать. Исследовать тот или иной эмотикон необходимо в контексте самого сообщения, а то и всей переписки в целом.

Профессор А.Р. Алварез подчеркивает, что эмодзи и смайлы в сообщениях стали своего рода современной стратегией защиты в судах, поскольку адвокаты ссылаются на них как на аргументы того, что подзащитные вкладывали в сообщение совершенно не тот смысл[268]. Он считает, что эмодзи не всегда помогают понять реальный смысл и намерение в сообщении[269].

Так, например, фраза «Тебе не поздоровится» может обретать разную эмоциональную окраску, если она написана просто:

«Тебе не поздоровится!»

В данном случае отсутствие смайлов может указывать на серьезность намерений автора.

Или же:

---

[266] Функция создания и поддержания контакта между собеседниками, когда контакт отсутствует.

[267] См.: *Галяшина Е.И.* Семиотика эмотиконов и анимационных картинок в аспекте судебной лингвистической экспертизы // Вестник Университета имени О.Е. Кутафина. 2022. № 2. – С. 46.

[268] См.: *Rodríguez Álvarez A.* No Words Needed? Emojis as Evidence in Judicial Proceedings // Legal developments on Cybersecurity and Related Fields. Law, Governance and Technology Series. – Springer International Publishing, 2024. P. 227.

[269] Там же. P. 229.

«Тебе не поздоровится  »

В данном случае мы можем предположить, что у автора были шуточные намерения.

Или «Тебе не поздоровится))))))))))»

Скобки в конце текста также придают мягкую эмоциональную окраску написанному, из чего эксперт может сделать вывод о несерьезности намерений автора. Однако анализ данной фразы без контекста не допустим, экспертам необходимо учитывать соотношение всего текста переписки, смайлов и иных знаков, используемых в тексте.

Также смайлы и стикеры зачастую заменяют слова в сообщениях. Например, при ведении переписки о наркотических веществах люди часто используют смайлы в виде травы, листочков. Однако существуют и смайлы, по своему изображению не имеющие ничего общего с наркотическими веществами, которые все же используются для обозначения таких веществ, потому что это стало принято «в народе».

Управление по борьбе с наркотиками США (DEA) опубликовало онлайн-руководство «Код-эмодзи для наркотиков», вот примеры некоторых смайлов-обозначений, представленных в нем:

«Метамфетамин:  ,  ,  ,  (котел, разбитое сердце, бриллиант, пробирка);

Героин:  ,  (сердце со стрелой, дракон);

Кокаин:  , ,  ,  ,  ,  ,  ,  (снежинка, облако со снегом, снеговик, бриллиант, восьмерка, ключ, лицо с высунутым языком, рыба);

Мефедрон:  ,  , ,  ,  (сердце, молния, крестик, таблетка, конфета);

Грибы:  (гриб)»[270].

Помимо наркотических веществ, иные понятия и слова также могут подменяться смайлами. Так, например, в переписке о взятке могут использоваться смайлы с изображением денег или дорогих предметов.

Эксперту и следователю также необходимо принимать в расчет наличие смайлов в тексте, в том числе и при составлении списка ключевых слов для индексации. На наш взгляд, при наличии большого количества эмотиконов в сообщении, в особенности, когда у следователя складывается впечатление, что данные эмотиконы заменяют некоторые слова, необходимо отправлять тексты данной переписки на психолого-лингвистическое исследование.

3. Фоноскопическая экспертиза голосовых сообщений

В настоящее время фоноскопическая экспертиза очень актуальна и обладает неоспоримыми преимуществами, по сравнению с экспертизой текста. Данный вид экспертизы представляет большой интерес для исследования электронной переписки, так как в наши дни большое количество информации в сети Интернет передается посредством голосовых сообщений. Исследования звучащей речи в голосовом сообщении обладают способностью решить как идентификационные, так и диагностические задачи. Результаты фоноскопической экспертизы могут наделить следователя и ориентирующей информацией, указать на черты личности и сузить круг подозреваемых.

Основы использования звукозаписи в криминалистике были заложены еще в начале XX в. «Впервые в отечественной криминалистике о возможности применения диктограмм для фиксации доказательств в 1929 г. написал А.Е. Брусиловский[271]. В 1934 г. он и М.С. Строгович предложили применять звукозапись при допросах по уголовным делам[272]. Но тогда внедрение в следственную практику этого предложения объективно сдерживалось отсутствием

[270] См.: Emojis Are the New Language of Drug Deals—Especially for Teens // URL: https://www.verywellhealth.com/emoji-drug-code-educates-parents-about-drug-deals-7068968 (дата обращения: 20.06.2023).
[271] См.: *Брусиловский А.Е.* Судебно-психологическая экспертиза. Ее предмет, методика и пределы. – Харьков, 1929.
[272] См.: *Брусиловский А.Е., Строгович М.С.* Свидетельские показания в качестве судебных доказательств // Методика следственной работы. – Киев, 1934. – С. 161.

соответствующей материально-технической базы, недостаточным развитием технических средств для записи звука[273]. Только появление в обиходе простого в обращении средства звукозаписи – магнитофона – обеспечило фиксацию и хранение речевой информации и применение звукозаписи во всех сферах человеческой деятельности, включая и уголовное судопроизводство»[274]. А.И. Винберг и А.А. Эйсман[275] обосновали правовую целесообразность применения звуковой записи в уголовном процессе для фиксации устной речи, после чего звукозапись стала активно применяться советскими следователями. Е.И. Галяшина в статье, посвященной истории судебной фоноскопической экспертизы, рассказывает, что «Г.Л. Грановский впервые высказал идею об использовании метода спектрографии в криминалистике (предложив назвать его “вокалоскопия”, по аналогии с дактилоскопией) для объективизации субъективного слухового восприятия эксперта и документирования результатов экспертизы, ссылаясь на первый пример из судебно-экспертной практики идентификации по голосу. Таким образом, технические, научные и правовые условия возникновения отечественной экспертизы фонограмм к 1964 г. окончательно сформировались»[276].

В настоящее время достижения в области исследования звучащей речи шагнули далеко вперед. Благодаря последним исследованиям стало возможным определять этническую и территориальную принадлежность лица. Исследуется комплекс акустических и лингвистических признаков, свойственных для речи с «акцентом». Так, например, Ф.О. Байрамова провела диссертационное исследование «системных отклонений в русской речи азербайджанцев на фонетическом уровне», систематизировала эти отклонения и выявила комплекс признаков азербайджанского акцента[277].

---

[273] См.: Основы экспертного криминалистического исследования магнитных фонограмм / А.А. Ложкевич [и др.]. – М.: ВНИИ МВД СССР, 1977.
[274] См.: *Галяшина Е.И.* Об истории судебной фоноскопической экспертизы // Вестник Университета имени О.Е. Кутафина. 2014. № 3. С. 182–183.
[275] См.: *Винберг А.И., Эйсман А.А.* Фототелеграфия и звукозапись в криминалистике. – М., 1946. С. 21.
[276] См.: *Галяшина Е.И.* Об истории судебной фоноскопической экспертизы. С. 186.
[277] См.: *Байрамова Ф.О.* Указ. соч.

Также фоноскопия занимается исследованием связи голоса с определенными заболеваниями, с ростом и весом человека. Заболевания дыхательных путей и челюстно-лицевой области всегда имеют взаимосвязь с дефектами речи. Существуют исследования, которые освещают взаимосвязь сломанного носа, отсутствия зубов или наличие врожденных расщелин верхней губы со специфическими речевыми признаками. Это может быть полезным для установления индивидуальных признаков неизвестных лиц по голосу и речи. Возможным стало и определение психологических характеристик говорящего по звучащей речи[278]. Определение роста и веса говорящего по устной речи основывается на связи длины и размеров тела с размерами внутренних органов. Ученые утверждают, что такие исследования очень точны: средняя ошибка составляет 5–7см для роста и 5–10 кг для веса[279].

Установление уровня речевой культуры помогает определить социальный статус лица. Учеными было разработано понятие «социолект» – социального диалекта личности, речевых особенностей, которые позволяют установить принадлежность человека к определенной социальной группе (возрастной, профессиональной, классовой). Так, например, профессию лица можно определить по просодическим[280] характеристикам звучащей речи. В ходе собственного практического опыта нами было отмечено, что работники правоохранительных органов ставят ударение в слове возбу́ждено на букву «у», в то время как другие люди ставят ударение на букву «о» – возбуждено́. Или, например, сотрудники налоговых органов предпочитают говорить пеня́, недо́имка и пр.

[278] См.: *Журавлева А.А., Коваль С.Л.* Диагностика психологических качеств диктора по устной речи // Труды международной конференции по компьютерной лингвистике и интеллектуальным технологиям «Диалог 2007». – М., 2007. С. 183–187.
[279] См.: *Викторов А.Б., Остроухов А.В., Лобанова М.А.* О возможности создания автоматизированного комплекса диагностирования обликовых признаков // Информатизация и информационная безопасность правоохранительных органов. – М., 2006. – С. 5.
[280] Просодический – касающийся ударения, относящийся к явлениям высоты тона, длительности, силы звука.

Возможным стало и определение психологических характеристик говорящего по звучащей речи[281]. Однако такие исследования основываются исключительно на анализе статистического материала и психологических тестах.

Методы установления обликовых характеристик личности подразумевают аудитивный анализ экспертами и сравнение проанализированной звучащей речи со статистическими материалами. Объективность таких исследований базируется исключительно на уровне подготовки эксперта, его слуховом опыте и количестве предыдущих его ошибок. Инструментальные и технические средства исследования звучащей речи (спектрограммы, осциллограммы и т. д.) не разработаны в той мере, в какой можно было бы считать такие экспертизы объективными. Соответственно, выводы по таким экспертизам могут иметь ориентирующее значение, причем следует в них указывать уровень вероятности сделанного вывода.

Объектами фоноскопического исследования является фонограмма (звукозапись) записи речи диктора, магнитная пленка или другой носитель, на котором эта фонограмма зафиксирована, разнообразные по типу и модели звукозаписывающие и звуковоспроизводящие устройства, особенности режима работы которых фиксируются на фонограмме[282]. Голосовые сообщения являются фонограммой записи речи диктора, поэтому подпадают под объект исследования.

Найти в переписке сообщения с голосовой записью можно путем поиска сообщений с файлами-вложениями либо голосовых сообщений. Сделать это можно как с помощью сплошного просмотра, так и прибегнув к индексации. Инструменты индексации позволяют осуществить поиск по такому критерию, как наличие аудиофайлов в сообщении.

На разрешение эксперта можно поставить вопросы о сравнении записи из сообщения с записью, собранной следователем в качестве образца. Также перед экспертом можно поставить вопросы о выводах об определенных характеристиках лица, записавшего сообщение. Помимо этого, эксперт может разобрать нечеткие

[281] См.: *Журавлева А.А., Коваль С.Л.* Диагностика психологических качеств диктора по устной речи.
[282] См.: *Баранов Ю.Н.* Указ. соч. С. 19.

слова в записи, перевести аудиозапись в текст, сделать выводы об обстановке, в которой осуществлялась запись.

Идентификация говорящего на звукозаписи или установление тождества производится по устойчивым признакам. Анализ речи заключается в поиске, выявлении и оценке таких признаков звучащей речи, по которым и осуществляется идентификация лица. На данный момент такой анализ возможен только лишь совмещением технических методом и участия человека. Так, А.Ш. Каганов[283] отмечает, что идентифицировать лицо по звучащей речи возможно лишь при использовании как технических достижений, так и экспертного анализа, основанного на опыте и навыках эксперта. Компьютерные выводы подкрепляются выводами, основанными на слуховом опыте эксперта. Такую теорию он называет концепцией «стыка», которая подразумевает под собой исследование звучащей речи в тесной взаимосвязи технических методов, экспертных (акустических), а также юридических.

При этом надо иметь в виду, что идентификация – это всегда сравнительное исследование, поэтому для заключения о тождестве объектов необходимо для начала собрать и предоставить надлежащий образец звучащей речи подозреваемого.

При наличии круга предполагаемых авторов голосового сообщения необходимо отобрать у них образцы звучащей речи для сравнительного исследования. Е.И. Галяшина пишет, что экспертное решение о принадлежности голоса и речи, записанного на фонограмме конкретному проверяемому (подозреваемому) лицу, должно основываться на положениях, дающих возможность проверить в условиях судопроизводства обоснованность и достоверность сделанных выводов на базе общепринятых научных и практических данных[284].

---

[283] См.: *Каганов А.Ш.* Звучащая речь как объект криминалистической экспертизы. – М.: Юрайт, 2023. – С. 270.

[284] См.: *Галяшина Е.И.* К вопросу о достоверности криминалистической идентификации личности по цифровым фонограммам устной речи. С. 19–24.

Получение образца звучащей речи относится к задачам следователя. Необходимо предварительно уточнить у эксперта, каким именно должен быть образец, имеет ли значение, что именно и сколько по времени должен произносить подозреваемый. Следователю необходимо соблюсти все рекомендации эксперта касаемо как самого процесса сбора образца, так и используемой для этого техники.

