ФГАОУ ВО «Балтийский федеральный университет
имени Иммануила Канта»

На правах рукописи

Болвачев Михаил Александрович

ИСПОЛЬЗОВАНИЕ СОЦИАЛЬНЫХ СЕТЕЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ

Специальность 12.00.12 –
криминалистика; судебно-экспертная деятельность;
оперативно-розыскная деятельность

Диссертация
на соискание ученой степени кандидата юридических наук

Научный руководитель:
доктор юридических наук, профессор,
Заслуженный работник высшей школы РФ
Волчецкая Татьяна Станиславовна

Калининград
2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы диссертационного исследования.

Компьютерные и мобильные устройства в настоящее время стали неотъемлемой частью общества, начиная от бытовой деятельности до систем военного, жизнеобеспечивающего или крупного производственного назначения. Их повсеместное использование не только способствует упрощению и ускорению тех процессов, в которых они применяются, но и открывает новые возможности как для преступника, так и для расследования преступлений. Особое место в информатизации общества занимает глобальная сеть Интернет. Высочайшие темпы развития глобальной сети, ее повсеместное использование от личного общения и творчества до бизнеса и сферы государственных услуг позволяет выделить новое, виртуальное пространство взаимодействия людей. По данным Miniwatts Marketing Group[1] количество интернет-пользователей в Российской Федерации на 31 декабря 2021 года составляет 116,3 миллиона человек, при увеличении аудитории за 20 лет более чем на 3700%.

Способность компьютерных данных к свободному копированию приводит к невероятной скорости и масштабам перемещения информации в киберпространстве, благодаря чему, использование сети Интернет становится опаснее использования «традиционных» методов совершения преступлений.

Децентрализованный характер и отсутствие контроля за пространством сети Интернет предоставляет новые возможности для преступной деятельности, вследствие чего происходит активное использование сети Интернет в преступных целях. Кроме того, преступная

[1] Top 20 countries with the highest number of internet users [Электронный ресурс] – Режим доступа: http://www.internetworldstats.com/top20.htm – Загл. с экрана. (дата обращения: 20.05.2022)

деятельность не ограничивается исключительно «компьютерными преступлениями», перечисленными в главе 28 УК РФ, использование сети Интернет возможно и при совершении более «традиционных» преступлений, таких как мошенничество, клевета, оборот порнографических материалов, склонение к употреблению наркотических веществ, вымогательство и т.п.

Необходимо отметить факт заметной переориентации на использование Интернет-технологий при совершении различных преступлений организованных преступных формирований не только транснационального, но и регионального характера, что позволяет говорить о формировании криминального Интернет-сообщества, а также увеличения его влияния на каждый из информационных процессов как в пространстве сети Интернет, так и в реальном мире.

Развитие Интернет-технологий и социальных сетей, в частности, открывают перед экстремистами новые возможности по осуществлению пропаганды ксенофобских идей, вербовки в свои ряды или осуществления координации действий. Идеи ненависти наиболее часто находят свое воплощение не в форме митинга или демонстрации, не в форме листовок или прокатов, а в форме различного рода цифрового контента. Самиздат экстремистской литературы был вытеснен материалами цифрового характера. Использование сети Интернет не только позволило распространять экстремистскую идеологию без затрат на создание книг, плакатов или листовок. Способность компьютерных данных к свободному копированию приводит к невероятной скорости и масштабам перемещения информации в киберпространстве, благодаря чему использование сети Интернет становится опаснее использования «традиционных» методов распространения экстремистских идей.

В настоящее время социальными сетями в России пользуется более 67,8% населения России, причем, среди молодежи доля ежедневных

пользователей социальных сетей достигает 91%[1]. В социальных сетях пользователи формируют свое «второе я» в виртуальном пространстве, а такое их отражение уже позволяет третьим лицам получить психологическую характеристику личности, а также всю социально значимую информацию. В связи с этим, социальные сети являются важным источником информации для раскрытия и расследования преступлений.

В то же время, анализ социальных сетей при расследовании преступлений, является сложной комплексной задачей для большинства сотрудников правоохранительных органов. Это обусловлено, во-первых, «виртуальным» характером среды совершения преступлений подобного рода; во-вторых, отсутствием научного анализа материалов следственной и судебной практики, а также научно обоснованных методических рекомендаций по организации работы с социальными сетями.

Экстремизм, как прямая угроза конституционному строю, за достаточно короткий срок превратился в одну из главных проблем современной России. Его проявления достаточно разнообразны - от возбуждения гражданской ненависти или вражды до функционирования многочисленных незаконных вооруженных формирований, ставящих перед собой цели изменения конституционного строя Российской Федерации и нарушения ее территориальной целостности. При этом преступности экстремистского характера не чужды и элементы организованности.

Признание особой опасности угроз экстремистского характера и определение противодействия экстремизму в качестве одного из ведущих направлений государственной правоохранительной деятельности уже неоднократно осуществлялось официально.

---

[1] Ежегодный отчет международного агентства We Are Social [Электронный ресурс] – Режим доступа: https://wearesocial.com/uk/blog/2021/01/digital-2021-uk/?ref=vc.ru (дата обращения: 20.05.2022)

На сегодняшний день ситуация в сфере противодействия экстремизму продолжает оставаться достаточно проблемной, что получает отражение в общественном сознании. Основными средствами распространения идей экстремизма и ресурсами вербовки в настоящее время являются социальные сети.

Указанные обстоятельства и обусловили выбор темы диссертационного исследования, а также его структуру и содержание.

Степень разработанности проблемы. Анализируемая категория преступлений вызывала и вызывает научный интерес, в первую очередь, ученых в области уголовного права и криминологии.

Основы методики расследования преступлений в сфере компьютерной информации были представлены в диссертационном исследовании В.А. Мещерякова (2001г.).

Изучению отдельных проблем информационного обеспечения раскрытия и расследования преступлений посвящены работы известных ученых-криминалистов, таких как Т.В. Аверьянова, И.Л. Бачило, Р.С. Белкин, И.А. Возгрин, Т.С. Волчецкая, А.Ф. Волынский, В.А. Волынский, А.Ю. Головин, С.И. Давыдов, А.В. Дулов, А.М. Ищенко, З.И. Кирсанов, В.Я. Колдин, А.М. Кустов, Н.П. Майлис, В.А. Образцов, А.С. Овчинский, А.А. Протасевич, Р.А. Усманов, А.И. Усов, Н.П. Яблоков, С.А. Ялышев и другие.

Вопросам противодействия преступности в глобальной компьютерной сети Интернет, а также проблемам борьбы с преступностью в сфере высоких технологий уделяли внимание такие ученые, как: А.В. Бегичев, В.А. Бельков, О.Ю. Введенская, В.Б. Вехов, Ю.В. Гаврилин, А.Н. Григорьев, Е.С. Дубоносов, П.Э. Меньшова, В.М. Мешков, В.А. Мещеряков А.С. Микаева, А.Л. Осипенко, А.Б. Смушкин, В.С. Соловьев, В.В. Шипилов и другие.

Теоретическим и методологическим основам раскрытия и расследования преступлений в сфере экстремистской и террористической

деятельности была посвящена докторская диссертация Р.В. Кулешова (2017г.).

Методика расследования транснациональной преступной деятельности экстремистского характера была представлена в докторской диссертации В.О. Давыдова (2018г.).

В разные годы те или иные проблемы противодействия преступлениям экстремистского и террористического характера рассматривались в диссертационных исследованиях ученых-криминалистов Ю.С. Бирюкова (2002 г.), О.В. Шлегеля (2008 г.), В.С. Капицы (2009 г.), Ж.В. Вассалатий (2010 г.), Д.Г. Скорикова (2014 г.), Т.А. Аристарховой (2015 г.), Д.Н. Еремина (2016 г.) и других ученых

Высоко оценивая значение трудов названных авторов для развития отечественной юридической мысли, следует отметить, что до настоящего времени в криминалистической науке не предпринималось попыток научного исследования теоретических и прикладных аспектов использования социальных сетей в расследовании преступлений, и, в частности, для повышения эффективности противодействия преступлениям экстремистской направленности. Это и обусловило возникновение идеи о необходимости разработки криминалистических основ исследования социальных сетей.

Объектом исследования является криминалистически значимая информация о личности, отражённая в социальных сетях, а также деятельность по выявлению, исследованию и использованию этой информации в расследовании и профилактике преступлений экстремистской направленности.

Предметом исследования являются закономерности отражения криминалистически значимой информации о личности в социальных сетях, а также закономерности выявления, исследования и использования этой

информации в расследовании и профилактике преступлений экстремистской направленности**.**

Цель диссертационного исследования заключается в разработке теоретических основ выявления, изучения и использования криминалистически значимой информации из социальных сетей для повышения эффективности расследования преступлений экстремистской направленности.

Достижение поставленной цели обусловило необходимость решения **следующих задач:**

1. Разработать понятие, выявить сущность и раскрыть особенности социальной сети как источника криминалистически значимой информации в расследовании различных видов преступлений.

2. Выявить особенности социальной сети как особого места совершения преступления.

3. Определить и аргументировать ситуационную обусловленность использования социальных сетей в процессе расследования преступлений.

4. Установить особенности получения информации из социальных сетей при взаимодействии с органами, осуществляющими оперативно-розыскную деятельность.

5. Разработать тактические приемы, направленные на использование криминалистической информации из социальных сетей при подготовке и проведении отдельных следственных действий при расследовании преступлений экстремистской направленности.

6. Создать научно-обоснованные организационно-тактические рекомендации по использованию специальных знаний при расследовании преступлений, совершенных с использованием социальных сетей в расследовании преступлений экстремистской направленности.

7. Установить факторы распространения экстремистской идеологии в молодежной среде в социальных сетях, на основе которых разработать меры криминалистической профилактики преступлений экстремистской направленности в пространстве социальных сетей.

Методологическую основу диссертационного исследования составили *общенаучные и частные методы*, апробированные наукой криминалистикой, основанные на *диалектическом материалистическом подходе*, включающие *методы анализа, синтеза, индукции, дедукции, аналогии и обобщения.* С целью определения структуры и элементов механизма преступлений экстремистской направленности, совершенных в социальных сетях, применены *системно-структурный метод и метод моделирования*. Применение с*истемного подхода* позволило установить корреляционные связи и взаимодействие элементов механизма преступлений экстремисткой направленности в социальных сетях, объединив их в целостную структуру, что позволило раскрыть объект исследования. Применение *статистического метода* способствовало анализу и обобщению эмпирического материала о практике расследования преступлений, совершенных в сети Интернет, связанных с побуждением несовершеннолетних к суициду. *Сравнительно-правовой метод* был использован при изучении норм уголовно-процессуального права, практики их применения *Социологический метод* использовался при проведении интервьюирования сотрудников Центра по противодействию экстремизма при УВД по Калининградской области; при оценке результатов исследований Всероссийского центра изучения общественного мнения. *Ситуационный подход* позволил осуществить научную разработку унифицированных научно-методических рекомендаций и прикладных аспектов, определяющих специфические особенности расследования данного вида преступной деятельности.

Нормативно-правовую базу исследования Конституция Российской Федерации, международные нормативно-правовые акты, затрагивающие проблематику исследования, уголовное и уголовно-процессуальное законодательство, законодательство о противодействии экстремистской деятельности; акты официального толкования норм права; подзаконные нормативные акты, регулирующие деятельность сотрудников правоохранительных и иных государственных органов в области борьбы с преступлениями экстремистской направленности.

Теоретическую основу исследования составили труды видных ученых-криминалистов: Т.В. Аверьяновой, О.Я. Баева, А.Р. Белкина, Р.С. Белкина, А.В. Варданяна, В.Б. Вехова, Т.С. Волчецкой, Е.И. Галяшиной, Ю.П. Гармаева, А.Ю. Головина, О.П. Грибунова, В.О. Давыдова, С.И. Давыдова, Л.Я. Драпкина, Е.С. Дубоносова, В.Н. Карагодина, Д.В. Кима, А.С. Князькова, И.М. Комарова, Р.В. Кулешова, А.М. Кустова, Н.П. Майлис, И.А. Макаренко, Н.И. Малыхиной, М.Ш. Махтаева, Г.М. Меретукова, В.А. Мещерякова, И.П. Можаевой, Н.А. Подольного, А.С. Подшибякина, О.В. Полстовалова, Н.И. Порубова, Е.Р. Россинской, Д.А. Степаненко, И.В. Тишутиной, Т.В. Толстухиной, А.И. Усова, Е.Н. Холоповой, С.И. Цветкова, Л.Г. Шапиро, А.А. Эксархопуло, Н.П. Яблокова и других авторов.

Эмпирической основой исследования послужили данные, полученные в результате изучения и обобщения материалов 132 уголовных дел по преступлениям экстремистской направленности, рассмотренных судами первой инстанции, г. Москвы, Московской, Калининградской областей, Ставропольского края, Республик Дагестан, Татарстан за период с 2012 по 2022 гг.; интервьюирования следователей и оперативных сотрудников; результаты исследований Всероссийского центра изучения общественного мнения.

Научная новизна исследования заключается в том, что на основе системного, междисциплинарного и ситуационного подходов автором на монографическом уровне разработана теоретическая концепция получения и исследования криминалистически значимой информации из социальных сетей и показана возможность использования ее потенциала в процессе расследования преступлений экстремистской направленности.

Научная новизна диссертации, в частности, заключается в том, что в ней:

- выявлены криминалистически значимые особенности социальных сетей, выявлена их сущность и возможности как источника получения информации в процессе раскрытия и расследования преступлений;

уточнено понятие социальной сети в аспекте криминалистической науки; рассмотрены основные виды социальных сетей;

- установлены характерные особенности и признаки социальной сети как места совершения преступлений;

- раскрыт потенциал использования социальных сетей для получения криминалистически значимой информации о личности участника уголовного процесса;

- на основе анализа материалов уголовных дел выделены типовые криминальные ситуации совершения преступлений экстремистской направленности в социальных сетях;

- выявлены возможности социальных сетей как инструмента поиска и сбора доказательств о лицах без вести пропавших, разыскиваемых, а также о лицах, осуществляющих вербовку к участию в незаконных действиях;

- на основе анализа следственной практики, интервьюирования следователей установлены типовые исходные следственные ситуации, возникающие на первоначальном этапе расследования преступлений экстремистской направленности, совершаемых в социальных сетях; для

каждой из следственной ситуаций разработаны методические рекомендации по их разрешению;

- установлены основные направления прикладного использования информации из социальных сетей в процессе раскрытия и расследования преступлений экстремистской направленности;

- выявлены особенности получения информации из социальных сетей при взаимодействии с органами, осуществляющими оперативно-розыскную деятельность;

- выдвинута научная гипотеза о целесообразности использования категории «виртуального агента» при разработке методик расследования преступлений экстремистской направленности, совершенных с использованием социальных сетей;

- предложено определение понятия «виртуальный агент»;

- описаны ситуационно обусловленные тактические приемы и рекомендации по их использованию в процессе подготовки и проведения отдельных следственных действий с использованием информации из социальных сетей;

- разработаны научно-обоснованные организационно-тактические рекомендации по применению специальных знаний при расследовании преступлений экстремистской направленности, совершенных с использованием социальных сетей;

- на основе выделения факторов распространения экстремистской идеологии в молодежной среде в социальных сетях, выявлены особенности, разработаны меры криминалистической профилактики преступлений экстремистской направленности, совершенных в сети Интернет.

Основные положения, выносимые на защиту:

1. В целях дальнейшего уточнения современного научного языка криминалистики предложено авторское определение понятия социальная

сеть, понимаемая автором как веб-сервис, в котором лицо формирует социальные отношения с другими пользователями, а также осуществляет поиск, создает, распространяет и использует различного рода информацию, тем самым оставляя свои цифровые следы. Как место человеческой деятельности социальная сеть обладает способностью хранить в себе цифровые следы, выявление, исследование и фиксация которых необходимы в целях эффективного раскрытия и расследования преступлений.

