Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Юридический институт
Кафедра уголовного процесса и криминалистики

УТВЕРЖДАЮ
Заведующий кафедрой
_____ А.Д. Назаров
подпись
« _____» _____ 2018г.

БАКАЛАВРСКАЯ РАБОТА

40.03.01-Юриспруденция
код-наименование направления

Расследование преступлений, совершенных посредством социальных сетей

Научный руководитель _____ доц. каф, к.ю.н. И.Г. Иванова
подпись, дата

Выпускник _____ М.И. Гуров
подпись, дата

Красноярск 2018

Содержание

Введение

В конце XX – начале XXI века быстрыми темпами начали развиваться информационные технологии, Интернет и социальные сети. Государственные институты различных стран предпринимают попытки правового регулирования действий граждан в социальных сетях. Внутри социальных сетей действуют определенные правила, соответствующие законодательству страны, которые пользователи обязаны соблюдать. В случае несоблюдения этих правил срабатывает механизм привлечения к ответственности нарушителя, как со стороны социальной сети, так и со стороны государства. Уголовные дела, связанные с привлечением к ответственности лиц, совершивших преступления с использованием социальной сети, вызывают большой интерес общественности. В связи с чем, полагаем, что тема бакалаврской работы, учитывая современные реалии, является практически и научно значимой.

Исследования в выпускной квалификационной работе проведены на примере социальной сети «Вконтакте», поскольку она является одной из самых популярных и быстроразвивающихся в России.

Цель работы – раскрыть криминалистическую характеристику и методику расследования преступлений, совершенных посредством социальных сетей.

Для достижения данной цели были поставлены следующие задачи:

1) Изучить криминалистическую характеристику преступлений, совершенных посредством социальных сетей;

2) Выявить типичные следственные ситуации и направления расследования преступлений, совершенных посредством социальных сетей;

3) Описать следственные и иные действий, производимые при расследовании преступлений, совершенных посредством социальных сетей;

4) Раскрыть некоторые проблемы выявления и расследования рассматриваемой группы преступлений.

Теоретическую базу работы составили труды известных российских ученых-криминалистов, таких, как Р.С. Белкин, Е.П. Ищенко, М.В. Савельева, Н.П. Яблоков и др.

Нормативной основой работы явились федеральные законы (Уголовно-процессуальный кодекс РФ, ФЗ «Об информации», «О связи» и др.), постановления Правительства Российской Федерации и иные нормативные акты.

Эмпирической базой послужили опубликованная судебная практика и статистические данные.

Структурно работа состоит из введения, четырех глав, заключения и списка использованных источников. В первой главе рассматривается криминалистическая характеристика преступлений, совершенных посредством социальных сетей. Во второй главе описываются типичные следственные ситуации и направления расследования. В третьей главе исследуются вопросы производства следственных действий при расследовании преступлений, совершенных посредством социальных сетей. В четвертой главе раскрыты некоторые проблемы выявления и расследования преступлений, совершенных посредством социальных сетей. В заключении сделаны основные выводы.

1 Криминалистическая характеристика преступлений, совершенных посредством социальных сетей

1.1 Понятие и содержание криминалистической характеристики преступления.

Успех расследования любого преступления, каким бы сложным оно не казалось вначале, зависит от умения разобраться в его криминалистической сути. Для этого следователю необходимо знать типовые криминалистически значимые черты различных видов преступной деятельности, уметь целенаправленно выявлять необходимые для этого данные по каждому конкретному деликту, сопоставлять их с криминалистической характеристикой преступления соответствующего вида[1].

Е.П. Ищенко предлагает под криминалистической характеристикой понимать систему описания криминалистически значимых признаков вида или группы преступлений, проявляющихся в особенностях способа, механизма и обстановки совершения, личности виновного и иных обстоятельств конкретного преступного посягательства, существенных для его успешного раскрытия и расследования[2].

М.С. Прохоров говорит о том, что типовая криминалистическая характеристика вида преступления представляет собой систему научного описания криминалистически значимых признаков вида, разновидности, группы преступлений и, прежде всего, проявляющихся в особенностях таких ее элементов, как способ, механизм и обстановка их совершения, личности их субъекта и иных свойственных для характеризуемого вида преступления элементах, с раскрытием корреляционных связей и взаимозависимостей между ними, знание которых в совокупности с содержательной стороной описания обеспечивает успешное расследование преступлений[3].

---

[1] Яблоков, Н.П. Криминалистика: учебник / Н. П. Яблоков. – Москва: Юристъ, 2005. – С. 65.
[2] Ищенко, Е.П. Криминалистика: курс лекций / Е. П. Ищенко. – Москва : АСТ, 2007. – С. 63.
[3] Прохоров, М.С. Криминалистическая характеристика преступлений / М. С. Прохоров // Известия Российского государственного педагогического университета. – 2008. – № 3. – С. 354.

По мнению В.Д. Зеленского, под криминалистической характеристикой следует понимать совокупность объективных сведений об обстоятельствах определенного вида или группы преступлений, полученных в результате научных исследований и анализа передовой следственной практики, способствующих раскрытию, расследованию и предупреждению преступлений[4].

В структуру криминалистической характеристики преступлений включаются следующие данные:

1) о типичных чертах самого преступного события (объект преступного посягательства; место, время, условия и другие обстоятельства, характеризующие обстановку, выявленные при анализе уголовных дел данного вида как закономерности);

2) о механизме следообразования, характерного для данного вида преступных посягательств;

3) о способе подготовки, совершения и сокрытия преступления;

4) об особенностях личности преступника (возрастные, половые, психологические и др.);

5) о мотивах и целях совершения преступлений;

6) о поведении потерпевшего (виктимологический аспект);

7) о связи расследуемого преступления с другими преступными проявлениями;

8) о закономерных связях, существующих между различными элементами криминалистической характеристики;

9) о последствиях преступления и др.[5]

В науке нет единства мнений в определении количественного и качественного состава элементов криминалистической характеристики, в определении ее структуры и закономерностей, а также их взаимосвязей, в наделении ее элементов статусом основных и факультативных, в зависимости

[4] Зеленский, В.Д. Криминалистика: учебник / В. Д. Зеленский, Г. М. Меретуков ; под. общ. ред. В. Д. Зеленского. – Санкт-Петербург : Юридический центр, 2015 – С. 99.
[5] Ищенко, Е.П. Криминалистика: курс лекций / Е. П. Ищенко. – Москва : АСТ, 2007. – С. 63.

от значения для расследования преступлений. В качестве последних, в самом общем виде, могут быть признаны такие признаки объективной и субъективной стороны состава преступления, как: личность или преступник, способ совершения преступления, обстановка совершения преступления, поскольку именно эти признаки являются наиболее важными, как с точки зрения теории уголовного права (при квалификации деяния), так и с точки зрения уголовного процесса (соотношение данных элементов с обстоятельствами, подлежащими доказыванию), и криминалистики (идентификация личности преступника, потерпевшего, исследование обстановки совершения преступления, поиск орудия преступления, определение способа и механизма совершения преступления)[6].

1.2 Способы преступлений, совершенных посредством социальных сетей.

А.С. Князьков отмечает, что способ совершения преступления представляет собой систему взаимосвязанных и взаимообусловленных действий по подготовке, совершению и сокрытию преступлений, детерминированных условиями внешней среды и свойствами личности, условиями места и времени и зачастую связанных с использованием соответствующих орудий и средств[7].

В свою очередь, В.П. Колмаков включает в способ совершения преступления только те действия, которые непосредственно направлены на совершение общественно опасных деяний, считая, что действия по сокрытию во всех случаях остаются за рамками способа совершения[8].

Н.П. Яблоков указывает, что под способом совершения преступления в криминалистическом смысле целесообразно понимать объективно и

---

[6] Прохоров, М.С. Криминалистическая характеристика преступлений / М. С. Прохоров // Известия Российского государственного педагогического университета. – 2008. – № 3. – С. 355.

[7] Князьков, А.С. Криминалистическая характеристика преступления в контексте его способа и механизма / А. С. Князьков // Вестник Томского государственного университета. – 2011. – № 7. – С. 52.

[8] Колмаков, А.В. Значение способа совершения преступления для квалификации преступлений / А. В. Колмаков // Пробелы в российском законодательстве. – 2009. – № 11. – С. 47.

субъективно обусловленную систему поведения субъекта до, в момент и после совершения преступления, оставляющую различного рода характерные следы вовне, позволяющие с помощью криминалистических приемов и средств получить представление о сути происшедшего, своеобразии преступного поведения правонарушителя, его отдельных личностных данных и соответственно определить наиболее оптимальные методы решения задач раскрытия преступления[9].

Объектом исследования в работе являются преступления, совершенные посредством социальных сетей. Это означает, что преступления совершались при помощи, с использованием социальных сетей.

Согласно пункту 1.1 Правил сайта «Вконтакте», социальная сеть – это размещенная на сайте в сети Интернет по определенному адресу и доступная пользователю через сайт, мобильную версию сайта, приложения и иные ресурсы, представляющая собой результат интеллектуальной деятельности в форме программы для ЭВМ[10].

Гражданский кодекс РФ в статье 1261 раскрывает содержание понятия «программа для ЭВМ». Согласно данной статье, программа для ЭВМ – это представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения[11].

Соответственно и социальная сеть представлена в объективной форме совокупностью данных и команд, и порождаемых аудиовизуальных отображений, предназначенных для функционирования ЭВМ и мобильных устройств в целях получения определенного результата в виде организации функционала социальной сети.

---

[9] Яблоков, Н.П. Криминалистика: учебник / Н. П. Яблоков. – Москва: Юристъ, 2005. – С. 65.
[10] Правила пользования сайтом Вконтакте [Электронный ресурс] – Режим доступа: https://vk.com/terms
[11] Гражданский кодекс Российской Федерации: федер. закон от 26.01.1996 г. № 14-ФЗ // Собрание законодательства РФ. – 5.12.1994. – № 32. – Ст. 3301.

Исходя из проведенного анализа судебной практики за последние несколько лет, можно выделить несколько составов преступлений, предусмотренных Уголовным кодексом РФ, которые чаще остальных совершаются при помощи социальных сетей. Одними из самых распространенных преступлений являются преступления против общественной безопасности, основ конституционного строя и безопасности государства, а именно: публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма (ст. 205.2), публичные призывы к осуществлению экстремистской деятельности (ст. 280), возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (ст. 282).

Довольно часто с использованием социальных сетей совершаются такие преступления, как клевета (ст. 128.1), мошенничество (ст. 159), незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества (ст. 228.1), незаконные изготовление и оборот порнографических материалов или предметов (ст. 242).

По мере компьютеризации населения, роста доступности средств массовых коммуникаций наблюдается рост количества преступлений, совершаемых в отношении неприкосновенности частной жизни (ст. 137), тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст. 138). Так, согласно приговору Вологодского областного суда от 17.11.2016 Анферьев был привлечен к уголовной ответственности по ч. 1 ст. 137 УК РФ. Подсудимый распространял фотографии интимного содержания лица без его согласия[12].

[12] Приговор Вологодского областного суда по уголовному делу № 1-914/2016 по обвинению Анферьева И.М. по ч. 1 ст. 137 УК РФ. 2016 год [Электронный ресурс] // Справочная система «СудАкт». – Режим доступа: http://sudact.ru/regular/doc/hwzIJ69MfXmR/ (Дата обращения: 24.04.2018).

В рассматриваемую группу попадают также преступления, предусмотренные статьями 272 и 273 УК РФ (неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных компьютерных программ). Так, Лямбирский районный суд Республики Мордовия 03.10.2017 года вынес приговор в отношении Галабира, который с помощью социальной сети «Вконтакте» распространял вредоносные компьютерные программы, тем самым совершил преступление, предусмотренное ч. 2 ст. 273 УК РФ[13].

Помимо вышеперечисленных, в последнее время получили распространение преступления, предусмотренные ст. 110 и 110.1 УК РФ (доведение до самоубийства; склонение к совершению самоубийства или содействие совершению самоубийства). Реже совершаются следующие преступления: организация занятия проституцией (ст. 241), организация деятельности экстремистской организации (ст. 282.2), организация незаконного вооруженного формирования или участие в нем (ст. 208), организация преступного сообщества (преступной организации) или участие в нем (ней) (ст. 210). Так, приговором Октябрьского районного суда г. Рязани от 28.09.2017 года был осужден В.А. Кротов по ч. 2 ст. 210 УК РФ, который был организатором распространения наркотических средств по региону, для чего использовал сеть «Вконтакте»[14]. Приговором Железнодорожного районного суда г. Самары от 31.10.2016 был осужден К.О. Кипенский по ч. 1 ст. 241 УК РФ, который в социальной сети «Вконтакте» отправлял потерпевшим и другим неустановленным лицам объявления о работе для девушек с высокой заработной платой и предлагал потерпевшим оказывать платные интимные услуги сексуального характера[15].

---

[13] Приговор Лямбирского районного суда Республики Мордовия по уголовному делу № 1-67/2017 по обвинению Галабира С.В. по ч. 2 ст. 273 УК РФ. 2017 год [Электронный ресурс] // Справочная система «СудАкт». – Режим доступа: http://sudact.ru/regular/doc/cCtVyfZHr9Hm/ (Дата обращения: 24.04.2018).

[14] Приговор Октябрьского районного суда г. Рязани по уголовному делу № 1-229/2017 по обвинению Кротова В.А. по ч.2 ст.210 УК РФ. 2017 год [Электронный ресурс] // Справочная система «СудАкт». – Режим доступа: http://sudact.ru/regular/doc/STfEbGVF4GU9/ (Дата обращения: 24.04.2018).

[15] Приговор Лямбирского районного суда Республики Мордовия по уголовному делу № 1-330/2016 по обвинению Кипенского К.О. по ч.1 ст.241 УК РФ. 2016 год [Электронный ресурс] // Справочная система «СудАкт». – Режим доступа: http://sudact.ru/regular/doc/vgZFRk4dPOdb/ (Дата обращения: 24.04.2018).

Говоря о способах совершения преступлений данной группы, стоит заметить, что их разнообразие ограничивается функционалом социальной сети и зависит от механизма совершения преступления.

Чаще других среди способов совершения преступлений исследуемой группы встречается распространение изображений. Изображение гражданина представляет собой его индивидуальный облик, запечатленный в какой–либо объективной форме, в частности в произведении изобразительного искусства, на фотографии или в видеозаписи[16]. Причем под изображением гражданина следует понимать внешний облик гражданина, включающий в себя не только лицо, но и внешний вид гражданина в целом[17]. Изображения могут содержать элементы, порочащие честь и достоинство личности, экстремистского, порнографического и иного характера. Так, согласно приговору Гагаринского районного суда города Севастополь ФИО1 был привлечен к уголовной ответственности по ч. 1 ст. 137 УК РФ. Используя сайт «Вконтакте», он отправил нескольким пользователям изображения потерпевшей в обнаженном виде, а также совершающей действия сексуального характера. Данными действиями было нарушено право потерпевшей на неприкосновенность частной жизни[18].

Среди способов можно выделить также распространение видео- и аудиозаписей. Аудиозаписи позволяют фиксировать любую информацию, которая может быть выражена в звуковой форме. Особое значение аудиозаписей с точки зрения их содержания состоит в возможности с их помощью фиксировать разговоры, предшествующие и сопровождающие действия (бездействие), и иные компоненты так называемого «звукового ряда»

---

[16] Определение Санкт-Петербургского городского суда по гражданскому делу № 33-4484/2013. 2013 год [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=SARB&n=46138#09433362545822297 (Дата обращения: 24.04.2018).

[17] Определение Алтайского краевого суда по гражданскому делу № 33-3897/2013 о возмещении морального вреда. 2013 год [Электронный ресурс] // Справочная система «РосПравосудие». – Режим доступа: https://rospravosudie.com/court-altajskij-kraevoj-sud-altajskij-kraj-s/act-490754873/ (Дата обращения: 24.04.2018).