Однако не во всех случаях подозреваемый готов идти навстречу следствию и предоставить свой голос для записи. В некоторых случаях следователю необходимо проверить лицо, которому еще не сообщено о проведении экспертизы в отношении его голоса. В таких ситуациях получить запись голоса для экспертизы можно, назначив проведение оперативно-розыскных мероприятий.

Оперативные работники вправе использовать любую технику для записи речи, в том числе и устройства, сведения о которых относятся к государственной тайне. Они также могут предоставлять копию звукозаписи следователю. «Допускается представление материалов, документов и иных объектов, полученных при проведении ОРМ, в копиях (выписках), в том числе с переносом наиболее важных частей (разговоров, сюжетов) на единый носитель, о чем обязательно указывается в сообщении (рапорте) и на бумажном носителе записи переговоров»[285].

5. Экспертизы видеозаписей

Как отмечалось ранее, необходимость в назначении экспертиз по видеозаписям возросла с популяризацией мгновенных видеосообщений в мессенджерах.

Криминалистическую экспертизу непосредственно сообщений-кружочков ученые не рассматривали, однако исследования экспертизы видеозаписей довольно обширны, в том числе видеозаписей, изъятых с мобильного устройства или смартфона.

[285] См.: Приказ МВД России, Министерства обороны РФ, ФСБ России, Федеральной службы охраны РФ, Федеральной таможенной службы, Службы внешней разведки РФ, Федеральной службы исполнения наказаний, Федеральной службы РФ по контролю за оборотом наркотиков, Следственного комитета РФ от 27.09.2013 № 776/703/509/507/1820/42/535/398/68 «Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд» // СПС «КонсультантПлюс».

Для экспертного исследования видеозаписей назначаются видеотехническая и портретная экспертизы. В рамках видеотехнической экспертизы проводится техническое исследование видеозаписей. Эксперты-видеотехники при производстве данного исследования ограничены в круге решаемых задач, а именно:

1) определение средней скорости движения объектов, зафиксированных в представленной на исследование видеограмме;

2) выявление монтажа и модификации видеограммы или ее части, представленной на исследование;

3) улучшение качества видеоизображений[286].

Портретная экспертиза производится в целях установления наличия или отсутствия тождества лиц, изображения которых представлены на различных носителях портретной информации (фотоснимках, кино- и видеозаписях) на основе изучения признаков внешнего облика человека[287].

В ходе портретной экспертизы учитываются разные факторы, влияющие на изображение на видеозаписи. Среди них выделяются следующие функционально-технические характеристики аппаратуры для видеозаписи: факторы материальной части средств видеозаписи; факторы процесса записи видеоизображения с камеры на носитель видеоинформации; факторы состояния внешности объекта запечатления, характеризующие объект фиксации на видеозаписи; факторы условий хранения видеозаписи[288].

Несомненно, все перечисленные факторы влияют на точность результатов исследования, но во многом его качество зависит от дальнейшего развития и совершенствования технологий автоматического распознавания лиц[289]. Действительно, некоторые авторы считают, что «традиционная методика портретной экспертизы, разработанная еще в прошлом столетии, ориентирована

---

[286] См.: О перспективах развития видеотехнической экспертизы // URL: https://мвд.рф/document/3382853?ysclid=lv5l28cpb0594385657 (дата обращения: 13.10.2023).

[287] См.: *Белкова Г.Г.* Некоторые проблемы криминалистической экспертизы видеоизображения // Новый юридический вестник. 2017. № 2 (2). С. 57–60.

[288] См.: *Ильин Н.Н.* Проблемные вопросы, связанные с автоматическим распознаванием человека по признакам внешности, запечатленным на видеоизображениях // Энциклопедия судебной экспертизы. 2018. № 4. С. 116–121.

[289] См.: *Долгинов С.Д.* Указ. соч.

преимущественно на фотоснимки с хорошо отобразившимися на них элементами лица, и в меньшей степени на видеоизображения, которые уступают по качеству, но выигрывают за счет динамики запечатленных движений»[290].

«Непрерывное развитие технологий в современном мире дало возможность разработать алгоритм для распознавания не только лиц, но и эмоциональных состояний, вплоть до сложных, составных эмоций. Каждая эмоция определяется по уникальной вариации сокращения лицевых мышц. Если действие одних мышц видно отчетливо, то других – едва заметно. Алгоритм находит конкретного человека по базе среди нескольких миллионов лиц за секунды. Важно, что эту способность он не утрачивает в «уличных» условиях, когда человек повернут вполоборота, надвинул на лоб шапку или надел солнечные очки. Технология устойчива к возрастным изменениям, перемене ракурса и освещенности[291]. На сегодняшний день одна из главных проблем технического характера – точность распознавания. Даже наиболее продвинутые в настоящее время технологии распознавания, построенные на основе сверхточной нейронной сети, «имеют точность в диапазоне 70–82 % для сложных сцен со множеством объектов, динамической сменой фона, поз и других параметров видеосцены»[292].

При назначении портретной экспертизы следователю необходимо внимательно отнестись к объектам, направляемым на исследование. А.С. Блохин, А.Б. Зотов, А.Ш. Каганов. Л.Ф. Назин отмечали важность происхождения видеозаписей: оно должно быть в обязательном порядке указано следователем (судом) в постановлении (определении) о назначении экспертизы, т. е. оно должно содержать краткое описание видеокадра, в котором запечатлен внешний облик исследуемого человека и указан источник происхождения видеозаписи, что весьма существенно для оценки ее достоверности. Осведомленность эксперта о ситуации, в которой возникла необходимость назначения портретной экспертизы, помогает

[290] См.: *Попов В.Л.* Особенности производства портретных экспертиз по низкокачественным видеоизображениям // Юридическая наука и правоохранительная практика. 2015. № 4. С. 156–162.
[291] См.: *Долгинов С.Д.* Указ. соч.
[292] См.: *Семенова А.Н., Аджиев Н.Д., Чочиева А.Н.* Сравнение современных методов детектирования объектов на изображении // Тенденции развития науки и образования. 2019. № 56-3. С. 28–31.

уяснить и уточнить вопросы, указанные в постановлении (определении), поставить и разрешить в процессе экспертизы дополнительные вопросы[293].

6. Экспертизы биологических следов

На устройстве, посредством которого было отправлено электронное сообщение, могут быть оставлены следы, отражающие биологические функции человека, такие как отпечатки пальцев, потожировые следы человека. Соответственно, устройство может быть отправлено на дактилоскопическую экспертизу, на молекулярно-генетическую экспертизу.

Современные возможности дактилоскопии представлены в работах С.С. Самищенко, Е.Р. Россинской, А.И. Бастрыкина, О.И. Авраменко. В современной дактилоскопии исследуются отдельные участки внутренней поверхности ладоней человека, также нижняя поверхность стоп ног человека, имеющая рисунок кожных покровов, аналогичный рисунку внутренней поверхности кистей рук. На сегодняшний момент предметом криминалистической дактилоскопии является установление конкретного лица, оставившего следы кожного покрова на месте происшествия, а также времени и условий следообразования.

Дактилоскопическое исследование можно назначить в том случае, если было выявлено, что определенное сообщение было отправлено с конкретного устройства, принадлежащего гражданину. Например, гражданин И. утверждает, что данное сообщение не отправлял, и у него взяли телефон и отправили сообщение без его ведома. В данном случае можно провести дактилоскопическую экспертизу, поставив перед ней вопрос: имеются ли на устройстве еще чьи-то отпечатки, кроме отпечатков гражданина И. Однако это будет считаться доказательством «от противного», которое, конечно, будет приниматься во внимание, но не будет являться идентификацией в полном смысле этого слова.

[293] См.: Концептуальные основы криминалистической экспертизы видеозаписей (теория, практика, методология исследования): монография / А.С. Блохин [и др.]. – М.: Юрлитинформ, 2011.

Возможна и обратная ситуация. Если будет установлено, что с определенного устройства было отправлено интересующее следствие сообщение, но подозреваемый отрицает, что это устройство принадлежит ему, то выявление его отпечатков пальцев позволит его изобличить.

Отпечаток пальца представляет собой потожировой след, и если предметом изучения дактилоскопии служат именно папиллярные узоры отпечатка, то сам состав потожирового вещества может лечь в основу иных видов экспертиз. Потожировой след человека Т.Ф. Моисеева определяет как «отпечаток потожировых выделений поверхности кожного покрова человека на различных соприкасающихся с ним предметах, ...отображающий индивидуальные и групповые свойства»[294]. «Представляет интерес также, что по составу вещества ПЖС возможно определить: пол и возраст человека; возможные заболевания (чаще всего патологии внутренних органов, ожирение и т. п.); относительное время оставления ПЖС одним и тем же человеком (давность образования следа); установление следов наркотических средств и парфюмерных изделий в ПЖС и пр.»[295].

Помимо потожирового вещества, на устройстве могут быть оставлены иные биологические выделения человека, такие как частицы кожного эпителия (от прикосновений пальцев рук или щеки, к которой прикладывают смартфон во время разговора), частицы слюны, крови и иных биологических выделений человека. Все они могут являться объектами экспертного генетического исследования.

Задачи такого исследования могут быть как идентификационные, т. е. установления тождества оставленных объектов лицу, подозреваемому в совершении преступления, так и диагностические, такие как определение половой принадлежности.

И.О. Перепечина отмечает, что «эксперты зачастую сталкиваются с проблемами следующего характера: при назначении судебных молекулярно-генетических

---

[294] См.: *Моисеева Т.Ф.* Комплексное криминалистическое исследование потожировых следов человека. – М.: Горец-издат, 2000. – С. 14.
[295] Там же. С. 112.

экспертиз сведения о событии преступления нередко представляются органами предварительного следствия слишком кратко, затрудняя восприятие характера происшедшего события, вопросы формулируются без учета обстоятельств дела, объекты исследования направляются без должного отбора и анализа»[296]. Исходя из этого, можно порекомендовать следователям подробнее излагать обстоятельства расследуемого события в постановлении о назначении экспертизы, направлять на экспертизу устройство, которое было изъято аккуратно, в перчатках, герметично упаковано. Также «важным фактором для обеспечения результативности экспертизы является взаимодействие следователя с экспертом»[297].

[296] См.: *Перепечина И.О., Галина Л.Р.* Использование методов ДНК-анализа при расследовании преступлений, связанных с доведением несовершеннолетних до самоубийства (ст. 110 УК РФ) // Преступное поведение несовершеннолетних и преступления, связанные с доведением их до самоубийства (ст.ст. 110–110.2 УК РФ): проблемы расследования и профилактики: материалы Всероссийской науч.-практ. конф. (Москва, 24 декабря 2020 г.) / Под общ. ред. Д.Н. Кожухарика. – М.: Московская академия Следственного комитета Российской Федерации, 2021. – С. 125.
[297] Там же. С. 126.

Заключение

Автором были рассмотрены основные вопросы, связанные с исследованием криминалистически значимой информации из электронных сообщений. По итогам автором предложены технические и тактические средства и рекомендации по работе с такими сообщениями. Проведенное исследование позволило соискателю сформировать следующие научные практические выводы и предложения, отражающие поставленные цель и задачи исследования.

1. Было раскрыто и сформулировано понятие электронного сообщения, которое представляет собой ограниченный объем компьютерной информации, предназначенный для передачи от отправителя через средства электросвязи определенному количеству пользователей, характеризующийся следующими группами свойств: содержание и сопутствующая информация.

1.1 Под содержанием электронного сообщения понимается ограниченный объем компьютерной информации, который может представлять собой как текстовую информацию, так и графическую, аудиовизуальную и иную, воспринимаемую человеком посредством компьютерных устройств.

1.2 Под сопутствующей информацией понимаются технические данные, описывающими характер сообщения и особенности его прохождения через информационно-телекоммуникационную сеть.

2. Были выделены основы для классификации электронных сообщений для целей криминалистического исследования. Была разработана классификация электронных сообщений по основаниям в зависимости от:

2.1. возможности непосредственного восприятия неподготовленным получателем на: зашифрованные и незашифрованные;

2.2. возможности проведения индексированного поиска по ключевым словам и фразам на: индексируемые и неиндексируемые;

2.3. программных средств создания и отправки, созданные и отправленные: с помощью одного и того же средства; с помощью стороннего средства; программным средством без участия человека;

2.4. критерия достоверности, понимаемой как оценка правдивости передаваемых сведений, сообщения делятся на дезинформационные (образующие состав преступления (криминальные) и ложные, но не содержащие признаков состава преступления (предкриминальные)) и не дезинформационные (правдивые).

3. Автором были исследованы и подробно освящены в работе электронные средства и программное обеспечение, используемые для обмена электронными сообщениями, выделены их криминалистически значимые характеристики.

4. Была разработана методика установления места нахождения электронных средств, программного обеспечения и места хранения электронных сообщений на устройствах и носителях.