2. Социальные сети являются информативным источником криминалистически значимой информации о личности участника уголовного процесса: место работы или учебы, интересы, предрасположенности, социальные связи. По геотегам фотографий можно получить информацию о местоположении лица; по соотнесению времени и места фотографий есть возможность определить маршруты перемещений; по статусу можно установить текущее эмоциональное состояние человека. Кроме того, источником информации могут выступать и другие профили, где имела место публикация материалов, связанных с интересующим лицом или событием. Потенциал использования социальных сетей в расследовании преступлений может быть определен как инструмент в расследовании для поиска и сбора доказательств или информации о людях, в том числе без вести пропавших, разыскиваемых, а также лиц, осуществлявших вербовку к участию в незаконных действиях.

3. Трансграничный характер сети Интернет, портативность устройств выхода в сеть приводит к тому, что социальная сеть может также рассматриваться и в качестве места совершения преступления. Именно там находится интересующая следствие информация в виде переписки, опубликованных материалов, лог-файлов, IP-адресов. В этом ракурсе цифровые объекты выступают в качестве потенциальных средств

совершения преступления, которые могут быть дифференцированы на: а) объекты материального мира, используемые для доступа к сети Интернет (персональные компьютеры, ноутбуки, планшеты, мобильные телефоны и др.); б) цифровые объекты, посредством которых осуществлялась преступная деятельность непосредственно в социальных сетях: медиа-объекты, инструменты и интерфейс социальной сети. К ним могут быть отнесены отдельные текстовые сообщения, фотографии или иллюстрации, видео- или аудиозаписи.

4. Выявлены и описаны типовые криминальные ситуации, характерные для совершения преступлений экстремистской направленности в пространстве социальных сетей. В зависимости от содержания экстремистских сообщений в социальных сетях автором выделены:

- однозначные ситуации, в которых экстремистский смысл сообщения в социальной сети никак не скрывается, а разжигающие ненависть и вражду призывы и другие экстремистские идеи провозглашаются прямо и открыто;
- неоднозначные ситуации, когда смысловая направленность высказываний в социальной сети носит закамуфлированный экстремистский характер, и поэтому нуждается в установлении и выявлении.

5. На основе анализа следственной практики выявлены исходные типовые следственные ситуации, возникающие на первоначальном этапе выявления и расследования преступлений экстремистской направленности в зависимости от предпринятых попыток сокрытия информации преступником.

Ситуация 1. Установлен факт совершения преступления экстремистской направленности в социальной сети, а профиль социальной сети, использованный при совершении преступления, носит личный характер

(публикация была осуществлена с личного аккаунта, без использования каких-либо средств сокрытия).

Ситуация 2. Установлен факт совершения преступления экстремистской направленности в социальной сети, в то время как профиль социальной сети, использованный при совершении преступления, носит обезличенный характер (публикации была произведена с использованием псевдонима, либо с применением средств сокрытия IP-адреса).

Для каждой из указанных ситуаций разработаны научно обоснованные методические рекомендации по их разрешению, выбору комплекса следственных действий, применению алгоритма использования различных тактических приемов.

6. В результате анализа особенностей получения информации из социальных сетей при взаимодействии с органами, осуществляющими оперативно-розыскную деятельность, были разработаны научно-практические рекомендации по использованию так называемого «виртуального агента» в целях выявления фактов подготовки или совершения преступлений экстремистской направленности. «Виртуальный агент» выступает в качестве условного названия аккаунта, который может быть потенциально использован сотрудниками оперативных подразделений для его внедрения в виртуальную среду и тем самым преодоления настроек приватности закрытых экстремистских и проэкстремистских групп, движений и организаций.

Под «виртуальным агентом» предлагается понимать аккаунт в социальной сети, искусственную персону, позволяющую без посредников получить информацию по фактам вербовки, планируемым акциям экстремистского толка, кругу лиц, причастных к деятельности организации, а также дающую возможность выходить на прямой контакт с пользователями закрытых экстремистских сообществ.

7. Разработаны ситуационно обусловленные тактические приемы производства отдельных следственных действий при расследовании преступлений экстремистской направленности, совершенных в пространстве социальных сетей. Описаны тактические приемы проведения производства осмотра интернет–страницы в социальной сети, который рекомендуется проводить в присутствии понятых, с использованием техники записи-захвата экрана, фиксирующей действия в программной сфере. Разработан алгоритм действий следователя по обнаружению, исследованию и фиксации цифровых следов из социальной сети в процессе проведения различных следственных действий.

При фиксации результатов следственного действия в протоколе рекомендуется последовательно описывать: действия следователя с момента включения Интернет-браузера, с указанием адреса страницы с сети Интернет, имени обладателя страницы в социальной сети, указанием лица, разместившего экстремистский материал. В протоколе также целесообразно фиксировать информацию о дате и времени публикации, дате последнего посещения пользователем своей страницы, а также, в зависимости от конкретной ситуации, иные сведения об опубликованном материале.

Тактические приемы допроса подозреваемого, обвиняемого при расследовании преступления экстремисткой направленности, совершенного с использованием социальных сетей, разработаны с учетом того, что допрашиваемые преимущественно являются убежденными сторонниками пропагандируемых идей. При проведении обыска или выемки в условиях, когда интересующими объектами являются компьютерные устройства, целесообразно к проведению следственного действия привлекать специалиста. При проведении следственных действий лиц, не обладающих знанием языка, на котором ведется уголовное судопроизводство, с участием переводчика, следует учитывать то, что переводчик может разделять

убеждения лица, совершившего преступление экстремистской направленности. В таких ситуациях представляется обоснованным рекомендовать применение видеофиксации для того, чтобы при необходимости обеспечить возможность оценки достоверности и качества перевода.

8. Разработаны научно обоснованные рекомендации по использованию различных форм специальных знаний при расследовании преступлений экстремистской направленности: консультаций специалистов в различных отраслях науки и техники; участия специалистов при производстве следственных действий; проведения судебных экспертиз. При расследовании преступлений экстремистской направленности, совершенных в сети Интернет, предложено выделять две основные группы использования специальных знаний в зависимости от сферы деятельности: специальные знания в сфере информационных технологий и специальные знания в области лингвистики, религии, психологии.

9. Выделена особенность объекта лингвистических экспертиз по делам о преступлениях экстремисткой направленности: объектом таких экспертиз являются как сам текст в широком смысле, так и сопутствующие элементы (антураж), включающие в себя изображения, видеоряд, аудиозаписи или саундтрек. Разработаны типовые формулировки вопросов эксперту для назначения экспертизы экстремистских материалов в социальных сетях.

10. Выделены факторы распространения экстремистской идеологии в молодежной среде в социальных сетях, включающие в себя: подверженность чужому влиянию, внушению и манипулированию; недостаточную стрессоустойчивость; глубокое погружение в Интернет-пространство; романтизацию и героизацию антиобщественных и агрессивных действий. Выделены группы риска, а также общие и частные признаки лиц, попавших

под влияние экстремисткой идеологии. На основе отмеченных факторов разработаны меры криминалистической профилактики преступлений, экстремистской направленности, совершенных в социальных сетях.

Теоретическая значимость исследования заключается в том, что сформулированные в нем выводы и положения о понятии, криминалистических особенностях социальной сети и методических основах ее использования могут найти свое применение в дальнейших научных исследованиях по проблемам криминалистической техники, криминалистической тактики, методики расследования отдельных видов преступлений; криминалистической методики расследования преступлений экстремистской направленности.

Практическая значимость результатов исследования заключается в том, что научно обоснованные рекомендации, изложенные в диссертации, могут способствовать оптимизации практической деятельности по расследованию и профилактике преступлений экстремистской направленности. Отдельные выводы исследования могут применяться:

- в практической деятельности органов предварительного расследования при предупреждении, раскрытии и расследовании преступлений экстремистской направленности, совершенных с использованием социальных сетей;
- в экспертной деятельности по анализу экстремистских материалов;
- в деятельности оперативных сотрудников и сотрудников прокуратуры;
- в учебном процессе образовательных учреждений юридического профиля при освоении учащимися дисциплины «криминалистика» и соответствующих специальных курсов;

- при повышении квалификации следователей, дознавателей, прокуроров и оперативных сотрудников.

Апробация и внедрение результатов исследования. Основные результаты исследования докладывались и обсуждались на международных, всероссийских и региональных научно-практических конференциях, проходивших в Балтийском федеральном университете имени Иммануила Канта (2018, 2019, 2020, 2021, 2022 гг.), Алтайском государственном университете (2018, 2021 гг.), Калининградском филиале Санкт-Петербургского университета МВД России (2018, 2019, 2020 гг.), Томском государственном университете (2021), Гданьском университете (Польша) (2021г.), Карагандинском университете Казпотребсоюза (Казахстан) (2021, 2022 гг.).

Теоретические положения и выводы, содержащиеся в диссертационном исследовании, нашли отражение в 9 научных статьях, 3 из которых были опубликованы в научных журналах, входящих в перечень, рекомендуемый ВАК при Минобрнауки России для публикации основных результатов диссертационных исследований на соискание ученой степени кандидата юридических наук.

Положения диссертации обсуждались на заседаниях кафедры уголовного процесса, криминалистики и правовой информатики юридического института Балтийского федерального университета имени Иммануила Канта.

По результатам проведенного исследования разработаны методические рекомендации, которые внедрены в практическую деятельность Центра по противодействию экстремизму УМВД по Калининградской области, профилактическую деятельность Координационного центра по вопросам формирования у молодежи активной гражданской позиции, предупреждения межнациональных и межконфессиональных конфликтов, противодействия

идеологии терроризма и профилактики экстремизма. Ряд научных выводов и положений диссертации были использованы при разработке целого ряда дополнительных профессиональных программ (программ повышения квалификации), реализуемых Центром дополнительного образования БФУ им. И. Канта. Отдельные положения диссертационного исследования были внедрены в учебный процесс Высшей школы права БФУ имени И. Канта, а также Калининградского филиала Санкт-Петербургской академии МВД РФ.

Структура и объем диссертации. Диссертация состоит из введения, двух глав, включающих семь параграфов, заключения, списка литературы и приложений.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИСПОЛЬЗОВАНИЯ СОЦИАЛЬНОЙ СЕТИ В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

1.1. Понятие, сущность и специфика социальной сети как источника информации при расследовании различных видов преступлений

Компьютерные и мобильные устройства в наше время являются неотъемлемой частью общества, начиная от бытовой деятельности до систем военного, жизнеобеспечивающего или крупного производственного назначения. Их повсеместное использование не только способствует упрощению и ускорению тех процессов, в которых они применяются, но и открывает новые возможности как для преступника, так и для расследования преступлений.

Согласно исследованиям, ВЦИОМ к 1 мая 2019 года процент граждан России, подключенных к глобальной сети, достигло 84%, процент лиц, выходящих в Интернет, изменился от 28% до 69% за восемь лет[1], особого внимания заслуживает показатели совершеннолетних граждан младше 25 лет - 95%. Более того, с 2017 года число лиц, оценивающих серьезную роль сети Интернет в своей жизни, выросло с 32% до 48%. За это время, по материалам МСЭ, число Интернет-пользователей во всем мире увеличилось на 37,5%, достигнув четырех миллиардов человек[2].

---

[1] См.: Жизнь без интернета: рай или апокалипсис? [Электронный ресурс] URL: https://wciom.ru/index.php?id=236&uid=9681 – Загл. с экрана. (дата обращения: 20.05.2022)

[2] См.: The State of Broadband: Broadband catalyzing sustainable development [Электронный ресурс] URL:https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.18-2017-PDF-E.pdf – Загл. с экрана. (дата обращения: 20.05.2022)

Значение сети Интернет в формировании общества нового типа отразилось еще в 2011 году в материалах Генеральной Ассамблеи ООН на семнадцатой сессии Совета ООН по правам человека Франк Ла Рю Специальный докладчик ООН по вопросу о праве на свободу мнений и их свободное выражение представил доклад, посвященный роли сети Интернет в реализации прав человека, а также предложение по правам человека на поиск, получение, а также передачу информации и идей любого вида при помощи сети Интернет. Из доклада следовало, что глобальная сеть как средство передачи и поиска информации значительно превосходит телевидение, радио или любые альтернативы.

Следовательно, Интернет выступает средством, позволяющим потенциально неограниченному числу лиц реализовать своё право не только на свободу слова и мнения, но и другие права человека (ориг. “enabler” of other human rights). Интернет обеспечивает рост экономики, развитие в социальной и политических сферах, и обеспечивает развитие человечества в целом.

В частности, использование результатов научно-технического прогресса для интеграции людей в Интернет-пространство и новые формы социального взаимодействия привело к появлению такого феномена как социальные сети.

Необходимо отметить, что такая концепция встречалась задолго до появления самого Интернета и компьютерных технологий как таковых. Писатель, философ и общественный деятель XIX века Владимир Одоевский в своем незаконченном утопическом романе «4338-й год», написанном в 1837 году выдвинул идею, в общих чертах аналогичную концепции социальных

сетей и сети Интернет[1]: "Мы получили домашнюю газету от здешнего первого министра, где, между прочим, и мы были приглашены к нему на вечер. Надобно тебе знать, что во многих домах, особенно между теми, которые имеют большие знакомства, издаются подобные газеты; ими заменяется обыкновенная переписка... Обязанность издавать такой журнал раз в неделю или ежедневно возлагается в каждом доме на столового дворецкого. Это делается очень просто: каждый раз, получив приказание от хозяев, он записывает все ему сказанное, потом в камеру-обскуру снимает нужное число экземпляров и рассылает их по знакомым. В этой газете помещаются обыкновенно извещение о здоровье или болезни хозяев и другие домашние новости, потом разные мысли, замечания, небольшие изобретения, а также и приглашения, когда же бывает зов на обед, то и le menu". Что поразительно совпадает с ролью социальных сетей в современном обществе.

Впервые в научной литературе понятие «социальная сеть» (ориг. social field of this kind as a network) приводилось английским социологом Джоном Барнсом в работе «Классы и собрания в норвежском островном приходе» в 1954 г. Данное определение «социальная сеть» включает человека, его круг знакомых, а также взаимных социальных связей между этими людьми[2]. Размеры такой социальной сети по отношению к отдельному человеку превышает 100 человек. В прошлом, в условиях отсутствия современных средств телекоммуникации, они представляли собой сети человеческих взаимоотношений. В отличие от иных социальных структур, представляющих достаточно жесткую систему устоявшихся социальных

[1] Цит. По: В.Ф. Одоевский "Повести и рассказы", ГИХЛ, 1959. [Электронный ресурс] URL: http://az.lib.ru/o/odoewskij_w_f/text_0490.shtml – Загл. с экрана. (дата обращения: 20.05.2022)

[2] См.: J. A. Barnes Class and committees in a norwegian island parish [Электронный ресурс] URL:http://pierremerckle.fr/wp-content/uploads/2012/03/Barnes.pdf (дата обращения: 20.05.2022)

отношений, социальные сети обладают гибкостью, позволяющей управлять малыми социальными взаимодействиями.

В теории социальных сетей традиционно выделяют два-три уровня анализа социальных сетей:

1. микроуровень — уровень отдельных лиц или малых сетей;
2. мезоуровень (выделяется не всегда) — уровень относительно крупных социальных групп;
3. макроуровень — уровень крупных и глобальных обществ[1].

Социальные сети могут формироваться по общим интересам, конкретным потребностям, ресурсам или сферам влияния, социальным статусам и потенциально не ограничены в факторах их формирования, включая и преступную деятельность.