[18] Приговор Гагаринского районного суда г. Севастополя по уголовному делу № 1-183/2016 по обвинению ФИО1 по ч. 1 ст. 137 УК РФ. 2016 год [Электронный ресурс] // Справочная система «СудАкт». – Режим доступа: http://sudact.ru/regular/doc/1N5srs50gto9/ (Дата обращения: 24.04.2018).

(выкрики, возгласы, музыка, иные сопутствующие звуки и шумы). С помощью видеозаписи возможно запечатление любой визуальной информации, которая может, как сопровождаться, так и не сопровождаться звуковой информацией. Использование видеозаписи позволяет точно зафиксировать и сохранить значительную часть информации о произошедшем действии. С помощью аудио и видеозаписей возможно фиксирование не только самого результата действий (бездействия), но и собственно, информации о том, как это действие протекало во времени, а также обстановки, в которой происходило действие (бездействия), и иные обстоятельства, сопровождавшие действие (бездействия) и предшествовавшие ему, наличие которых может поставить под сомнение его законность. С помощью аудио и видеозаписей информация фиксируется в динамике. При исследовании записей существует большая вероятность восстановить события, именно в том виде и в той последовательности, в которой они имели место в действительности, настолько, насколько позволяют их зафиксировать технические средства[19].

Согласно приговору Калужского областного суда Е.И. Зинов был привлечен к уголовной ответственности по ч. 1 ст. 282 УК РФ. Данным гражданином были размещены на своей странице во «Вконтакте», видео- и аудиозаписи экстремистского характера, содержание которых оскорбляет Государственный флаг РФ и День воинской славы России – 9 мая.

Третьим самым распространенным способом совершения преступлений с использованием социальных сетей является распространение текстов на персональной странице и в сообществах. Примером является приговор Хасавюртского городского суда от 06.05.2015 года, согласно которому по ч. 2 ст. 128.1 был осужден Р.А. Асакаев На сайте «Вконтакте» им был распространен текст, содержащий сведения, порочащие честь и достоинство

[19] Короткий, С.А. Соотношение аудио и видеозаписей с письменными доказательствами в гражданском процессе / С. А. Короткий // Научные ведомости Белгородского государственного университета. – 2009. – № 1. – С. 132.

потерпевшей[20]. Кировским районным судом города Красноярска от 03.12.2012 года осужден Р.М. Агаев по ч. 1 ст. 205.2 УК РФ, который на персональной странице в «Вконтакте» размещал комментарии экстремистского содержания[21].

1.3 Личность потерпевшего.

Криминалистическая теория и практика использует термин «личность» в широком смысле этого слова, включая в свойства личности всю совокупность криминалистически значимых человеческих качеств: морфологические, физиологические, психические, социальные. Так, криминалисты традиционно используют словосочетание «установление личности потерпевшего», понимая под этим процессом выявление и использование совокупности свойств разного уровня. Таким образом, под криминалистическим изучением личности потерпевшего следует понимать установление криминалистически значимой информации о потерпевшем, включающей в себя сведения о присущих ему 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[22].

Потерпевшим по рассматриваемой группе преступлений может стать любой пользователь социальной сети.

Функционал социальной сети «Вконтакте» позволяет пользователю совершать различные действия на своей персональной странице и в сообществах. Согласно пункту 5.11 правил «Вконтакте», после регистрации

---

[20] Приговор Хасавюртского городского суда по уголовному делу № 1-96/2015 по обвинению Асакаева Р.А. по ч. 2 ст. 128.1 УК РФ. 2015 год [Электронный ресурс] // Справочная система «СудАкт». – Режим доступа: http://sudact.ru/regular/doc/KWaHTTfQfcLw/ (Дата обращения: 24.04.2018).

[21] Приговор Кировского районного суда г. Красноярска по уголовному делу № 1-570/2012 по обвинению Агаева Р.М. по ч.1 ст.205.2 УК РФ. 2012 год [Электронный ресурс] // Справочная система «СудАкт». – Режим доступа: http://sudact.ru/regular/doc/Xwtcb1oLGI/ (Дата обращения: 24.04.2018).

[22] Зеленский, В.Д. Криминалистика: учебник / В. Д. Зеленский, Г. М. Меретуков ; под. общ. ред. В. Д. Зеленского. – Санкт-Петербург : Юридический центр, 2015 – С. 125.

пользователь получает право самостоятельно в личных целях создавать, использовать и определять содержание собственной персональной страницы, а именно: добавлять текстовый, фото, видео, аудио контент, делиться записями из сообществ. Также, согласно пункту 5.13.1, пользователь вправе создавать группы, публичные страницы и встречи для целей информирования других пользователей о каких-либо событиях, мероприятиях, организациях, как коммерческих, так и некоммерческих, их создании и деятельности, иных интересующих пользователей материалах, и/или/либо возможного обсуждения их с другими пользователями.

Пункты 5.2 и 5.3 правил «Вконтакте» гласят, что пользователем социальной сети является физическое лицо, зарегистрированное на сайте в соответствии с установленным правилами порядком, достигшее возраста, допустимого в соответствии с законодательством Российской Федерации для акцепта правил сайта, и обладающее соответствующими полномочиями.

«Вконтакте» не устанавливает ограничения на возраст пользователей. Однако, 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[23].

5 апреля 2017 года в Государственную Думу был внесен законопроект «О правовом регулировании деятельности социальных сетей». Разработчики данного акта предложили полностью запретить пользование социальными сетями лицам до 14 лет. Данная инициатива активно обсуждалась в СМИ и, к счастью, не прошла далее стадии законопроекта.

Согласно ст. 42 УПК РФ потерпевшим является физическое лицо, которому преступлением причинен физический, имущественный, моральный

[23] Правила пользования сайтом «Вконтакте» [Электронный ресурс] – Режим доступа: https://vk.com/terms

вред, а также юридическое лицо в случае причинения преступлением вреда его имуществу и деловой репутации.

Информация о личности потерпевшего может быть получена при анализе его персональной страницы с социальной сети. Функционал социальной сети позволяет установить круг общения потерпевшего, его половые, возрастные характеристики, увлечения и т.д.

Группы потерпевших в исследуемой категории дел отличаются многообразием. Так, Баринов С.В. отмечает, что по преступлениям, совершенным посредством социальных сетей, направленным против неприкосновенности частной жизни, а также преступлениям, направленным против чести, достоинства и деловой репутации потерпевшими чаще всего являются женщины в возрасте от 21 до 35 лет[24].

Потерпевшим может стать любое лицо, которое по причине неосмотрительности откроет файл или перейдет на страницу, содержащую вирусную программу (такая ситуация характерна для таких преступлений, как неправомерный доступ к компьютерной информации, а также создание, использование и распространение вредоносных компьютерных программ).

Изученная судебная практика свидетельствует о том, что в связи с распространением преступлений, указанных в статье 282 УК РФ, потерпевшими все чаще становятся пользователи, относящиеся к малочисленным этническим и другим социальным группам населения.

1.4 Личность преступника.

По мнению Р.Л. Ахмедшина, личность преступника – это совокупность свойств, присущих совершающему или совершившему преступление человеку, составляющих его индивидуальность. Криминологи изучают эту совокупность свойств для того, чтобы на их основе определить факторы, влияющие на совершение конкретного преступления,

[24] Баринов, С.В. Использование специальных знаний в расследовании преступных нарушений неприкосновенности частной жизни / С. В. Баринов // Вестник Удмуртского университета. – 2015. – № 6. – С. 40.

которые могут быть использованы в процессе расследования и рассмотрения уголовного дела, а также при создании основ и методик индивидуальной профилактики. Личность преступника отличается своей общественной опасностью, степень которой зависит от глубины деформации нравственно-психологических ее качеств[25].

С.В. Баринов в своем исследовании, посвященном преступлениям против неприкосновенности частной жизни, совершаемым в социальных сетях, приводит некоторые статистические данные. Согласно этим данным, преступниками, совершившими преступления против неприкосновенности частной жизни в социальных сетях, чаще всего (в 78 % случаев) являются мужчины в возрасте от 17 до 35 лет. В то же время он отмечает, что возраст и пол не являются значительными препятствиями в освоении технологий, используемых при совершении преступных деяний рассматриваемой группы. Например, следственными органами Следственного комитета по Республике Бурятия расследовалось уголовное дело, возбужденное в отношении 63-летней гражданки С., жительницы города Улан-Удэ.

Установлено, что 91 % уголовных дел возбуждались в отношении жителей крупных и средних городов: Москва, Казань, Белгород, Набережные Челны, Елец, Оренбург, Новочебоксарск, Ивангород и т.д. Однако по мере продолжения процессов компьютеризации населения и проникновения информационно-телекоммуникационных сетей вглубь территории страны примеры совершения преступных нарушений неприкосновенности частной жизни, совершенные в сети Интернет, фиксируются в отдаленных от центра географически небольших населенных пунктах. Характерным примером может являться преступление, совершенное гражданином Н. в поселке Пионерский Елизовского района Камчатского края. Таким образом, территориальные границы совершения указанных преступлений

[25] Ахмедшин, Р.Л. Криминалистическая характеристика личности преступника: природа и содержание / Р. Л. Ахмедшин // Вестник Томского государственного университета. – 2014. – № 7. – С. 24.

ограничиваются только территорией покрытия информационно-телекоммуникационных сетей.

Лица, совершившие преступления рассматриваемой группы, владеют навыками работы с компьютером чаще на уровне обычного пользователя, но иногда и продвинутого пользователя, то есть, обладают специальными знаниями (например, могут взломать электронную почту, профиль в социальной сети и т.д.), являются активными участниками социальных сетей, имеют в личном пользовании компьютерную технику, устройства для фото и видеосъемки. Они ранее не судимые, не имеющие устойчивых связей с криминалитетом, не ведущие антисоциальный образ жизни. Совершаемые преступления чаще всего – первый криминальный опыт в жизни. Уровень благосостояния преступников можно считать, как удовлетворительный. Род занятий: учащиеся, работающие, временно безработные[26].

В.В. Дьяков отмечает, что круг лиц, совершающих преступления в сфере компьютерной информации довольно широк. По данным специальных исследований, это могут быть, как и высококвалифицированные специалисты, так и дилетанты, имеющие разный социальный статус и уровень образования. Учитывая специфику преступлений в сфере компьютерной информации, для решения задач расследования, важно получить представление о «портрете» преступника.

Сведения о поле лиц, совершивших расследуемую категорию преступлений, характеризует их как деяние характерные для мужчин (от 86% до 92%), доля женщин колеблется от 4,8 до 12,2%. Однако, просматривается положительная динамика возрастания доли женщин-преступниц, по причине профессиональной ориентации некоторых специальностей (секретарь, делопроизводитель, бухгалтер, контролер, кассир и другие) по использованию в работе средств компьютерной техники. Все чаще встречаются факты

[26] Баринов, С.В. Использование специальных знаний в расследовании преступных нарушений неприкосновенности частной жизни / С. В. Баринов // Вестник Удмуртского университета. – 2015. – № 6. – С. 41.

пособничества женщин совершению преступлений в сфере компьютерной информации[27].

Проведенный В.В. Дьяковым анализ статистических данных позволил ему выделить некоторые общие характеристики личности преступника: это молодой человек, имеющий среднее (средне-специальное) образование, в возрасте 18-24 лет, противоправные действия он совершает преимущественно без соучастников, ранее в противозаконных действиях незамечен, с достаточно высоким уровнем технического и специального образования. По роду своей профессиональной деятельности они связанны либо с определенным режимом работы, либо с затруднениями осуществления контроля при исполнении последними своих профессиональных обязанностей, имеют свободный доступ к компьютерным системам. Важно отметить психологические аспекты личности: замкнутость, скрытность. Специфические интересы личности, связанные с увлечением литературой по компьютерной технике, информационным технологиям, программным обеспечением[28].

1.5 Следовая картина.

Вопросы, касающиеся сущности, понятия и классификации следов, достаточно полно и глубоко исследованы в работах отечественных криминалистов. В соответствии с положениями этих работ «в самом общем и широком смысле слова, след в криминалистике – это любое изменение, причинно обусловленное стадией совершения преступления»[29].

Исходя из приведенного понимания, традиционно следы в криминалистике подразделяются на две основные группы: материальные и идеальные. Данное деление было предложено более двадцати лет назад и практически не претерпело каких–либо существенных изменений. Вместе с

[27] Дьяков, В.В. О личности преступника, как компоненте системы криминалистической характеристики преступлений в сфере компьютерной информации / В. В. Дьяков // Бизнес в законе. – 2008. – № 6. – С. 130.
[28] Дьяков, В.В. О личности преступника, как компоненте системы криминалистической характеристики преступлений в сфере компьютерной информации / В. В. Дьяков // Бизнес в законе. – 2008. – № 6. – С. 131.
[29] Губанов, Д.А. Концептуальный подход к анализу онлайновых социальных сетей / Д. А. Губанов // Управление большими системами: сборник трудов. – 2013. – № 5. – С. 332.

тем, исследователи ряда криминалистических проблем, связанных с использованием цифровых носителей информации (аудио и видеозаписи), при расследовании «традиционных» преступлений и преступлений в сфере компьютерной информации, в первую очередь (компьютерные программы, базы данных и т.п.), столкнулись с ситуацией, когда в процессе отражения событий и явлений, связанных с преступлением, возникают следы, которые не могут быть в полной мере отнесены ни к одному из выделяемых криминалистикой видов, хотя обнаруживают в себе свойства как одних, так и других. Такую разновидность следов было предложено назвать «виртуальными следами».[30]

Преступления, совершенные посредством социальных сетей, оставляют специфическую следовую картину. Кроме непосредственно материальных или идеальных следов, следы остаются также в памяти электронных устройств. Поэтому некоторые авторы, основываясь на достижениях научно-технического прогресса, предлагают дополнить классическую классификацию следов специфической группой виртуальных следов.

Понятие «виртуальные следы» в криминалистике предложил использовать В.А. Мещеряков. По его мнению, виртуальные следы – это любое изменение состояния автоматизированной информационной системы (образованного ею «кибернетического пространства»), связанное с событием преступления и зафиксированное в виде компьютерной информации (т.е. информации в виде, пригодном для машинной обработки) на материальном носителе, в том числе и на электромагнитном поле[31].

В.Ю. Агибалов поддерживает его выводы и выделяет виртуальные следы в отдельную группу, наравне с идеальными и материальными. Основанием для этого служит то, что «в результате электронно-цифрового отражения на материальном носителе фиксируется лишь образ, состоящий из

[30] Мещеряков, В.А. «Виртуальные следы» под «скальпелем Оккама» / В.А. Мещеряков // Информационная безопасность регионов. – 2009. – № 1. – С. 28.

[31] Мещеряков, В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. / В. А. Мещеряков // Издательство Воронежского государственного университета. – 2002. – № 3. – С. 107.

цифровых значений параметров формальной математической модели наблюдаемого реального физического явления»[32].

Такой же позиции придерживается другая группа авторов. В.О. Давыдов, А.Ю. Головин полагают, что возможно дополнение классической классификации следов промежуточной группой виртуальных следов. Под ними данные ученые понимают «зафиксированное в виде цифрового образа формальной модели изменение состояния информации в памяти абонентских электронных устройств (терминалов, биллинговых систем и т.д.), вызванное алгоритмом установленного программного обеспечения и связанное с событием преступления (имеющее уголовно–релевантное значение)»[33].

Другое значение рассматриваемому понятию предлагает дать А.Г. Волеводз. По его мнению, во-первых, виртуальные следы – это данные, сохраненные провайдером (информация о сеансе связи, статистические или динамические IP-адресные журналы регистрации провайдера в сети Интернет, телефонные номера, скорость передачи сообщения, исходящие сеансы связи, типы использованных протоколов и т.д.), LOG-файлы. Во-вторых, виртуальные следы – это следы, остающиеся на компьютерах, используемых для совершения преступных действий, либо через которые проходит или поступает информация (таблицы размещения файлов FAT, NTFS и др., системные реестры операционных систем, отдельные кластеры магнитного носителя информации, файлы и каталоги хранения сообщений электронной почты, файлы конфигурации программ удаленного доступа и иное)[34].