5. Автором были рассмотрены возможности криминалистической идентификации отправителей электронных сообщений. В ходе исследования данного вопроса было выявлено, что в использовании идентификации в алгоритме доказывания для установления отправителя электронного сообщения потенциально идентифицирующими (отображающими) объектами могут выступать: данные учетной записи (аккаунта) или адреса, с которого было отправлено сообщение; цифровые следы[298] на устройстве; признаки в самом содержании сообщения; признаки, содержащиеся в активности пользователя в сети; звучащая речь в голосовом сообщении; видеоизображения в сообщениях; биологические следы на устройстве.

Ни по одному из источников на сегодняшний момент не возможна идентификация лица в криминалистическом смысле. Установление лица, написавшего сообщение и совершившего преступление, является задачей

[298] Любая криминалистически значимая компьютерная информация, т. е. сведения (сообщения, данные), находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе с помощью электромагнитных взаимодействий либо передающиеся по каналам связи посредством электромагнитных сигналов (В.Б. Вехов).

следователя в ходе расследования и решается комплексно: использованием идентификации в алгоритме доказывания, сбором доказательств, установлением фактов с опорой на данные об идентификации пользователя в интернет-среде.

6. Был исследован процесс индексированного поиска электронных сообщений, относимых к расследуемому событию. В рамках данного исследования был разработан алгоритм методических рекомендаций по подбору ключевых слов для индексации с целью поиска относимой информации в массиве электронных сообщений, составляющих электронную переписку, который характеризуется следующими этапами:

I. Формулировка цели;

II. Оценка имеющейся у нас информации в соответствии с расследуемым событием;

III. Сопоставление имеющейся и искомой информации;

IV. Выявление основных слов, фраз, которые могут содержаться в искомой информации;

V. Определение особенностей, которые могут быть присущи общению между предполагаемыми адресатами (сленг, шифр). Формирование синонимов с учетом характерных особенностей;

VI. Формирование заключительного списка ключевых слов.

7. Были разработаны тактическо-криминалистические рекомендации по изъятию и фиксации электронных сообщений, по использованию следователем данных об электронных сообщениях в процессе расследования в качестве криминалистически значимой информации.

8. Рассмотрены возможности использования электронных сообщений в процессе допроса подозреваемого (обвиняемого).

9. Раскрыты возможности судебно-экспертного исследования электронных сообщений, были разработаны тактические рекомендации по назначению судебных экспертиз в ходе предварительного расследования преступления, обоснованные современной судебно-следственной практикой.

Изученная в данном исследовании проблема является важной и актуальной, так как развитие современных технических достижений и использование их в преступном мире предъявляет все большие требования к криминалистам. Настоящее исследование обуславливает необходимость дальнейшей научной разработки отдельных аспектов обозначенной проблемы, разработки методических рекомендаций по исследованию электронных сообщений в ходе расследования. Авторское исследование технических, тактических и методических аспектов работы с электронными сообщениями может лечь в основу последующих работ, связанных с криминалистическим исследованием электронных доказательств.

Библиография

Нормативные правовые акты Российской Федерации

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // СПС «Консультант Плюс».

2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 04.08.2023) // СПС «КонсультантПлюс».

3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // СПС «Консультант Плюс».

4. Федеральный закон от 31.05.2001 № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» // СПС «КонсультантПлюс».

5. Федеральный закон от 06.07.2016 № 374-ФЗ (ред. от 29.12.2022) «О внесении изменений в Федеральный закон “О противодействии терроризму” и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности // СПС «Гарант».

6. Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ // СПС «КонсультантПлюс».

7. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ // СПС «КонсультантПлюс».

8. Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» // СПС «КонсультантПлюс».

9. Постановление Правительства РФ от 27.10.2018 № 1279 «Об утверждении Правил идентификации пользователей информационно-телекоммуникационной сети “Интернет” организатором сервиса обмена мгновенными сообщениями» // СПС «КонсультантПлюс».

10. Постановление Правительства РФ от 10.09.2007 г. № 575 «Об утверждении Правил оказания телематических услуг связи» // СПС «Гарант».

11. Постановление Правительства РФ от 31.12.2021 № 2607 «Об утверждении Правил оказания телематических услуг связи» (с изменениями и дополнениями) // СПС «Гарант».

12. Приказ МВД России, Министерства обороны РФ, ФСБ России, Федеральной службы охраны РФ, Федеральной таможенной службы, Службы внешней разведки РФ, Федеральной службы исполнения наказаний, Федеральной службы РФ по контролю за оборотом наркотиков, Следственного комитета РФ от 27.09.2013 № 776/703/509/507/1820/42/535/398/68 «Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд» // СПС «КонсультантПлюс».

13. Приказ Минюста России от 27.12.2012 № 237 «Об утверждении Перечня родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России, и Перечня экспертных специальностей, по которым представляется право самостоятельного производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Минюста России» // СПС «Гарант».

14. Приказ ФСБ России от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения» // СПС «Гарант».

15. Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств» СТО БР ИББС-1.3-2016» (принят и введен в действие Приказом Банка России от 30.11.2016 № ОД-4234) // СПС «КонсультантПлюс».

Зарубежные нормативные правовые акты

16. Декларация о свободе обмена информацией в интернете (принята Комитетом Министров Совета Европы от 28.05.2003 на 840-м заседании заместителей Министров) // СПС «КонсультантПлюс».

17. Модельный закон «Об электронной торговле» (принят в г. Санкт-Петербурге 25.11.2008 на 31-м пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ, Постановление № 31-12) // СПС «КонсультантПлюс».

18. Резолюция № С 42/2008 Всемирного почтового союза «Изучение о придании постоянного характера Всемирной почтовой конвенции и Соглашению о почтовых платежных услугах» (принята в г. Женеве 12.08.2008 XXIV Конгрессом Всемирного почтового союза) // СПС «Консультант Плюс».

19. Типовой закон ЮНИСИТРАЛ об электронной торговле // URL: https://uncitral.un.org/ru/texts/ecommerce/modellaw/electronic_commerce (дата обращения: 20.12.2023).

20. 18 U.S. Code Chapter 119 – Wire and electronic communications interception and interception of oral communications // URL: https://www.law.cornell.edu/uscode/text/18/part-I/chapter-119 (дата обращения: 20.12.2023).

21. 18 U.S. Code § 2703 – Required disclosure of customer communications or records // URL: https://www.law.cornell.edu/uscode/text/18/2703 (дата обращения: 10.10.2023).

22. The Privacy and Electronic Communications (EC Directive) Regulations 2003 // URL: https://www.legislation.gov.uk/uksi/2003/2426/contents/made (дата обращения: 10.10.2023).

23. Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA patriot act) act of 2001 // Public law 107–56– Oct. 26, 2001.

24. U.S. Constitution – Fourth Amendment // URL: https://www.law.cornell.edu/constitution/fourth_amendment (дата обращения: 25.05.2023).

Судебные решения российских судов и материалы судебной практики

Акты Пленума Верховного Суда Российской Федерации

25. Постановление Пленума Верховного суда России от 21.12.2010 № 28 «О судебной экспертизе по уголовным делам» // СПС «КонсультантПлюс».

26. Постановление Пленума Верховного Суда РФ от 25.12 2018 г. № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации)» // СПС «Гарант».

27. Постановление Пленума ВС РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть “Интернет”» // СПС «Консультант Плюс».

Иные судебные решения

28. Апелляционное постановление Верховного Суда Чувашской Республики № 22-2095/2018 от 20 сентября 2018 г. по делу № 22-2095/2018 // URL: https://sudact.ru/regular/doc/G7XjNyFHR5Lq/?regular-txt=&regular-case_doc=&regular-lawchunkinfo=&regular-date_from=&regular-date_to=&regular-

workflow_stage=&regular-area=&regular-court=&regular-judge=&_=1713701692989&snippet_pos=1058#snippet (дата обращения: 20.01.2023).

29. Определение Восьмого кассационного суда общей юрисдикции от 24.06.2022 № 88-11303/2022 // URL: http://8kas.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=24390969&case_uid=80db1ca9-aea3-4653-b066-32df8e53fc40&delo_id=2800001&new=2800001 (дата обращения: 14.04.2024).

30. Определение Конституционного Суда РФ от 20.03.2007 № 178-О-О «Об отказе в принятии к рассмотрению жалобы гражданина Донского Александра Павловича на нарушение его конституционных прав пунктами 4 и 6 части первой и частью третьей статьи 6 Федерального закона “Об оперативно-розыскной деятельности” и статьями 13, 89 и 186 Уголовно-процессуального кодекса Российской Федерации» // СПС «КонсультантПлюс».

31. Определение Конституционного Суда РФ от 25.01.2018 № 189-О «Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Д.А. на нарушение его конституционных прав статьями 176,177 и 195 УПК РФ» // СПС «КонсультантПлюс».

32. Определение Седьмого кассационного суда общей юрисдикции от 19.04.2022 №№ 88-5860/2022, 2-6379/2021 // URL: http://7kas.sudrf.ru/modules.php?name=sud_delo&srv_num=1&H_date=19.04.2022 (дата обращения: 14.04.2024)

33. Приговор Кировского районного суда г. Красноярска (Красноярский край) № 1-242/2018 от 9 июля 2018 г. по делу № 1-242/2018 // URL: https://sudact.ru/regular/doc/LxeUj9ESahoP/?regular-txt=&regular-case_doc=&regular-lawchunkinfo=&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=&regular-court=&regular-judge=&_=1713701978587&snippet_pos=7748#snippet (дата обращения: 20.01.2023).

34. Приговор Комсомольского районного суда г. Тольятти (Самарская область) № 1-93/2017 от 17 марта 2017 г. по делу № 1-93/2017 // URL:

https://sudact.ru/regular/doc/tvlXejt5ag6u/?regular-case_doc=&regular-lawchunkinfo=&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=&regular-court=&regular-judge=&_=1713701172091&snippet_pos=12720#snippet (дата обращения: 20.01.2023).

35. Решение Тверского районного суда г. Москвы от 21.03.2022 по делу № 02-2473/2022 // СПС «Гарант».

Иные документы

36. ГОСТ Р 53898-2013 «Системы электронного документооборота. Взаимодействие систем управления документами. Требования к электронному сообщению» // СПС «КонсультантПлюс».

37. ГОСТ Р ИСО 15489-1-2007. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Общие требования (утв. Приказом Ростехрегулирования от 12.03.2007 № 28-ст) // СПС «КонсультантПлюс».

38. Межгосударственный стандарт ГОСТ 20886-85 «Организация данных в системах обработки данных. Термины и определения» (утв. постановлением Государственного комитета СССР по стандартам от 31.01.1985 № 240) // СПС «Гарант».

Диссертационные исследования и авторефераты диссертаций

39. *Байрамова Ф.О.* Исследование акцента в интерферированной русской речи: на материале русской речи азербайджанцев: автореф. дис. ... канд. филол. наук: 10.02.01, 10.02.21. – М., 2012. – 22 с.

40. *Баранов Ю.Н.* Теоретические основы применения лингвистических знаний в криминалистике при производстве фоноскопических и автороведческих экспертиз: дис. … канд. юрид. наук: 12.00.09. – М.: РГБ, 2005. – 202 с.

41. *Беспамятнова Г.Н.* Языковая личность телевизионного ведущего: дис. ... канд. филол. наук: 10.02.04. – Воронеж, 1994. – 217 с.

42. *Воробьева А.А.* Методика идентификации интернет-пользователя на основе стилистических и лингвистических характеристик коротких электронных сообщений: дис. … канд. наук. – СПб., 2017. – 154 с.

43. *Вул С.М.* Об использовании признаков письменной речи в криминалистической экспертизе письма: автореф. дис. ... канд. юрид. наук. – Харьков, 1975.

44. *Зазулин А.И.* Правовые и методологические основы использования цифровой информации в доказывании по уголовному делу: дис. … канд. юрид. наук. – Екатеринбург, 2018. – 251 с.

45. *Комиссаров А.Ю.* Криминалистическое исследование письменной речи с использованием ЭВМ: дис … канд. юрид. наук: 12.00.09. – М., 2001. – 224 с.

46. *Романов А.С.* Методика и программный комплекс для идентификации автора неизвестного текста: автореф. дис. … канд. тех. наук: 05.13.18. – Томск, 2010. – 237 с.

47. *Шевелев О.Г.* Разработка и исследование алгоритмов сравнения стилей текстовых произведений: дис. ... канд. техн. наук: 05.13.18. – Томск, 2006. –176 с.

Монографии, учебники, учебные пособия

48. Антология кинизма. Фрагменты сочинений кинических мыслителей / Антисфен, Диоген, Кратет, Керкид, Дион и др. – М.: Наука, 1984. – 400 с.

49. *Ахохова Е.А.* Семиотика и лингвистика: Конспект лекций: учеб. пособие. – Нальчик: Полиграфсервис и Т, 2007. – 44 с.

50. *Баев О.Я.* Тактика следственных действий. – М.: Юрлитинформ, 2013. – 456 с.