Формирование социальных сетей в обществе закономерно начинается с микроуровня. Личная связь между близкими людьми на таком уровне является естественным началом формирования социальных сетей между ними. Отношения с другими группами и личностями завязываются путём построения связей с государственными структурами, политическими организациями, институтами, промышленными ассоциациями, профсоюзами, прессой, религиозными организациями или любыми другими группами людей, позволяющие создать подходящие условия для установления доверия, продолжительных регулярных контактов, взаимодействия и взаимовлияния[2].

---

[1] См.: Брун О.Н. Развитие теорий социальных сетей: от локального к глобальному социуму : диссертация ... кандидата социологических наук : 22.00.01 / Брун Ольга Евгеньевна; [Место защиты: Моск. гос. ин-т междунар. отношений]. - Москва, 2012. - 154 с.

[2] См.: Воронкин А.С. Социальные сети: эволюция, структура, анализ /"Образовательные технологии и общество". - 2014. - № 9. - С.651

Социальные сети могут также характеризоваться как формальные и неформальные, вертикальные и горизонтальные[1].

Неформальные социальные сети строятся на личных свободных отношениях внутри группы. Формальные сети строятся на основе четкой регламентации прав и обязанностей каждого члена.

В вертикальных сетях выделяется лидерская группа или индивид, которые определяют цели, характер действий группы, её ритуалы и внутренние правила, а также алгоритм контакта, противодействия или взаимодействия с другими группами. Члены таких групп обладают разным положением внутри группы.

Горизонтальные сети не предполагают наличия субординации, полномочий и ответственности, такие группы обычно представляют собой объединения лиц примерно одинакового социального статуса.

В глобальной сети Интернет социальные сети как медиа сервисы в большей степени соответствуют неформальным горизонтальным социальным сетям в социологии.

Пик становления социальных сетей Интернета относится к становлению Web 2.0 проектированию сети Интернет, связанной с социализацией сайтов[2], где пользователю была предоставлен подход к виртуальной среде, отличительными особенностями которого стали:

- Возможность индивидуализации настроек сайта, а также создание личной зоны пользователя, куда входят личные файлы, изображения, фото, видео или блоги.

---

[1] См.: Мельникова М.С., Яковлев И.П. Понятие «социальная сеть» в социологических теориях и интернет-практиках// Вестник СПбГУ. Сер.9.2014. Вып.1. с 255

[2] См.: Amy Shuen. Web 2.0: A Strategy Guide. — O'Reilly, 2008. — 272 p. — ISBN 978-0-596-52996-3.

- Поощрение, поддержка и доверие «коллективному разуму» пользователей сервисов, выражающемся в контентном наполнении с их стороны.
- При формировании сообщества большое получает соревновательный элемент, выражающийся в репутации или рейтинге, которые позволяют группе осуществлять саморегуляцию и создавать для пользователя дополнительные цели присутствия на ресурсе.

Следовательно, характерной чертой приложений Веб 2.0 стала переориентация на большее взаимодействие с конечным пользователем.

Это привело к тому, что сам конечный пользователь является не только пассивным пользователем приложения, но и его участником.

Именно основоположник концепции Web 2.0 Тим О'Рейли в 2005 году впервые использовал понятие «социальная сеть» в контексте глобальной сети Интернет в своей статье «What Is Web 2.0»[1].

Под социальной сетью в наиболее узком значении принято понимать Интернет-платформу, веб-сайт, или сервис, предназначенный для формирования, организации и визуализации социальных взаимоотношений, посредством социальных граф[2].

Социальная сеть как Интернет-ресурс может быть проанализирована с различных позиций, но тем не менее, в контексте предмета исследования наиболее целесообразным обратить внимание на определение социальной сети как *виртуализированной социальной среды, в которой человек занимается установкой, расширением и углублением своих социальных*

[1] См.: Tim O'Reilly What Is Web 2.0 Design Patterns and Business Models for the Next Generation of Software [Электронный ресурс] URL: https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=3 (дата обращения: 20.05.2022)

[2] См.: Вебер К.С., Пименова А.А. Сравнительный анализ социальных сетей // Вестник Тамбовского университета. Серия: Естественные и технические науки. - 2014. - т.19, вып. 2. - С.634

связей, формируя специфическую структуру отношений, а также самореализуется, социализируется, генерирует и потребляет любую, интересующую его информацию. Такой подход прежде всего позволяет акцентировать внимание на человеческой интеракции в пространстве социальных сетей, определить их функциональное значение, которое и повлекло невероятные темпы распространения и ощутимую привлекательность социальных сетей для совершения преступлений.

Социальные сети как медиа ресурсы относительно социальных сетей в социологии характеризуются горизонтальными, слабыми связями между участниками, а также высокой степенью интерактивности, такие сети носят открытый характер, предлагают возможность направлять информацию как в форме монолога, так и диалога или полилога. Такие сети способствуют накоплению и реализации социального капитала, более того, они становятся отражением тяги людей к сотрудничеству, к созданию коллективов, социальных норм и ценностей, а также общественных отношений, прежде всего, построенных на **взаимности и доверии**. Это обусловлено характерным недостатком доверительных отношений между людьми в современном обществе, напряженностью, но и желанием человека быть свободным в процессе коммуникации.[1]

Функциональные возможности подавляющего большинства социальных сетей предоставляют каждому её пользователю возможность создать свой виртуальный аватар (Аватара - санскр. «нисхождение») - создать профиль, содержащий широкий перечень личной информации о себе: место жительства, работу, семью, интересы, хобби, увлечения, цели и любую

[1] См.: Лещенко А. М. Социальные сети как механизм конструирования коммуникации в современном обществе: автореферат дис. ... кандидата философских наук : 09.00.11 / Лещенко Александр Михайлович; [Место защиты: Пятигорский государственный гуманитарно-технологический университет]. - Пятигорск, 2011. - 25 с.

другую информацию, *что открывает широкие возможности использования такого аватара в процессе расследования преступления*. Аватар пользователя содержит информацию о личности, ориентирующую и иную криминалистически значимую информацию. Наличие аватара связано с возможностью использовать механизмы поиска самой социальной сети, а также поисковых систем глобальной сети для нахождения близких по интересам людей, единоверцев, знакомых, дальних родственников, а также людей, общение с которыми необходимо по работе или по другим причина. Все это приводит к тому, что человек осознанно формирует свое цифровое отражение (аватару) в виртуальном пространстве, различные проявления которого, в том числе представляющие ценность для расследования преступления, можно узнать после тщательного изучения его страницы в социальной сети. Процесс криминалистического исследования личности, в таком случае, может охватывать и социальную сеть.

Современная социальная сеть как минимум предлагает следующий набор стандартных сервисов:

- Формирование и сохранение аккаунта с контактными данными;
- Список контактов/друзей;
- Ведение переписки, голосовых сообщений;
- Возможность ограничения общения и блокировки пользователей на своей странице (черный список);
- Место облачного хранения мультимедийных данных пользователя с функцией передачи;
- RSS – ленты новостей, нового контента, размещенного другими пользователями или иной обобщенной информации.

Следовательно, пользователь в определенном смысле получает собственное «место жительства» в Интернете[1], где его могут при необходимости найти, общаться, получать информацию о его жизни. В контексте расследования преступления само это «место жительства» может стать местом происшествия, в том числе преступления экстремистского характера.

В результате наполнение социальной сети осуществляется его пользователями, которые имеют возможность формирования социальных связей между собой и создание социальных объектов, таких как тематические группы и другие, которые, в свою очередь, доступны другим пользователям для обозрения. Имея колоссальное количество ежесекундно растущего контента, персональную службу обмена сообщениями и мультимедийными файлами, поисковую систему, игры и приложения, социальные сети стали наиболее популярными порталами сети Интернет, ставшими местом виртуальной жизни в Интернете.

Благодаря уникальным возможностям социальных сетей для их пользователей, они быстро разрослись и стали чрезвычайно популярны. Количество пользователей сетей год от года увеличивается огромными темпами. Растет не только их количество, но и время, которое проводит усредненный пользователь в социальных сетях. Подобное явление во многом связано с широким функционалом социальных сетей.

Среди функций социальной сети следует выделить следующие:

- Идентификации
- Обмена информации
- Коммуникации
- Формирования идентичности

---

[1] См.: Печенкин В. Анализ социальных сетей: в ожидании чуда // Журнал «Компьютера». 2005. № 42. С. 15-20.

- Самоактуализации (самопрезентации)
- Социализации
- Развлекательная[1]

В рамках криминалистического изучения социальных сетей важно отметить функцию обмена информацией. Все современные социальные сети предлагают две основные формы обмена информацией: публично и приватно. Приватный обмен информацией реализуется как между двумя участниками, где каждый может как передавать, так и принимать сообщения и медиафайлы (личные файлы), так и между несколькими участниками (групповые чаты). Такая форма обмена информацией характеризуется недоступностью для третьих лиц. Публичный обмен информацией представляет собой распространение по принципу «один-многим» путем размещения информации на собственной странице, её «стене» или её аналогах, а также путем комментариев (в том числе медиафайлами), где получателем информации неограниченное (все пользователи сети Интернет) или условно неограниченное (все зарегистрированные пользователи социальной сети, все подписчики, все друзья). Следовательно, отдельно, как средство распространения информации социальные сети обладают беспрецедентными возможностями, что также стало фактором широкого распространения социальных сетей. Так, около 85% всех пользователей сети Интернет состоят хотя бы в одной социальной сети[2].

Одна из важнейших особенностей социальных сетей связана с ее контентным наполнением. В отличии от обычных веб-страниц это наполнение осуществляется лично зарегистрированным пользователем, а не администрацией, следовательно, оно приобретает более личный характер:

---

[1] См. об этом подробнее: Садыгова Т. С. Социально-психологические функции социальных сетей // Вектор науки ТГУ. - 2012. - №3 (10). - С. 192-194.

[2] Цит. по: Воронкин А.С. Социальные сети: эволюция, структура, анализ //"Образовательные технологии и общество". - 2014. - № 9. - С.650

информация в виде текста или медиафайлов так или иначе отражает личные особенности пользователя, разместившего контент. В частности, профессором Щебетенко С.А. было отмечено, что такие личностные черты как экстраверсия и нейротизм являются характерными предпосылками многих поведенческих показателей активности в сети, среди которых есть количество друзей, количество записей на стене, количество фотографий, количество отметок «мне нравится» под пользовательской фотографией и т.д. [1]

Разность подходов к значению социальных сетей в жизни общество привела к тому, что с одной стороны формирование социальных сетей понимается как формирование новой формы социального взаимодействия, становления киберпространства как полноценного места человеческой деятельности. С другой же стороны встречаются и полностью противоположные подходы, оценивающие социальную сеть с позиции опасности для человека. С такой позиции социальная сеть может быть рассмотрена как эскапизм, при котором возможен переход временного замещения реального мира в самостоятельную доминирующую реальность, полностью поглощающую человека. Кроме того, трансграничный характер социальной сети приводит к активному взаимопроникновению культур, непрерывному обмену культурными ценностями и моментальному распространению информации. В результате, человек, независимо от его желания, становится «гражданином (виртуального) мира». Фактически все еще находясь в своей культурной среде, он постоянно испытывает

[1] См.: Щебетенко С.А. Большая пятерка черт личности и активность пользователей в социальной сети «ВКонтакте» //Вестник Южно-Уральского государственного университета. Серия: Психология. - 2013. – Том 6 № 4. - С.73

чужеродное социокультурное воздействие на личность, которая не может в таких условиях оставаться стабильной[1].

Толерантность как одна из основных черт социальной сети подкрепляет возможности существования взаимоисключающих идеологий, однако агрессивная пропаганда или вирусное распространение материалов приводит к тому, что при изначальной толерантности сети начинается процесс своего рода «естественного отбора», в котором личность человека подвергается информационному воздействию наиболее бескомпромиссной идеи.

Специфика наполнения социальной сети, её функциональные особенности находят свое отражение на странице профиля в социальной сети, который представляет собой консолидированный сборник информации о лице, который может быть использован как в следственной, так и оперативно-розыскной деятельности.

Социальная сеть как явления многогранное может быть рассмотрено с различных позиций.

Социология как источник самого понятия «социальная сеть» рассматривает Интернет-ресурсы как новую форму социальных сетей в обществе, как новую систему, осуществляющую общение на универсальном цифровом языке, которая и включает в себя в глобальном масштабе производство и распространение информации в обществе и адаптирует её относительно личных вкусов и предпочтений личности. Социальные сети закономерно растут по экспоненте, создавая тем самым новые формы и пути общения, «формируя жизнь и формируясь жизнью в одно и тоже время»[2].

---

[1] См. об этом подробнее: Шипицин А.И. Феномен социальных сетей в современной культуре // Известия Волгоградского государственного педагогического университета. – 2011. – С. 38

[2] См.: Кастельс М. Галактика Интернет: Размышления об Интернете, бизнесе и обществе. Екатеринбург: У-Фактория, 2004

С такой позиции социальные сети рассматриваются как новое пространство для человеческой взаимосвязи, которое вместе с тем, содержит в себе некоторые проблемы. Социальная интеракция в социальной сети не предполагает искренних и глубоких чувств и эмоций, которые необходимы в полноценном общении, поскольку связь внутри любой социальной сети носит функциональный характер. Наблюдается эффект дистанцирования, влекущий к «простодушию» обитателей социальной сети. В социальных сетях проявляется первичная задача Интернета - передавать информацию. Вследствие чего возникает ситуация, в которой человек, не связанный личным общением с собеседником теряет потребность в эмпатии. Он буквально не видит своего собеседника, его интерес к другому лицу в основном не носит правдивый характер[1].

Психология рассматривает социальные сети как фактор формирования социальных установок, в том числе у молодежи[2]. Социальные установки, отражающиеся в содержании контента виртуальных социальных сетей, формируются посредством социально-психологического механизма, ключевыми элементами которого являются: акцентированные потребности, удовлетворяемые через формирование стереотипов, подражание и идентификацию[3]. Формирование таких установок основаны на удовлетворяемых в социальных сетях потребностью в формировании, повышении и удержании статуса, потребностью в повышении и поддержании личной самооценки, идентификации и общей потребностью в успехе в той или иной форме.

---

[1] См.: Маркова Т.В. Щербатых Д.А. Философия социальных сетей // Интерактивная наука. – 2018.

[2] См.: Безбогова М. С. Социальные сети как фактор формирования социальных установок современной молодежи : автореферат дис. ... кандидата психологических наук : 19.00.05 / Безбогова Марина Сергеевна; [Место защиты: Гос. ун-т упр.]. - Москва, 2017. - 25 с.

[3] См.: там же.

Необходимо отметить значение социальных сетей в политическом и экономическом исследованиях. В настоящий момент, очень многие политики, политические организации и партии заинтересованы в использовании социальных сетей для реализации своих программ и распространении идей. Очень важно, что они рассматривают социальные сети не только как сайты для информирования пользователей о своих идеях (базовая функция сети Интернет), но и как площадку для обсуждений и отстаивания своих взглядов и принципов, что наиболее часто происходит в созданных для этого группах/сообществах социальной сети или на странице конкретного политика[1].

Поскольку социальная сеть как часть интернет-пространства существует в цифровой сфере она закономерно становится объектом исследования компьютерно-технических наук[2], направленных как на автоматизацию работы в пространстве таких сетей, получения информации из таких сетей, а также возможностей технического развития самих социальных сетей.

Социальные сети как элемент глобальной сети обладают значительным перспективами для криминалистической науки. Потенциал использования социальных сетей в расследовании преступлений может быть определен как инструмент в расследовании для поиска и сбора доказательств или информации о людях, в том числе без вести пропавших, разыскиваемых, а также лиц, осуществлявших вербовку к участию в незаконных действиях. Опыт зарубежных стран, в лице США с показателем в 86,1 % преступлений,

---

[1] См. об этом подробнее: Ануфриева, Г. В. Язык общения в социальных сетях / Г. В. Ануфриева // Русская речевая культура и текст : материалы XII Международной научной конференции, Томск, 20–21 мая 2022 года. – Томск: Томский центр научно-технической информации, 2022. – С. 111-117.