По мнению А.А. Абрамовой, виртуальные следы – это цифровой образ, электронные сигналы, остающиеся в памяти электронных и подобных им

---

[32] Агибалов, В.Ю. Виртуальные следы в криминалистике и уголовном процессе / В. Ю. Агибалов // Общество: политика, экономика, право. – 2012. – № 5. – С. 34.

[33] Давыдов, В.О. Значение виртуальных следов в расследовании преступлений экстремистского характера / В. О. Давыдов // Известия Тульского государственного университета. Экономические и юридические науки. – 2016. – № 3. – С. 257.

[34] Волеводз, А.Г. Следы преступлений, совершенных в компьютерных сетях / А. Г. Волеводз // Российский следователь. – 2015. – № 3. – С. 46.

устройств, передаваемые с помощью заданного алгоритма и имеющие уголовно-релевантное значение[35].

Таким образом, современная криминалистика признает наличие малоизученных виртуальных следов, но не все криминалисты согласны с использованием термина «виртуальный». В настоящее время среди ученых нет единого мнения в определении понятия и сущности данного вида следов. Например, Г.М. Шаповалова, Ю.В. Гаврилин, М.В. Салтаевский, В.В. Борисов, С.А. Потапов, И.С. Потапова считают дефиницию «информационные следы» наиболее содержательной. В.А. Милашев использует термин «бинарные следы», А.С. Егорышев – «следы неправомерного доступа», А.О. Сукманов – «электронно-цифровые следы».

В.В. Борисов говорит о том, что «информационные следы» – это информационная запись, сделанная на компьютерной технике подозреваемых в преступлении лиц с помощью специального программного средства и произведенную субъектом уголовно-процессуальной системы (например, следователем)[36]. В данном определении сделан акцент именно на «записи», то есть автор говорит о том, что информационный след обязательно фиксируется в памяти устройств.

М.В. Салтевский выделяет информационно-виртуальные следы – следы, остающиеся на материальных носителях; отображающиеся в компьютерных программах, базах данных, текстовых файлах; изменения, выявляемые как непосредственно, так и при удаленном доступе[37].

Таким образом, проанализировав различные точки зрения касательно понятий «виртуальные следы» и «информационные следы», можно сделать следующие выводы. На наш взгляд, применение термина «информационные следы» является наиболее удачным. Вся информация традиционно делится на

[35] Абрамова, А.А. Значение виртуальных следов в расследовании финансирования терроризма / А. А. Абрамова // Общество: политика, экономика, право. – 2017. – № 12. – С. 25.
[36] Борисов, В.В. Об особенностях фиксации информационных следов в практике защиты информации / В. В. Борисов // Известия Южного федерального университета. – 2009. – № 7. – С. 102.
[37] Салтевский, М.В. Новый подход в технологии собирания и исследования информационных следов / М. В. Салтевский // Пробелы в российском законодательстве. – 2008. – № .5. – С. 27.

аналоговую и цифровую. Аналоговая информация – это информация, которую видит, слышит и с которой работает человек благодаря своим органам чувств (фото, видео, аудиозаписи). Цифровая информация – это информация, с которой работает вычислительная техника (коды). Соответственно, все следы, с которыми необходимо работать при расследовании преступлений, совершенных посредством социальных сетей, могут быть представлены либо в виде аналоговой, либо в виде цифровой информации. Именно поэтому они «информационные». К тому же, основанием для выделения данной группы следов может считаться специфическая среда, на которую они воздействуют, а именно электромагнитное поле. Итак, информационные следы – это следы, хранящиеся в памяти электронных устройств в виде двоичного кода и содержащие криминалистически значимую информацию о совершенном преступлении.

Любые действия с программируемыми устройствами непосредственно отражаются в памяти данных устройств. Поэтому следы могут быть обнаружены и в памяти самого устройства, с которого осуществлялся выход в сеть Интернет. Таковыми могут являться сведения о работе в сети Интернет, локальных и иных сетях (содержатся в «логах» или log-файлах).

Следы, оставленные пользователем при использовании социальной сети, хранятся в центрах обработки данных – дата-центрах. Дата-центром (центр хранения и обработки данных) называется специализированное здание для размещения серверного и сетевого оборудования и подключения абонентов к каналам сети Интернет. Дата-центр исполняет функции обработки, хранения и распространения информации. В оборудовании дата-центров вся информация кодируется и затем хранится в виде двоичного кода (нулей и единиц)[38].

При поиске следов преступлений, совершенных либо подготовленных в социальных сетях, необходимо учитывать такие особенности следообразования в социальных сетях, как наличие аккаунта, его привязка к

[38] Грошев, А.С. Информатика: учебник для вузов / А. С. Грошев. – Архангельск: Архангельский государственный технический университет, 2010. – С. 17.

адресу электронной почты либо к номеру мобильного телефона, архив сообщений, статистика активности на странице пользователя.

Следы преступлений, совершенных посредством социальных сетей, могут быть самыми различными, их разнообразие ограничено только функционалом социальной сети. Например, следом может являться текстовая информация, противоправно размещенная в социальной сети: информация экстремистского характера; информация о продаже наркотических средств и психотропных веществ, а также иных предметов и веществ, запрещенных к гражданскому обороту на территории Российской Федерации, об оказании незаконных услуг; информация, порочащая честь, достоинство и деловую репутацию лиц.

Следами преступления могут являть данные об активности пользователя в социальной сети, например, время входа и выхода из персональной страницы. Данные сведения могут быть предоставлены администрацией социальной сети в порядке ответа на запрос правоохранительных органов.

Следами исследуемой категории преступлений могут являться также так называемые «фейковые» страницы. Создается внешне аналогичная страница, при переходе на которую, ошибочно приняв за реальную, в систему пользователя может попасть компьютерный вирус. Дальнейшее зависит от целей создания вируса. Кроме того, после ввода на «фейковой» странице своих личных данных, необходимых для авторизации, злоумышленникам открывается доступ к аккаунту пользователя[39].

1.6 Обстановка совершения преступления.

Обстановку совершения рассматриваемой группы преступлений составляют сведения о месте, времени и других условиях, оказывающих влияние на их совершение. Эти сведения могут быть абсолютно разными, однако в любом случае преступления данной группы будут совершаться с

[39] Введенская, О.Ю. Особенности следообразования при совершении преступлений посредством сети интернет / О. Ю. Введенская // Юридическая наука и правоохранительная практика. – 2015. – № 3. – С. 104.

использованием различных программируемых устройств, имеющих доступ в сеть Интернет: компьютеры, ноутбуки, планшеты, телефоны и др. Преступления данной группы могут быть совершены в любое время и в любом месте (насколько это позволяет распространенность сети Интернет). Н.П. Яблоков отмечает, что для обстановки совершения преступлений исследуемой группы характерно несовпадение между местом совершения противоправных действий и местом наступления общественно опасных последствий[40].

А.М. Ишин указывает, что преступления, совершаемые в сети Интернет, как правило, характеризуются повышенной скрытностью совершения, обеспечиваемой за счет сложности сетевой инфраструктуры и развитых механизмов анонимности. Многие преступления имеют трансграничный характер, при котором преступник, объект преступного посягательства, жертва находятся под юрисдикцией различных государств. Преступные действия в основном носят дистанционный характер, без физического контакта преступника и жертвы, причем часть таких действий может выполняться в автоматизированном режиме. При этом эпизоды преступления, происходящие в пределах различных юрисдикций, по отдельности могут восприниматься как не связанные друг с другом и не заслуживающие оперативно-розыскного реагирования.

Применение стандартизированных орудий совершения преступлений (программного обеспечения) нивелирует индивидуальный «почерк» преступников, а использование особых способов сокрытия следов повышает сложность выявления преступления. Важно учитывать, что следы преступных действий в сетевом пространстве распределяются по множеству объектов при отсутствии четко выраженного места совершения преступления[41].

[40] Яблоков, Н.П. Криминалистика: учебник. / Н. П. Яблоков. – Москва: Юристъ, 2005. – С. 65.
[41] Ишин, А.М. Современные проблемы использования сети Интернет в расследовании преступлений / А. М. Ишин // Вестник Балтийского федерального университета. – 2013. – № 8. – С. 57.

Весьма значительна специфика такой составляющей обстановки, как место и время совершения преступлений в сфере компьютерной информации. Данные преступления происходят в специфической среде – виртуальном кибернетическом пространстве. Особенностью их является то, что в результате использования информационных сетей (проводных и беспроводных технологий) в одном преступлении одновременно могут быть задействованы множество компьютеров. Соответственно, находиться эти компьютеры могут в пространственно удаленных друг от друга местах и даже в разных государствах. Каждое из таких мест имеет свою обстановку. Следует отметить, что преступник действует не только в конкретной обстановке, но и в конкретное время, порой в значительной мере влияющее на его поведение. Работа некоторых программ связана со временем, установленным на компьютере, которое может быть изменено по желанию преступника. Установление точного времени совершения преступления является сложной задачей, разрешение которой не всегда возможно, в том числе в связи с отсутствием его синхронизации с эталоном[42].

В результате компьютерного преступления в обстановке могут оставаться характерные изменения. Такие изменения можно обнаружить при анализе лог-файлов операционной системы и иных программ, ведущих учет действий, совершаемых на компьютере. Однако, как правило, специфика электронно-цифровых следов проявляется в том, что многие изменения остаются практически незаметными. Кроме того, на обстановку, складывающуюся после совершения преступления, накладывают отпечаток условия и обстоятельства, происходящие впоследствии. Так, некоторые электронно-цифровые следы-последствия преступления затираются новыми без возможности восстановления. Отметим, что аналогичные последствия происходят и с некоторыми традиционными следами, например, запаховыми.

[42] Прохоров, М.С. Криминалистическая характеристика преступлений / М. С. Прохоров // Известия Российского государственного педагогического университета. – 2008. – № 3. – С. 353.

Это требует при обнаружении преступлений в сфере компьютерной информации скорейшего проведения неотложных следственных действий[43].

Таким образом, можно сделать вывод о том, что криминалистическая характеристика преступлений, совершенных посредством социальных сетей, имеет определенные отличительные черты. Наличие этих черт связано со спецификой социальных сетей как таковых, их своеобразием и функционалом.

[43] Поляков, В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики / В. В. Поляков // Известия Алтайского государственного университета. – 2013. – № 2. – С. 114.

2 Типичные следственные ситуации и направления расследования преступлений, совершенных посредством социальных сетей

Р.С. Белкин отмечает, что преступления расследуются в конкретных условиях времени, места, окружающей его среды, взаимосвязях с другими процессами объективной деятельности, поведением лиц, оказавшихся в сфере уголовного судопроизводства, и под влиянием иных, порой остающихся неизвестными для следователя факторов. Эта сложная система взаимосвязей в итоге образует ту конкретную обстановку, в которой работает следователь и иные субъекты, участвующие в доказывании, и в которой протекает конкретный акт расследования. Такая обстановка получила в криминалистике общее название следственной ситуации. Иными словами, это существующая в данный момент реальность, в условиях которой действует следователь. Ситуация расследования характеризует состояние следственного производства, решенные и нерешенные задачи, результаты, возникшие трудности[44].

В.Д. Зеленский говорит о том, что следственная ситуация – это понятие, характеризующее процесс расследования, его состояние на том или ином этапе. Это сложившееся на конкретный момент расследования положение, характеризующееся: состоянием следственной обстановки; степенью познания криминальной ситуации; тактико-процессуальными и психологическими особенностями следствия; планово-организационным обеспечением следственной деятельности[45].

Исходя из этого, следственную ситуацию можно определить, как степень информационной осведомленности следователя о преступлении, а

[44] Белкин, Р. С. Криминалистика: учебник для вузов / Р. С. Белкин, Т. В. Аверьянова ; под. общ. ред. Р. С. Белкина. – Москва : НОРМА, 2000. – С. 78.
[45] Зеленский, В.Д. Криминалистика: учебник / В. Д. Зеленский, Г. М. Меретуков ; под. общ. ред. В. Д. Зеленского. – Санкт-Петербург : Юридический центр, 2015. – С. 120.

также состояние процесса расследования, сложившееся на конкретный определенный момент времени.

Р.С. Белкин пишет, что следственная ситуация образует в своей совокупности динамическую систему, постоянно изменяющуюся под воздействием объективных и субъективных факторов. Объективные факторы – это те не зависящие от участников расследования причины, которые вызывают изменения ситуации; субъективные факторы – причины, порождаемые действиями и поведением участников расследования и иных лиц, оказавшихся в той или иной степени втянутыми в сферу судопроизводства[46].

Д.Н. Балашов отмечает, что современное состояние науки криминалистики характеризуется стремлением дать следователю возможность для творческого применения своих знаний и сил при расследовании преступлений и при этом избежать «рутинной» работы, т.е. работы, которую выполнить необходимо, но ее содержание типично, повторяется при расследовании преступлений данной категории. Задача науки криминалистики заключается в том, чтобы на базе изучения практики систематизировать все встречающиеся ситуации, типизировать их и применительно к каждой разработать программу действий следователя[47].

Е.П. Ищенко указывает, что от складывающихся следственных ситуаций зависят методические рекомендации по определению основных направлений и методов расследования для первоначального и последующих этапов. Многие из них имеют типовой характер и различаются лишь объемом информации о событии преступления и виновных лицах. Для первоначального этапа характерны такие типичные ситуации:

---

[46] Белкин, Р. С. Криминалистика: учебник для вузов / Р. С. Белкин, Т. В. Аверьянова ; под. общ. ред. Р. С. Белкина. – Москва : НОРМА, 2000. – С. 85.

[47] Балашов, Д.Н. Криминалистика: учебник / Д. Н. Балашов. – Москва : ИНФРА-М, 2005. – С. 54.

1) есть сведения о событии преступления и виновном лице, но еще не ясно, было ли это событие в действительности, имело ли оно преступный характер и причастно ли к нему указанное (обычно, потерпевший) лицо;

2) имеется событие с признаками преступления, известны конкретные лица, несущие за это ответственность, но характер их вины не ясен;

3) выявлено событие с признаками преступления, совершить которое и воспользоваться результатами которого по своему положению могли только лица из определенного круга либо для совершения которого требуются особые профессиональные навыки или знания;

4) выявлено событие, имеющее признаки преступления, но отсутствуют сведения о виновном лице.

Характер типичных следственных ситуаций на последующем этапе расследования определяется результатами, достигнутыми на первоначальном этапе. В одних случаях это розыск уже установленного преступника, в других – еще не установленного, в-третьих – собирание данных, изобличающих виновное лицо, предъявление ему обвинения, доказывание его виновности.

Типичные следственные ситуации и направления дальнейшего расследования на завершающем этапе связаны с качеством и полнотой данных, положенных в основу обвинения, которое обвиняемый может полностью, частично или вообще не признать. Тогда проверяются его доводы, собираются дополнительные доказательства, а расследование либо завершается направлением дела в суд, либо приостанавливается, прекращается по различным основаниям[48].

Типичные следственные ситуации по исследуемой категории преступлений можно классифицировать по различным основаниям. По источнику информации выделяют ситуации, когда:

1) преступление выявлено самим пользователем;

[48] Ищенко, Е.П. Криминалистика: курс лекций / Е. П. Ищенко. – Москва : АСТ, 2007. – С. 213.

2) преступление выявлено правоохранительными органами;

3) преступление выявлено модераторами социальной сети.

В случае выявления преступления пользователем социальной сети самостоятельно, последний может реализовать право, установленное в статье 141 УПК РФ и обратиться с заявлением в правоохранительные органы либо же просто сообщить о преступлении. Также пользователь вправе обратиться к администрации «Вконтакте» с просьбой удалить неправомерную информацию, т.к., согласно пункту 8.5 Правил, она предпринимает действия по защите прав и интересов лиц и обеспечению соблюдения требований законодательства Российской Федерации только после обращения заинтересованного лица к администрации сайта в установленном порядке[49].

При расследовании преступлений, совершенных посредством социальных сетей, необходимо обязательно проводить предварительную проверку сообщений и заявлений. В рамках данных проверок правоохранительные органы могут контактировать в запросно-ответной форме с социальными сетями и таким образом получать от них имеющую значение информацию.