51. *Безлепкин Б.Т.* Комментарий к Уголовно-процессуальному кодексу Российской Федерации. – М.: Проспект, 2021. – 640 с.

52. *Белкин Р.С.* Курс криминалистики: учеб. пособие для вузов. 3-е изд., доп. – М.: НОРМА, 2001. – 837 с.

53. *Браун С.* «Мозаика» и «Всемирная паутина» для доступа к Internet: пер. с англ. – М.: СК Пресс, 2016. – 167 с.

54. *Брусиловский А.Е.* Судебно-психологическая экспертиза. Ее предмет, методика и пределы. – Харьков, 1929.

55. *Брусиловский А.Е., Строгович М.С.* Свидетельские показания в качестве судебных доказательств // Методика следственной работы. – Киев, 1934.

56. *Васильев А.А., Демин К.Е.* Электронные носители данных как источники получения криминалистически значимой информации: учеб. пособие. – М.: МГОУ, 2009. – 198 с.

57. *Вехов В.Б.* Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки: монография. – Волгоград: ВА МВД России, 2008. – 404 с.

58. *Викторов А.Б., Остроухов А.В., Лобанова М.А.* О возможности создания автоматизированного комплекса диагностирования обликовых признаков // Информатизация и информационная безопасность правоохранительных органов. – М., 2006.

59. *Винберг А.И., Эйсман А.А.* Фототелеграфия и звукозапись в криминалистике. – М., 1946. С. 21.

60. Винер, Н. Кибернетика и общество / Н. Виннер. - М. : Издательство иностранной литературы, 1958. – 199с.

61. *Галицкий А.В., Рябко С.Д., Шаньгин В.Ф.* Защита информации в сети – анализ технологий и синтез решений. – М.: ДМК Пресс, 2004. – 616 с.

62. *Гросс Г.* Руководство для судебных следователей как система криминалистики. – М., 2002. – 1088 с.

63. *Губанов Д.А., Новиков Д.А., Чхартишвили А.Г.* Социальные сети: модели информационного влияния, управления и противоборства. – М.: Физматлит, 2010. – 228 с.

64. *Гуц А.К.* Кибернетика: учебное пособие. – Омск: Изд-во Омск. гос. ун-та, 2014. – 188 с.

65. *Дворецкий И.Х.* Латино-русский словарь. – М.: Русский язык, 1976. – 1088 с.

66. *Жванков В.А.* Человек как носитель криминалистически значимой информации. – М.: АПО, 1993. – 36 с.

67. *Журавлева А.А., Коваль С.Л.* Диагностика психологических качеств диктора по устной речи // Труды международной конференции по компьютерной лингвистике и интеллектуальным технологиям «Диалог 2007». – М., 2007. С. 183–187.

68. *Жижина М.В., Завьялова Д.В.* Расследование преступлений в сфере компьютерной информации в Российской Федерации и зарубежных странах. – М.: Проспект, 2023. – 136 с.

69. *Зинин А.М.* Криминалистическая идентификация человека по признакам внешности: учебное пособие для вузов / А. М. Зинин [и др.] ; под редакцией А. М. Зинина. — 2-е изд. — Электрон. дан. — Москва: Юрайт, 2022. – 323с.

70. *Ивлев Ю.В.* Логика для юристов / Под ред. М.Н. Марченко, Е.А. Суханова, П.Ф. Лунгу. – М.: Юридический колледж МГУ, 1996. – 304 с.

71. *Игнатьев М.Е.* Фактор внезапности, его процессуальное и криминалистическое значение для расследования преступлений. – М.: Юрлитинформ, 2004. – 141 с.

72. *Каганов А.Ш.* Звучащая речь как объект криминалистической экспертизы. – М.: Юрайт, 2023. – 270 с.

73. *Колдин В.Я.* Вещественные доказательства: Информационные технологии процессуального доказывания / Под общ. ред. д. ю. н., проф. В.Я. Колдина. – М.: НОРМА, 2002. – 768 с.

74. *Колдин В.Я.* Судебная идентификация. – М.: ЛексЭст, 2002. – 528 с.

75. *Комаров И.М.* Проблемы киберкриминалистики (цифровой криминалистики) // Проблемы криминалистики / Г.М. Меретуков [и др.]. – Краснодар: КубГАУ, 2018. – С. 133–137.

76. Концептуальные основы криминалистической экспертизы видеозаписей (теория, практика, методология исследования): монография / А.С. Блохин [и др.]. – М.: Юрлитинформ, 2011. – 200 с.

77. *Краснова Л.Б.* Компьютерные объекты в уголовном процессе и криминалистике: учеб. пособие / Науч. ред. В.А. Мещеряков. – Воронеж: Изд-во Воронеж. гос. ун-та, 2006.

78. Криминалистика: учебник / Отв. ред. Н.П. Яблоков. 3-е изд., перераб. и доп. – М.: Юристъ, 2005. – 781 с.

79. Криминалистика: учебник / Под ред. д-ра юрид. наук, проф. И.М. Комарова – М.: Биоинформсервис, 2023. – 712 с.

80. Криминалистика: учебник / Под ред. Н.П. Яблокова. 4-е изд., перераб. и доп. – М.: Юр.Норма, НИЦ ИНФРА, 2019. – 752 с.

81. Криминалистика: учебник для бакалавров / Под редакцией Л.Я. Драпкина. – М.: Юрайт, 2015. – 831 с.

82. *Крылов В.В.* Расследование преступлений в сфере информации. – М.: Городец, 1998. – 264 с.

83. *Крылов В.В.* Современная криминалистика. Правовая информатика и кибернетика. – М.: ЛексЭст, 2007. – 270 с.

84. *Леонтьев А.А., Шахнарович А.М., Батов В.И.* Речь в криминалистике и судебной психологии. – М., 1977. – 62 с.

85. *Моисеева Т.Ф.* Комплексное криминалистическое исследование потожировых следов человека. – М.: Горец-издат, 2000. – 223 с.

86. *Образцов В.А., Бертовский Л.В., Бертовская Н.Л.* Фикции в криминальной, оперативно-розыскной и следственной практике: монография. – М.: Юрлитинформ, 2012. – 408 с.

87. *Образцов В.А.* Криминалистика. Цикл лекций по новой программе курса. – М.: Юрикон, 1994. – 208 с.

88. *Осипенко А.Л.* Сетевая компьютерная преступность. Теория и практика борьбы: монография. – Омск: Омская академия МВД России, 2009. – 480 с.

89. Основы экспертного криминалистического исследования магнитных фонограмм / А.А. Ложкевич [и др.]. – М.: ВНИИ МВД СССР, 1977.

90. *Перепечина И.О.* Генетическая идентификация личности // Криминалистика: учебник / Под ред. д-ра юрид. наук, проф. И.М. Комарова. Гл. 14. – М.: Юрлитинформ, 2023.

91. *Першин А.Н.* Документированная информация: криминалистические подходы к понятию и исследованию Монография / А.Н. Першин – Москва: Проспект, 2020. – 312с.

92. *Россинская Е.Р., Галяшина Е.И.* Настольная книга судьи. Судебная экспертиза. – М., 2010. – 464 с.

93. *Россинская Е.Р., Семикалентова А.И., Рядовский И.А.* Теория информационно-компьютерного обеспечения криминалистической деятельности: монография. – М.: Проспект, 2022. – 256.

94. *Россинская Е.Р.* Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе. – М: Норма, 2006. – 218 с.

95. *Саенко Г.В., Тушканова О.В.* Компьютерная экспертиза. Исследование компьютерной информации. – М.: ЭКЦ МВД России, 2010.

96. Семантические исследования в судебной лингвистической экспертизе: методическое пособие / А.М. Плотникова [др.]; под ред. проф. С.А. Смирновой. – М.: ФБУ РФЦСЭ при Минюсте России, 2018. – 136 с.

97. *Смит П., Бэрри К., Пулфорд А.* Коммуникации стратегического маркетинга. – М.: Юнити-Дана, 2001. – 415 с.

98. Собирание электронных доказательств по уголовным делам на территории России и зарубежных стран: опыт и проблемы / Под общ. и науч. ред. С.П. Щербы. – М.: Проспект, 2022. – 168 с.

99. *Сотов А.И.* Компьютерная информация под защитой. Правовое и криминалистическое обеспечение безопасности компьютерной информации: монография. – М.: Ru-science.com, 2017. – 127 с.

100. *Тушканова О.В.* Терминологический справочник судебной компьютерной экспертизы: справочное пособие. – М.: ЭКЦ МВД России, 2005. – 568 с.

101. *Федотов Н.Н.* Форензика – компьютерная криминалистика. – М.: Юридический Мир, 2007. – 432 с.

102. *Центров Е.Е.* Руководство по следственной тактике : монография / Е.Е. Центров. – Москва : Норма : ИНФРА-М, 2024. – 576с.

103. *Шаньгин В.Ф.* Защита компьютерной информации. Эффективные методы и средства. – М: ДМК Пресс, 2010. – 544 с.

104. *Шеннон К.* Математическая теория связи // Работы по теории информации и кибернетике: сборник статей: пер. с англ. / Предисл. А.Н. Колмогорова; под ред. Р.Л. Добрушина и О.Б. Лупанова. – М.: Издательство иностранной литературы, 1963. – С. 243–322.

105. *Шеннон К.Э.* Работы по теории информации и кибернетике: Сборник статей: Пер. с англ. / С предисл. А.Н. Колмогорова; под ред. Р.Л. Добрушина и О.Б. Лупанова. – М.: Изд-во иностранной литературы, 1963. – 829 с.

106. *Шеннон К.* Теория связи в секретных системах // Работы по теории информации и кибернетике: сборник статей: пер. с англ. / Предисл. А.Н. Колмогорова; под ред. Р.Л. Добрушина и О.Б. Лупанова. – М.: Издательство иностранной литературы, 1963. – С. 333–402.

107. Электронные носители информации в криминалистике: монография / И.В. Александров [и др.]. – М.: Юрлитинформ, 2017. –300 с.

Методические материалы

108. Производство судебной компьютерно-технической экспертизы. I. Общая часть. II. Диагностическое и идентификационное исследование

аппаратных средств: методическое пособие. – М.: ФБУ РФЦСЭ при Минюсте России, 2009. – 79 с.

109. Производство судебной компьютерно-технической экспертизы. Часть V. Актуальные задачи исследования компьютерной информации (методическое пособие) / Под ред. А.И. Усова. – М.: ЭКОМ, 2011. – 270 с.

Научные статьи

110. *Антонович Е.К.* «Использование цифровых технологий при допросе свидетелей на досудебных стадиях уголовного судопроизводства (сравнительно-правовой анализ законодательства Российской Федерации и законодательства некоторых иностранных государств)» С. 1 // СПС «Консультант Плюс».

111. *Архипова Н.А.* Тактика осмотра и выемки электронных сообщений, передаваемых по сетям электросвязи // Закон и право. 2018. № 6. С. 132–135.

112. *Багмет А.М., Скобелин С.Ю.* Особенности применения криминалистической техники для извлечения и анализа данных мобильных устройств // Сборник материалов Международной научно-практической конференции «Совершенствование деятельности правоохранительных органов по борьбе с преступностью в современных условиях» (1–2 ноября 2013 г.). Вып. 10. Тюмень: ТГАМЭУП, 2013. С. 13–17.

113. *Баженов С.В.* Оперативно-розыскное мероприятие «получение компьютерной информации // Научный вестник Омской академии МВД России, 2017. № 2. С. 31–34.

114. *Белкова Г.Г.* Некоторые проблемы криминалистической экспертизы видеоизображения // Новый юридический вестник. 2017. № 2 (2). С. 57–60.

115. *Васюков В.Ф.* Некоторые вопросы проведения следственных действий, направленных на обнаружение, фиксацию и изъятие электронных сообщений, переданных посредством мобильных абонентских устройств сотовой связи // Российский следователь. 2016. № 23. С. 15–18.

116. *Вехов В.Б., Смагоринский Б.П., Ковалев С.А.* Электронные следы в системе криминалистики // Судебная экспертиза. 2016. Вып. 2 (46). – С. 10–19.

117. *Викторов А.Б., Остроухов А.В., Лобанова М.А.* О возможности создания автоматизированного комплекса диагностирования обликовых признаков // Информатизация и информационная безопасность правоохранительных органов. Сб. трудов XV Международной научной конференции. 23–24 мая 2006 г. – М.: Академия управления МВД России, 2006. – С. 328–331.

118. *Воробьева А.А., Гвоздев А.В.* Идентификация анонимных пользователей Интернет порталов на основании технических и лингвистических характеристик пользователя // Научно-технический вестник механики и оптики. 2014. № 1 (89). С. 139–144.

119. *Галаган Т.А., Казаков З.А.* Разработка информационной системы «Служба биллинга» // Вестник Амурского государственного университета. Серия: Естественные и экономические науки. 2013. № 63. С. 27–31.

120. *Галяшина Е.И.* Актуальные проблемы экспертизы цифровых фонограмм // Теорія та практика судовой експертизи і кримі: Зборник научных трудов. Выпуск 8. Харюв: Право, 2008. С. 248–257.