[2] См.: Будыльский Д.В. Автоматизация мониторинга общественного мнения на основе интеллектуального анализа сообщений в социальных сетях: диссертация ... кандидата технических наук: 05.13.10 / Будыльский Дмитрий Викторович;[Место защиты: Брянский государственный технический университет].- Брянск, 2015.- 169 с.

в расследовании которых использовались социальные сети[1], позволяет оценить значение социальных сетей в условиях информационного общества.

Социальная сеть как новое пространство человеческой интеракции обладает возможность отражать в себе как сам процесс такого взаимодействия, так и его последствия – следы. Существование цифрового следа наравне со следами материальными и идеальными достаточно давно является объектом научных дискуссий[2], но этом случае, социальная сеть как киберпространство обладает способностью к изменению и хранению информации о таком изменении[3].

Поиск информации в пространстве социальной сети, с позиции познавательной деятельности, имеет существенное сходства с таким следственным действием, как осмотр, где одной из целей выступает обнаружение следов преступления, а также выяснение других обстоятельств, имеющих значение для уголовного дела.

Отдельно необходимо отметить перспективу социальной сети как источника ориентирующей криминалистически-значимой информации: в зависимости от наполнения аккаунта в социальной сети можно получить информацию:

- о местоположении лица (по геотегам фотографий)

---

[1] Цит. по: Олиндер Н.В., Гамбарова Е.А. Проблемные вопросы поиска и восприятия информации о человеке в сети интернет и ее использование при расследовании преступлений // Юридический вестник Самарского университета. 2016. Т.2, №4, С. 56

[2] См. об этом подробнее: Вехов В.Б. Дорожка электронных следов: понятие и особенности судебного компьютерно-технического исследования // Уголовное производство: процессуальная теория и криминалистическая практика. Материалы VII Международной научно-практической конференции. Ответственные редакторы М.А. Михайлов, Т.В. Омельченко. 2019. С. 19.

[3] Бычков В.В., Вехов В.Б. Электронное следообразование преступной деятельности в сети Интернет//Расследование преступлений: проблемы и пути их решения. 2020. № 1 (27). С. 107.

- определить маршруты перемещений (по соотнесению времени и места фотографий)
- определить интересы, предрасположенности, социальные связи
- текущее эмоциональное состояние (по статусу)
- место работы или учебы
- другой информации, нашедшей отражение в профиле сети

Кроме того, источником информации могут выступать и другие профили, где имела место публикация материалов, связанных с интересующим лицом или событием.

Федеральным законом от 30.12.2020 N 530-ФЗ "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" понятие «социальная сеть» нашло некоторое легальное закрепление через статью 10.6. «Особенности распространения информации в социальных сетях», где появилось понятие «владелец социальной сети»[1].

В контексте указанного закона под социальной сетью можно понимать сайт и (или) страницу сайта в сети "Интернет", и (или) информационную систему, и (или) программу для электронных вычислительных машин, которые предназначены и (или) используются их пользователями для **предоставления и (или) распространения посредством созданных ими персональных страниц информации** на государственном языке Российской Федерации, государственных языках республик в составе Российской Федерации или иных языках народов Российской Федерации, **на которых может распространяться реклама**, направленная на привлечение внимания потребителей, находящихся на территории Российской Федерации, и **доступ к которым в течение суток составляет более пятисот тысяч**

[1] Федеральный закон от 30.12.2020 N 530-ФЗ "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации"// СПС «Консультант Плюс».

пользователей сети "Интернет", находящихся на территории Российской Федерации.

Вместе с тем, указанное понятие не в полной мере может удовлетворять интересам криминалистического анализа. Так, «распространение информации на персональных страницах» существенно уменьшает долю социального взаимодействия, о которой указывалось ранее.

Следовательно, в рамках криминалистического исследования под *социальной сетью мы понимаем веб-сервис, в котором лицо формирует социальные отношения с другими пользователями, а также осуществляет поиск, создает, распространяет и использует различного рода информацию, тем самым оставляя свои цифровые следы.*

Как место человеческой деятельности социальная сеть обладает способностью хранить в себе цифровые следы, которые могут быть использованы в целях противодействия преступности.

Рассматривая социальную сеть как виртуализированную социальную среду целесообразно отметить, что преступная деятельность как одна из форм человеческой деятельности закономерно окажет свое влияние на социальные сети[1]. Контентное наполнение социальных сетей осуществляется и злоумышленниками в результате преступной деятельности так и вне её.

Однако процесс формирования и совершенствования нормативно-правовой базы, необходимой для регулирования возникающих проблем, не успевает за активным развитием сети Интернет, из-за чего уровень российского законодательства в сфере отношений в сети Интернет, так и уровень знаний правоприменителя отстает от необходимого уровня, что

[1] Аристов, С. К. Регулирование медиапространства как основа безопасной коммуникационной среды / С. К. Аристов, А. А. Ароянц // Коммуникационные процессы: теория и практика : Сборник материалов XVII международной научно-практической очно-заочной конференции, Краснодар, 28 октября 2021 года / Отв. редактор М.Б. Щепакин. – Краснодар: Кубанский государственный технологический университет, 2022. – С. 105.

говорит об отсутствии эффективно действующей нормативно-правовой базы по регулированию сети Интернет[1]. При этом, даже сформированная нормативная основа может не обеспечить эффективного применения правовых норм, что прежде всего связано с тем, что Интернет и социальные сети как его часть представляют собой открытую децентрализованную систему, что исключает само существование такой организационной структуры, которая могла бы обеспечивать контроль за содержанием или действиями пользователей глобальной сети.

Распределенный характер и практически полное отсутствие непосредственного контроля за пространством сети Интернет предоставляет новые возможности для преступной деятельности, вследствие чего происходит активный переход преступной деятельности в киберпространство.

Все преступления, совершенные с использованием сети Интернет, можно разделить на две категории:

- преступления, связанные с взаимодействием «человек-техника» (несанкционированные действия с информацией, разработка вредоносного ПО)
- преступления, которые связаны с взаимодействием «человек-человек», где сеть Интернет обеспечивает это взаимодействие. (мошенничество, доведение до самоубийства и преступления экстремистской направленности)

Сложности первой категории имеют техническую природу, в то время как во второй категории возникает необходимость определения уровня коммуникации: межличностного, контакт-коммуникационного и масс-

[1] См.: Микаева А.С. Проблемы правового регулирования в сети Интернет и их причины / Микаева А.С. //"Актуальные проблемы российского права". - 2016. - N 9. - С.45

коммуникационного для дальнейшей квалификации деяния и назначения наказания[1].

Отдельно необходимо отметить психологическое восприятие информации из социальной сети: страница пользователя в сети воспринимается как персональное пространство, что вызвано особенностями социальных сетей, такими как возможность самостоятельного выбора пользователем собеседников, возможность фильтрации информационного содержимого при помощи членства в интересующих пользователя группах или сообществах. Именно такая персонализация в дальнейшем, отражающаяся в RSS ставит доверие пользователя социальной сети к получаемой информации изначально выше, чем к информации, получаемой из любых других источников: от федеральных СМИ[2] до Интернет-СМИ[3].

Следовательно, Интернет-пространство создает фундаментально отличную от реального мира среду, характеризующуюся высокой в силу «простодушия» степенью доверия к информации и собеседникам, действующим в сети Интернет. Из-за этого Интернет-пространство человеком подсознательно не воспринимается как источник опасности – физической угрозы нет и быть не может. Данные обстоятельства

---

[1] См.: Рыдченко, К.Д. Административно-правовое обеспечение информационно-психологической безопасности органами внутренних дел Российской Федерации: дис. … канд. юрид. наук : 12.00.14 / К.Д. Рыдченко. — Воронеж, 2011. – С. 166

[2] См. об этом подробнее: Лыткина, О. А. Влияние СМИ на молодежную аудиторию / О. А. Лыткина // Афанасьевские чтения. Инновации и традиции педагогической науки - 2022 : Сборник материалов XXII Всероссийской научно-практической конференции, посвященной 105-летию со дня рождения доктора педагогических наук, профессора В.Ф. Афанасьева (Алданского), Якутск, 22 марта 2022 года. – Киров: Межрегиональный центр инновационных технологий в образовании, 2022. – С. 103.

[3] См.: Гладышев В.В. «Социальные сети как инструмент для пропаганды экстремизма». // Национальный центр информационного противодействия терроризму и экстремизму в образовательной среде и сети интернет. Ростов-на-дону [Электронный ресурс] URL:http://nac.gov.ru/publikacii/stati-knigi-broshyury/gladyshev-v-socialnye-seti-kak-instrument-dlya.html (дата обращения 20.05.2022)

предоставляет злоумышленнику широкие возможности для подготовки и совершения преступлений.

Распространение сети Интернет, открыло новые возможности и для экстремистской деятельности. В пространстве социальных сетей могут найти свою реализацию следующие экстремистские действия[1]:

- Оправдание терроризма, совершенное публично;
- Распространение идей превосходства или исключительности человека, либо неполноценности по признакам его расовой, национальной, социальной, конфессиональной или языковой принадлежности;
- Возбуждение расовой, национальной, социальной или межконфессиональной розни;
- Распространение идей или демонстрирование публично нацистской символики или атрибутики либо, сходных до степени смешения с нацистской;
- Призывы в сети Интернет к осуществлению экстремистских деяний либо распространение в сети заведомо экстремистских материалов;
- Организация или подготовка экстремистских деяний, или подстрекательство к их осуществлению;
- Публичное демонстрирование символики или атрибутики экстремистских организаций.

Значительную опасность представляет собой финансирование экстремистской деятельности, а также иное содействие в её организации, подготовке и осуществлении. Так, уже 9 марта 2016 года глава Росфинмониторинга Юрий Чиханчин заявил, что через социальные сети россияне перевели террористам десятки миллионов рублей, спецслужбами

[1] См.: О противодействии экстремистской деятельности: федеральный закон от 25.07.2002 N 114-ФЗ [Электронный ресурс]. Доступ из справ.-правовой системы «Консультант Плюс». Ст. 2

была выработана карта активностей переводов, для определения точек наибольшей финансовой поддержки[1].

Трансграничное распространение информации, используемое в экстремистских целях, создает угрозу нанесения ущерба стабильности государства и международной безопасности. Доктрина информационной безопасности Российской Федерации от 5 декабря 2016 года отмечает широкое использование экстремистскими организациями механизмов информационного влияние на сознание индивидуумов, групп и общества в целом с целью создания социальной и межнациональной напряженности, пропаганды расовой и межконфессиональной ненависти, продвижения экстремистской идеологии, а также вербовки[2]. Противодействие использованию компьютерных технологий для распространения экстремистской идеологии, рас пропаганды ксенофобских идей, национальной или расовой исключительности с целью подрыва суверенитета, создания политической или социальной нестабильности, а также насильственного изменения основ конституционного строя, или нарушения территориальной целостности Российской Федерации является одной из основных направлений обеспечения информационной безопасности в области государственной и общественной безопасности.

Опасность экстремизма как международной угрозы находит свое отражение и в документах Организации Объединенных Наций. Так, совместном докладе Управления ООН по наркотикам и преступности и Целевой группы по осуществлению контртеррористических мероприятий «Использование Интернета в террористических целях» 2012 года

---

[1] Глава финразведки РФ раскрыл схему финансирования террористов через Сеть [Электронный ресурс]. – Режим доступа: https://riafan.ru/507859-rossiyane-podderzhali-terroristov-desyatkami-millionov-rublei. – Загл. с экрана.

[2] См.: Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

указывается на растущую вместе с самой сетью Интернет тенденцию распространения экстремистских материалов в глобальной сети, вытесняющую использование как физических носителей, так и компакт-дисков или DVD дисков[1], что способствует увеличению аудитории воздействия. Экстремистами используются такие средства, как выделенные веб-сайты, тематические чат-комнаты, форумы, онлайн-журналы, видео- и файловые хостинги, и особенности социальные сети. Отмечается, что современные возможности поисковых систем с использованием служб индексирования позволяют легче обнаружить и получить доступ к экстремистским материалам.

На расширенном заседании Совета Безопасности при рассмотрении проекта Стратегии противодействия экстремизму в Российской Федерации до 2025 года президентом Российской Федерации Владимиром Путиным актуальность противодействия экстремизму была обозначена как не вызывающая никаких сомнений. Опасной была названа сама природа экстремизма, как разрушительной идеологии нетерпимости, агрессивный, подстрекательский, а нередко насильственный характер экстремизма, связанный с террором. Отмечается, что именно среде молодежи лидеры экстремистских организаций осуществляют вербовку последователей, пропагандируют свои идеи посредством прежде всего сети Интернет. «Идеология экстремизма набирает силу в виртуальном пространстве, причём набирает, буквально выстреливая в реальную жизнь.»[2] Пропаганда

---

[1] См.: The Use of the Internet for Terrorist Purposes [Электронный ресурс]. – URL:http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf (дата обращения: 20.05.2022)

[2] См.: Владимир Путин провёл в Кремле расширенное заседание Совета Безопасности. Рассматривался проект Стратегии противодействия экстремизму в Российской Федерации до 2025 года [Электронный ресурс]. – URL:http://kremlin.ru/events/president/news/47045. – Загл. с экрана. (дата обращения: 20.05.2022)

экстремистских идей в сети Интернет находит свою реализацию в пространстве социальных сетей. Связано это прежде всего с тем, что в пространстве социальных сетей в основном пребывают именно подростки и молодежь, являющиеся наиболее мобильной частью населения. А также возможности мгновенной передачи информации на неопределенный круг лиц посредством «лайков» и «репостов».

Из этого следует, что Интернет как феномен цифровой эпохи уже стал неотъемлемой частью современной жизни, проникая в каждую из сфер общества, от экономики до межличностных отношений. Именно возможность построения социального взаимодействия в сети Интернет стало основой появления и причиной популярности социальных сетей в современном обществе. Нарастающие темпы компьютеризации, стремительное удешевление услуг доступа к глобальной сети, а также его повсеместное использование привело к постановке вопроса об отнесении права пользования сетью Интернет к правам человека.

Вместе с тем проникновение преступности в сферу социальных сетей, а также отражение преступной деятельности в данной сфере влечет закономерную необходимость использования социальной сети в криминалистике, как перспективнейшего источника информации о преступлении, его участниках, и иной информации.

Проблема современной преступности и её отражения в пространстве социальной сети включает в себя общие проблемы, связанные с интернет-преступностью: анонимность, простота совершения преступления, сопряженная с минимальными рисками, неограниченным расстоянием и широким кругом охвата. Однако личный характер социальной сети вкупе с функциональной основой и принципами работы социальной сети открывает новые возможности и для криминалистической науки.

Следовательно, возникает необходимость в формировании научно обоснованных методов использования социальных сетей в противодействии как киберпреступности, так и преступности традиционной.

1.2. Особенности социальной сети как особого места совершения преступления

Вызывает опасение, что огромный технический потенциал и без граничные возможности Интернет все чаще в современных условиях могут быть использованы в преступных целях. При этом Интернет, с одной стороны, позволил более эффективно и безнаказанно совершать ранее существовавшие традиционные преступления, с другой – породил новые, неизвестные мировому сообществу еще совсем недавно виды общественно опасных посягательств. Глобальная сеть в последние годы стала использоваться не только для совершения общеуголовных преступлений, но и крайне опасных деяний международного значения – таких как «Интернет экстремизм», что создает угрозу безопасности целых государств и всего мирового сообщества.