В случае выявления преступления правоохранительными органами последние вправе возбудить уголовное дело. Выявление преступления может быть результатом проведения мониторинга социальной сети. Данное действие могут осуществлять сотрудники ФСБ, Прокуратуры, Следственного комитета РФ и другие ведомства.

Преступление, совершенное с использованием социальных сетей, также может быть выявлено в результате проведения следственных действий по другому уголовному делу. Например, приговором Октябрьского районного суда г. Рязани от 28.09.2017 года был осужден Кротов В.А. по ч. 2 ст. 228.1 УК РФ. В процессе изучения информации, содержащейся на его персональной

[49] Правила пользования сайтом Вконтакте [Электронный ресурс] – Режим доступа: https://vk.com/terms

странице в «Вконтакте», было установлено, что данное лицо не просто занималось сбытом наркотических веществ, а также выполняло функции так называемого «куратора региона». Следовательно, было выявлено преступление, предусмотренное ст. 210 УК РФ[50].

Также преступление может быть выявлено модераторами социальной сети. Администрация сайта «Вконтакте» применяет особый механизм борьбы с неправомерными действиями пользователей. Так, согласно пунктам 6.3.1-6.3.16 Правил, пользователям запрещается загружать, хранить, публиковать, распространять и предоставлять доступ или иным образом использовать любую информацию, которая содержит экстремистские материалы; оскорбляет, порочит честь и достоинство или деловую репутацию или нарушает неприкосновенность частной жизни других пользователей или третьих лиц; пропагандирует и/или способствует разжиганию ненависти или вражды, пропагандирует фашизм или идеологию расового превосходства; о распространении наркотиков и т.д. Также пользователям запрещается распространять вредоносные программы; осуществлять незаконные сбор и обработку персональных данных других лиц и т.д. Вышеназванные действия могут быть квалифицированы как преступления особенной части УК РФ.

Согласно пункту 8.6 Правил, администрация сайта вправе по своему собственному усмотрению, а также при получении информации от других пользователей либо третьих лиц о нарушении пользователем настоящих правил, изменять (модерировать), блокировать или удалять любую публикуемую пользователем информацию, нарушающую запреты, установленные настоящими Правилами, приостанавливать, ограничивать или прекращать доступ пользователя ко всем или к любому из разделов или функционалу сайта в любое время по любой причине или без объяснения

[50] Приговор Октябрьского районного суда г. Рязани по уголовному делу № 1-229/2017 по обвинению Кротова В.А. по ч. 2 ст. 210, ч. 4 ст. 228.1 УК РФ. 2017 год [Электронный ресурс] // Справочная система «СудАкт». – Режим доступа: http://sudact.ru/regular/doc/STfEbGVF4GU9/ (Дата обращения: 24.04.2018).

причин, с предварительным уведомлением или без такового. Администрация сайта закрепляет за собой право удалить персональную страницу пользователя и/или приостановить, ограничить или прекратить доступ пользователя к любой из функциональных возможностей сайта, если администрация обнаружит, что, по ее мнению, пользователь представляет угрозу для сайта и/или его пользователей.

Также, согласно пункту 5.13.8, в случае обнаружения факта нарушения в сообществе законных прав и интересов третьих лиц, действующего законодательства Российской Федерации, а также положений настоящих Правил администрация сайта вправе удалять контент и иную информацию со страницы сообщества и/или блокировать доступ к ним[51].

Типичные следственные ситуации, складывающиеся при расследовании преступлений исследуемой группы, можно также классифицировать в зависимости от того, имеется ли достоверная информация о личности преступника:

1) Информация о личности преступника имеется в полном объеме;

2) Информация о личности преступника имеется в неполном объеме;

3) Установить информацию о преступнике не представляется возможным.

На наш взгляд, можно согласиться с М.В. Савельевой, и в первом, максимально информативном случае, направление расследования будет включать следующие действия:

1) изучение материалов предварительной проверки и возбуждение уголовного дела;

2) осмотр места происшествия;

3) задержание подозреваемого;

4) допрос подозреваемого;

[51] Правила пользования сайтом Вконтакте [Электронный ресурс] – Режим доступа: https://vk.com/terms

5) обыски по месту жительства и работы подозреваемого;

6) допрос потерпевших и свидетелей;

7) выемка компьютерной или иной техники;

8) назначение судебных экспертиз.

В ходе расследования может сложиться ситуация, когда информация о личности преступника получена в неполном объеме, но установить ее можно путем проведения дополнительных следственных и иных действий. Например, при регистрации в социальной сети пользователь указал недостоверные данные, однако удалось получить IP-адрес устройства, с помощью которого осуществлялись преступные действия. В таком случае целесообразным будет следующее направление расследования:

1) опрос заявителя и свидетелей;

2) осмотр места происшествия с участием специалистов;

3) ОРМ для установления причин преступления, выявления злоумышленников;

4) допрос свидетелей и потерпевших;

5) выемка и исследование компьютерной или иной техники;

6) задержание подозреваемого;

7) допрос подозреваемого;

8) обыски по месту жительства и работы подозреваемого;

9) назначение судебных экспертиз[52].

Третья ситуация расследования, когда отсутствует информация о лице, совершившем преступление, представляет наибольшую сложность для правоохранительных органов. В настоящее время существуют технические возможности совершить преступление в социальных сетях и при этом сохранить свою анонимность. В сети Интернет существует множество статей по данной тематике. Среди основных рекомендаций по сохранению

[52] Савельева, М.В. Криминалистика: учебник / М. В. Савельева. – Москва: «Дашков и К», 2009. – С. 141.

анонимности в сети выделяют такие, как: использование специализированного иностранного софта; использование VPN и Прокси-серверов; чистка log-файлов и др. Также в сети Интернет встречаются предложения о сдаче в аренду номера телефона (sms-reg.com, sms-area.org, onlinesim.ru).

О проблеме установления личности преступника и установлении места совершения преступления пишет О.В. Овчинникова. Она утверждает, что когда необходимая для установления обстоятельств уголовного дела цифровая информация размещена в виртуальном пространстве телекоммуникационной сети Интернет, ее фиксация имеет существенную специфику: отсутствуют сведения о местонахождении техники и личности преступника. Указанные сведения об этом могут быть получены только после установления интернет-провайдера, выяснения IP-адреса компьютера и его местонахождения. Более того, размещение информации может быть произведено не со стационарного компьютера, имеющего свой адрес, а через систему предоставления беспроводного доступа в Интернет в торговых комплексах, кафе и других местах общего пользования. В этом случае определить место совершения преступления становится технически невыполнимо.

Данные обстоятельства создают проблемы при организации предварительной проверки сообщения о преступлении в связи с трудностью определения территориальности. Высокий процент (около 50%) зарегистрированных сообщений направляется по подследственности, многие (около 25%) направляются неоднократно. Сложившаяся ситуация является недопустимой, поскольку она препятствует своевременному осуществлению правосудия и может привести к утрате доказательственной информации[53].

Н.А. Морозова предлагает внести изменения в уголовно-процессуальное законодательство по вопросу определения места происшествия при

[53] Овчинникова, О.В. Собирание электронных доказательств, размещенных в сети Интернет / О. В. Овчинникова // Правопорядок: история, теория, практика. – 2016. – № 3. – С. 45.

совершении преступления в телекоммуникационной сети Интернет[54]. Полагаем, что данный вопрос является организационным, а не процессуальным, поэтому данную проблему можно было бы урегулировать изданием ведомственного нормативного акта (например, инструкции), регламентирующего порядок предварительной проверки сообщения о преступлении с использованием сети Интернет в общем, и социальных сетей в частности.

Ю.Н. Троегубов, с точки зрения своего предмета исследования, указывает на проблему установления лица, разместившего в сети экстремистский или террористический материал. Современные технологии беспроводного доступа в сеть (например, Wi-Fi), имеющиеся в свободной продаже сетевые платы с динамическим IP-адресом и т. п., фактически исключают обнаружение такого лица. После обнаружения такого лица встает проблема его идентификации, как автора или издателя какого-либо материала, а не просто как владельца средства вычислительной техники, посредством которого в сети был размещен материал[55].

В качестве меры, направленной на решение указанных проблем, можно назвать принятие Правительством РФ Постановления № 758 от 31.07.2014 года, которым вносятся изменения в целый ряд нормативных актов: ППРФ от 21.04.2005 года № 241 «О мерах по организации оказания универсальных услуг связи»; ППРФ от 23.01.2006 года № 32 «Об утверждении Правил оказания услуг связи по передаче данных»; ППРФ от 10.09.2007 года № 575 «Об утверждении Правил оказания телематических услуг связи». Так, согласно пункту 2 данного Постановления, в случае заключения срочного договора об оказании разовых услуг по передаче данных в пунктах коллективного доступа оператор связи осуществляет идентификацию

[54] Морозова, А.Н. Проблемы привлечения к уголовной ответственности за экстремизм в информационной сети Интернет / А. Н. Морозова // Российский следователь. – 2014. – № 5. – С. 39.
[55] Троегубов, Ю.Н. Проблемы противодействия экстремизму в сети Интернет / Ю. Н. Троегубов // Гуманитарный вектор. Серия: История, политология. – 2014. – № 3. – С. 147.

пользователей и используемого ими оконечного оборудования оператора связи. Идентификация пользователя осуществляется оператором связи путем установления фамилии, имени, отчества (при наличии) пользователя, подтверждаемых документом, удостоверяющим личность. Идентификация оконечного оборудования осуществляется средствами связи оператора связи, путем определения уникального идентификатора оборудования сетей передачи данных.

Порядок идентификации установлен таким образом, что оператор вправе выбирать, как именно осуществлять идентификацию пользователя. Например, он может сделать это посредством запроса в соответствующий орган власти. В то же время пользователь обязан предоставить любую идентификационную информацию, например, имя, фамилию, отчество, номер водительского удостоверения и так далее.

Таким образом, если точка доступа Wi-fi установлена оператором связи, то он должен отправить пользователю запрос на получение идентификационных данных по SMS или предложить специальную форму для указания данных перед открытием доступа в сеть Интернет. Однако, если точка доступа Wi-fi установлена частным лицом, никаких обязанностей у него в связи с изменениями не существует.

Данное постановление напрямую следует из Федерального закона № 97-ФЗ от 05.05.2014 года «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты РФ по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей»[56].

[56] О внесении изменений в некоторые акты Правительства Российской Федерации в связи с принятием Федерального закона "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей : Постановление Правительства РФ от 31.07.2014 г. № 758 // Российская газета. – 2014. – 5 авг.

3 Производство следственных действий при расследовании преступлений, совершенных посредством социальных сетей

При расследовании преступлений, совершенных посредством социальных сетей, может проводиться целый ряд следственных и иных действий, производство которых необходимо для полного установления всех обстоятельств, имеющих значение для дела. Среди них важное значение имеют осмотр, обыск и выемка, назначение экспертиз, следственный эксперимент.

3.1 Обыск и выемка.

Обыск – это следственное действие, направленное на принудительное обследование участков местности, помещений и иных сооружений и личных вещей, находящихся в ведении обыскиваемого лица и членов его семьи или организации, осуществляемое в рамках уголовно-процессуального закона управомоченным на то лицом, при соблюдении гарантий прав и законных интересов граждан и юридических лиц, с целью поиска (обнаружения) и изъятия (задержания) конкретных источников доказательственной информации (материальных объектов), могущих иметь значение для дела[57].

Согласно ст. 182 УПК РФ, основанием производства обыска является наличие достаточных данных полагать, что в каком-либо месте или у какого-либо лица могут находиться орудия, оборудование или иные средства совершения преступления, предметы, документы и ценности, которые могут иметь значение для уголовного дела.

В зависимости от характера обыскиваемых объектов различают следующие виды обыска: обыск помещений – состоит в принудительном обследовании жилых домов, квартир, служебных помещений, всевозможных

[57]Яблоков, Н.П. Криминалистика: учебник / Н. П. Яблоков. – Москва : Юристъ, 2005. – С. 73.

хранилищ (складов, сараев, погребов и др.), если там могут находиться интересующие следствие объекты; обыск на местности – состоит в принудительном обследовании приусадебных и иных участков, находящихся в пользовании определенных лиц; личный обыск – заключается в принудительном обследовании одежды, обуви и тела обыскиваемого.

По способу организации обыск может быть единичным, когда он производится в одном месте, и групповым, проводимым одновременно на нескольких объектах. Групповой обыск необходим в тех случаях, когда есть основания полагать, что искомые предметы или документы находятся у близких между собой лиц или у одного лица, но в разных местах (на квартире, даче, в служебном помещении) и разновременное проведение этих обысков может способствовать сокрытию искомого заинтересованными лицами.

В зависимости от того, обыскивался ли ранее данный объект, обыски подразделяются на первичные и повторные. Повторный обыск проводится в том случае, если первый обыск не дал положительных результатов, и имеются основания полагать, что разыскиваемые предметы могли быть не обнаружены при первичном обыске или появились на ранее обследованном объекте в последующем[58].

Производство обыска делится на три этапа: подготовительный, рабочий и заключительный.

В научной литературе разработаны некоторые тактические рекомендации, которыми надлежит руководствоваться при производстве обыска. При производстве следует: обеспечить внезапность, планомерность, целенаправленность; учитывать психологические черты обыскиваемого и обеспечить безопасность обыска; учитывать особенности предметов поиска и характера обследуемого объекта; использовать технико-криминалистические

[58] Балашов, Д.Н. Криминалистика: учебник / Д. Н. Балашов. – Москва : ИНФРА-М, 2005. – С. 54.

средства и методы; использовать помощь специалистов и сведения, полученные оперативным путем[59].

Уголовно-процессуальный кодекс РФ регламентирует порядок производства обыска и выемки электронных носителей информации. Так, при производстве обыска и выемки изъятие электронных носителей информации производится с участием специалиста. По ходатайству законного владельца изымаемых электронных носителей информации или обладателя содержащейся на них информации специалистом, участвующим в обыске и выемке, в присутствии понятых с изымаемых электронных носителей информации осуществляется копирование информации на другие электронные носители информации, предоставленные законным владельцем изымаемых электронных носителей информации или обладателем содержащейся на них информации. При производстве обыска и выемки не допускается копирование информации, если это может воспрепятствовать расследованию преступления либо, по заявлению специалиста, повлечь за собой утрату или изменение информации. Электронные носители информации, содержащие скопированную информацию, передаются законному владельцу изымаемых электронных носителей информации или обладателю содержащейся на них информации. Об осуществлении копирования информации и о передаче электронных носителей информации, содержащих скопированную информацию, законному владельцу изымаемых электронных носителей информации или обладателю содержащейся на них информации в протоколе делается запись (п. 3.1 и 9.1 статей 182 и 183 УПК РФ).

А.Р. Гузин отмечает, что анализ указанных положений позволяет сделать вывод о том, что, во-первых, из них не ясен механизм определения специалистом на месте изъятия носителей возможности утраты или изменения информации при ее копировании (представляется, что для этих целей необходима как минимум экспертиза); во-вторых, законодатель не регламентирует случаи отказа в удовлетворении ходатайства владельца или

[59] Савельева, М.В. Криминалистика: учебник / М. В. Савельева. – Москва : «Дашков и К», 2009. – С. 141.

обладателя информации, если носитель содержит информацию, запрещенную к свободному распространению (охраняемая законом тайна, информация экстремистского характера, детская порнография, вредоносные программы и др.); в-третьих, вызывает трудности процесс установления обладателя информации, которая содержится на носителях.

Все затрагиваемые проблемы не находят однозначного решения ни на практике, ни в теории, в связи с чем необходима детальная регламентация собирания, проверки и оценки доказательственной информации, изымаемой с электронных носителей, а также реализации гарантий прав участников уголовного судопроизводства, чьи интересы затрагиваются в ходе подобного рода направления доказывания[60].