121. *Галяшина Е.И.* К вопросу о достоверности криминалистической идентификации личности по цифровым фонограммам устной речи // Известия Тульского государственного университета. Экономические и юридические науки. 2016. № 3-2. С. 19-24.

122. *Галяшина Е.И.* Об истории судебной фоноскопической экспертизы // Вестник Университета имени О.Е. Кутафина. 2014. № 3. С. 181–195.

123. *Галяшина Е.И.* Прикладные основы фоноскопической экспертизы // Теория и практика судебной экспертизы: сборник монографий. – СПб.: Питер, 2003.

124. *Галяшина Е.И.* Разграничение деятельности судебного эксперта-лингвиста и лингвиста-аналитика: компетенции, методы и технологии // Acta

Linguistica Petropolitana. Труды института лингвистических исследований. 2019. Vol. 15.1. P. 104–129.

125. *Галяшина Е.И.* Семиотика эмотиконов и анимационных картинок в аспекте судебной лингвистической экспертизы // Вестник Университета имени О.Е. Кутафина. 2022. № 2. – С. 45–47.

126. *Галяшина Е.И.* Судебная лингвистическая экспертиза и пределы допустимости использования методов лингвистической науки // Вестник Московского университета МВД России. 2018. № 4. С. 31–36.

127. *Гасанова Р.Б. (Печникова Р.Б.)* Идентификационное значение голосовых сообщений при расследовании преступлений // Научная школа уголовного процесса и криминалистики Санкт-Петербургского государственного университета: материалы конференций 2020–2021 годов; сборник статей / кол. авторов; под. ред. Н.П. Кирилловой, С.П. Кушниренко, Н.Г. Стойко (отв. ред.), В.Ю. Низамова (отв. ред.). – М.: РУСАЙНС, 2021. – С. 85–88.

128. *Громова А.В., Литвинова Т.А.* Компьютерные технологии в судебной автороведческой экспертизе: проблемы и перспективы использования // Вестник Волгоградского государственного университета. 2020. № 1. С. 77–88.

129. *Долгинов С.Д.* Цифровые видеоизображения в криминалистической идентификации // Ex jure. 2022. № 3. С. 116–127.

130. *Ильин Н.Н.* Проблемные вопросы, связанные с автоматическим распознаванием человека по признакам внешности, запечатленным на видеоизображениях // Энциклопедия судебной экспертизы. 2018. № 4. С. 116–121.

131. *Ищенко Е.П., Костюченко О.Г.* Современные технико-криминалистические средства, применяемые для обнаружения доказательств на электронных носителях информации // Вестник Восточно-сибирского института МВД России. 2021. № 2. С. 181–189.

132. *Карнеева Л.М.* Судебная этика и тактика допроса // Этика предварительного следствия. 1976. № 15. С. 55–58.

133. *Колдин В.Я.* Анализ информационных полей как метод декодирования криминалистической информации // Вестник криминалистики. 2012. № 4 (44).

134. *Комиссаров В., Гаврилов М., Иванов А.* Обыск с извлечением компьютерной информации // Законность. 1999. № 3.

135. Компьютерная обработка текстов при помощи ИС «СМАЛТ» / А.А. Рогов [и др.] // Проблемы развития гуманитарной науки на Северо-западе России: опыт, традиции, инновации: Материалы научной конференции. – Петрозаводск, 2004. Т. 1.

136. *Корма В.Д., Образцов В.А.* К вопросу о структуре и особенностях криминалистической теории следственного познания // Сборник научных статей по материалам Всероссийской научно-практической конференции (с международным участием) «Современные проблемы отечественной криминалистики и перспективы ее развития». – Краснодар: Кубан. гос. аграр. ун-т им. И.Т. Трубилина, 2019. – С. 60–66.

137. *Маилян А.В.* Актуальные вопросы расследования и раскрытия кибермошенничества «Фишинг» // Философия права. 2022. № 2 (101). С. 112–115.

138. Межсайтовая лингвистическая идентификация интернет-пользователей / А.А. Воробьева [и др.] // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18, № 3. С. 447–456.

139. *Мещеряков В.А.* «Виртуальные следы» под «скальпелем Оккама» // Информационная безопасность регионов. 2009. № 1 (4). С. 28–33.

140. *Мещеряков В.А.* Криминалистические особенности дачи - получения взятки с использованием электронных платежных систем // Воронежские криминалистические чтения. 2007. № 8. С. 208-217

141. *Морозов Н.А.* Лингвистические спектры // Известия АН ОРЯС. 1915. Т. 20, кн. 4. С. 93−134.

142. *Назайкин А.Н.* Медиатекст будущего – «сенсотекст» // МедиаАльманах. 2019. № 5. С. 12−21.

143. *Назарова Т.В., Громова А.В.* Объекты и задачи лингвистических и автороведческих экспертиз, проводимых в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации // Судебная экспертиза Беларуси. 2016. № 1(2). С. 43–46.

144. *Нестеров А.Д.* Получение информации из облачных хранилищ при расследовании инцидентов в сфере информационной безопасности // Advances In law studies. 2015. № 22. // URL: http://sci-article.ru/stat.php?i=1433879423 (дата обращения: 14.05.2023).

145. *Никитин В.В.* Существующие системы аутентификации и идентификации пользователей: основные проблемы и направления их модернизации // Вестник Московского университета МВД России. 2014. № 2. С. 165–172.

146. *Олиндер Н.В., Гамбарова Е.А.* Проблемные вопросы поиска и восприятия информации о человеке в сети Интернет и ее использование при расследовании преступлений // Юридический вестник Самарского университета. 2016. Т. 2, № 4. С. 55–59.

147. *Перепечина И.О., Галина Л.Р.* Использование методов ДНК-анализа при расследовании преступлений, связанных с доведением несовершеннолетних до самоубийства (ст. 110 УК РФ) // Преступное поведение несовершеннолетних и преступления, связанные с доведением их до самоубийства (ст.ст. 110–110.2 УК РФ): проблемы расследования и профилактики: материалы Всероссийской науч.-практ. конф. (Москва, 24 декабря 2020 г.) / Под общ. ред. Д.Н. Кожухарика. – М.: Московская академия Следственного комитета Российской Федерации, 2021. – С. 121–126.

148. *Першин А.Н.* Электронный документ и электронное сообщение: понятие и особенности поиска в электронной среде // Научный вестник Омской академии МВД России. 2015. № 3 (58). С. 34–38.

149. *Печникова (Гасанова) Р.Б.* Индексация электронных сообщений, используемых в качестве доказательств при расследовании преступлений // Universum: экономика и юриспруденция. 2021. № 6 (81).

150. *Печникова Р.Б.* Криминалистическая тактика изъятия мобильных устройств для обеспечения сохранности электронной переписки» // Юридическое образование и наука. 2022. № 7. С. 16–19.

151. *Печникова Р.Б.* Алгоритм выявления ключевых слов и составления их списка для индексации электронных сообщений в ходе расследования преступлений // Юридическое образование и наука. 2023. № 2. С. 35–37.

152. *Печникова Р.Б.* Indexing of electronic messages during the investigation of crimes // Евразийская адвокатура. 2023. № 3 (62). С. 101–105.

153. *Печникова Р.Б.* Использование данных об электронных сообщениях в процессе допроса подозреваемого (обвиняемого) // Евразийский юридический журнал. 2023. № 7 (182). С. 354–357.

154. *Платенкин А.В.* Особенности использования электронных доказательств при проведении допроса подозреваемого // World science. 2016. Vol. 4, № 5 (9). С. 9–11.

155. *Подволоцкий И.Н.* Современные криминалистические тенденции идентификации человека по видеоизображенниям // Вестник Академии экономической безопасности МВД России. 2015. № 2. С. 54–56.

156. *Пономарев И.П.* Цифровое алиби и его проверка» // Вестник Воронежского государственного университета. 2011. № 2 (11). С. 437–444.

157. *Попов В.Л.* Особенности производства портретных экспертиз по низкокачественным видеоизображениям // Юридическая наука и правоохранительная практика. 2015. № 4. С. 156–162.

158. *Пучкова Д.В.* Особенности проведения лингвистической экспертизы текстов интернет-коммуникаций // Международный журнал гуманитарных и естественных наук. 2020. Вып. 1-12 (50). С. 111–114.

159. *Ратинов А.Р.* О допустимости и правомерности некоторых тактических приемов// Следственная практика. 1964. № 64. С. 106–115.

160. *Романов А.С., Шелупанов А.А., Бондарчук С.С.* Обобщенная методика идентификации автора неизвестного текста // Доклады ТУСУРа. 2010. № 1 (21), ч. 1. С. 108.

161. *Россинская Е.Р.* К вопросу о частной теории информационно-компьютерного обеспечения криминалистической деятельности» // Известия ТулГУ. Экономические и юридические науки. 2016. Вып. 3. Ч. 2: Юридические науки. С. 109–117.

162. *Россинская Е.Р.* Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности // Вестник Восточно-Сибирского института МВД России. 2019. № 2 (89). С. 193–202.

163. *Россинская Е.Р., Рядовский И.А.* Тактика и технология производства невербальных следственных действий по делам о компьютерных преступлениях: теория и практика // Киберпространство. 2021. Т. 74, № 9 (178). С. 102–118.

164. *Семенова А.Н., Аджиев Н.Д., Чочиева А.Н.* Сравнение современных методов детектирования объектов на изображении // Тенденции развития науки и образования. 2019. № 56-3. С. 28–31.

165. *Сидорова К.С.* Способы установления IP-адреса и сведений о нем при расследовании уголовных дел // Вестник Сибирского института бизнеса и информационных технологий. 2018. № 2. С. 88–92.

166. *Смушкин А.Б.* Виртуальные следы в криминалистике // Законность. 2012. № 8. С. 43–45.

167. *Смушкин А.Б.* Криминалистическое исследование мобильных устройств // Электронное приложение к российскому юридическому журналу №2. 2020. С.48-52.

168. *Соколов Ю.Н.* Наложение ареста на электронные сообщения, их осмотр и выемка («Российский следователь». 2020. № 10. С. 38–41) // СПС Консультант Плюс.

169. *Соколова Т.П.* Проблемы методического обеспечения судебной автороведческой экспертизы // Теория и практика судебной экспертизы в современных условиях: материалы VII Международной научно-практической конференции. – М.: РГ-Пресс, 2019. – С. 4–7.

170. *Сотов А.И.* Исследование электронной переписки путем индексации // Сборник материалов по результатам работы Международного научно-практического форума – круглого стола, посвященного памяти профессора кафедры криминалистики Колдина Валентина Яковлевича. – М.: Юрлитинформ, 2021 – С. 177–182.

171. *Сотов А.И.* Исследование электронной переписки путем индексации // Юридическое образование и наука. 2021. № 10. С. 33–36.

172. *Ткачев А.В.* Исследование компьютерной информации в криминалистике // Эксперт-криминалист. 2012. № 4. С. 5–8.

173. *Ткачев А.В.* К вопросу о придании особого процессуального и криминалистического статуса компьютерной (цифровой) информации // Эксперт-криминалист. 2022. № 2.

174. *Ткачев А.В.* К вопросу о разграничении цифровых (электронных) следов от других источников криминалистической информации // Сборник XXIII ежегодной Международной научно-практической конференции «Государство и право России в современном мире». – М.: Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2023. Т. 4. – С. 267–270.

175. *Хайруллова Э.Т., Шадрина Е.С.* Современное состояние дактилоскопической регистрации // Ученые записки казанского юридического института МВД России. 2019. Т. 4, № 2 (8). С. 92–96.

176. *Хмелев Д.В.* Распознавание автора текста с использованием цепей А.А. Маркова // Вестник МГУ. Сер.9. Филология. 2000. № 2. С. 115–126.

177. *Центров Е.Е.* Особенности использования сведений о закономерностях, изучаемых криминалистикой в процессе раскрытия и расследования преступлений // Вестник криминалистики. 2011. № 3 (39).

178. *Центров Е.Е.* Признание обвиняемым своей вины при отграничении его от вопросов и действий наводящего характера // Вестник Московского университета. Серия 11: Право. 2020. № 2. С. 33–44.

179. *Центров Е.Е.* Расследование преступлений: учет и преодоление современных тенденций, присущих криминальной среде // Вестник Московского университета. Сер. 11 Право. 2014. № 4. С. 70–77.

180. *Шевелев О.Г., Петраков А.В.* Классификация текстов с помощью деревьев решений и сетей прямого распространения // Вестник Томского государственного университетата. 2006. № 290. С. 300–307.

181. *Яковлев А.Н.* Правовой статус цифровой информации, извлекаемой из компьютерных и мобильных устройств: «электронная почта» // Вестник Воронежского института МВД России. 2014. № 4. С. 45–47.

Литература на иностранных языках

182. *Britz M.T.* Computer Forensics and Cyber Crime: An Introduction. – Pearson, 2013. – 386 p.

183. *Casey E.* Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. – Academic Press, 2011. – 840 p.