Повышенный интерес преступников к Интернету не случаен. Его уникальность состоит в том, что он не находится в ведении конкретного физического или юридического лица и даже отдельного государства. Здесь практически отсутствуют действенные формы контроля за информационными потоками, что открывает неограниченные возможности для доступа к ним, и они все шире используется в криминальной деятельности.

Любое преступление, вне зависимости от того, совершено ли оно в прошлом, совершается сейчас или совершится в будущем, всегда будет обладать неотъемлемой характеристикой – местом совершения преступления. Объективный характер преступления влечет обязательную необходимость его существования материальном мире. Вместе с тем, если преступление совершается при помощи использования социальной сети возникает закономерный вопрос: где это преступление было совершено?

Необходимость определения места совершения преступления продиктовано как материальным и процессуальным законодательством, так и криминалистическими рекомендациями по расследованию преступлений: место совершения преступления встречается как в уголовном законодательстве[1], уголовно-процессуальном[2], в криминалистической характеристике и криминальной ситуации. Место совершения преступления в совокупности со временем совершения преступления образуют пространственно-временных координаты преступления, вследствие чего они сами будучи элементами криминальной ситуации становятся объединительным началом, организовывая все элементы единую ситуацию[3].

Расследование преступлений, совершенных в пространстве социальных сетей требует не только исследовать признаки, образующие состав преступления, но и тщательного изучения следов преступления, позволяющих определить криминалистически значимую информацию относительно преступления, преступника, а также иные обстоятельства, которые, в том числе, могут быть связаны с преступным деянием косвенно, не существенные для его квалификации, но представляющие важность для расследования преступления, что лежит в основе криминалистической характеристики преступления, которая выступает в качестве основы методики расследования преступления[4].

Тем не менее, понятие криминалистической характеристики разными авторами трактуется по-разному, при этом некорректно говорить о

---

[1] См.: ст. 11 УК РФ

[2] См.: ст. 176 УПК РФ

[3] См.: Волчецкая Т.С. Криминалистическая ситуалогия: Монография. / Под ред. проф. Н.П. Яблокова. Москва; Калинингр. ун-т. - Калининград,1997. ст.76

[4] См.: Грушихина В.А. Криминалистическая характеристика преступлений, связанных с распространением материалов экстремистской направленности / Грушихина В.А. // Вестник Иркутского государственного технического университета. - 2015. - № 5. - С.372

истинности или ложности того или иного подхода, поскольку криминалистическая характеристика как система должна оставаться гибкой и подвижной, в следствии чего, представляется вредным для науки как попытки создания конечного перечня элементов криминалистической характеристики преступления для всех преступлений, содержащихся в Уголовном кодексе РФ, так и создавать неподлежащий корректированию универсальный перечень[1].

Профессором Р.С. Белкиным была предложена криминалистическая характеристика содержащая характеристику исходной информации, «совокупности данных о способе совершения, а также сокрытия преступления и его последствиях, личности лица, совершившего преступление, его вероятных мотивах и целях, личности потерпевшего преступления, а также других обстоятельствах совершения преступления, таких как обстановка, время и **место** совершения преступления»[2].

По мнению профессора Н.П. Яблокова, криминалистическая характеристика, включает в себя три основных элемента: криминалистические черты способа совершения преступления, типичные следственные ситуации (следственные ситуации включают в себя **место** совершения преступления) и характер информации, подлежащей выяснению[3].

Профессором В.Б. Веховым предложено включать в структуру криминалистической характеристики следующие данные: криминалистически значимые сведения о личности преступника, мотивации

---

[1] См.: Мартынов А.Н. Криминалистическая характеристика преступлений: проблема структурированности / Мартынов А.Н. // Вестник Южно-Уральского государственного университета. Серия: Право. - 2014. - № 2. - С.52

[2] См.: Белкин Р.С. Курс криминалистики: Криминалистические средства, приемы и рекомендации. В 3-х томах. Т. 3. - М.: Юристъ, 1997. - С. 68.

[3] См.: Яблоков Н.П. Криминалистика: природа, система, методологические основы. 2-е изд. М., 2009. С. 56.

и цели, типичных способах совершения преступления, предметах и **местах** посягательств, а также сведения о потерпевшей стороне[1].

При достаточном многообразии подходов к содержанию криминалистической характеристики заметно однозначное отнесение места совершения преступления к ключевым элементам криминалистической характеристики преступления. Она позволяет определить направление начальных мероприятии по расследованию таких преступлений, выступая в качестве первичной основы методики расследования преступления, используемой в ориентировочных целях как доследственной проверки по преступлениям экстремистской направленности, совершенных с использованием социальных Интернет-сетей, так и непосредственного расследования.

Немаловажным является место совершения преступления в контексте следственного осмотра места происшествия. Осмотр места происшествия считается одним из первостепенных следственных действий. Как первоначальное следственное действие он необходим в каждом случае, когда по обстоятельствам дела возникает предположение о том, что там могут быть обнаружены изменения в окружающей обстановке, вещественные доказательства, иные следы преступления. Их изучение дает возможность следователю установить характер события, а подчас форму вины субъекта, мотив преступления и др.[2]

---

[1] См.: Вехов, В.Б. Криминалистическая характеристика и совершенствование практики расследования и предупреждения преступлений, совершаемых с использованием средств компьютерной техники: автореферат дис. ... кандидата юридических наук: 12.00.09 / Вехов Виталий Борисович - Волгоград, 1995 С. 15

[2] См.: Бирюков С.Ю., Скориков Д.Г., Шинкарук В.М. Особенности расследования преступлений экстремистской направленности: учебное пособие / Бирюков С.Ю., Скориков Д.Г., Шинкарук В.М. - Волгоград: ВА МВД России, 2013. - С.40

Обычно под местом происшествия понимается помещение, хранилище, участок местности[1] в котором обнаружены предметы и/или следы (труп, кровь, следы взлома или иных механических повреждений, наркотические вещества, оружие и т.п.), указывающие на возможное совершение преступления. Место происшествия не полностью равнозначно месту совершения преступления. Так, местом происшествия может быть не только то место, где совершено преступление, но и то, где обнаружены различные следы, указывающие на его отношение к совершенному деянию. Это может быть место подготовки к преступлению или сокрытия преступления, вещественных доказательств и т.д.

В контексте социальных сетей совершение преступления при помощи сети Интернет закономерно оставит следы в самой глобальной сети[2], устройстве злоумышленника, потерпевшего.

На первоначальном этапе расследования преступления в условиях критического недостатка информации, её источниками могут быть сам потерпевший, его компьютерное устройство (поскольку само помещение, где устройство находится во многих случаях не представляет интереса с точки зрения криминалистически значимой информации) и непосредственно социальная сеть (в том числе при помощи устройства потерпевшего), в части, относящейся к расследуемому делу. Но характерной ситуацией возбуждения ненависти или вражды является полное отсутствие потерпевшего. При совершении данного преступления в той или иной социальной сети призыв,

---

[1] См.: Методические рекомендации по выявлению и расследованию преступлений, предусмотренных статьей 177 Уголовного кодекса Российской Федерации (злостное уклонение от погашения кредиторской задолженности)" (утв. ФССП России 21.08.2013 N 04-12) (ред. от 03.10.2016)

[2] См. об этом подробнее: Иванова Л.В., Пережогина Г.В. Цифровое пространство как место совершения преступления в условиях глобальных ограничений//Вестник Тюменского государственного университета. Социально-экономические и правовые исследования. 2020. Т. 6. № 4. С. 162.

как правило, носит обезличенный характер и направлен безотносительно конкретного человека. Разжигание ненависти направлено на целую расу, этнос, национальной конфессию и т.п., что полностью исключает саму возможность определения конкретного потерпевшего. Следовательно, нередки ситуации, в которых единственным источником информации выступает сама социальная сеть. В свою очередь, совершение преступления в социальной сети представляет существенный интерес с позиции криминалистической ситуалогии.

Ситуационный подход, будучи понятием многомерным, получил широкое распространение во множестве сфер общества. В своей сути он представляет собой разложение познаваемого события на составляющие его ситуации[1]. Для целей расследования критически важно правильно диагностировать такие ситуации с учетом объективных и субъективных факторов. Ситуационный подход оказался достаточно эффективным для совершенствования традиционных фундаментальных понятий криминалистической науки, включающих механизм преступления и криминалистическую характеристику преступления. Дихотомия криминальной и криминалистической деятельности также находит свое отражение в ситуационном моделировании. Ситуации, образуемые в ходе подготовки, совершения или сокрытия преступления, называются ситуациями преступной деятельности или криминальными ситуациями.

Классическая модель криминальной ситуации состоит из следующих элементов[2]:

1. Субъект преступления

---

[1] См.: Волчецкая Т. С. Ситуационный подход в обучении криминалистике // Вестник криминалистики. 2000. Вып. 1. С. 4.

[2] См.: Волчецкая Т.С., Осипова Е.В. Криминалистическое моделирование в уголовном судопроизводстве // Учебно-методическое пособие. Калининград, 2020. С.16

2. Объект преступления
3. Время совершения преступления
4. **Место совершения преступления**
5. **Средства совершения преступления**
6. Обстановка совершения преступления
7. Цель совершения преступления
8. Способ и механизм совершения преступления
9. Мотив совершения преступления
10. Результат преступного деяния

Фундаментальное значение места-времени совершения преступления также зафиксировано с ситуационной модели.

На заре становления ситуационного подхода в криминалистике с помощью места протекания криминальной ситуации осуществлялась дифференциация криминальных ситуаций по наличию или отсутствию строгой локализации в пространстве[1]: в жилых помещениях, населенных пунктах, дорогах – строгая локализация; вне жилого помещения, населенного пункта, на значительном расстоянии от дороги – отсутствие строгой локализации. Такой подход в полной мере удовлетворял запросам криминалистики и в значительной мере удовлетворяет сейчас. «Традиционные» преступления могут быть локализованы в пространстве. Тем не менее, возникает проблема локализации преступлений совершенных, посредством социальных сетей.

Разность архитектуры и функциональных особенностей социальных сетей приводит к необходимости учитывать, в зависимости от ситуации, в качестве места социальную сеть в целом, отдельные страницы, переписки и т.д. По аналогии со строгой локализацией «традиционных» преступлений

[1] См.: Волчецкая Т.С. Криминалистическая ситуалогия: Монография. / Под ред. проф. Н.П. Яблокова. Москва; Калинингр. ун-т. - Калининград,1997. Ст. 85-86

такие преступления также могут иметь или не иметь строгую локализацию уже в сети Интернет. Основными источниками идей экстремизма и ресурсами вербовки являются социальные сети. Именно в социальных сетях, в так называемых «закрытых группах», проводится идеологическая подготовка пользователей сети. Основной «мишенью» создателей этих групп являются молодые люди (наиболее активные пользователи социальных сетей), мигранты (социальный статус и положение в обществе зависят от окружения и среды, в которой они пребывают, оказавшись на территории нашей страны).

Некоторые группы умышленно делаются закрытыми, чтобы спровоцировать дополнительный интерес к ним. Вице-премьер Дмитрий Рогозин называет всевозможные онлайн-сервисы «элементом кибервойны», которая ведется, в том числе и против России. Социальные сети, блоги, сетевые форумы и пр. исполняют роль троянских коней, выступающих средством для получения доступа к персональным данным пользователей, манипулирования социальными массами. Вести контроль за социальными сетями более сложно по сравнению с другими Интернет-ресурсами. Администрация социальных сервисов не всегда в состоянии оперативно реагировать на появления киберэкстремистских групп. По оценкам различных исследовательских центров, самой распространенной среди молодежи в нашей стране является социальная сеть «Вконтакте». По заявлениям пресс-службы «Вконтакте», их представители плотно взаимодействует с правоохранительными органами в части, касающейся выявления и удаления экстремистских материалов в аккаунтах зарегистрированных пользователей. Однако, несмотря на достаточно широкое определение понятия экстремизма в уголовном кодексе РФ, публикуемые экстремистские материалы не всегда признаются экстремистскими в ходе экспертиз, либо о них становится известно

правоохранительным органам, когда эти материалы уже получили распространение. В случае необходимости деятельность той или иной группы, содержащей материалы экстремистской направленности, может быть приостановлена.

Сложность заключается в том, что в социальных сетях распространены группы ведущие «мягкую» пропаганду, которая в явном виде не нарушает правил социальных сетей и законодательства РФ. Еще одна сложность заключается во взаимодействии с зарубежными социальными сетями: данные социальные сети находятся вне поля российского законодательства, являясь открытой площадкой для публикации материалов экстремистской направленности.

Кроме того, транснациональный характер сети Интернет приводит к необходимости учитывать такие ситуации, когда полный доступ к ресурсу получен не может или значительно затруднен. Так, в сравнении с социальной сетью Facebook[1] социальная сеть «В контакте» может сотрудничать с правоохранительными органами России без значительных затруднений. Facebook в то же время является иностранной социальной сетью, контакт с которой в значительной степени затруднен. Вместе с тем, согласно данным исследовательской группы Mediascope охват сети Facebook в России составляет 5,3 млн человек, что несмотря на значительно меньший по сравнению с «В контакте» показатель, данная социальная сеть может представлять интерес в контексте противодействия преступности.

Выступая в роли «места» социальной интеракции между людьми, социальная сеть закономерно становится потенциальным местом совершения преступления.

В таком случае возникает закономерный вопрос о том, что может быть средством совершения таких преступлений. В криминалистической науке

[1] Заблокирована Роскомнадзором на территории Российской Федерации

средство совершения преступления рассматривается двояко. С одной стороны, под средством совершения преступления может пониматься все, что направлено на достижение преступного результата. С другой, стороны под средством понимаются предметы – объекты материального мира[1]. Более того, орудие оборудование или иное средство совершения преступления входит в число вещественных доказательств[2]. В таком случае, первым вариантом становится отнесение устройства, с которого осуществлялся выход в глобальную сеть к средству совершения преступления. Будучи оборудованием для выхода в глобальную сеть Интернет, такое устройство сохранит на себе следы выхода в виде cookie-файлов, log-файлов, медиаданных или метаданных.

Однако в условиях развития облачных технологий, технологий синхронизации устройств. Преступление может совершаться совокупностью действий, включающих использование нескольких устройств (мобильного телефона, персонального компьютера, планшета, ноутбука и т.д.) имеющих доступ к социальной сети.

Тогда целесообразным представляется обратить внимание не только на объекты материального мира, но и на цифровые объекты, которые могут быть размещены в социальных сетях. К числу таких объектов могут быть отнесены отдельные текстовые сообщения, фотографии или иллюстрации, видеозаписи или аудиозаписи. Следовательно, любые медиа объекты, будучи объектами цифровой среды могут считаться средствами совершения преступления.

Механизм совершения преступления с использованием социальных сетей в значительной степени отличается от механизма совершения

---

[1] См.: Хлус А.М. Средства совершения преступлений как элемент их криминалистической структуры / А.М. Хлус // Российское право: образование, практика, наука, 2018. № 1. - 112 с. - С. 24

[2] УПК РФ ст. 81

«традиционного» преступления. Такая специфика связана, прежде всего, с механизмом следообразования[1].

Преступления, совершенные с использованием компьютерных устройств неизменно связаны с образованием следов в программной сфере используемых устройств. Данные следы, в силу своей природы, не обладают всей совокупностью характерных особенностей «традиционных» материальных или идеальных следов[2]. Невозможность отнесения данных следов к идеальным очевидна, поскольку носителем идеальных следов может быть только человек.

Соответственно, информация предстает не в виде образов или воспоминаний, а в виде двоичного кода, фиксируемого на материальном носителе того или иного вида. Кроме того, такие особенности как подверженность воздействию субъективных факторов тоже не может быть отнесена к цифровым следам, поскольку воздействие таких факторов возможно исключительно на мыслящий объект.