Также, на наш взгляд, стоит согласиться с позицией О.В.Овчинниковой, которая полагает целесообразным более детально регламентировать порядок изъятия электронной информации, определив способ ее фиксации в зависимости от местонахождения цифровых данных:

1) энергозависимое устройство, предназначенное для переноса и хранения информации (USB-накопитель, карта памяти, внешний жесткий диск);

2) персональное цифровое устройство (компьютер, ноутбук, планшет, мобильный телефон);

3) виртуальное пространство телекоммуникационной сети Интернет.

Согласно проведенному ею опросу, в первых двух случаях, как правило, изымается не цифровая информация, а само электронное устройство. При этом 95% опрошенных следователей отметили, что участие специалиста при изъятии электронных носителей информации нарушает принцип процессуальной экономии, поскольку его роль сводится к упаковке предметов, производство которой может быть осуществлено следователем; 5%

[60] Гузин, А.Р. Проблемы регламентации собирания электронной информации в действующем законодательстве / А. Р. Гузин // Juvenisscentia. – 2017. – № 7. – С. 49.

опрошенных согласились с целесообразностью участия специалиста при необходимости отсоединения электронного устройства от сети, либо демонтажа устройства для изъятия его составных частей (жесткий диск и т.д.). Автором был проведен мониторинг уголовных дел, по результатам которого было выяснено, что цифровые носители информации признаются допустимым доказательством даже в случае отсутствия специалиста в ходе их изъятия. Следовательно, суды придерживаются аналогичной точки зрения.

Сложившуюся судебную и следственную практику можно нормативно закрепить, внеся в ч. 9.1 ст. 182 УПК РФ дополнение об усмотрении следователя при привлечении к участию в следственном действии специалиста, а также установить срок на предоставление копий изымаемой информации – в течение 5 суток, поскольку в ходе обыска не всегда имеется техническая возможность для копирования[61].

А.Р. Гузин предлагает дополнить ч. 9.1 ст. 182 и ч. 3.1 ст. 183 УПК РФ предложением: «Допускается изъятие электронных носителей информации без участия специалиста, если электронные носители информации изымаются целиком и изъятие производится без копирования содержащейся на них информации»[62].

3.2 Осмотр.

Следственный осмотр – это следственное действие, заключающееся в непосредственном восприятии, исследовании и фиксации объектов материальной обстановки, предметов и документов в целях обнаружения следов преступления, выяснения обстановки происшествия и других обстоятельств, имеющих отношение к происшедшему событию[63].

---

[61] Овчинникова, О.В. Собирание электронных доказательств, размещенных в сети Интернет / О. В. Овчинникова // Правопорядок: история, теория, практика. – 2016. – № 3. – С. 47.

[62] Гузин, А.Р. Проблемы регламентации собирания электронной информации в действующем законодательстве / А. Р. Гузин // Juvenis scentia. – 2017. – № 7. – С. 46.

[63] Яблоков, Н.П. Криминалистика: учебник / Н. П. Яблоков. – Москва : Юристъ, 2005. – С. 147.

Сущность осмотра заключается в том, что следователь с помощью органов своих чувств убеждается в существовании и характере фактов, имеющих доказательственное значение. При осмотре следователь не только наблюдает, но и производит различные измерения и вычисления, сравнивает наблюдаемые объекты, как между собой, так и с другими объектами и явлениями, в определенных пределах экспериментирует с исследуемыми объектами и, наконец, описывает и запечатлевает все то, что обнаружили и выявили он и другие участники осмотра. Результаты осмотра позволяют следователю определить направление расследования, представить механизм расследуемого события[64].

Согласно ст. 176 УПК РФ, целью смотра места происшествия, местности, жилища, иного помещения, предметов и документов является обнаружение следов преступления, выяснение других обстоятельств, имеющих значение для уголовного дела.

Следственный осмотр – это достаточно общее, собирательное понятие, которое включает в себя виды различных осмотров. По объему выделяют основной и дополнительный виды осмотра. Основной осмотр производится впервые, а дополнительный проводится после основного и предполагает осмотр предметов, которые не были осмотрены ранее. По последовательности проведения выделяют первоначальный и повторный осмотры. Первоначальный осмотр производится впервые, а повторный осмотр проводится в случае, когда первичный осмотр проводился неквалифицированно, без использования технико-криминалистических средств, при неблагоприятных условиях (при плохом освещении, в плохую погоду). К моменту проведения повторного осмотра обстановка претерпевает значительные изменения с момента расследуемого события, и это может сказаться на его результатах. По объектам осмотра выделяют осмотр места

[64] Белкин, Р.С. Криминалистика: учебник для вузов / Р. С. Белкин, Т. В. Аверьянова ; под. общ. ред. Р. С. Белкина. – Москва : НОРМА, 2000. – С. 89.

происшествия, трупа, предметов и документов, животных и их трупов, участков местности и помещений, не являющихся местом происшествия, осмотр жилища, освидетельствование[65].

Одним из ключевых видов осмотра является осмотр места происшествия. Е.П. Ищенко характеризует осмотр места происшествия как неотложное следственное действие, состоящее в непосредственном восприятии, исследовании и фиксации следователем обстановки этого места, относящихся к нему следов и предметов, их взаимосвязей и характерных особенностей в целях выяснения существа произошедшего события, механизма совершения преступления и других обстоятельств, значимых для правильного разрешения уголовного дела судом[66].

Осмотр места происшествия подразделяется на следующие этапы: подготовительный, рабочий и заключительный. Подготовительный этап подразделяется на две стадии. В первую включаются действия следователя до выезда на место происшествия, во вторую – подготовительные действия по прибытии на место осмотра.

В структуру первой стадии входят такие действия как: установление и уточнение поступившей информации; формирование следственной группы; проверка готовности и исправности необходимых технических средств; принятие мер к обеспечению охраны места его совершения и др.

По прибытии на место происшествия следователь, как руководитель данного следственного действия, должен предпринять следующие действия: наметить план и согласовать свои действия с учетом имеющейся обстановки; уточнить границы осмотра, последовательность действий по обнаружению, фиксации и изъятию следов; разъяснить права и обязанности участникам предстоящего следственного действия.

---

[65] Савельева, М.В. Криминалистика: учебник / М. В. Савельева. – Москва: «Дашков и К», 2009. – С. 141.
[66] Ищенко, Е.П. Криминалистика: курс лекций / Е. П. Ищенко. – Москва : АСТ, 2007. – С. 34.

Рабочий этап осмотра места происшествия включает в себя также две стадии: общий осмотр и детальный осмотр. На общей стадии осмотра все объекты осматриваются без прикосновения к ним, без изменения их положения, в неподвижном состоянии. Поэтому эта стадия иногда называется статической. По окончании общего осмотра места происшествия следователь приступает к его детальному осмотру. В ходе детальной стадии осмотра производится тщательное исследование всех объектов и следов, обнаруженных на месте происшествия, в целях обнаружения, закрепления и изъятия следов преступления[67].

Осмотр места происшествия должен вестись методично, по четко определенной системе, чтобы не упустить из виду какие-либо важные узлы и детали.

Выделяют следующие приемы осмотра места происшествия: 1) эксцентрический, когда движение идет по развертывающейся спирали от центра к периферии; 2) концентрический – осмотр ведется по спирали от периферии к центру; 3) фронтальный (линейный), когда следователь двигается по линии от одного края территории или помещения к другому; 4) по секторам (узловой) – следователь разбивает место происшествия на квадраты (сектора) и исследует последовательно каждый сектор.

Заключительный этап осмотра места происшествия включает в себя следующие действия: составление протокола осмотра; упаковку объектов, изъятых с места происшествия; принятие мер к сохранению тех имеющих доказательственное значение объектов, которые невозможно или нецелесообразно изымать с места происшествия и др.

В.В. Коломинов отмечает, что по преступлениям, совершенным посредством социальных сетей, осмотр места происшествия производится с целью выявления: компьютерных следов, а также их объектов-носителей

[67] Зеленский, В.Д. Криминалистика: учебник / В. Д. Зеленский, Г. М. Меретуков ; под. общ. ред. В. Д. Зеленского. – Санкт-Петербург : Юридический центр, 2015 – С. 190.

(например, компьютера или системного блока, диска, дискет, флэшнакопителей и т.п.); традиционных (например, трасологических) следов присутствия конкретного лица на месте происшествия; особенностей доступа, организации, функционирования и устройства различных видов сетей, используя которые было совершено преступление. Необходимо подвергнуть осмотру компьютерно-техническое средство и содержимое хранящихся в нем файлов. Данный осмотр следует осуществлять в рамках детального осмотра программных средств, находящихся на конкретном компьютере. Это затрудняется тем, что следователь без специальных познаний не в состоянии обнаружить файлы с криминалистической информацией[68].

Р.И. Оконенко утверждает, что в ходе подготовки к производству осмотра необходимо получить первичную информацию о системах организации процесса функционирования компьютерно-технических средств, а также установить те, которые могли быть использованы в результате совершения преступлений. Во всех случаях совершения преступлений в сфере компьютерной информации при производстве осмотра места происшествия, необходимо учитывать текущее состояние компьютерно-технических средств и время, прошедшее с момента совершения преступления до момента осмотра. Такое положение обусловлено тем, что в большинстве случаев, с момента совершения преступного деяния до производства следственных действий проходит определенный (как правило, значительный) промежуток времени. В этот период может производиться: неоднократное включение и выключение компьютерно-технического средства; осуществление различных операций, в том числе, идентичных преступным действиям; использование компьютерно-технических средств значительным количеством сотрудников юридического

[68] Коломинов, В.В. Осмотр места происшествия по делам в сфере компьютерной информации / В. В. Коломинов // Сибирские уголовно-процессуальные и криминалистические чтения. – 2017. – № 3. – С. 53.

лица и т.п. Все это ведет к потере как традиционных, так и «компьютерных» следов преступных действий мошенников[69].

Е.Р. Россинская указывает на необходимость исключения намеренной порчи или уничтожения хранящейся в компьютерах информации. Следовательно, на подготовительном этапе осмотра следователю необходимо принять меры по охране компьютерной и иной техники[70].

По данной категории дел может быть произведен осмотр не одного, а сразу нескольких мест происшествия:

а) рабочее место, рабочая станция – место обработки информации, ставшей предметом преступного посягательства;

б) удаленное место управления сетевыми ресурсами, хранения или резервирования информации, в частности, сервер, ставший предметом преступного посягательства или сохранивший свидетельства о нем и о работе системы за определенный период;

в) место использования технических средств для неправомерного доступа к компьютерной информации, создания, использования и распространения вредоносных программ для ЭВМ, непосредственного нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети;

г) место наступления вредных последствий (несанкционированное уничтожение, блокирование, модификация либо копирование компьютерной информации, нарушение работы ЭВМ, системы ЭВМ или их сети), место хранения информации, полученной в результате неправомерного доступа к данным, содержащимся на машинных носителях или в ЭВМ[71].

---

[69] Оконенко, Р.И. Электронные доказательства как новое направление совершенствования российского уголовно-процессуального права / Р. И. Оконенко // Актуальные проблемы российского права. – 2015. – № 4. – С. 54.

[70] Россинская, Е.Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе / Е. Р. Россинская. – Москва : Норма, 2005. – С. 39.

[71] Оконенко, Р.И. Электронные доказательства как новое направление совершенствования российского уголовно-процессуального права / Р. И. Оконенко // Актуальные проблемы российского права. – 2015. – № 4. – С. 55.

Также может производиться осмотр предметов. Так, по уголовному делу, рассмотренному Шумерлинским районным судом Республики Чувашия, была осмотрена информация об исходящих и входящих сообщениях, логах авторизации пользователя, хранящихся на сервере ООО «Вконтакте» (электронный адрес, адрес электронной почты, IP-адрес регистрации, сведения о посещениях и др.), которая в последующем послужила доказательством по уголовному делу[72].

Особое место при расследовании преступлений, совершенных посредством социальных сетей, является осмотр персональной страницы преступника. На это есть ряд причин. Во-первых, социальные сети позволяют быстро получать разнообразную справочно-вспомогательную информацию по расследуемому уголовному делу. Во-вторых, проводя тщательный анализ имеющейся в социальных сетях информации о лице или лицах, имеющих отношение к расследуемому уголовному делу, можно получать данные о них самих, их связях, увлечениях, отношении к чему-либо и подобном, также можно определить их местоположение. Проанализировав список друзей пользователя, можно установить его приблизительный круг общения. Изучив подписки и записи пользователя на странице можно установить его интересы, хобби, отношение к устоявшимся социальным ценностям, мировоззрение и даже некоторые черты характера. Указанные данные могут помочь в составлении социально-психологического портрета пользователя и дальнейшем расследовании преступления. Также немаловажным является тот факт, что при производстве осмотра персональной страницы в социальной сети могут быть выявлены следы иных преступлений. В связи с вышесказанным, можно констатировать, что осмотр страницы преступника в

[72] Приговор Шумерлинского районного суда Республики Чувашия по уголовному делу № 1-63/2014 по обвинению ФИО1 по ч.1 ст. 137 УК РФ. 2014 год [Электронный ресурс] // Справочная система «СудАкт». – Режим доступа: http://sudact.ru/regular/doc/ctgKWVDZPtWW/ (Дата обращения: 24.04.2018).

социальной сети, при расследовании исследуемой категории преступлений, является обязательным действием[73].

3.3 Назначение экспертиз.

При расследовании преступлений рассматриваемой группы может быть назначено проведение целого ряда судебных экспертиз: компьютерно-технических – для исследования средств компьютерной техники, трасологических – для анализа следов взлома, дактилоскопических – исследование следов рук, как на внешних, так и на внутренних поверхностях компьютеров и их комплектующих, лингвистических.

Также могут быть назначены судебно-экономические экспертизы, когда преступления в сфере движения компьютерной информации связаны с преступлениями в кредитно-финансовой сфере. Весьма распространены технико-криминалистические экспертизы документов, когда компьютер используется как средство для изготовления поддельных документов, фальшивых денежных билетов и пр[74].

При наличии на компьютере звуковых и мультимедийных файлов возможно производство судебной фоноскопической экспертизы[75].

Основным видом экспертиз, производимых при расследовании исследуемой категории преступлений, будут являться компьютерно-технические экспертизы. Порядок их проведения регламентирован главой 27 главой УПК РФ, Постановлением Пленума Верховного Суда РФ «О судебной экспертизе по уголовным делам» и другими актами.

---

[73] Коломинов, В.В. Осмотр места происшествия по делам в сфере компьютерной информации / В. В. Коломинов // Сибирские уголовно-процессуальные и криминалистические чтения. – 2017. – № 3. – С. 54.
[74] Белкин, Р. С. Криминалистика: учебник для вузов / Р. С. Белкин, Т. В. Аверьянова ; под. общ. ред. Р. С. Белкина. – Москва : НОРМА, 2000. – С. 90.
[75] Хаитжанов, А.А. Криминалистическая характеристика лиц, совершающих преступления в сфере информации / А. А. Хаитжанов // Труды Международного симпозиума «Надежность и качество». – 2011. – № 1. – С. 3.

Е.Р. Россинская подразделяет судебные компьютерно-технические экспертизы на несколько видов, среди которых выделяет компьютерно-сетевую. Наибольшее значение для расследования преступлений, совершенных посредством социальных сетей, будет иметь именно эта разновидность компьютерно-технической экспертизы.

Судебная компьютерно-сетевая экспертиза, основывается, прежде всего, на функциональном предназначении компьютерных средств, реализующих какую-либо сетевую информационную технологию. Она выделена в отдельный вид в связи с тем, что лишь использование специальных знаний в области сетевых технологий позволяет соединить воедино полученные объекты, сведения о них и эффективно решить поставленные экспертные задачи. Особое место в компьютерно-сетевой экспертизе занимают экспертные исследования, связанные с интернет-технологиями.