184. *Casey E.* Handbook of Digital Forensics and Investigation. – Academic Press, 2009. – 600 p.

185. Do Facebook status updates reflect subjective well-being? / P. Liu [et al.] // Cyberpsychology, behavior, and social networking. 2015. Vol. 18, No. 7. Pp. 373–379.

186. *Easttom Ch.* Computer Crime Investigation and the Law // Practical Guide to Computer Forensics Investigations / D.R. Hayes. – USA, Course Technology, 2011 – 517 p.

187. *EC-Council.* Computer Forensics: Investigating Data and Image Files. – Cengage Learning, 2016. – 151 p.

188. *Gottschalk P.* Fraud Investigation Reports in Practice. Convenience and Corporate Crime. – London: Routledge, 2023. – 228 p.

189. *Kersta L.G.* Voiceprint Identification // Nature. 1962. Vol. 196. Pp. 1253–1257.

190. *Kosinski M., Stillwell D., Youyou W.* Computer-based personality judgments are more accurate than those made by humans // Proceedings of the national Academy of Sciences of the United States of America (PNAS). 2015. Vol. 112, No. 4. Pp. 1036–1040.

191. *Maras M.-H.* Computer Forensics: Cybercriminals, Laws, and Evidence. – Jones & Bartlett Learning, 2014. – 408 p.

192. *Nelson B., Phillips A., Steuart C.* Guide to Computer Forensics and Investigations. – USA, CENGAGE, 2019. – 770 p.

193. *Orin S.* Kerr: Fourth Amendment Seizures of Computer Data // The Yale Law Journal. 2010. Vol. 119. Pp. 700–724. // URL: https://www.yalelawjournal.org/pdf/853_76rix2f4.pdf (дата обращения: 20.05.2023).

194. *Rodríguez Álvarez A.* No Words Needed? Emojis as Evidence in Judicial Proceedings // Legal developments on Cybersecurity and Related Fields. Law, Governance and Technology Series. Springer International Publishing, 2024.

195. *Sammons J.* The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. – Syngress, 2012. – 208 p.

196. *Stephenson P.* Investigating Computer Crime: A Primer. – London: Routledge, 2013. – 404 p.

197. *Waluyo A., Setiyo M.T., Mahfud A.Z.* Digital Forensic Analysis on Caller ID Spoofing Attack // 2022 7th International Workshop on Big Data and Information Security (IWBIS). 2022. 01-03 October.

198. *Waugh S., Adams A., Tweedie F.J.* Computational stylistics using Artificial Neural Networks // Literary and Linguistic Computing. 2000. Vol. 15, No. 2. Pp. 187–198.

Интернет-ресурсы

199. Атрибутор // URL: http://www.textology.ru/web.htm (дата обращения: 20.05.2023).

200. Безопасность платформы Apple. Май 2022 г. // URL: https://help.apple.com/pdf/security/ru_RU/apple-platform-security-guide-rs.pdf (дата обращения: 14.04.2024).

201. *Бозов А.А.* Методические рекомендации: Использование возможностей сотовой связи при раскрытии и расследовании преступлений // URL: https://alexboz.pravorub.ru/personal/30734.html?ysclid=lskn84o691724196356 (дата обращения: 10.10.2023).

202. *Жижина М.В.* Извлечение данных с мобильных телефонов: проблемы на практике // Уголовный процесс. 2024. № 3. Март. // URL: https://e.ugpr.ru/1071993?ysclid=lv2jzy6cfg597645352&fromId2=true&from=id2 (дата обращения: 14.04.2024).

203. *Иванов А.Н., Силантьев Д.Н.* Выемка электронной почты в сети Интернет // URL: http://www.crime-research.org/library/Removing.html (дата обращения: 23.11.2023).

204. *Иванов Н.А.* Применение специальных познаний при проверке «цифрового алиби» // URL: https://wiselawyer.ru/poleznoe/15880-primenenie-specialnykh-poznanij-proverke-cifrovogo-alibi?ysclid=lu8uhw6n54525886018 (дата обращения: 10.10.2023).

205. Идентификация, аутентификация и авторизация – в чем разница? // URL: https://www.kaspersky.ru/blog/identification-authentication-authorization-difference/29123/?ysclid=lv2qp0i6a1644362662 (дата обращения: 20.05.2023).

206. *Макаров А.* Исследование облачных хранилищ при расследовании преступлений // URL: https://www.anti-malware.ru/analytics/Technology_Analysis/analysis_cloud_storage_investigation_of_crimes (дата обращения: 14.01.2023).

207. О перспективах развития видеотехнической экспертизы // URL: https://мвд.рф/document/3382853?ysclid=lv5l28cpb0594385657 (дата обращения: 13.10.2023).

208. Правила пользования сайтом «ВКонтакте» // https://vk.com/terms?ysclid=lnnpsaqiy313123338 (дата обращения: 13.10.2023).

209. *Секераж Т.Н., Кузнецов В.О.* Комплексная судебная психолого-лингвистическая экспертиза: формы, виды, перспективы развития // URL: https://www.lingvisticheskaja-ekspertiza.com/post/2018/12/27/-d0-9a-d0-9e-d0-9c-d0-9f-d0-9b-d0-95-d0-9a-d0-a1-d0-9d-d0-90-d0-af-d0-a1-d0-a3-d0-94-d0?ysclid=lv5g816y24592296841 (дата обращения: 20.05.2023).

210. *Собецкий И.В.* О доказательственном значении лог-файлов // URL: http://www.bnti.ru/showart.asp?aid=806&lvl=01.02.01.&ysclid=liythp76wi586757589 (дата обращения: 10.10.2023).

211. Суд признал виновным фигуранта «дела 27 июля» Егора Жукова // URL: https://www.rbc.ru/rbcfreenews/5dea00d49a794767a9bc4b20?ysclid=lmixefzae010319 6460 (дата обращения: 27.02.2023).

212. Судебная автороведческая экспертиза // URL: http://www.sudexpert.ru/possib/author.php (дата обращения: 12.11.2023).

213. Штампомер – описание работы программы // URL: http://www.shtampomer.narod.ru/manual.htlm (дата обращения: 20.05.2023).

214. *Толчёнова М.* Идентификация, аутентификация, авторизация: чем они различаются // URL: https://skillbox.ru/media/code/identifikatsiya-autentifikatsiya-avtorizatsiya-chem-oni-razlichayutsya/?ysclid=lslnhvbgrx165365124 (дата обращения: 20.05.2023).

215. Emojis Are the New Language of Drug Deals—Especially for Teens // URL: https://www.verywellhealth.com/emoji-drug-code-educates-parents-about-drug-deals-7068968 (дата обращения: 20.06.2023).

216. Global network initiative [сайт]. Защита и развитие свободы выражения мнений и неприкосновенности частной жизни в информационно-коммуникационных технологиях // URL: https://globalnetworkinitiative.org/ (дата обращения: 20.01.2023).

217. ProtonMail или что же это на самом деле? // URL: https://habr.com/ru/post/227575/ (дата обращения: 29.04.2023).

218. *Smith R.E.* Authentication: from passwords to public keys // URL: https://archive.org/details/authenticationfr0000smit (дата обращения: 20.05.2023).

219. Stored Communications Act: Reform of the Electronic Communications Privacy Act (ECPA) / Congressional research service. 2015 // URL: https://fas.org/sgp/crs/misc/R44036.pdf (дата обращения: 12.01.2023).

220. WhatsApp: официальный сайт. Информация для правоохранительных органов // URL: https://faq.whatsapp.com/26000050 (дата обращения: 12.01.2023).

221. WeChat. The Forensic Aspects Of and Uses for Evidence from a Super-App // URL: https://belkasoft.com/WeChat-forensics (дата обращения: 14.10.2023).

222. ZyLAB General Search Language Guide // ZYLAB. 2016. P. 118. // URL: https://docs.zylab.com/articles/#!zylab-one-search-language-guide-publication/10824 (дата обращения: 20.05.2023).

Приложения

Приложение №1

Алгоритм составления списка ключевых слов для индексации

Приложение №2

Результаты анкетирования сотрудников следственного аппарата

В ходе исследования автором было собрано и обработано 120 анкет. Анкетирование проводилось путем личного заполнения печатных бланков респондентами.

В анкетировании принимали участие следователи, старшие следователи, следователи-криминалисты, руководители следственных органов. Участники анкетирования работают в межрайонных следственных отделах, отделе криминалистики следственного управления следственного комитета России, главных следственных управлениях, следственном управлении Министерства внутренних дел России. География анкетирования охватывает различные субъекты Российской Федерации.

В анкетировании принимали участия респонденты, занимающие следующие должности:

Следователь (СК РФ)	27	22,5%
Старший следователь (СК РФ)	16	13,3%
Следователь-криминалист (СК РФ)	14	11,6%
Старший следователь-криминалист (СК РФ)	10	8,3%
Следователь по особо важным делам (СК РФ)	8	6,7%
Инспектор (СК РФ)	1	0,8%
Руководитель следственного органа (СК РФ)	1	0,8%

Заместитель руководителя следственного органа	2	1,6%
Следователь (МВД РФ)	26	21,7%
Старший следователь (МВД РФ)	12	10%
Начальник следственного отдела (МВД РФ)	2	1,67%
Заместитель начальника следственного отдела (МВД РФ)	1	0,8%

Стаж работы респондентов:

1 год и менее	16	13,3%
2 года	11	9,2%
3 года	8	6,7%
4 года	6	5%
5 лет	7	5,58%
6 лет	7	5,58%
7 лет	10	8,3%
8 лет	8	6,7%
9 лет	4	3,3%
10 лет	10	8,3%
11 лет	2	1,7%
12 лет	3	2,5%
13 лет	1	0,8%
14 лет	3	2,5%
15 лет	4	3,3%

16 лет	4	3,3%
17 лет	5	4,3%
18 лет	2	1,7%
19 лет	-	-
20 лет	6	5%
25 лет	2	1,7%
30 лет	1	0,8%

География анкетирования:

Ярославская область	100	83,3%
Республика Хакасия	1	0,8%
Самарская область	4	3,4%
Московская область	1	0,8%
г. Москва	3	2,6%
Калужская область	1	0,8%
Ростовская область	2	1,7%
Волгоградская область	1	0,8%
Республика Татарстан	2	1,7%
Тамбовская область	1	0,8%
Ивановская область	1	0,8%
Республика Адыгея	1	0,8%
Не указали	2	1,7%

Целями и задачами анкетирования было рассмотрение основных аспектов использования электронных сообщений в расследовании, анализ осведомленности работников следствия о технических и тактических особенностях обнаружения, изъятия и фиксации электронных сообщений, их осведомленности о возможностях технического и программного обеспечения для исследования таких сообщений.

Данное анкетирование также было направлено на выявление сложностей работы следователей с электронными сообщениями.

В ходе изучения результатов анкетирования было выявлено, что почти все (92,56%) работники в процессе расследования осуществляют следственные действия, связанные с изъятием и исследованием электронной переписки.

Необходимость исследования переписки возникает по следующим категориям расследуемых дел: преступления против личности – 47,9%, должностные преступления – 33%, хищения – 20,6%, преступления в сфере экономической деятельности – 53,7%, преступления в сфере компьютерной информации - 28,9%, преступления против общественной безопасности и общественного порядка – 14%, преступления против государственной власти – 14,8%.

У 86% следователей возникают сложности с исследованием электронных сообщений однако, у большинства они возникают редко. Чаще всего, электронная переписка, с которой они сталкиваются в ходе расследования ведется в мессенджерах (82,64%), более редко в социальных сетях (42,14%) и совсем редко по электронной почте (9,9%). Чаще всего переписку удается обнаружить на устройстве, с которого она велась (94,21%), более редко она изымается с сервера организатора обмена сообщениями (9,91%) и обнаруживается на устройстве лица, не принимавшего участие в переписке, но состоящего в той же группе (общем чате) (6,6%).

Изъятие электронной переписки осуществляется путем выемки, запроса, получения информации от допрашиваемого, в ходе оперативно-розыскных мероприятий. 66% опрошенных иногда прибегают к назначению компьютерно-технической экспертизы для исследования электронных сообщений.

Чаще всего (в 59,5% случаев) следователи находят сообщения, относящиеся к расследуемому событию просто листая переписку, пока не найдут интересующие их события; 28,1% используют поиск по дате; 51,24% используют поиск по ключевым словам и 28,93% назначают для этого экспертизу или привлекают

специалиста. С понятием индексации знакомы, но не применяли на практике 37,19% следователей; знакомы и применяют 10,74% и не знакомы целых 52,06% опрошенных. Среди тех, кто использует данный инструмент используют следующее программное обеспечение: dtSearch Desktop (7,44%), dtSearch Network (4,13%), ZyLab (3,31%), Relativity (1,65%), BelkaSoft (4,96%), Архивариус (12,4%).