Следовательно, компьютер или иное техническое устройство исключает субъективные факторы воздействия. Тем не менее, возникает необходимость в средствах воспроизведения для получения информации из цифровых следов. Как необходимо воспроизведение мыслей и образов человеком в вербальной или иных формах, так и воспроизведение цифровых следов требует технических устройств, которыми могут являться как сами носители, так и устройства считывания, непосредственное изучение виртуальных следов не представляется возможным. Однако, в соотношении цифровых следов и следов материальных, в криминалистической науке

---

[1] См. об этом подробнее: Мещеряков В.А., Цурлуй О.Ю. Криминалистические особенности получения компьютерной информации с цифровых носителей при производстве отдельных следственных действий // Эксперт-криминалист. 2020. № 2. С. 16.

[2] См. об этом подробнее: Мещеряков В.А. Следы цифрового века//Вопросы экспертной практики. 2019. № S1. С. 426

мнение ученых разделилось: с одной стороны, такие следы определяются как вид материальных следов, с другой – выдвигаются предположения о необходимости выделения данных следов в отдельный вид, который может быть назван как «виртуальные следы»[1], «цифровые следы»[2], «компьютерные следы», «компьютерно-технические следы», или «бинарные следы».

«Невидимость» как характеристика цифровых следов является неоспоримой, но тем не менее возникает вопрос в возможности отнесения таких невидимых следов к материальным невидимым следам. Тогда возникает необходимость определить, к какому виду материальных следов можно отнести цифровые.

Объективный характер цифровых следов, в понимании следов материальных, тоже отличен, поскольку в них существует доля субъективной природы, так как они зависят от способов считывания, а также не имеют жесткой связи с устройством, осуществившим запись информации, что ведет к тому, что такая информация проще поддается фальсификации или повреждению вследствие ошибок считывания или записи, переформатирования.

В частности, при изменении системного времени устройства, время, регистрируемое файлами при их создании или изменении, будет соответствовать не реальному времени, а тому, которое указано в системе и было изменено. Поэтому при определении временных характеристик цифрового объекта необходимо учитывать возможность изменения пользователем системного времени компьютерного устройства[3], что может

---

[1] См.: Мещеряков В.А. «Виртуальные следы» под «скальпелем Оккама»//Информационная безопасность регионов. 2009. № 1 (4). С. 35

[2] См. об этом подробнее: Россинская Е.Р., Рядовский И.А. Концепция цифровых следов в криминалистике // Аубакировские чтения: материалы Международной научно-практической конференции (19 февраля 2019 г.). Алматы, 2019. С. 7.

[3] См.: Григорьев А.Н., Мешков В.М. Получение информации о времени при работе с электронными следами / Григорьев А.Н., Мешков В.М. // Вестник

привести к сложностям в определении временных характеристик исследуемой компьютерной информации.

Следовательно, цифровые следы, в силу своей природы, целесообразно выделять как новый вид следов наравне с материальными и идеальными следами. «Цифровые следы - следы совершения любых действий (включения, создания, открывания, активации, внесения изменений, удаления) в информационном пространстве компьютерных и иных цифровых устройств, их систем и сетей»[1]. Цифровой след может состоять из большого количества отдельных информационных элементов, которые могут быть записаны как на одном, так и на нескольких физических носителях цифровой информации, подключенных как к одному, так и нескольким компьютерам (компьютерным устройствам), объединенным в вычислительную сеть[2].

В таком случае, если рассматривать цифровые следы преступлений как отдельный вид следов, целесообразно выделить характерные отличительные черты, которые позволят разграничить те или иные следы по данным видам. Основой такого разграничения, исходя из виртуальной природы данных следов, будет их цифровой характер.

Социальная сеть как ресурс глобальной сети Интернет закономерно будет содержать в себе цифровые следы совершения преступления. Вместе с тем если объективная сторона преступления может быть реализована в цифровом пространстве достаточно сложно определить фактическое место совершения преступления[3]. К числу таких преступлений можно отнести[1]:

калининградского филиала санкт-петербургского университета МВД России. - 2017. - № 2 (48). - С. 10

[1] См.: Смушкин А.Б. Виртуальные следы в криминалистике / А.Б. Смушкин // Законность. - 2012. - N 8. - С. 43.

[2] См.: Шевченко Е.С. О криминалистической трактовке понятия "киберпреступность" / Е.С. Шевченко // Информационное право. - 2014. - N 3. - С.15

[3] См. об этом подробнее: Славин В. Е. О некоторых вопросах определения места предварительного расследования киберпреступлений / В. Е. Славин, В. О. Головизин, М. В. Сапсай // Наука и бизнес: пути развития. – 2019. – № 12(102). – С. 275–277.

1. Преступления, связанные с экстремистской и террористической деятельностью;
2. Преступления против свободы, чести и достоинства личности;
3. Общественно опасные деяния, связанные с незаконным оборотом наркотических средств и психотропных веществ;
4. Преступления, связанные с незаконным распространением порнографических материалов;
5. Вымогательство;
6. Нарушение неприкосновенности частной жизни и тайны переписки;
7. Интернет-мошенничество.

В таких условиях возникает определенная сложность с обнаружением места совершения преступления. Без непосредственного контакта, в ситуации, когда потерпевший и злоумышленник могут находиться не на разных улицах, а на разных континентах, они могут никогда не пересекаться в пространстве.

Как было замечено ранее место совершения преступления — это описанная в законе конкретная территория или помещение, где совершается преступление. Такой подход в полной мере соответствует пониманию места как части пространства. Социальная сеть, как страница сети Интернет, расположена на одном из множества серверов и технически является компьютерной информацией – совокупностью электрических сигналов, не является и никогда не может являться частью пространства.

В такой ситуации возможно выделить следующие варианты места совершения преступления:

---

[1] См.: Соловьев В.С. Преступность в социальных сетях интернета (криминологическое исследование по материалам судебной практики) // Криминологический журнал Байкальского государственного университета экономики и права. - 2016. - Т. 10, № 1. - С. 61-70

- Местоположение сервера, на котором хранятся данные социальной сети.

- Местоположение потерпевшего

- Местоположение злоумышленника,

Наиболее предпочтительным и логичным, на первый взгляд, представляется определение места совершения преступления по месту, где физически находится социальная сеть – сервер. Однако в связи с масштабами современных социальных сетей представляется невозможной непосредственная работа с сервером и его поиск. Так, количество серверов социальной сети «ВКонтакте» превышает десять тысяч. Кроме того, поиск серверов не имеет практического значения, поскольку совершение преступления в пространстве социальной сети образует следовую картину, состоящую из цифровых следов, для изучения которых отсутствует необходимость в непосредственной работе с сервером[1]. Разумеется, не будет по местоположению сервера и других следов, поскольку ни злоумышленник, ни потерпевший там находиться не могли.

Местоположение потерпевшего от вымогательства в социальной сети, мошенничества или иного преступного деяния на момент совершения преступления может содержать информацию о преступном результате или следы реализации объективной стороны преступления. Однако поскольку взаимодействие людей в социальной сети происходит опосредовано, через аккаунты, доступ к которым может осуществляться независимо от устройства (информация храниться на серверах социальной сети), местоположение потерпевшего на момент совершения преступления не содержит никакой информации о преступлении, которая не может быть

[1] См. об этом подробнее: Иванова Л.В., Пережогина Г.В. Цифровое пространство как место совершения преступления в условиях глобальных ограничений//Вестник Тюменского государственного университета. Социально-экономические и правовые исследования. 2020. Т. 6. № 4. С. 162.

получена удаленно. Немаловажно отметить, что существенной особенностью, к примеру, преступлений экстремистской направленности в пространстве социальных сетей является проблема определения личности потерпевшего. При совершении преступления в пространстве социальной сети экстремистские материалы, как правило, носят обезличенный характер, направленный не на конкретного человека, но на расу, этнос, национальной или конфессию[1]. Что в принципе исключает возможность определения конкретного потерпевшего.

В ходе взаимодействия злоумышленника с компьютерной техникой образуются как материальные следы физического контакта, так и цифровые следы действий внутри системы используемого устройства. Однако находясь за компьютерным устройством, злоумышленник совершает действия, следы которых распределяются по множеству объектов, не связанных с его местоположением. Такими объектами являются его страница в социальной сети, страница группы или другого лица, где реализовывалась объективная сторона преступления, промежуточные узлы, система провайдера Интернет-соединения[2].

Вместе с тем, важно отметить, что многие современные компьютерные устройства характеризуются портативностью, к числу таких устройств относятся и смартфоны. В таком случае преступление может быть совершено из любой точки, плоть до общественного транспорта. Лицо, использующее компьютерное устройство для совершения преступления может как находиться в видимости третьих лиц, так и нет, тем не менее, внешняя

---

[1] См. об этом подробнее: Блинова, О. А. Религиозный киберэкстремизм: причины и способы борьбы с ним / О. А. Блинова // Религия и общество - 12 : сборник научных статей, Могилев, 12–17 марта 2018 года / Под общей редакцией В.В. Старостенко, О.В. Дьяченко. – Могилев: Могилевский государственный университет имени А.А. Кулешова, 2018. – С. 130.

[2] См.: Введенская О.Ю. Особенности следообразования при совершении преступлений посредством сети Интернет // Юридическая наука и правоохранительная практика. - 2015. - № 4. - С. 209-216

неотличимость преступных и непреступных действий без наблюдения за экраном устройства нивелирует целесообразность обозначения таких лиц в качестве очевидцев.

Кроме того, на момент начала расследования, когда осмотр места происшествия критически важен, отсутствует какая-либо информация за исключением, находящейся в социальной сети, вследствие чего, осмотр места нахождения злоумышленника не представляется возможным.

В таком случае, ни одна из представленных альтернатив не имеет практической пользы.

Проведение следственных действий и оперативно-розыскных мероприятий в социальной сети неразрывно связано с проблемами их законодательного регулирования[1]. В уголовно-процессуальном законодательстве предусмотрено проведение осмотра места происшествия, местности, жилища, иного помещения, предметов и документов, вследствие чего достаточно сложно определить, чем будет являться осмотр социальной сети как интернет-страницы.

Немаловажной особенностью совершения преступления в социальной сети является механизм сокрытия самого злоумышленника, поскольку одной из особенностей действий в пространстве является именно их непрямой характер, сопряженный с обезличенностью и анонимностью[2].

Наиболее простым способом сокрытия в социальной сети является использование псевдонимов, сопряженное с публикацией не

[1] См. об этом подробнее: Кот Е.А. Особенности проведения осмотров по делам, связанным с побуждением в сети Интернет несовершеннолетних к совершению самоубийства /Е.А. Кот // Вестник Сибирского юридического института МВД России. – 2021. – № 3. – С. 182.

[2] См.: Гармаев Ю.П. Противодействие уголовному преследованию по уголовным делам о киберпреступлениях и средства его преодоления: проблемы теории и дидактики // В сборнике: Цифровые технологии в юриспруденции: генезис и перспективы. Материалы I Международной межвузовской научно-практической конференции. 2020. С. 34

соответствующих действительности данных о себе или не публикацией данных вообще.

Вместе с тем необходимо указать, что нередки преступные действия с использованием личных аккаунтов, без использования псевдонимов[1].

Специфика совершения преступления посредством социальной сети приводит к изменению ситуационной модели преступления: сеть выступает как место совершения преступления, в то время как средствами будут являться как объекты материального мира – компьютерные устройства, которые использовались для доступа к сети Интернет, так и цифровые объекты, посредством которых осуществлялась преступная деятельность непосредственно в сети. С одной стороны, будучи местом совершения преступления она содержит значительное количество криминалистически значимой информации в виде цифровых следов. Определить физическое местонахождение данных следов не представляется возможным, более того, не представляется целесообразным. Хранение информации на удаленных серверах, позволяют также удаленно такую информацию получать. С другой стороны, совершение преступления с использованием социальной сети приводит к возможности использования самой архитектуры и функциональных возможностей социальной сети. В частности, сокрытие преступления, или самого преступника происходит не только и столько в социальной сети (необходимо найти злоумышленника в реальности), сколько с непосредственным ее использованием дополнительных цифровых средств. Кроме того, в преступлениях, построенных по типу взаимодействия «человек-человек» инструментарий социальной сети становится средством взаимодействия между злоумышленником и жертвой, благодаря чему она может сохранить информацию о местонахождении устройств злоумышленника и жертвы.

[1] См.: Приложение 1

В отношении данных преступлений целесообразно расширительно толковать место происшествия, включая в него цифровое пространство и социальные сети, в частности. Именно в этом цифровом пространстве будет находиться интересующая следствие информация в виде переписки, опубликованных материалов, лог-файлов, IP-адресов.

1.3. Ситуационная обусловленность использования социальных сетей в процессе расследования преступлений

Развитие Интернет-технологий и социальных сетей, в частности, открывают перед экстремистами новые возможности по осуществлению пропаганды ксенофобских идей, вербовки в свои ряды или осуществления координации действий. Идеи ненависти наиболее часто находят свое воплощение не в форме митинга или демонстрации, не в форме листовок или плакатов. Самиздат экстремистской литературы был вытеснен материалами цифрового характера. Использование сети Интернет не только позволяет распространять экстремистскую идеологию без затрат на создание книг, плакатов или листовок. Способность компьютерных данных к свободному копированию приводит к невероятной скорости и масштабам перемещения информации в киберпространстве, благодаря чему использование сети Интернет становится опаснее использования «традиционных» методов распространения экстремистских идей.

Отмечается, что насильственные преступления по экстремистским мотивам до 90% случаев носят спонтанный характер[1], однако высокая доля таких преступлений совершается под влиянием чтения экстремистских информационных материалов и литературы[2], размещенных в пространстве сети Интернет.

---

[1] См.: Давыдов В.О. Информационная модель преступления как инструмент формирования криминалистической методики расследования (на примере исследования статистических зависимостей между элементами преступлений экстремистской направленности) // Известия Тульского государственного университета. Серия «Экономические и юридические науки». Выпуск 1. Ч. II. Юридические науки. Тула: Изд-во ТулГУ. 2012. с. 173

[2] См.: Приложение 1

Социальные сети, блоги, сетевые форумы и пр. исполняют роль троянских коней, выступающих средством для получения доступа к персональным данным пользователей, манипулирования социальными массами. Вести контроль за социальными сетями более сложно по сравнению с другими Интернет-ресурсами. Администрация социальных сервисов не в состоянии оперативно реагировать на появления киберэкстремистских групп. По оценкам различных исследовательских центров, самой распространенной среди молодежи в нашей стране является социальная сеть «Вконтакте». По заявлениям пресс-службы «Вконтакте», их представители плотно взаимодействует с правоохранительными органами в части, касающейся выявления и удаления экстремистских материалов в аккаунтах зарегистрированных пользователей.

Следовательно, в качестве одной из первопричин насильственных действий становится совершение экстремистского преступления посредством компьютерных сетей. Понятие экстремистской деятельности в законодательстве размыто, вследствие чего Федеральным законом «О противодействии экстремистской деятельности» она определяется через совокупность определенных действий.

Как уже указывалось ранее общественно опасные деяния, совершаемые при помощи компьютерных технологий, можно условно разделить на две группы: деяния, связанные с взаимодействием человека и техники, и деяния, связанные с организованным при помощи технических средств взаимодействием человека с человеком (группой людей)[1]. Рассматриваемые нами деяния относятся ко второй группе, где социальные выступают в качестве места социального взаимодействия. Данная группа

[1] См. об этом подробнее: Соловьев В.С. Преступность в социальных сетях интернета (криминологическое исследование по материалам судебной практики) // Криминологический журнал Байкальского государственного университета экономики и права. 2016. Т. 10, № 1. С. 61

преступлений характеризуется, в том числе, необходимостью определения уровня коммуникации: межличностного (человек - человек), контакт-коммуникационного (человек - группа) и масс-коммуникационного (человек - общество), необходимого для квалификации деяния и назначения наказания.