Судебная экспертиза этого рода производится для решения следующих задач:

а) определение свойств и характеристик аппаратного средства и программного обеспечения, установление места, роли и функционального предназначения исследуемого объекта в сети (например, для программного средства в отношении к сетевой операционной системе; для аппаратного средства – отношение к серверу, рабочей станции, активного сетевого оборудования и т.д.);

б) выявление свойств и характеристик вычислительной сети, установление ее архитектуры, конфигурации, выявление установленных сетевых компонент, организации доступа к данным;

в) определение соответствия выявленных характеристик типовым для конкретного класса средств сетевой технологии, определение принадлежности средства к серверной или клиентской части приложений;

г) определение фактического состояния и исправности сетевого средства, наличия физических дефектов, состояния системного журнала, компонент управлением доступа;

д) установление первоначального состояния вычислительной сети в целом и каждого сетевого средства в отдельности, возможного места покупки (приобретения), уточнение изменений, внесенных в первоначальную конфигурацию (например, добавление дополнительных сетевых устройств, устройств расширения на сервере либо рабочих станциях и проч.);

е) определение причин изменения свойств вычислительной сети (например, по организации уровней управления доступом), установление факта нарушения режимов эксплуатации сети, фактов (следов) использования внешних («чужих») программ и т.п.;

ж) определение свойств и состояния вычислительной сети по ее отображению в информации носителей данных (например, RAID-массивы; жесткие диски, флоппи-диски, CD-ROM, ZIP-накопители и т.п.);

з) определение структуры механизма и обстоятельства события в сети по его результатам (например, сценария несанкционированного доступа, механизма распространения в сети вредоносных функций и т.д.);

и) установление причинной связи между использованием конкретных аппаратно-программных средств вычислительной сети и результатами их применения.

Как видно, задачи судебной компьютерно-сетевой экспертизы охватывают практически все основные задачи основных родов СКТЭ, т.е. решение аппаратных, программных и информационных аспектов при установлении фактов и обстоятельств дела.

Производство компьютерно-технической экспертизы позволяет получить ответы на крайне важные для расследования преступления вопросы. Наиболее часто встречаемыми в практике вопросами являются следующие.

1. Имеются ли признаки работы данного компьютерного средства в сети Интернет?

2. Какие аппаратные средства использовались для подключения к Интернету?

3. Имеются ли заготовленные соединения с узлом сети Интернет, и каковы их свойства (номера телефонов провайдера, имена и пароли пользователя, даты создания)?

4. Каково содержание установок программы удаленного доступа к сети и протоколов соединений?

5. Какие имеются адреса Интернета, по которым осуществлялся доступ с данного компьютерного средства?

6. Имеется ли какая-либо информация о проведении электронных платежей и использовании кодов кредитных карт?

7. Имеются ли почтовые сообщения, полученные (а также отправленные) по электронной почте?

8. Имеются ли сообщения, полученные (отправленные) посредством использования программ персональной связи через Интернет, и каково их содержание?[76]

Помимо компьютерно-сетевой экспертизы, нередко назначаются также аппаратно-компьютерная экспертиза, программно-компьютерная экспертиза, информационно-компьютерная экспертиза (данных).

Аппаратно-компьютерная экспертиза предназначена для исследования аппаратных компьютерных средств, определения вида, типа, модели, технических показателей, параметров, функционального предназначения и функциональных возможностей конкретного компьютера в сети или системы, первоначального технического состояния и конфигурации аппаратного средства, а также состояния и конфигурации на момент исследования и т.д.

[76] Россинская, Е.Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе / Е. Р. Россинская. – Москва : Норма, 2005. – С. 37.

Программно-компьютерная экспертиза исследует программное обеспечение с целью определения: общей характеристики программного обеспечения и его компонентов, функционального предназначения программы, наименования, типа, версии и вида представления программы, реквизитов разработчика и законного владельца, даты создания, объема программы, аппаратных требований, совместимости программы с программными оболочками и иными программами на конкретном компьютере, работоспособности программы, алгоритма программного средства, программных средств, применяемых при разработке исследуемой программы, вносились ли в исследуемую программу изменения, время, цели, состав изменения, новые свойства, которые приобрела программа после изменений и т.д.

Информационно-компьютерная экспертиза исследует пользовательскую информацию и информацию, созданную программами. В ходе информационно-компьютерной экспертизы определяются: вид записи данных на носителе, физическое и логическое размещение данных, свойства, характеристики, вид и параметры данных на носителе информации, тип данных на носителе, доступность данных, наличие средств защиты, признаков преодоления защиты, состояние данных, их свойства и назначение, данные о пользователе, содержание информации, ее первоначальное состояние, произведенные с данными операции (копирование, модификация, блокирование, стирание и т.д.) и хронология этих операций и т.д.[77]

При расследовании исследуемой категории преступлений может проводиться фоноскопическая экспертиза. Судебная фоноскопическая экспертиза проводится в целях установления личности говорящего по признакам голоса и речи, записанной на фонограмме, выявления признаков стирания, копирования, монтажа и иных изменений, привнесенных в

[77] Россинская, Е.Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе / Е. Р. Россинская. – Москва : Норма, 2005. – С. 37.

фонограмму в процессе или после окончания звукозаписи, определения условий, обстоятельств, средств и материалов звукозаписи, а также иных фактов, имеющих значение судебных доказательств. Согласно приговору Ленинского районного суда г. Новосибирска от 01.11.2013 года при расследовании преступления, предусмотренного ч. 1 ст. 282 УК РФ, была назначена фоноскопическая экспертиза. По результатам ее проведения было установлено и изучено содержание определенных видеофайлов («Зло приближается», «Народное ополчение. Мы собираем силу!»), размещенных на странице пользователя[78].

Следующий вид экспертиз, проводимых при расследовании данной группы преступлений, – лингвистическая экспертиза. Объектами судебных лингвистических экспертиз являются речевые проявления в форме письменного текста или устного высказывания. В качестве примера можно привести заключение лингвистической экспертизы по уголовному делу, рассмотренному Калининским районным судом г. Новосибирска. Согласно заключению лингвистической экспертизы, действия, к которым призывает ФИО1 на своей странице в социальной сети «Вконтакте», содержат языковые признаки унижения, оскорбления отдельных групп лиц по национальному, половому, расовому и социальному признаку, а также призывы к осуществлению террористической деятельности в отношении отдельных групп лиц[79].

При расследовании преступлений, совершенных посредством социальных сетей, также может быть назначена психологическая экспертиза. При производстве психологической судебной экспертизы по уголовному делу, рассмотренному Нижневартовским городским судом, установлено, что

[78] Приговор Ленинского районного суда г. Новосибирска по уголовному делу № 1-811/2013 по обвинению Борщева Д.А. по ч.1 ст. 282 УК РФ. 2013 год [Электронный ресурс] // Справочная система «СудАкт». – Режим доступа: http://sudact.ru/regular/doc/VZ6fYmnuR8Hx/ (Дата обращения: 24.04.2018).

[79] Приговор Калининского районного суда г. Новосибирска по уголовному делу № 1-810/2013 по обвинению ФИО1 по ч. 1 ст. 282 УК РФ. 2013 год [Электронный ресурс] // Справочная система «СудАкт». – Режим доступа: http://sudact.ru/regular/doc/2mUHDFHcGgNk/ (Дата обращения: 24.04.2018).

публичное представление и восприятие видеозаписи, размещенного на странице М.Н. Габбасова будет влиять на общественное сознание и в целом обеспечивать формирование у целевой аудитории готовности к реализации поведения с подчеркиванием готовности отстаивать выбранную поведенческую модель. Видеозапись имеет своей целью влияние на общественное сознание и при условии их представления для публичного восприятия обладают признаком публичности. В видеозаписи используются механизмы психического воздействия[80].

Также при расследовании преступлений, совершенных посредством социальных сетей, назначаются комплексные судебные экспертизы. Так, согласно приговору Калужского областного суда от 16.11.2017 года, при расследовании уголовного дела в отношении И.В. Любшина была произведена комплексная историко-психолого-лингвистическая экспертиза. Согласно заключению, в материалах, размещенных на странице подсудимого во «Вконтакте», имеются высказывания, содержащие негативную оценку автором русских, и мнение об их неполноценности, о положительном отношении и непризнании преступными действий лиц и подчиненных им организаций, осужденных приговором Международного Нюрнбергского военного трибунала. Эксперты указали, что перечисленные материалы имеют цель оказать влияние на точку зрения пользователей социальной сети «Вконтакте» и способны оказывать такое влияние[81].

Назначение такого рода экспертиз особенно часто осуществляется при расследовании преступлений экстремистской направленности.

---

[80] Приговор Нижневартовского городского суда по уголовному делу № 1-1475/2014 по обвинению Габбасова М.Н. по ч.1 ст. 282 УК РФ. 2014 год [Электронный ресурс] // Справочная система «СудАкт». – Режим доступа: http://sudact.ru/regular/doc/CiCPFRhUdFgE/ (Дата обращения: 24.04.2018).

[81] Приговор Калужского областного суда по уголовному делу № 2-14/2017 по обвинению Любшина И.В. по ч. 1 ст. 282 УК РФ. 2017 год [Электронный ресурс] // Справочная система «СудАкт». – Режим доступа: http://sudact.ru/regular/doc/z1JyiOCqwZmJ/ (Дата обращения: 24.04.2018).

3.4 Следственный эксперимент.

В соответствии со ст. 181 УПК РФ следователь в целях проверки и уточнения данных, имеющих значение для уголовного дела, вправе назначить следственный эксперимент – воспроизведение действий, а также обстановки или иных обстоятельств расследуемого события. При этом проверяется возможность восприятия каких-либо фактов, совершения определенных действий, наступления конкретного события; кроме того, выясняются последовательность произошедшего события и механизм образования следов. Иными словами, следственный эксперимент позволяет выяснить реальность или невозможность того или иного действия, события, явления в условиях конкретной следственной ситуации путем производства опытов, экспериментов.

Е.П. Ищенко отмечает, что выяснив нереальность проверенных действий, событий, следователь исключает данные факты из числа действительных. Если же объективная возможность их существования подтверждается, это облегчает доказывание конкретных обстоятельств уголовного дела.

Основным отличием следственного эксперимента от других процессуальных действий является то, что следователь не ограничивается наблюдением и (или) восприятием на слух криминалистически значимой информации с ее последующей фиксацией, а воссоздает необходимые условия расследуемого события и производит опыты, чтобы определить, могло или не могло при данных условиях иметь место конкретное обстоятельство или явление. Таким образом, под следственным экспериментом понимается процессуальное действие, с помощью которого выясняется объективная возможность наличия обстоятельства, существенного для дела, путем воспроизведения условий проверяемого события и производства опытов[82].

[82] Ищенко, Е.П. Криминалистика: курс лекций / Е. П. Ищенко. – Москва : АСТ, 2007. – С. 79.

Целью данного следственного действия может являться, например, проверка возможности входа в социальную сеть и проведение в ней различных действий. Так, приговор Верховного суда Республики Бурятия от 27.11.2016 года гласит, что согласно протоколу следственного эксперимента, в ходе проверки возможности В.А. Оленникова войти на страницу «Вконтакте» в сети Интернет, подозреваемый В.А. Оленников, находясь по адресу места работы в рабочем кабинете, при помощи служебного компьютера, подключенного к сети Интернет, путем введения адреса vk.com в соответствующую строку браузера «Opera» получил доступ к сайту социальной сети «Вконтакте». Далее В.А. Оленников ввел соответствующие данные в строки для логина и пароля сети «Вконтакте», осуществив переход на свою персональную страницу[83].

Необходимость в проведении следственного эксперимента определяется с учетом значимости выясняемого обстоятельства и возможности его проверки опытным путем. Следственный эксперимент должен рассматриваться как метод исследования отдельных обстоятельств расследуемого события, поскольку воспроизведение совокупности объективных и субъективных обстоятельств преступления в целом может привести к его повторению, т.е. является общественно опасным. Необходимые опытные действия в ходе эксперимента (воспроизведение звуков, преодоление преград, заполнение хранилищ и т.п.) производятся лицами, показания которых проверяются, или специально приглашенными для этой цели лицами[84].

Р.С. Белкин предлагает классифицировать эксперименты по видам на основании цели проведения данного действия. С учетом этого все многообразие следственных экспериментов сводится к следующим четырем видам, внутри которых возможна более дробная детализация.

---

[83] Приговор Верховного суда Республики Бурятия по уголовному делу № 1-34/2016 по обвинению Оленникова В.А. по ч.1 ст.241 УК РФ. 2016 год [Электронный ресурс] // Справочная система «СудАкт». – Режим доступа: http://sudact.ru/regular/doc/vgZFRk4dPOdb/ (Дата обращения: 24.04.2018).

[84] Савельева, М.В. Криминалистика: учебник / М. В. Савельева. – Москва: «Дашков и К», 2009. – С. 141.

1. Установление возможности восприятия (видимости, слышимости и т.п.) какого-либо факта при определенных условиях (вообще или конкретным лицом).

2. Возможность совершения определенных действий в данных условиях (вообще или конкретным лицом).

3. Возможность существования какого-либо факта (явления) при определенных обстоятельствах.

4. Установление механизма преступного события в целом или его отдельных этапов[85].

Так, согласно приговору Псковского городского суда от 10.10.2017 года, в ходе расследования преступления был произведен следственный эксперимент. Свидетель при помощи персонального компьютера, имеющего выход в сеть Интернет, осуществила вход в социальную сеть «Вконтакте», далее, путем ввода личного логина и пароля перешла на страницу пользователя под именем «СН», продемонстрировала наличие в социальной сети группы «Барахолка г. Пскова», участником которой свидетель является. После чего свидетель перешла в личные сообщения, среди которых указала на переписку с ФИО1. Согласно продемонстрированной переписке, между свидетелем и ФИО1 достигнута договоренность о приобретении медицинских препаратов. Таким образом, целью проведения вышеуказанного действия было установление механизма преступного события[86].

Для некоторых сложных экспериментов необходимо привлекать специалистов. Специалист поможет следователю разобраться в природе и обстоятельствах проверяемого события, подготовить и провести опыты, всесторонне и точно зафиксировать, и оценить результаты эксперимента. Выбор специалиста (криминалиста, автотехника, программиста и т.д.) зависит от характера проверяемого обстоятельства, а также технических средств,

---

[85] Белкин, Р.С. Криминалистика: учебник для вузов / Р. С. Белкин, Т. В. Аверьянова ; под. общ. ред. Р. С. Белкина. – Москва : НОРМА, 2000. – С. 110.

[86] Приговор Псковского городского суда по уголовному делу № 1-320/2017 по обвинению Филипповой Я.А. по ч. 1 ст. 228.1 УК РФ. 2017 год [Электронный ресурс] // Справочная система «СудАкт». – Режим доступа: http://sudact.ru/regular/doc/jQWewXWhU11/ (Дата обращения: 24.04.2018).

используемых при производстве следственного эксперимента и фиксации его результатов. Участие специалистов обеспечивает полный учет условий изучаемого события, более точное их воспроизведение, детализацию опытов, безопасность участвующих лиц и правильное использование терминологии при составлении протокола эксперимента[87].

[87]Яблоков, Н.П. Криминалистика: учебник / Н. П. Яблоков. – Москва : Юристъ, 2005. – С. 247.

4 Некоторые проблемы выявления и расследования преступлений, совершенных посредством социальных сетей

Большое значение при расследовании преступлений, совершенных посредством социальных сетей, имеет оперативно-розыскная деятельность. 6 июля 2017 года в Федеральный закон «Об оперативно-розыскной деятельности» в ч. 1 ст. 6 была внесена поправка, согласно которой к общему перечню оперативно-розыскных мероприятий было добавлено «Получение компьютерной информации»[88].

Следует отметить, что до момента официального закрепления в федеральном законе «Об оперативно-розыскной деятельности в РФ» получения компьютерной информации, оно фактически осуществлялось в рамках снятия информации с технических каналов связи. В то же время особенности развития компьютерных технологий, совершенствование их технических возможностей не только в сфере связи, но и в других областях человеческой деятельности, выявили потребность в правовой регламентации особенностей получения компьютерной информации отдельным специализированным ОРМ[89].

В контексте проводимого исследования необходимо ответить на ряд вопросов, касающихся данного нововведения, а именно: уяснить суть понятия «компьютерная информация», понять, где она находится и каким образом получается.