54,55% следователей ответили, что они смогли бы самостоятельно сформировать список ключевых слов; 37,19% ответили, что смогут, но беспокоятся, что он не будет исчерпывающим; 5,79% ответили, что считают, что не смогут составить такой список. Индексация, по мнению 55,37% должна проводиться в рамках экспертизы, и по мнению 55,89% следователями самостоятельно.

В случае, если доступ к устройству, на котором хранится переписка заблокирован, 22,31% направляют запрос оператору обмена сообщениями для истребования переписки; 70,24% пытаются узнать пароль в ходе проведения запроса; 61,98% направляют устройство на экспертизу; 11,57% используют собственные навыки и специальное ПО для получения доступа к переписке. В случае возникновения затруднений при использовании электронной переписки 9,92% обратятся к специальной литературе; 94,21% обратятся к помощи коллег или специалистов и 11,57% попытаются самостоятельно решить проблему.

Необходимым появление рекомендаций для работников следственного аппарата по работе с электронными сообщениями считают 96,69%, в то время как 3,31% ответили, что не обращались бы к таким рекомендациям.

1. **Как часто в процессе расследования Вы осуществляете следственные действия, связанные с изъятием и исследованием электронной переписки?**

Никогда	9	7,38%
Редко	55	45,08%
Часто	50	40,98%

Почти всегда	8	6,56%

2. **По каким категориями расследуемых преступлений возникает необходимость исследования электронной переписки?**

Преступления против личности	58	20,86%
Должностные преступления	40	14,39%
Хищения	25	8,99%
Преступления в сфере экономической деятельности	65	23,38%
Преступления в сфере компьютерной информации	35	12,59%
Преступления против общественной безопасности и общественного порядка	17	6,12%
Преступления против государственной власти	20	7,19%
Иное	18	6,47%

3. **Возникают ли у Вас сложности с исследованием электронной переписки?**

Никогда	18	15%
Редко	96	80%
Часто	5	4,16%
Почти всегда	1	0,83%

4. **С помощью каких сервисов чаще всего ведется электронная переписка, с которой Вы сталкиваетесь в ходе расследования:**

Социальные сети	51	31,29%%
Мессенджеры	100	61,35%
Электронная почта	12	7,36%

5. **Где чаще всего Вам удается обнаружить электронную переписку, в отношении которой выполняются следственные действия?**

На устройстве, с которого осуществлялась переписка	114	85,07%
На сервере провайдера услуг	12	8,96%
На устройстве лица, не принимавшего участие в переписке, но состоящего в той же группе (общем чате).	8	5,97%

6. **С помощью каких следственных действий выполняется изъятие электронной переписки для исследования ?**

Выемка	85	40,86%
Осмотр	52	25%
Запрос оператору социальной сети/сервиса обмена сообщениями	20	9,62%
Получение информации о переписки в ходе допроса и	25	12,02%

приобщение скринов к протоколу допроса		
Приобщение к материалам дела результатов оперативно-розыскных мероприятий	26	12,5%

7. Часто ли для получения доступа к переписке и ее исследования Вы прибегаете к назначению компьютерно-технической экспертизы?

Никогда	9	7,76%
Иногда	81	69,83%
Довольно часто	22	18,96%
Почти всегда	4	3,45%

8. Ставите ли Вы какие-либо из нижеперечисленных вопросов на разрешение эксперта (пометьте те, которые ставите)?

содержится ли на данном носителе информация, и если да, то каково его целевое назначение?	55	11,36%
каков вид (тип, модель, марка) представленного носителя информации?	21	4,34%
доступен ли для чтения представленный носитель информации с использованием	22	4,55%

пользовательских программных средств? если нет, то каковы причины отсутствия доступа к носителю информации?		
определить, какие сведения о собственнике (пользователе) компьютерной системы (в т.ч. имена, пароли, права доступа и пр.) имеются на носителях данных представленных на судебную компьютерно-техническую экспертизу?	26	5,37%
определить, имеются ли признаки функционирования данного компьютерного средства в составе локальной вычислительной сети? каково содержание установленных сетевых компонентов?	1	0,21%
определить, имеются ли признаки работы представленного компьютерного средства в сети Интернет?	37	7,64%

находилась ли на носителе информация, которая была уничтожена. Если да, то какая именно?	85	17,56%
содержится ли на данном носителе информация, имеющая ключевые слова?	59	12,19%
установлены ли на носителе программы (приложения) для мгновенного обмена сообщениями (мессенджеры)?	60	12,40%
если да, возможен ли к ним доступ?	42	8,68%
какая информация содержится в мессенджерах? Имеется ли там информация, содержащая ключевые слова?	76	15,70%

9. Какое устройство Вы используете для выгрузки электронных сообщений и получения доступа к ним?

Непосредственно изъятое устройство, с которого велась переписка	52	48,60%

(смартфон, компьютер, планшет и пр.)		
Свой рабочий стационарный компьютер	26	24,30%
Специальное оборудование	29	27,10%

10. При исследовании электронной переписки, каким образом Вы находите сообщения, относящиеся к расследуемому событию? (Зачастую, массив переписки бывает очень большим).

Листаю переписку, пока не найду интересующие меня сообщения	72	35,47%
Использую поиск по дате	34	16,75%
Использую поиск по ключевым словам	62	30,54%
Назначаю экспертизу или привлекаю специалиста	35	17,24%

11.Знакомы ли Вы с понятием индексации электронных сообщений?

Да, но не применял на практике	45	37,19%
Да, применяю на практике	13	10,74%
Нет, не знаком	63	52,07%

12. Если знакомы, то скажите, использовали ли Вы в своей работе что-либо из нижеперечисленного программного обеспечения?

dtSearch Desktop	9	21,95%

dtSearch Network	5	12,20%
ZyLab	4	9,76%
Relativity	2	4,88%
BelkaSoft	6	14,63%
Архивариус	15	36,58%

13. Индексация электронных сообщений в самом простом виде представляет из себя поиск в массиве данных по ключевым фразам и словам. Формирование ключевых слов осуществляется с учетом контекста расследуемого события. **Смогли бы Вы формировать список ключевых слов для такого поиска?**

Да, смогу	66	55,93%
Да, смогу, но беспокоюсь, что он будет не исчерпывающим	45	38,14%
Нет	7	5,93%

14. **На Ваш взгляд, проведение вышеописанного поиска (индексации) должно проводиться в рамках компьютерно-технической экспертизы или может быть выполнено непосредственно следователем?**

В рамках экспертизы	67	51,15%
Следователем	64	48,85%

15. **В случае, если доступ к устройству, на котором хранится переписка заблокирован, какие действия Вы предпринимаете?**

Направляю запрос оператору обмена	27	13,43%

сообщениями для истребования переписки		
Пытаюсь узнать пароль в ходе проведения допроса	85	42,29%
Направляю устройство на экспертизу	75	37,31%
Использую собственные навыки и специальное ПО для получения доступа к переписке	14	6,97%

16. **Как вы поступите в случае возникновения затруднений при исследовании электронной переписки?**

Обращусь к специальной литературе.	12	8,57%
Обращусь к помощи коллег или специалистов	114	81,43%
Попытаюсь сам решить проблему	14	10%

17. **Считаете ли Вы необходимым появление рекомендаций для работников следственного аппарата по работе с электронной перепиской?**

Да, это было бы полезно	117	96,69%
Нет, я бы не обращался к таким рекомендациям	4	3,31%

Приложение №3

Результаты анализа материалов надзорного производства прокуратуры

В ходе проведения исследования было изучено 105 надзорных производств прокуратуры за 2020-2023гг. по уголовным делам, в которых фигурировали электронные сообщения. Изучение материалов проводилось в соответствии с заранее установленными вопросами.

Целями и задачами анализа надзорных производств по уголовным делам были обобщение данных об использовании электронных сообщений в расследовании, выявление особенностей обнаружения, изъятия и использования таких сообщений в расследовании преступлений.

1. По каким статьям возбуждены уголовные дела, в которых электронные сообщения фигурируют в процессе расследования?

ч.1 ст.105 - 3

п. «а» ч.2 ст.105 - 1

п. «к» ч. 2 ст.105 - 1

ч.1 ст.109 - 2

ч.1 ст.110 - 4

п. «д» ч.2 ст.110 - 3

ч.4 ст.111 - 2

ч.1 ст.119 - 9

ч.1 ст.134 - 6

ч.3 ст.134 - 4

ч.1 ст.135 - 6

ч.2 ст.135 - 2

ч.1 ст.138 - 2

ч.1 ст.157 - 7

п. «г» ч.3 ст.158 - 8

ч.1 ст.159 - 1

ч.2 ст.159 - 4

ч.3 ст.159 - 2

ч.1 ст. 163 - 3

ч.1 ст.171.2 - 5

п. «а» ч.2 ст.171.1 - 1

ч.1 ст.228.1 - 15

п. «б» ч.2 ст.228.1 - 12

ч.1 ст.272 - 1

ч.1 ст.327 - 1

2. Средства создания и отправки электронных сообщений, посредством которых были отправлены сообщения, содержащиеся в уголовных делах:

Мессенджер «Telegram» - 29

Мессенджер «WhatsApp» - 18

Мессенджер «Viber» - 10

Мессенджер на сайте «Авито» - 14

Социальная сеть «Вконтакте» - 23

Социальная сеть «Одноклассники» - 3

Социальная сеть «Facebook» - 7

Сервис электронной почты «Yandex.ru» - 1

3. Сведения о том, каким образом были получены сообщения в ходе расследования:

-в ходе обыска и выемки - 16

-запрос компании организатору обмена сообщениями - 9

-в ходе осмотра устройства – 48

-приобщение материалов переписки в ходе допроса - 18

-в рамках компьютерно-технической экспертизы - 14

4. Сведения о том, как электронные сообщения были использованы в ходе расследования:

-как основное доказательство – 29 (27,62%)

-как ориентирующая информация (средство изобличения) – 76 (72,38%)

5. Сведения о том, каков характер у электронных сообщений, фигурирующих в материалах дела:

-сообщение как средство совершения преступления - 47 (44,76%)

-сообщение как средство коммуникации (передачи информации) - 58 (55,24%)

Приложение №4

Результаты анализа судебных решений по делам, в ходе расследования которых исследовались электронные сообщения

В ходе исследования нами было проанализировано 100 судебных решений за 2016-2024г., находящихся в открытом доступе, по уголовным делам, в ходе которых была так или иначе изъята, зафиксирована и использована электронная переписка:

Апелляционное постановление № 22-2319/2018 от 30 июля 2018 г. по делу № 22-2319/2018, Хабаровский краевой суд (Хабаровский край) ; Приговор № 1-1011/2020 1-154/2021 от 9 июня 2021 г. по делу № 1-1011/2020 Автозаводский районный суд г. Тольятти (Самарская область); Приговор № 1-96/2021 от 13 июля 2021 г. по делу № 1-96/2021 Железнодорожный районный суд г. Орла (Орловская область) ; Приговор № 1-90/2021 от 30 марта 2021 г. по делу № 1-90/2021 Железнодорожный районный суд г. Орла (Орловская область) ; Апелляционное постановление № 22-2780/2021 от 14 мая 2021 г. Пермский краевой суд (Пермский край) ; Приговор № 1-12/2021 1-200/2020 от 25 марта 2021 г. по делу № 1-12/2021 Заводской районный суд г. Орла (Орловская область) ; Приговор № 1-257/2020 от 24 ноября 2020 г. по делу № 1-257/2020 Новокуйбышевский городской суд (Самарская область); Приговор № 1-15/2020 1-372/2019 от 24 ноября 2020 г. по делу № 1-15/2020 Кстовский городской суд (Нижегородская область); Постановление № 1-416/2019 от 16 июля 2019 г. по делу № 1-416/2019 Псковский городской суд (Псковская область) ; Приговор № 1-125/2019 от 19 июля 2019 г. по делу № 1-125/2019 Аксайский районный суд (Ростовская область) ; Приговор № 1-152/2019 от 23 августа 2019 г. по делу № 1-152/2019 Северный районный суд г. Орла (Орловская область) ; Приговор № 1-784/2019 от 9 декабря 2019 г. по делу № 1-784/2019 Автозаводский районный суд г. Тольятти (Самарская область) ; Приговор № 1-57/2020 от 29 апреля 2020 г. по делу № 1-57/2020 Ржевский городской суд (Тверская область); Приговор № 1-216/2020 от 8 октября 2020 г. по делу № 1-216/2020 Щекинский районный суд (Тульская область); Приговор № 1-513/2020 от 8 октября 2020 г. по делу № 1-513/2020 Промышленный районный суд г. Самары (Самарская область); Приговор № 1-830/2020 от 26 октября 2020 г. по делу № 1-830/2020 Советский районный суд г. Красноярска (Красноярский край); Приговор № 1-298/2020 от 30 октября 2020 г. по делу № 1-298/2020 Московский районный суд г. Твери (Тверская область); Приговор № 1-245/2020 от 30 октября 2020 г. по делу № 1-245/2020 Новоуральский городской суд (Свердловская область); Приговор № 1-55/2019 1-831/2018 от 17 января 2019 г. по делу № 1-55/2019 Нижневартовский городской суд (Ханты-Мансийский автономный округ-Югра);