Так, ситуация общения посредством переписки в социальной сети является примером межличностного взаимодействия, в котором закономерно отсутствует признак публичности, характерный для некоторых из рассматриваемых преступлений. Однако, функциональные возможности социальных сетей предполагают осуществление массовой рассылки однотипных сообщений на контакт-коммуникационном и масс-коммуникационных уровнях, при условии, что каждое отдельное сообщение остается на уровне межличностного общения. Что требует выявления закономерных связей между различными элементами криминальных ситуаций посредством ситуационного анализа[1].

Особая роль ситуационного подхода позволяет дифференцировать все многообразие ситуаций, возникающих как в процессе преступной, так и в процессе правоприменительной деятельности, и на этой основе разрабатывать рекомендации технического, тактического и методического порядка в целях решения задач уголовного судопроизводства.

В криминалистическом знании следственная ситуация рассматривается как «… степень информационной осведомленности следователя о преступлении, а также состояние процесса расследования, сложившееся на любой определенный момент времени, анализ и оценка которого позволяют

[1] См. также: Волчецкая Т.С., Кот Е.А. Криминалистический анализ использования Интернет-ресурсов как места и средства побуждения несовершеннолетних к суициду // Известия Тульского государственного университета. Экономические и юридические науки. 2020. № 3. С. 3–10.

следователю принять наиболее целесообразное по делу решение»[1]. При этом в качестве основных составляющих ситуации, предопределяющих ее содержание и формирование, выделяют: психологический, информационный, процессуальный, тактический, материальный и организационно-технический компоненты[2].

В литературе справедливо отмечено, что правильная диагностика исходной ситуации, как правильно поставленный диагноз, позволяет, используя типовую криминалистическую характеристику преступлений, ликвидировать информационную неопределенность, правильно классифицировать ситуацию, которая обусловливает методологию работы в этой ситуации[3].

Любое преступление может быть разложено на криминальные ситуации, которые могут отражаться как в материальных следах, остающихся на месте происшествия, так и в мысленных образах участников события преступления, так в называемых идеальных следах. Выявление названных следов помогает следователю мысленно воссоздать криминальные ситуации, а на этой основе позже мысленно «воссоздать» механизм расследуемого события в целом. В ходе расследования конкретного преступления ситуационный подход позволяет следователю построить динамичную модель преступного события и получить всю необходимую доказательственную информацию[4].

---

[1] См.: Волчецкая, Т. С. Криминалистическая ситуалогия: специальность 12.00.09 «Уголовный процесс» : диссертация на соискание ученой степени доктора юридических наук / Волчецкая Татьяна Станиславовна. – Москва, 1997. С. 39.

[2] См. подробней: Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р. Криминалистика: Учебник для вузов/Под ред. заслуженного деятеля науки РФ, проф. Р.С. Белкина. – 4-е изд., перераб. и доп. – М.: Издательство НОРМА, 2019. С. 503.

[3] Зорин Г. А. Теоретические основы криминалистики. Минск, 2000. С. 65.

[4] См. об этом подробнее: Волчецкая Т.С. Криминалистическая ситуалогия: современное состояние и перспективы // Ситуационный подход в юридической науке и практике: современные возможности и перспективы развития: мат-лы междунар.

Все случаи рассматриваемых преступлений можно условно подразделить на две группы:

1. ситуации, когда экстремистский смысл сообщения никак не скрывается, а разжигающие ненависть и вражду призывы и сведения иди другие экстремистские идеи провозглашаются прямо и открыто, в связи с чем они воспринимаются одинаково всеми субъектами;

2. ситуации, когда смысловая направленность высказываний носит закамуфлированный характер, поэтому нуждается в установлении и выявлении.

В таком случае возникают сложности с определением самого факта возбуждения ненависти или вражды.

Такие уловки достаточно точно охватываются классификацией, подготовленной в рамках исследовательского проекта "Язык вражды" А.М. Верховским, которая включает три языковые группы[1]:

1. Жесткий язык вражды, заключающийся в:

– прямых и непосредственных призывах к осуществлению насильственных действий;

– общие лозунги, своей целью ставящие призыв к насилию;

– призывы к дискриминации в прямой и непосредственной форме;

– общие лозунги, призывающие к насильственным действиям;

– призывы к насилию и дискриминации в завуалированной форме.

2. Средний язык вражды, включает в себя:

науч.-практ. конф., посвященной 15-летию научной школы криминалистической ситуалогии / под ред. Т.С. Волчецкой. Калининград: Изд-во БФУ им. И. Канта, 2017. С. 13

[1] См. об этом подробнее: Верховский А.М. Язык мой... Проблема этнической и религиозной нетерпимости в российских СМИ / Сост. А.М. Верховский. - М.: РОО "Центр "Панорама", 2002. С.42-43

– действия, направленные на оправдание случаев насилия и дискриминации в истории;

– выражение сомнения в общепризнанных исторических фактах насилия и дискриминации;

– позиционирование той или иной этнической или религиозной группы как виновных в преступлениях прошлого;

– попытка дискредитации этнических и религиозных групп, заключающаяся в связывании с российскими и иностранными политическими и государственными структурами;

– утверждения предрасположенности к совершению преступлений той или иной этнической или религиозной группы;

– рассуждения о несправедливом превосходстве той или иной этнической или религиозной группы в финансовом благополучии, представительстве во властных структурах, прессе и т.д.;

– обвинение той или иной этнической или религиозной группы в негативном влиянии на общество, государство (в частности, в "размывании национальной идентичности");

– призывы не допустить закрепление в регионе (районе, городе и т.д.) мигрантов, принадлежащих к той или иной этнической или религиозной группе.

3. Мягкий язык вражды заключается в:

– создании негативного образа той или иной этнической или религиозной группы;

– упоминании в уничижительном контексте названия этнической или религиозной группы;

– утверждении о неполноценности, заключающейся в недостатке культурности, интеллектуальных способностей, неспособности к

созидательному труду той или иной этнической или религиозной группы как таковой;

– утверждении о моральной неполноценности той или иной этнической или религиозной группы;

– упоминании представителей этнической или религиозной группы, или группу в целом в оскорбительном или унизительном контексте;

– цитировании экстремистских высказываний и текстов.

Благодаря такому разделению возможных языковых средств возбуждения вражды становится возможным определения характера действия при расследовании преступлений. Особого внимания заслуживают вторая и третья группа. Средний и мягкий язык вражды закономерно влечет необходимость привлечения специальных знаний, прежде всего в форме лингвистических или комплексных экспертиз с участием психологов, религиоведов и т.д.

Раскрытие и расследование преступлений, экстремистской направленности, совершенных с использованием социальных сетей, является сложной задачей для большинства сотрудников правоохранительных органов. Это обусловлено, во-первых, «виртуальным» характером среды совершения преступлений подобного рода, трудностями выявления и доказывания факта распространения экстремистских материалов в сети интернет; во-вторых, отсутствием обобщений материалов следственной и судебной практики, методических рекомендаций по организации расследования данного вида преступлений. Ситуационный подход играет большую роль в упрощении процесса анализа и мысленной реконструкции следователем элементов расследуемого преступления.

Как любая другая среда человеческой деятельности социальная сеть обладает способностью хранить в себе информацию о человеке, его следы[1].

Вместе с тем, при более подробном анализе экстремистских преступлений в пространстве социальных сетей можно столкнуться со сложностями в обнаружении как материальных, так и идеальных следов, необходимых для построения ситуационной модели преступления. Глобальное информационное пространство, информационная среда социальных сетей нематериальны и по сути своей несводимы к физическому носителю, в котором воплощены[2]. Следовательно, любая ситуация преступления экстремистской направленности в социальной сети связана с острым недостатком материальных следов[3]. Разумеется, в ходе взаимодействия лица с компьютерной техникой образуются как материальные следы физического контакта, так и следы действий внутри системы используемого устройства, вместе с тем, важно отметить, что многие современные компьютерные устройства характеризуются портативностью, к числу таких устройств, с помощью которых возможно осуществлять выход в Интернет и, соответственно, возможно совершить преступление экстремистского характера относятся и смартфоны. В таком случае размещение экстремистских материалов можно совершить из любой точки, плоть до публикации во время перемещения в общественном транспорте.

---

[1] См. об этом подробнее: Григорьев А. Н. Получение информации о времени при работе с электронными следами / А. Н. Григорьев, В. М. Мешков // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. – 2017. – № 2(48). – С. 10.

[2] См. : Иванова Л.В., Пережогина Г.В. Цифровое пространство как место совершения преступления в условиях глобальных ограничений//Вестник Тюменского государственного университета. Социально-экономические и правовые исследования. 2020. Т. 6. № 4.

[3] См. об этом подробнее: Давыдов В.О., Головин А.Ю. Значение виртуальных следов в расследовании преступлений экстремистского характера // Известия Тульского государственного университета. Экономические и юридические науки. 2016. № 3-2. С. 254-259.

Вместе с тем аналогичная проблема связана и с идеальными средами, поскольку лицо, использующее компьютерное устройство для совершения преступления может как находиться в видимости третьих лиц, так и нет, тем не менее, внешняя неотличимость преступных и непреступных действий без наблюдения за экраном устройства нивелирует целесообразность обозначения таких лиц в качестве очевидцев, что практически исключает возможность исследования идеальных следов.

«Виртуальный» характер таких преступлений в полной мере оправдывает необходимость рассматривать цифровые среды[1] - следы совершения любых действий (включения, создания, открывания, активации, внесения изменений, удаления) в информационном пространстве компьютерных и иных цифровых устройств, их систем и сетей»[2].

[1] См.: Иванова Л.В., Пережогина Г.В. Цифровое пространство как место совершения преступления в условиях глобальных ограничений//Вестник Тюменского государственного университета. Социально-экономические и правовые исследования. 2020. Т. 6. № 4.

[2] См.: Смушкин А.Б. Виртуальные следы в криминалистике // Законность. 2012. N 8. С. 43

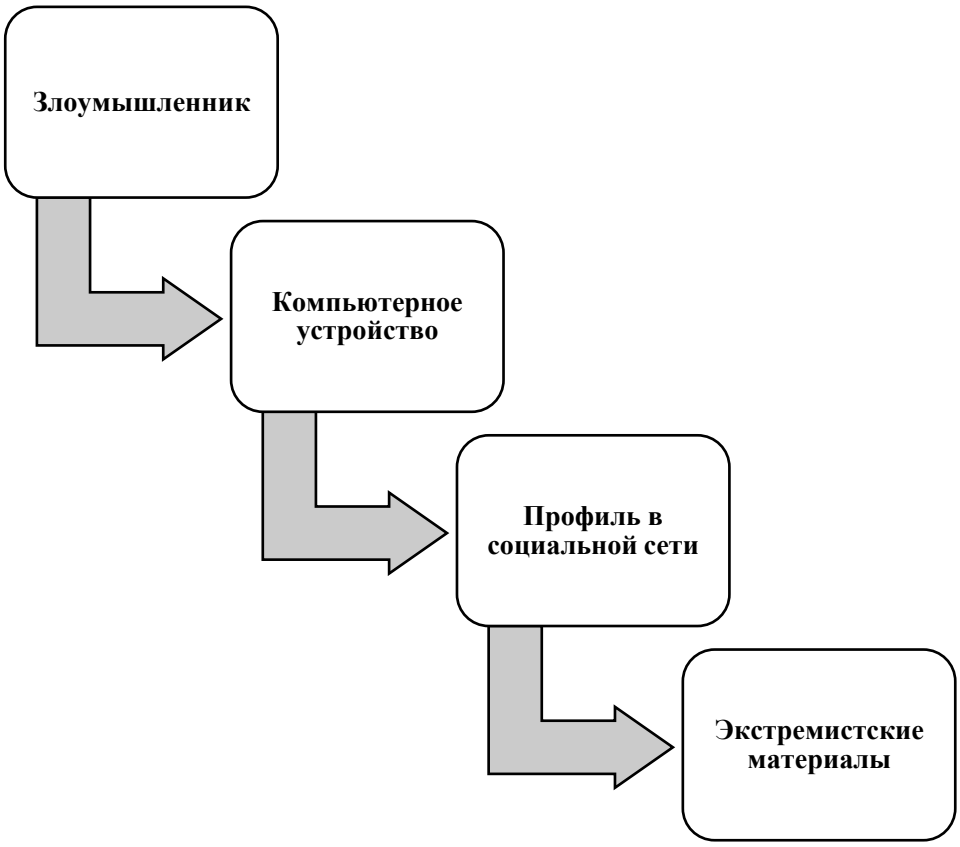

Рис. 1. Схема связи между злоумышленником и экстремистскими материалами в социальных сетях

Специфика использования социальной сети влияет на общую модель совершаемого преступления, в «традиционном» преступлении перед следователем стояла задача определить связи между преступником и экстремистскими материалами, аналогичная задача в случае использования социальных сетей претерпевает существенные усложнения. Так, возникает необходимость установить связь между материалом и профилем ее опубликовавшим, что является наиболее простым из рассматриваемой модели, поскольку в большинстве социальных сетей публикация осуществляется от имени профиля в социальной сети. Далее необходимо установить связь профиля в социальной сети и компьютерного устройства с которого осуществлялся доступ к профилю, чтобы в дальнейшем установить связь между устройством и непосредственно злоумышленником.

Такое усложнение связано, прежде всего, с возможностью несанкционированного доступа, как к профилю, так и устройству третьими лицами[1]. Ситуация требует доказательств исключительного доступа подозреваемого к профилю и устройству. Как правило, такая проблема решается путем соотнесения IP-адресов, с которых осуществлялся доступ к профилю и которыми пользовалось лицо. Вместе с тем социальные сети предоставляют свободную анкету профиля в социальной сети, что позволяет использовать как псевдоним, так и имитировать профили третьих лиц.

В исследовании профессора В.О. Давыдова. уже был представлен перечень исходных следственных ситуаций уголовных дел о преступлениях экстремистской направленности, совершенных с использованием компьютерных сетей, основанный на имеющихся сведениях о причинах возникновения общественно опасного деяния, способе его совершения и личности преступника[2].

Полностью соглашаясь с выводами уважаемого профессора В.О. Давыдова в отношении компьютерных сетей, считаем необходимым выделить социальные сети в особое место ситуационной модели преступлений экстремистской направленности. Так, особый характер социального взаимодействия в пространстве социальных сетей, рассмотренный нами ранее, «личный» характер профиля в социальных сетях приводит к необходимости учитывать новые характерные черты преступлений экстремистской направленности. Способ совершения преступления в социальных сетях, с одной стороны, всегда известен – это

---

[1] См. об этом подробнее: Марков, А. С. Руководящие указания по кибербезопасности в контексте ISO 27032 / А. С. Марков, В. Л. Цирлов // Вопросы кибербезопасности. – 2014. – № 1(2). – С. 30.

[2] См.: Давыдов, Владимир Олегович. Информационное обеспечение раскрытия и расследования преступлений экстремистской направленности, совершенных с использованием компьютерных сетей : диссертация ... кандидата юридических наук : 12.00.12 / Давыдов Владимир Олегович; [Место защиты: Рост. юрид. ин-т МВД РФ].- Тула, 2013.

использование интерфейса социальной сети для размещения сообщений публично или приватно. С другой стороны, информации об устройстве и местоположении злоумышленника на момент обнаружения преступления нет и быть не может. Отсутствует информация о средствах сокрытия личности в сети, способах подключения.

Публично направленный характер рассматриваемых преступлений исключает механизм сокрытия самого преступления, в данном случае необходимо рассматривать механизм сокрытия самого злоумышленника, поскольку одной из особенностей действий в пространстве является именно их непрямой характер, сопряженный с обезличенностью и анонимностью.