Получение компьютерной информации – это оперативно-техническое мероприятие, направленное на сбор сведений, циркулирующих в компьютере или сети компьютеров, а также содержащиеся на различных носителях машинной информации с последующей их фиксацией (или без неё) для

[88] 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 : федер. закон от 6.07.2016 г. № 374-ФЗ // Российская газета. – 2016. – 8 июля.

[89] Халиков, А.Н. Оперативно-розыскная деятельность: учебник / А. Н. Халиков. – Москва: ИНФРА-М, 2017. – С. 205.

решения оперативно-розыскных задач. Целью данного ОРМ является получение оперативных данных о подготовке, совершении преступлений проверяемыми лицами, установлении их криминальных связей, а также мест хранения компьютерной информации, могущей иметь доказательственное значение. При достижении указанной цели оперативными сотрудниками учитываются следующие особенности компьютерной информации: 1) возможность преобразование её из одной формы в другую и копирование на различных видах машинных носителей; 2) передачи её по сетям Интернет; 3) доступа к ней нескольких пользователей (в т.ч. несанкционированного доступа); 4) быстрое её уничтожение[90].

Статья 2 ФЗ «Об информации, информационных технологиях и защите информации» определяет информацию, как сведения (сообщения, данные) независимо от формы их представления[91]. Согласно ст. 1 Соглашения участников СНГ в борьбе с преступлениями в сфере компьютерной информации под таковой понимается информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи[92].

По мнению А.Е.Осипенко, под компьютерной информацией следует понимать не какой-то особый вид информации, а специфическую форму ее представления, приспособленную для обработки в компьютерных устройствах, передачи по каналам связи и хранения на специализированных носителях[93].

Данная позиция представляется верной, поскольку сами электрические сигналы в отличие от сведений, которые они содержат, не несут юридически

---

[90] Дубоносов, Е.С. Оперативно-розыскное мероприятие «получение компьютерной информации»: содержание и проблемы проведения. / Е. С. Дубоносов // Известия Тульского государственного университета. – 2017. – № 3. – С. 39.

[91] Об информации, информационных технологиях и о защите информации : федер. закон от 27.07.2006 г. № 149-ФЗ // Российская газета. – 2006. – 29 июля.

[92] О ратификации Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации : федер. закон от 1.10.2008 г. № 164-ФЗ // Российская газета. – 2008. – 3 окт.

[93] Осипенко, А.Л. Новое оперативно-розыскное мероприятие «получение компьютерной информации»: содержание и основы осуществления / А. Л. Осипенко // Вестник Воронежского института МВД России. – 2016. – № 2. – С. 86.

значимой информации. Таким образом, можно согласиться с определением, компьютерной информации, данным в примечании 1 статьи 272 УК РФ. Итак, под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Стоит отметить, что в литературе нет единства взглядов относительно информации, получаемой из компьютерных и иных средств. Так О.В. Овчинникова говорит о «электронной информации»[94], а В.В. Трухачев, В.Н. Чернышов, В.С. Лоскутова употребляют термин «цифровая информация»[95]. Однако, не смотря на имеющиеся различия в употребляемых понятиях, суть их, по большому счету, одинакова и термин «компьютерная информация» вполне подходит для использования.

Е.С. Дубоносов также пишет, что техническими объектами при проведении ОРМ являются: а) средства вычислительной техники, мобильные устройства, обеспечивающие доступ к сетевым ресурсам, носители компьютерной информации, устройства, фиксирующие компьютерные данные, сетевое оборудование; б) информационные объекты сети Интернет (например, сайты криминальных структур); в) места сетевого общения криминальных структур в социальных сетях. г) сетевые каналы коммуникации (электронная почта, мессенджеры и др.); д) базы данных, формирующихся в информационных системах государственных и коммерческих структур.

Содержательная часть получения компьютерной информации является весьма сложным в техническом плане действием по добыванию хранящейся в компьютерных сетях сведений о лицах и событиях, вызывающих оперативный интерес. В связи с этим для правильного его проведения привлекается специалист. В соответствии с ч. 4 ст. 6 Закона «Об ОРД», данное ОРМ проводится с использованием оперативно-технических сил и средств органов

---

[94] Овчинникова, О.В. Собирание электронных доказательств, размещенных в сети Интернет / О. В. Овчинникова // Правопорядок: история, теория, практика. – 2016. – № 3. – С. 45.

[95] Чернышов, В.Н. Проблемы собирания и использования цифровых доказательств / В. Н. Чернышов // Социально-экономические явления и процессы. – 2017. – № 5. – С. 82.

ФСБ, ОВД в порядке, определенном межведомственными нормативными актами или соглашениями[96].

Криминалистически важная информация содержится в памяти электронных устройств: компьютеров, ноутбуков, планшетов, телефонов и прочих устройств. Например, на жестких дисках персональных компьютеров содержатся так называемые «файлы регистрации» или «log-файлы». Они позволяют просматривать практически все активности пользователя устройства, в т.ч. время и даты подключения к сети Интернет, просматриваемые сайты. Данные файлы могут быть изъяты либо на месте производства следственных действий и иных действий, либо могут быть переданы на экспертизу.

Е.С. Дубоносов также затрагивает следующую крайне важную проблему. Осуществление ОРМ «получение компьютерной информации» неразрывно связано с проблемой ограничения охраняемых конституционных прав граждан. В связи с этим целесообразно внести дополнения в действующие законы и ведомственные подзаконные нормативные правовые акты относительно процедуры изъятия компьютерной информации. Так, на наш взгляд, для более полного соблюдения прав граждан в п. 9.1 ст. 182 УПК РФ можно было бы внести положение о том, что понятые, присутствующие при производстве различных действий с электронными устройствами, должны быть достаточно квалифицированы. То есть они должны знать функционал исследуемой техники, уметь владеть ею как минимум на уровне обычного пользователя.

Так как данное ОРМ предусматривает ограничение конституционных прав граждан, а также, как гласный, так и негласный сбор, хранение, использование и распространение информации о частной жизни лица, оно проводится по судебному разрешению. Процедура получения разрешения на проведение данного ОРМ аналогична получению разрешения на проведение

[96] Дубоносов, Е.С. Оперативно-розыскное мероприятие «получение компьютерной информации»: содержание и проблемы проведения. / Е. С. Дубоносов // Известия Тульского государственного университета. – 2017. – № 3. – С. 39.

иных ОРМ, ограничивающих конституционные права граждан. Изначально выносится мотивированное постановление руководителя органа, осуществляющего оперативно-розыскную деятельность, далее оно рассматривается судом и по итогам выносится решение о разрешении проведения данного ОРМ либо отказ в его проведении. Дальнейшее взаимодействие правоохранительных органов со структурами, формирующими массивы данных, должно базироваться на принципе соблюдения и уважения прав и свобод человека и гражданина. Представляется, что указанные структуры должны беспрепятственно предоставлять необходимую информацию при наличии судебного решения. В противном же случае речи о взаимодействии быть не может[97].

Важным является вопрос взаимодействия администрации социальных сетей и правоохранительных органов. Согласно статье 10.1 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149–ФЗ, 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[98]. Поэтому можно сделать вывод, что ООО «В Контакте» является организатором распространения информации, поскольку обеспечивает функционирование сайта «vk.com». Указанный сайт является программой для ЭВМ и его функционал позволяет принимать, передавать, доставлять и обрабатывать электронные сообщения пользователей. К тому же, сайт «vk.com» внесен в реестр организаторов распространения информации. Порядок ведения данного реестра

[97] Фойгель, Е.И. К вопросу о проблемах практической реализации нового оперативно-розыскного мероприятия «получение компьютерной информации» при раскрытии преступлений в сфере компьютерной информации / Е. И. Фойгель // Сибирские уголовно-процессуальные и криминалистические чтения. – 2016. – № 1. – С. 73.

[98] Об информации, информационных технологиях и о защите информации : федер. закон от 27.07.2006 г. № 149-ФЗ // Российская газета. – 2006. – 29 июля.

устанавливается Приказом Роскомнадзора от 22.12.2014 года № 188 «Об утверждении Порядка ведения реестра организаторов распространения информации в сети «Интернет». Факт того, что социальная сеть подпадает под определение организатора распространения информации, а также факт внесения социальной сети «Вконтакте» в реестр, накладывает на владельцев данного ресурса определенные обязательства, указанные также в статье 10.1 вышеназванного закона. Например, такие, как:

1) в установленном Правительством Российской Федерации порядке уведомить федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о начале осуществления деятельности;

2) хранить на территории Российской Федерации 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;

3) предоставлять указанную информацию уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, в случаях, установленных федеральными законами;

4) обеспечивать реализацию требований к оборудованию и программно-техническим средствам, в эксплуатируемых им информационных системах, для проведения правоохранительными органами мероприятий в целях реализации возложенных на них задач, а также принимать меры по недопущению раскрытия организационных и тактических приемов проведения данных мероприятий.

С 1 июля 2018 года вступает в силу важное нормативное положение, согласно которому организаторы связи будут обязаны хранить также и 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[99].

Пункт 4 ст. 10.1 ФЗ № 149 гласит, что порядок взаимодействия организаторов связи (ОРИ) с правоохранительными органами устанавливается Правительством Российской Федерации. Действительно, в данной сфере действует Постановление Правительства РФ от 31.07.2014 года № 743, утверждающее правила взаимодействия ОРИ с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации. Данным актом регулируются некоторые организационные и технические моменты взаимодействия сторон (использование оборудования и программно-технических средств, определение подразделения уполномоченных органов для взаимодействия с ОРИ и т.д.)[100].

Также ОРИ взаимодействуют с Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций. Должностные лица Роскомнадзора вправе направлять организаторам распространения информации запрос, касающийся сведений о сайтах или страницах сайтов в сети Интернет, о посещаемости сайтов и страниц сайтов в сети Интернет, функционирование которых обеспечивается организатором распространения информации, а ОРИ обязаны, в свою очередь, предоставить запрашиваемую информацию[101].

---

[99] Об информации, информационных технологиях и о защите информации : федер. закон от 27.07.2006 г. № 149-ФЗ // Российская газета. – 2006. – 29 июля.

[100] Об утверждении Правил взаимодействия организаторов распространения информации в информационно-телекоммуникационной сети "Интернет" с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации : Постановление Правительства РФ от 31.07.2014 г. № 743 // Российская газета. – 2014. – 11 авг.

[101] О порядке взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с организатором распространения информации в информационно-телекоммуникационной сети "Интернет" : Постановление Правтительства РФ от 31.07.2014 г. № 745 // Российская газета. – 2014. – 10 авг.

Пункт 3 Постановления Правительства Российской Федерации от 31.07.2014 г. № 759 содержит перечень информации, которую ОРИ обязаны хранить и предоставлять уполномоченным органам. Пункт 4 данного постановления гласит, что информация, указанная в пункте 3, не включает содержание электронных сообщений пользователей, направляемых или получаемых ими в рамках обмена данными с иными пользователями в сети «Интернет». Однако обязанность хранения электронных сообщений предусмотрена ст. 10.1 Федерального закона «Об информации». Соответственно возникает коллизия нормативных актов, которую необходимо разрешить, для правильного применения данных актов и предотвращения нарушения прав граждан. Данную коллизию можно решить, используя положения общей теории права. Так, Федеральный закон является нормативным актом, обладающим большей юридической силой, нежели Постановление Правительства, следовательно, применению в данном случае подлежат нормы Федерального закона. Таким образом, ОРИ обязаны хранить и предоставлять содержание всех электронных сообщений пользователей[102].

В этом контексте крайне интересной выглядит позиция заместителя руководителя Роскомнадзора Олега Иванова. В интервью «Российской газете» датированном 6 июля 2017 года он заявил: «Это неправда – содержание переписки закон об организаторах распространения информации ни хранить, ни передавать не требует. С какого сетевого адреса фигурант расследования выходил в Интернет, какие сайты посещал, с кем переписывался, кому звонил в мессенджере, в какое время и так далее. Само содержание переписки пользователей закон об организаторах распространения информации ни хранить, ни передавать не требует»[103]. Данная позиция представляется не обоснованной, поскольку с момента внесения поправок в п. 3 ст. 10.1 Федерального закона «Об информации» до момента этого заявления прошел

[102] Матузов, Н.И Теория государства и права: учебник / Н. И. Матузов. – Москва : Юристъ, 2004. – С. 142.
[103] Шадрина, Т.М. Кто следующий? Российские госмессенджеры тоже попадут в реестр / Т. М. Шадрина // Бизнес в законе. – 2017. – № 7314. – С. 148.

уже год (поправки были внесены Федеральным законом № 374-ФЗ от 06.07.2016).

Практически идентичный механизм взаимодействия существует между операторами связи и правоохранительными органами. На операторов связи, которые предоставляют услуги по пользованию сетью Интернет, также возложены обязанности по хранению и предоставлению информации[104].

Исходя из сказанного ранее, можно сделать следующий вывод: взаимодействие ОРИ с уполномоченными органами власти происходит в запросно-ответной форме. ОРИ обязаны хранить и по требованию предоставлять правоохранительным органам всю криминалистически значимую информацию о пользователях и их действиях в сети.

[104] О связи : федер. закон от 07.07.2003 г. № 126-ФЗ // Российская газета. – 2003. – 10 июля.

Заключение

По результатам проведенного исследования можно сделать следующие выводы.

Проведен анализ криминалистической характеристики преступлений, совершенных посредством социальных сетей. Было выяснено понятие «социальная сеть», а также ее функционал, изучены основные группы преступлений, совершаемых с использованием социальной сети. Приведена характеристика личности преступника и потерпевшего, указаны основные способы совершения преступлений. Подробно изучены следы преступлений исследуемой группы. Освящен вопрос необходимости выделения дополнительной категории следов – «виртуальные следы» и внесены предложения по ее наименованию, изучены различные точки зрения ученых на этот счет. Таким образом, было предложено выделить разновидность «информационных следов» под которыми следует понимать следы, хранящиеся в памяти электронных устройств в виде двоичного кода и содержащие криминалистически значимую информацию о совершенном преступлении. Также были изучены особенности такого элемента криминалистической характеристики преступления, как обстановка его совершения.

Проведен анализ типичных следственных ситуаций и направлений расследования преступлений, совершаемых посредством социальных сетей. Так, были выделены и охарактеризованы классификации типичных следственных ситуаций и описаны направления расследования.

Проведен анализ следственных и иных действий, производимых при расследовании указанных преступлений. Были изучены такие следственные действия, как обыск и выемка, осмотр, следственный эксперимент. Изучены вопросы назначения судебной компьютерно-технической и иных экспертиз.

Изучены некоторые проблемные вопросы выявления и расследования исследуемых преступлений. Охарактеризовано новое оперативно-розыскное

мероприятие «получение компьютерной информации» (применительно к тематике исследования), выяснен механизм взаимодействия правоохранительных органов и социальных сетей (взаимодействие между данными субъектами происходит в запросно-ответной форме).

В заключение следует отметить, что настал цифровой век криминалистки, который настоятельно требует не только переосмысления активно использующихся «традиционных» уголовно-процессуальных и криминалистических категорий, но и скорейшей разработки новых, отражающих сущность и особенности использования информационных технологий в расследовании преступлений.

Список использованных источников

I. Нормативно-правовые акты:

1) Гражданский кодекс Российской Федерации: федер. закон от 26.01.1996 г. № 14-ФЗ // Собрание законодательства РФ. – 5.12.1994. – № 32. – Ст. 3301.

2) Уголовно-процессуальный кодекс Российской Федерации : федер. закон от 18.12.2001 г. № 174-ФЗ // Российская газета. – 2001. – 23 янв.

3) Уголовный кодекс Российской Федерации : федер. закон от 13.06.1996 г. № 63-ФЗ // Российская газета. – 1996. – 18 июня.

4) О ратификации Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации : федер. закон от 1.10.2008 г. № 164-ФЗ // Российская газета. – 2008. – 3 окт.

5) Об информации, информационных технологиях и о защите информации : федер. закон от 27.07.2006 г. № 149-ФЗ // Российская газета. – 2006. – 29 июля.