Приговор № 1-14/2019 1-180/2018 от 14 февраля 2019 г. по делу № 1-14/2019 Пролетарский районный суд г. Саранска (Республика Мордовия); Приговор № 1-124/2018 от 2 ноября 2018 г. по делу № 1-124/2018 Смоленский районный суд (Смоленская область); Приговор № 1-400/2018 от 2 ноября 2018 г. по делу № 1-400/2018 Ленинский районный суд г. Саратова (Саратовская область) ; Приговор № 1-131/2018 от 26 сентября 2018 г. по делу № 1-131/2018 Вышневолоцкий городской суд (Тверская область); Приговор № 1-142/2018 от 6 сентября 2018 г. по делу № 1-142/2018 Октябрьский районный суд г. Саранска (Республика Мордовия); Приговор № 1-74/2018 1-754/2017 от 27 июня 2018 г. по делу № 1-74/2018 Ленинский районный суд г. Омска (Омская область); Приговор № 1-232/2018 от 27 июня 2018 г. по делу № 1-232/2018 Ленинский районный суд г. Саратова (Саратовская область) ; Приговор № 1-44/2018 от 20 июня 2018 г. по делу № 1-44/2018 Советский районный суд (Кировская область); Приговор № 1-116/2018 1-813/2017 от 21 мая 2018 г. по делу № 1-116/2018 Индустриальный районный суд г. Хабаровска (Хабаровский край); Приговор № 1-31/2018 1-670/2017 от 20 февраля 2018 г. по делу № 1-31/2018 Калининский районный суд г. Челябинска (Челябинская область); Приговор № 1-312/2016 1-6/2017 от 19 января 2017 г. по делу № 1-312/2016 Советский районный суд г. Волгограда (Волгоградская область); Приговор № 1-11/2017 1-354/2016 от 9 февраля 2017 г. по делу № 1-11/2017 Шахтинский городской суд (Ростовская область); Приговор № 1-359/2016 1-49/2017 от 15 марта 2017 г. по делу № 1-359/2016 Ханты-Мансийский районный суд (Ханты-Мансийский автономный округ-Югра); Приговор № 2-5/2017 от 28 марта 2017 г. по делу № 2-5/2017 Верховный Суд Республики Коми (Республика Коми); Приговор № 1-92/2017 от 4 апреля 2017 г. по делу № 1-92/2017 Октябрьский районный суд г. Пензы (Пензенская область) ; Приговор № 1-60/2017 от 6 апреля 2017 г. по делу № 1-60/2017 Железнодорожный районный суд г. Рязани (Рязанская область); Приговор № 1-86/2017 от 21 апреля 2017 г. по делу № 1-86/2017 Железнодорожный районный суд г. Рязани (Рязанская область) ; Приговор № 1-128/2017 от 27 апреля 2017 г. по делу № 1-128/2017 Октябрьский районный суд г. Архангельска (Архангельская область); Приговор № 22-929/2017 от 11 мая 2017 г. по делу № 22-929/2017 Кировский областной суд (Кировская область) ; Приговор № 1-148/2017 от 5 июня 2017 г. по делу № 1-148/2017 Ленинский районный суд г. Челябинска (Челябинская область) ; Приговор № 1-100/2016 1-5/2017 от 20 июня 2017 г. по делу № 1-100/2016 Индустриальный районный суд г. Ижевска (Удмуртская Республика); Приговор № 1-556/2017 от 31 августа 2017 г. по делу № 1-556/2017 Индустриальный районный суд г. Барнаула (Алтайский край); Приговор № 1-58/2017 от 29 сентября 2017 г. по делу № 1-58/2017 Орловский районный суд (Орловская область) ; Приговор № 1-1054/2016 от 10 октября 2016 г. по делу № 1-1054/2016 Чердаклинский районный суд (Ульяновская область); Приговор № 1-353/2016 от 15 ноября 2016 г. по делу № 1-353/2016 Октябрьский районный суд г. Пензы (Пензенская область) ; Приговор № 1-236/2016 от 2 декабря 2016 г. по делу № 1-236/2016 Ленинский районный суд г. Иваново (Ивановская область); Приговор № 1-310/2016 от 21 декабря 2016 г. по делу № 1-310/2016 Октябрьский районный

суд г. Архангельска (Архангельская область) ; Апелляционное определение от 28 марта 2019 г. по делу № 2-118/2018 Верховный Суд Российской Федерации; Приговор № 1-504/2021 от 4 июня 2021 г. по делу № 1-504/2021 Центральный районный суд г. Новокузнецка (Кемеровская область) ; Приговор № 1-14/2021 1-453/2020 от 24 марта 2021 г. Бийский городской суд (Алтайский край) ; Апелляционное постановление № 22-7259/2020 от 19 ноября 2020 г. по делу № 22-7259/2020 Московский областной суд (Московская область) ; Приговор № 1-114/2020 от 2 ноября 2020 г. по делу № 1-114/2020 Грозненский районный суд (Чеченская Республика) ; Приговор № 1-17/2020 1-352/2019 от 11 февраля 2020 г. по делу № 1-17/2020 Шпаковский районный суд (Ставропольский край); Приговор № 1-39/2021 от 30 июля 2021 г. по делу № 1-39/2021 Новосергиевский районный суд (Оренбургская область) ; Приговор № 2-21/2023 от 19 октября 2023 г. по делу № 2-21/2023 Ивановский областной суд (Ивановская область) ; Приговор № 1-3/2023 1-76/2022 от 16 октября 2023 г. по делу № 1-3/2023 Железноводский городской суд (Ставропольский край) ; Апелляционное постановление № 22-1120/2023 УК-22-1120/2023 от 27 сентября 2023 г. Калужский областной суд (Калужская область); Приговор № 1-167/2023 от 26 сентября 2023 г. по делу № 1-167/2023 Ленинский районный суд г. Орска (Оренбургская область) ; Апелляционное постановление № 22-1910/2023 от 7 сентября 2023 г. по делу № 1-В41/2023 Воронежский областной суд (Воронежская область) ; Апелляционное постановление № 22-5252/2021 22К-5252/2021 от 27 июля 2021 г. по делу № 3/2-60/2021 Краснодарский краевой суд (Краснодарский край); Апелляционное постановление № 22-2066/2023 от 19 октября 2023 г. по делу № 1-122/2023 Тамбовский областной суд (Тамбовская область) ; Приговор № 1-16/2021 1-310/2020 от 25 марта 2021 г. по делу № 1-16/2021 Центральный районный суд г. Барнаула (Алтайский край) ; Приговор № 1-52/2021 1-560/2020 от 30 марта 2021 г. по делу № 1-52/2021 Центральный районный суд г. Кемерово (Кемеровская область) ; Приговор № 2-34/2020 от 17 ноября 2020 г. по делу № 2-34/2020 Московский областной суд (Московская область) ; Приговор № 1-40/2020 от 23 октября 2020 г. по делу № 1-40/2020 Зарайский городской суд (Московская область) ; Приговор № 1-448/2020 от 22 октября 2020 г. по делу № 1-448/2020 Октябрьский районный суд г. Красноярска (Красноярский край); Приговор № 1-311/2020 от 6 октября 2020 г. по делу № 1-311/2020 Автозаводский районный суд г. Нижний Новгород (Нижегородская область); Приговор № 1-267/2020 от 8 октября 2020 г. по делу № 1-267/2020 Бугульминский городской суд (Республика Татарстан); Приговор № 1-35/2020 от 27 мая 2020 г. по делу № 1-35/2020 Волгоградский гарнизонный военный суд (Волгоградская область) ; Приговор № 1-1/2020 1-446/2019 от 27 января 2020 г. по делу № 1-1/2020 Димитровградский городской суд (Ульяновская область) ; Приговор № 1-12/2021 1-127/2020 1-764/2019 от 2 марта 2021 г. по делу № 1-12/2021 Ленинский районный суд г. Красноярска (Красноярский край) ; Апелляционное постановление № 10-11/2020 от 24 ноября 2020 г. по делу № 10-11/2020 Миллеровский районный суд (Ростовская область) ; Приговор № 1-117/2016 от 16 декабря 2016 г. по делу № 1-

117/2016 Горно-Алтайский городской суд (Республика Алтай) ; Приговор № 1-242/2017 1-3/2018 от 16 июля 2018 г. по делу № 1-242/2017 Ленинский районный суд г. Барнаула (Алтайский край); Приговор № 1-237/2018 от 23 июля 2018 г. по делу № 1-237/2018 Ленинский районный суд г. Барнаула (Алтайский край) ; Приговор № 1-73/2017 от 19 июня 2017 г. по делу № 1-73/2017 Октябрьский районный суд г. Саранска (Республика Мордовия) ; Апелляционное постановление № 22К-5432/2019 от 20 августа 2019 г. по делу № 22К-5432/2019 Пермский краевой суд (Пермский край) ; Приговор № 1-13/2023 1-550/2022 от 11 сентября 2023 г. по делу № 1-13/2023 Промышленный районный суд г. Ставрополя (Ставропольский край) ; Апелляционное постановление № 22-1171/2023 от 16 октября 2023 г. по делу № 1-218/2023 Рязанский областной суд (Рязанская область) ; Приговор № 1-40/2020 от 23 октября 2020 г. по делу № 1-40/2020 Зарайский городской суд (Московская область) ; Приговор № 1-1299/2020 от 26 ноября 2020 г. по делу № 1-1299/2020 Ленинский районный суд г.Тюмени (Тюменская область) ; Приговор № 1-3/2020 1-78/2019 1-793/2018 от 29 мая 2020 г. по делу № 1-3/2020 Советский районный суд г. Краснодара (Краснодарский край) ; Апелляционное постановление № 1-10/2021 22-1957/2021 от 22 июля 2021 г. по делу № 1-10/2021 Верховный Суд Республики Крым (Республика Крым) ; Приговор № 1-1299/2020 от 26 ноября 2020 г. по делу № 1-1299/2020 Ленинский районный суд г.Тюмени (Тюменская область) ; Приговор № 1-40/2020 от 23 октября 2020 г. по делу № 1-40/2020 Зарайский городской суд (Московская область) ; Приговор № 1-157/2019 от 6 мая 2019 г. по делу № 1-157/2019 Дмитровский городской суд (Московская область) ; Приговор № 1-448/2020 от 22 октября 2020 г. по делу № 1-448/2020 Октябрьский районный суд г. Красноярска (Красноярский край) ; Приговор № 1-37/2023 от 6 июня 2023 г. по делу № 1-37/2023 Советский районный суд (Кировская область) ; Приговор № 1-215/2023 от 4 сентября 2023 г. по делу № 1-215/2023 Советский районный суд г. Липецка (Липецкая область) ; Приговор № 1-183/2020 1-219/2020 1-26/2021 от 3 марта 2021 г. по делу № 1-183/2020 Дербентский районный суд (Республика Дагестан); Приговор № 1-232/2020 1-5/2021 от 9 марта 2021 г. по делу № 1-232/2020 Свердловский районный суд г. Костромы (Костромская область) ; Приговор № 1-536/2020 от 15 октября 2020 г. по делу № 1-536/2020 Ангарский городской суд (Иркутская область) ; Приговор № 1-83/2020 от 21 июля 2020 г. по делу № 1-83/2020 Куйбышевский районный суд г. Омска (Омская область) ; Приговор № 1-192/2019 от 26 декабря 2019 г. по делу № 1-192/2019 Богучарский районный суд (Воронежская область); Определение от 10 мая 2012 г. по делу № 2-07/12 Верховный Суд Российской Федерации ; Приговор № 1-102/2023 1-918/2022 от 21 сентября 2023 г. по делу № 1-102/2023 Ленинский районный суд г. Челябинска (Челябинская область) ; Приговор № 1-12/2019 1-182/2018 от 25 февраля 2019 г. по делу № 1-12/2019 Центральный районный суд г. Новосибирска (Новосибирская область) ; Приговор № 1-192/2023 1-903/2022 от 5 сентября 2023 г. по делу № 1-192/2023 Центральный районный суд г. Барнаула (Алтайский край) ; Приговор № 2-22/2021 от 21 июля 2021 г. по делу № 2-22/2021 Хабаровский краевой суд (Хабаровский край) ; Приговор № 1-313/2023 от 29 июня

2023 г. по делу № 1-313/2023 Ленинский районный суд г. Екатеринбурга (Свердловская область).

Материалы данных решений были изучены на предмет того, какая экспертиза в отношении электронных сообщений назначалась в ходе расследования.

Вид экспертизы	Количество дел	Процент
Судебная компьютерно-техническая экспертиза	50	50%
Лингвистическая экспертиза	22	22%
Автороведческая экспертиза	4	4%
Психолого-лингвистическая экспертиза	11	11%
Фоноскопическая экспертиза	8	8%
Портретная экспертиза видеозаписей	2	2%
Видеотехническая экспертиза	1	1%
Молекулярно-генетическая экспертиза	2	2%