6) 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 : федер. закон от 6.07.2016 г. № 374-ФЗ // Российская газета. – 2016. – 8 июля.

7) О связи : федер. закон от 07.07.2003 г. № 126-ФЗ // Российская газета. – 2003. – 10 июля.

8) Об утверждении Правил взаимодействия организаторов распространения информации в информационно-телекоммуникационной сети "Интернет" с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации : Постановление Правительства РФ от 31.07.2014 г. № 743 // Российская газета. – 2014. – 11 авг.

9) О внесении изменений в некоторые акты Правительства Российской Федерации в связи с принятием Федерального закона «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей» : Постановление Правительства РФ от 31.07.2014 г. № 758 // Российская газета. – 2014. – 5 авг.

10) О порядке взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с организатором распространения информации в информационно-телекоммуникационной сети "Интернет" : Постановление Правительства РФ от 31.07.2014 г. № 745 // Российская газета. – 2014. – 10 авг.

II. Специальная литература:

11) Абрамова, А. А. Значение виртуальных следов в расследовании финансирования терроризма / А. А. Абрамова // общество: политика, экономика, право. – 2017. – № 12. – С. 23-28.

12) Агибалов, В. Ю. Виртуальные следы в криминалистике и уголовном процессе / В. Ю. Агибалов // Общество: политика, экономика, право. – 2012. – № 5. – С. 34-37.

13) Ахмедшин, Р. Л. Криминалистическая характеристика личности преступника: природа и содержание / Р. Л. Ахмедшин // Вестник Томского государственного университета. – 2014. – № 7. – С. 21-26.

14) Балашов, Д. Н. Криминалистика: учебник / Д. Н. Балашов. – Москва : ИНФРА-М, 2005. – 630 с.

15) Баринов, С. В. Использование специальных знаний в расследовании преступных нарушений неприкосновенности частной жизни / С. В. Баринов // Вестник Удмуртского университета. – 2015. – № 6. – С. 37-42.

16) Белкин, Р. С. Криминалистика: учебник для вузов / Р. С. Белкин, Т. В. Аверьянова ; под. общ. ред. Р. С. Белкина. – Москва : НОРМА, 2000. – 780 с.

17) Борисов, В. В. Об особенностях фиксации информационных следов в практике защиты информации / В. В. Борисов // Известия Южного федерального университета. – 2009. – № 7. – С. 102-105.

18) Введенская, О. Ю. Особенности следообразования при совершении преступлений посредством сети интернет / О. Ю. Введенская // Юридическая наука и правоохранительная практика. – 2015. – № 3. – С. 101-105.

19) Волеводз, А. Г. Следы преступлений, совершенных в компьютерных сетях / А. Г. Волеводз // Российский следователь. – 2015. – № 3. – С. 46-48.

20) Грошев, А. С. Информатика: учебник для вузов / А. С. Грошев. – Архангельск: Архангельский государственный технический университет, 2010. – 330 с.

21) Губанов, Д. А. Концептуальный подход к анализу онлайновых социальных сетей / Д. А. Губанов // Управление большими системами: сборник трудов. – 2013. – № 5. – С. 330-336.

22) Гузин, А. Р. Проблемы регламентации собирания электронной информации в действующем законодательстве / А. Р. Гузин // Juvenis scentia. – 2017. – № 7. – С. 45-49.

23) Давыдов, В. О. Значение виртуальных следов в расследовании преступлений экстремистского характера / В. О. Давыдов // Известия Тульского государственного университета. Экономические и юридические науки. – 2016. – № 3. – С. 254–259.

24) Дубоносов, Е. С. Оперативно-розыскное мероприятие «получение компьютерной информации»: содержание и проблемы проведения / Е. С. Дубоносов // Известия Тульского государственного университета. – 2017. - № 3. – С. 34-41.

25) Дьяков, В. В. О личности преступника, как компоненте системы криминалистической характеристики преступлений в сфере компьютерной информации / В. В. Дьяков // Бизнес в законе. – 2008. – № 6. – С. 129-132.

26) Зеленский, В. Д. Криминалистика: учебник / В. Д. Зеленский, Г. М. Меретуков ; под. общ. ред. В. Д. Зеленского. – Санкт-Петербург : Юридический центр, 2015. – 760 с.

27) Ишин, А. М. Современные проблемы использования сети Интернет в расследовании преступлений / А. М. Ишин // Вестник Балтийского федерального университета. – 2013. – № 8. – С. 56- 61.

28) Ищенко, Е. П. Криминалистика: курс лекций. / Е. П. Ищенко. – Москва : АСТ, 2007. – 451 с.

29) Князьков, А. С. Криминалистическая характеристика преступления в контексте его способа и механизма / А. С. Князьков // Вестник Томского государственного университета. – 2011. – № 7. – С. 52-58.

30) Колмаков, А. В. Значение способа совершения преступления для квалификации преступлений / А. В. Колмаков // Пробелы в российском законодательстве. – 2009. – № 11. – С. 45-49.

31) Коломинов, В. В. Осмотр места происшествия по делам в сфере компьютерной информации / В. В. Коломинов // Сибирские уголовно-процессуальные и криминалистические чтения. – 2017. – № 3. – С. 53-55.

32) Короткий, С. А. Соотношение аудио и видеозаписей с письменными доказательствами в гражданском процессе / С. А. Короткий // Научные ведомости Белгородского государственного университета. – 2009. – № 1. – С. 132-137.

33) Матузов, Н. И Теория государства и права: учебник / Н. И. Матузов. – Москва : Юристъ, 2004. – 718 с.

34) Мещеряков, В. А. «Виртуальные следы» под «Скальпелем Оккама» / В. А. Мещеряков // Информационная безопасность регионов. – 2009. – № 1. – С. 28-29.

35) Мещеряков, В. А. Преступления в сфере компьютерной информации: основы теории и практики расследования / В. А. Мещеряков // Издательство Воронежского государственного университета. – 2002. – № 3. – С. 94-119.

36) Морозова, А. Н. Проблемы привлечения к уголовной ответственности за экстремизм в информационной сети Интернет / А. Н. Морозова // Российский следователь. – 2014. – №5. – С. 39-41.

37) Овчинникова, О. В. Собирание электронных доказательств, размещенных в сети Интернет / О. В. Овчинникова // Правопорядок: история, теория, практика. – 2016. – № 3. – С. 45-48.

38) Оконенко, Р. И. Электронные доказательства как новое направление совершенствования российского уголовно-процессуального права / Р. И. Оконенко // Актуальные проблемы российского права. – 2015. – № 4. – С. 54-56.

39) Осипенко, А. Л. Новое оперативно-розыскное мероприятие «получение компьютерной информации»: содержание и основы осуществления / А. Л. Осипенко // Вестник Воронежского института МВД России. – 2016. – № 2. – С. 84-90.

40) Поляков, В. В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики / В. В. Поляков // Известия Алтайского государственного университета. – 2013. – № 2. – С. 114-116.

41) Прохоров, М. С. Криминалистическая характеристика преступлений / М. С. Прохоров // Известия Российского государственного педагогического университета. – 2008. – № 3. – С. 353-355.

42) Россинская, Е. Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе / Е. Р. Россинская. – Москва: Норма, 2005. – 365 с.

43) Савельева, М. В. Криминалистика: учебник / М. В. Савельева. – Москва: «Дашков и К», 2009. – 525 с.

44) Салтевский, М. В. Новый подход в технологии собирания и исследования информационных следов / М. В. Салтевский // Пробелы в российском законодательстве. – 2008. – № 5. – С. 23-28.

45) Троегубов, Ю. Н. Проблемы противодействия экстремизму в сети Интернет / Ю. Н. Троегубов // Гуманитарный вектор. Серия: История, политология. – 2014. – № 3. – С. 143-151.

46) Фойгель, Е. И. К вопросу о проблемах практической реализации нового оперативно-розыскного мероприятия «получение компьютерной информации» при раскрытии преступлений в сфере компьютерной информации / Е. И. Фойгель // Сибирские уголовно-процессуальные и криминалистические чтения. – 2016. – № 1. – С. 73-77.

47) Хаитжанов, А. А. Криминалистическая характеристика лиц, совершающих преступления в сфере информации / А. А. Хаитжанов // Труды Международного симпозиума «Надежность и качество». – 2011. – № 1. – С. 1-5.

48) Халиков, А. Н. Оперативно-розыскная деятельность: учебник / А. Н. Халиков. – Москва: ИНФРА-М, 2017. – С. 205.

49) Цимбал, Н. Г. Использование информации социальных сетей Интернет в ходе предварительного расследования / Н. Г. Цимбал // Теория и практика общественного развития. – 2013. – № 4. – С. 425-426.

50) Чернышов, В. Н. Проблемы собирания и использования цифровых доказательств / В. Н. Чернышов // Социально-экономические явления и процессы. – 2017. – № 5. – С. 82-86.

51) Шадрина, Т. М. Кто следующий? Российские госмессенджеры тоже попадут в реестр / Т. М. Шадрина // Бизнес в законе. – 2017. – № 7314. – С. 148.

52) Яблоков, Н. П. Криминалистика: учебник / Н. П. Яблоков. – Москва: Юристъ, 2005. – 779 с.

III. Электронные источники:

53) Правила пользования сайтом Вконтакте [Электронный ресурс] – Режим доступа: https://vk.com/terms

IV. Судебная практика:

54) Определение Алтайского краевого суда по гражданскому делу № 33-3897/2013 о возмещении морального вреда. 2013 год [Электронный ресурс] // Справочная система «РосПравосудие». – Режим доступа: https://rospravosudie.com/court-altajskij-kraevoj-sud-altajskij-kraj-s/act-490754873/ (Дата обращения: 24.04.2018).

55) Определение Санкт-Петербургского городского суда по гражданскому делу № 33-4484/2013. 2013 год [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=SARB&n=46138#09433362545822297 (Дата обращения: 24.04.2018).

56) Приговор Верховного суда Республики Бурятия по уголовному делу № 1-34/2016 по обвинению Оленникова В.А. по ч. 1 ст. 241 УК РФ. 2016 год [Электронный ресурс] // Справочная система «СудАкт». – Режим доступа: http://sudact.ru/regular/doc/vgZFRk4dPOdb/ (Дата обращения: 24.04.2018).

57) Приговор Верховного суда Республики Удмуртия по уголовному делу № 2-19/2017 по обвинению Шустова А.А. по ч. 4, ч.5 ст. 228.1 УК РФ. 2017 год [Электронный ресурс] // Справочная система «СудАкт». – Режим доступа: http://sudact.ru/regular/doc/0xTf7PWMulNG/ (Дата обращения: 24.04.2018).

58) Приговор Вологодского областного суда по уголовному делу № 1-914/2016 обвинению Анферьева И.М. по ч. 1 ст. 137 УК РФ. 2016 год [Электронный ресурс] // Справочная система «СудАкт». Режим доступа: http://sudact.ru/regular/doc/hwzIJ69MfXmR/ (Дата обращения: 24.04.2018).

59) Приговор Гагаринского районного суда г. Севастополя по уголовному делу № 1-183/2016 по обвинению ФИО1 по ч. 1 ст. 137 УК РФ.

2016 год [Электронный ресурс] // Справочная система «СудАкт». – Режим доступа: http://sudact.ru/regular/doc/1N5srs50gto9/ (Дата обращения: 24.04.2018).

60) Приговор Калининского районного суда г. Новосибирска по уголовному делу № 1-810/2013 по обвинению ФИО1 по ч. 1 ст. 282 УК РФ. 2013 год [Электронный ресурс] // Справочная система «СудАкт». – Режим доступа: http://sudact.ru/regular/doc/2mUHDFHcGgNk/ (Дата обращения: 24.04.2018).

61) Приговор Калужского областного суда по уголовному делу № 2-14/2017 по обвинению Любшина И.В. по ч. 1 ст. 282 УК РФ. 2017 год [Электронный ресурс] // Справочная система «СудАкт». – Режим доступа: http://sudact.ru/regular/doc/z1JyiOCqwZmJ/ (Дата обращения: 24.04.2018).

62) Приговор Кировского районного суда г. Красноярска по уголовному делу № 1-570/2012 по обвинению Агаева Р.М. по ч. 1 ст. 205.2 УК РФ. 2012 год [Электронный ресурс] // Справочная система «СудАкт». – Режим доступа: http://sudact.ru/regular/doc/Xwtcb1oLGI/ (Дата обращения: 24.04.2018).

63) Приговор Ленинского районного суда г. Новосибирска по уголовному делу № 1-811/2013 по обвинению Борщева Д.А. по ч. 1 ст. 282 УК РФ. 2013 год [Электронный ресурс] // Справочная система «СудАкт». – Режим доступа: http://sudact.ru/regular/doc/VZ6fYmnuR8Hx/ (Дата обращения: 24.04.2018).

64) Приговор Лямбирского районного суда Республики Мордовия по уголовному делу № 1-330/2016 по обвинению Кипенского К.О. по ч. 1 ст. 241 УК РФ. 2016 год [Электронный ресурс] // Справочная система «СудАкт». – Режим доступа: http://sudact.ru/regular/doc/vgZFRk4dPOdb/ (Дата обращения: 24.04.2018).

65) Приговор Лямбирского районного суда Республики Мордовия по уголовному делу № 1-67/2017 по обвинению Галабира С.В. по ч. 2 ст. 273 УК РФ. 2017 год [Электронный ресурс] // Справочная система «СудАкт». – Режим

доступа: http://sudact.ru/regular/doc/cCtVyfZHr9Hm/ (Дата обращения: 24.04.2018).

66) Приговор Нижневартовского городского суда по уголовному делу № 1-1475/2014 по обвинению Габбасова М.Н. по ч. 1 ст. 282 УК РФ. 2014 год [Электронный ресурс] // Справочная система «СудАкт». – Режим доступа: http://sudact.ru/regular/doc/CiCPFRhUdFgE/ (Дата обращения: 24.04.2018).

67) Приговор Октябрьского районного суда г. Рязани по уголовному делу № 1-229/2017 по обвинению Кротова В.А. по ч. 2 ст. 210 УК РФ. 2017 год [Электронный ресурс] // Справочная система «СудАкт». – Режим доступа: http://sudact.ru/regular/doc/STfEbGVF4GU9/ (Дата обращения: 24.04.2018).

68) Приговор Октябрьского районного суда г. Рязани по уголовному делу № 1-229/2017 по обвинению Кротова В.А. по ч. 2 ст. 210, ч. 4 ст. 228.1 УК РФ. 2017 год [Электронный ресурс] // Справочная система «СудАкт». – Режим доступа: http://sudact.ru/regular/doc/STfEbGVF4GU9/ (Дата обращения: 24.04.2018).

69) Приговор Хасавюртского городского суда по уголовному делу № 1-96/2015 по обвинению Асакаева Р.А. по ч. 2 ст. 128.1 УК РФ. 2015 год [Электронный ресурс] // Справочная система «СудАкт». – Режим доступа: http://sudact.ru/regular/doc/KWaHTTfQfcLw/ (Дата обращения: 24.04.2018).

70) Приговор Шумерлинского районного суда Республики Чувашия по уголовному делу № 1-63/2014 по обвинению ФИО1 по ч. 1 ст. 137 УК РФ. 2014 год [Электронный ресурс] // Справочная система «СудАкт». – Режим доступа: http://sudact.ru/regular/doc/ctgKWVDZPtWW/ (Дата обращения: 24.04.2018).

Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Юридический институт
Кафедра уголовного процесса и криминалистики

УТВЕРЖДАЮ
Заведующий кафедрой
_____ А.Д. Назаров
подпись
« 01 » 06 2018г.

БАКАЛАВРСКАЯ РАБОТА

40.03.01-Юриспруденция
код-наименование направления

Расследование преступлений, совершенных посредством социальных сетей

Научный руководитель 01.06.18 доц. каф, к.ю.н. И.Г. Иванова
подпись, дата

Выпускник 01.06.18 М.И. Гуров
подпись, дата

Красноярск 2018