В таком случае, основой выделения исходных следственных ситуаций будет информация о личности преступника.

Если экстремистский характер публикации находит свое подтверждение, то исходными следственными ситуациями, возникающими перед субъектом проверки будут следующие[1]:

1. Установлен факт совершения преступления экстремистской направленности в социальной сети профиль социальной сети, использованный при совершении преступления, носит личный характер. (при публикации с личного аккаунта, без использования средств сокрытия)[2]

2. Установлен факт совершения преступления экстремистской направленности в социальной сети профиль социальной сети, использованный при совершении преступления, носит обезличенный характер. (при публикации с использованием псевдонима, использовании средств сокрытия IP-адреса)

---

[1] См.: Приложение 1

[2] В указанной ситуации необходимо учитывать, что наполнение профиля социальной сети информацией осуществляется непосредственно пользователем, в связи с чем существует возможность фальсификации информации профиля или существование «профилей-двойников»

В первом случае публикации с использованием личных аккаунтов, без использования псевдонимов, что в большей степени характерно для лиц, не состоящих в экстремистских группах, совершающих преступление в одиночку, такие лица, как правило, не обладают глубокими познаниями в области компьютерной техники и действуют без подготовки, по импульсу.

В данной ситуации установление связи между профилем социальной сети и лицом ее использовавшим существенно упрощается – достаточно исключить возможность доступа третьих лиц к устройству и профилю социальной сети.

Во втором случае наиболее простым способом сокрытия в социальной сети является использование псевдонимов, сопряженное с публикацией не соответствующих действительности данных о себе или не публикацией данных вообще. В таком случае установление связи между профилем в социальной сети и лицом, ее разместившим, требует использования специальных в области компьютерных технологий, для установления связи между адресом в сети Интернет, который был использован для доступа к социальной сети, непосредственно лица, этот доступ осуществившего.

Иным распространенным способом сокрытия личности, применяемых наряду с использованием псевдонимов является сокрытие IP-адреса[1]. Сокрытие IP-адреса может осуществляться следующими способами:

1. Использование прокси-сервера. Прокси-сервер выступая в качестве дополнительного звена в цепи связи компьютерного устройства злоумышленника и серверами Интернет-сети получает запрос от устройства и дублирует его на сервер но уже от своего IP-адреса, тем не менее, большая

[1] Гармаев Ю.П. Противодействие уголовному преследованию по уголовным делам о киберпреступлениях и средства его преодоления: проблемы теории и дидактики // В сборнике: Цифровые технологии в юриспруденции: генезис и перспективы. Материалы I Международной межвузовской научно-практической конференции. 2020. С. 29–35

часть прокси-серверов используют поле (x-forwarded-for) в котором отображается IP-адрес пользователя.

2. Использование анонимайзеров. Анонимайзер представляет собой прокси-сервер нацеленный именно на сокрытие IP-адреса. Он обладает собственным интерфейсом, через который осуществляется набор адресов сервера Интернет-сети.

3. Использование VPN подключений. Исходя из своего названия Virtual Private Network — виртуальная частная сеть, VPN представляет собой зашифрованную логическую сеть поверх сети Интернет, в данном случае. Отображается в сети будет адрес VPS – сервера, предоставляющего VPN-подключение.

4. Использование Socks-протокола. Socks-сервер принимает данные от устройства злоумышленника, отправляет их на сервера сети Интернет, а затем перенаправляет ответную информацию обратно. Принцип действия имеет схожесть с использованием прокси серверов, однако, канал связи пользователь - socks-сервер происходит не по общепринятым протоколам, а по специальным протоколам сервера (socks4, socks5 и т. д.). В результате передача IP-адреса полностью исключается.

В указанных условиях установление связи между профилем в социальной сети и лицом, ее разместившим дополнительно усложняется однократным или многократным изменением IP-адреса.

В исключительных случаях возникает нетипичная необходимость установить связь также между профилем в сети и публикуемыми материалами экстремистского характера.

Примером такой ситуации является автоматизированное размещение информации ботом из «предложки» (страница, на которую участники группы или социальной сети в целом, могут оправляет предложения для публикации) группы социальной сети.

В результате, необходимо также учитывать следующие ситуации:

- проникновения в систему с использованием чужих реквизитов идентификации и использования чужого профиля для публикации материалов экстремистского характера, в таком случае, устройство в которое было произведено проникновение отразит в Log-файлах реквизиты, использованные для проникновения, а также может быть индивидуализирован компьютер преступника, (IP-адрес, MAC-адрес сетевого оборудования, иная информация), с которого был произведен запрос на вход с чужими реквизитами, следовательно, имеет место доказательственная криминалистически значимая информация о событии преступления и о обстоятельства виновности обвиняемого (данные, отраженные в Log-файлах).

- использования вредоносных программ для удаленного доступа к информации для совершения преступления экстремисткой направленности, в таком случае, на устройстве, подвергнутом воздействию вредоносного ПО, останутся следы действия такого ПО, а также само вредоносное ПО, в некоторых случаях компьютерно-техническая экспертиза способна установить автора вредоносного ПО, что дает возможность установить вину обвиняемого, а следы действия вредоносного ПО позволяют определить событие преступления

Таким образом, типовые ситуации преступлений экстремистской направленности связаны, прежде всего, с доступностью информации «посредниках» в связях между экстремистскими материалами и злоумышленнике, в число которых входит связь «материал - профиль», «профиль - компьютерное устройство», «компьютерное устройство-злоумышленник». Вместе с тем каждая типовая ситуация таких преступлений обладает специфической следовой картиной нехарактерной для некомпьютерных преступлений.

ГЛАВА 2. ПРИКЛАДНЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ СОЦИАЛЬНЫХ СЕТЕЙ В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ

2.1. Тактика получения и использования информации из социальных сетей при взаимодействии следователя с органами, осуществляющими оперативно-розыскную деятельность

Своевременное и обоснованное возбуждение уголовного дела является одним из ключевых условий соблюдения принципа законности в уголовном процессе[1]. Уголовно-процессуальным законодательством установлено, что в каждом случае обнаружения преступления, руководитель следственного органа, следователь, дознаватель или орган дознания в пределах своей компетенции обязаны возбудить уголовное дело, принять все предусмотренные законом меры к установлению события преступления; лиц, виновных в совершении преступления[2].

Сущность подобного требования уголовно-процессуального закона, прежде всего, заключается в необходимости уменьшить временной промежуток между фактом совершения преступления и возбуждением уголовного дела. Значение такого подхода заключается, прежде всего, в том, что материальные следы, образовавшиеся в результате преступных действий, могут быть утрачены по прошествии времени в результате воздействия погоды, непосредственно самого злоумышленника, а также лиц, не имеющих намерение уничтожить следы, но при этом не также замечающих сами следы, либо не определяющих объекты в качестве следов,

---

[1] Копылова О.П. Проверка заявлений и сообщений о преступлениях: монография / Копылова О.П. // Тамбов: Изд-во Тамб. гос. техн. ун-та, 2010. - С.6

[2] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 27.10.2020) (Далее УПК) [Электронный ресурс]. Доступ из справ.-правовой системы «Консультант Плюс» Ст. 144

и, следовательно, действующие без умысла. Идеальные следы с течением времени имеют свойство сглаживаться в памяти очевидцев, что в дальнейшем препятствует либо исключает их использование в расследовании.

Другим фактором, связанным с временем между событием преступления и возбуждением уголовного дела, является возможность преступника скрыться, подготовить себе ложное алиби, избавиться от орудий преступления либо предметов, полученных в результате совершения преступления.

Длительный временной промежуток между преступлением и возбуждением уголовного дела имеет негативное влияние на общую и частную превенцию, поскольку лицо, совершившее преступление сохраняет возможность осуществлять преступную деятельность в дальнейшем, а безнаказанность преступления выступает стимулом для других действовать подобным образом.

В случае с преступлениями экстремистской направленности в пространстве социальных сетей необходимо обратить внимание на то, что у злоумышленника имеется возможность избавиться от использованного устройства, покинуть страну, предпринять меры по сокрытию собственного отношения к размещённым экстремистским материалам, удалив оригинал, распространенный в сети.

Вместе с тем, поскольку для преступлений в сети Интернет характерно в большей степени наличие виртуальных следов, важно отметить, что по прошествии времени у провайдера Интернет-связи может быть утрачена информация о подключениях, IP-адресах, использованных злоумышленником, а аккаунт, разместивший экстремистские материалы в сети удален, и удален кэш, позволявший увидеть информацию удаленного аккаунта.

Обнаружение преступлений экстремистской направленности в пространстве социальных сетей как правило происходит в результате[1]:

1. Проведения целевого мониторинга на предмет наличия материалов экстремистской направленности пространства социальных сетей (прежде всего русскоязычных), веб-страниц средств массовой информации, форумов и иных областей сети Интернет, на которых возможно и вероятно размещение экстремистских материалов сотрудниками правоохранительных органов.

2. Получении информации о преступлении от лиц, оказывающих правоохранительным органам содействие на основе конфиденциальности (конфидентов).

3. Получении информации в ходе проведения субъектами оперативно-розыскной деятельности оперативно-розыскных мероприятий.

4. Получении информации в ходе расследования преступления экстремистской направленности, совершенного без использования компьютерных устройств и выхода в сеть Интернет. (п. «л» ч. 2 ст. 105 УК РФ, п. «е» ч. 2 ст. 111 УК РФ, п. «е» ч. 2 ст. 112 УК РФ, п. «б» ч. 2 ст. 115 УК РФ, п. «б» ч. 2 ст. 116 УК РФ, п. «з» ч. 2 ст. 117 УК РФ, ч. 2 ст. 119 УК РФ)

5. При поступлении заявления в правоохранительные органы от физических и юридических лиц, представителей общественных организаций, депутатских запросов, а также обращений средств массовой информации.

6. При расследовании преступлений общеуголовной направленности, не связанных с экстремистской деятельностью.

---

[1] См. об этом подробнее: Давыдов В.О. О некоторых аспектах обнаружения признаков преступлений экстремистской направленности, совершаемых с использованием средств социальной компьютерной коммуникации, и принятия решений в стадии возбуждения уголовного дела / Давыдов В.О. // Актуальные проблемы российского права. - 2014. - № 9 (46). - С. 2009

В подавляющем большинстве случаев дела по преступлениям экстремистской направленности возбуждаются на основе результатов оперативно-розыскной деятельности и в дальнейшем их расследование осуществляется при активном оперативном сопровождении[1]. В связи с этим от качества результатов ОРД зависит как законное и обоснованное возбуждение уголовного дела о преступлениях указанного вида, так и успешное решение задач предварительного расследования.

Деятельность подразделений, осуществляющих ОРД, в стадии возбуждения уголовного дела можно рассматривать как взаимосвязанную последовательность трёх этапов:

1) выявление признаков преступления;

2) проверка полученной на предыдущем этапе информации;

3) оценка результатов проверки и принятие решения о представлении этих результатов следователю (важно отметить, что на последнем этапе может быть принято решение о недостаточности данных, указывающих на признаки преступления, вследствие чего принимается решение о возвращении ко предыдущему этапу деятельности оперативных подразделений).

При проведении мониторинга сети интернет и социальных сетей, в частности, целесообразно в качестве приоритетных областей проверок выбирать популярные сообщества, созданные по региональному принципу, группы региональных новостных агентств в социальных сетях, а также на персональные страницы пользователей, где место проживания указано в личных данных, либо регион проживания может быть установлено по фотографиям.

---

[1] См. об этом подробнее: Сумин А.А., Саморока В.А., Бекетов М.Ю. Практика расследования по уголовным делам экстремистской направленности: аналитический обзор / А.А. Сумин, В.А. Саморока, М.Ю. Бекетов // Под общ. ред. д.ю.н. А.А. Сумина. – М.: Московский университет МВД России. - 2013. - С.25

Необходимо отметить, что в случае, если пользователь аккаунта ограничил доступ к своей странице, то дальнейший мониторинг страницы не представляет оперативного интереса, поскольку факт закрытия альбомов, стены свидетельствует об отсутствии признака публичности образующего объективную сторону экстремистского преступления. Тем не менее, в отношении закрытых сообществ признак публичности[1], как расчёта на последующее ознакомление с информацией других лиц, соблюдается, поскольку информация в группе направлена на ознакомление с ней ограниченного круга лиц, что удовлетворяет критериям публичности.

В ходе доследственной проверки устанавливается содержание и назначение информации в Интернете, признание ее экстремистской, использованные злоумышленником при совершении преступления экстремистской направленности технические средства, принадлежность IP-адресов и доменных имен, устанавливается связь между использованными IP-адресами аккаунтом, с которого осуществлялось размещение экстремистских материалов[2].

При проведении доследственной проверки оперативно-розыскными подразделениями в следственные органы должны предоставляться сведения[3]:

1. где, когда, какие признаки и какого преступления обнаружены;
2. при каких обстоятельствах имело место их обнаружения;

---

[1] См.: О судебной практике по уголовным делам о преступлениях экстремистской направленности: постановление пленума Верховного Суда РФ от 28 июня 2011 г. N 11 (ред. от 20.09.2018) [Электронный ресурс]. Доступ из справ.-правовой системы «Консультант Плюс»

[2] См. об этом подробнее: Россинская, Е. Р. Учение о цифровизации судебно-экспертной деятельности и проблемы судебно-экспертной дидактики / Е. Р. Россинская // Правовое государство: теория и практика. – 2020. – № 4–1(62). – С. 88–101.

[3] См.: Валеев А. Х. Расследование преступлений, связанных с экстремистской деятельностью: Учебное пособие / А. Х. Валеев, А. Н. Данилко, А. В. Кудрявцев, В. Б. Поезжалов. – Уфа: УЮИ МВД России, 2015. – С.10

3. о лице, либо о лицах, совершивших преступление экстремистской направленности;

4. о свидетелях и очевидцах данного преступления;

5. о местонахождении предметов и документов, имеющих значение для дела.

Первой задачей при проведении доследственной проверки является определение характера размещенной информации. Определение характера размещённого материала, особенно в случае, если имеет место использование не жесткого языка вражды, а среднего или мягкого, зависит от результатов применения специальных знаний в виде лингвистической или комплексной лингвистической экспертизы с привлечением экспертов психологов, историков или религиоведов. При этом, необходимо отметить ключевую роль экспертизы в отнесении материалов к экстремистским[1].

В случае, если экстремистский характер публикации находит свое подтверждение, то имеет место быть факт самого преступления, в таком случае, перед субъектом проверки возникают следующие ситуации[2]:

1. Установлен факт совершения преступления экстремистской направленности в сети Интернет и субъект проверки располагает информацией о личности преступника. (при публикации с личного аккаунта, без использования средств сокрытия)

2. Установлен факт совершения преступления экстремистской направленности в сети Интернет, но субъект проверки не располагает информацией о личности преступника. (при публикации с использованием псевдонима и использовании средств сокрытия IP-адреса)

---

[1] См. об этом подробнее: 11. Постановление Пленума Верховного Суда РФ от 28.06.2011 N 11 (ред. от 28.10.2021) "О судебной практике по уголовным делам о преступлениях экстремистской направленности"// СПС «Консультант Плюс».

[2] См.: Валеев А. Х., Данилко А.Н., Кудрявцев А. В. Указ. соч. С.12

3. Установлен факт совершения преступления экстремистской направленности в сети Интернет, но субъект проверки не располагает информацией ни о личности преступника, ни о способе совершения преступления.

Поскольку сеть Интернет представляет собой особое пространство, именуемое киберпространством, целесообразно использование агентов, достаточно часто используемых при обеспечении противодействия «традиционным» преступлениям. Вместе с тем, такой агент носит виртуальный характер, что позволяет сотрудникам правоохранительных органов самим выступать в качестве агента, исключая посредника в получении информации, минимизируя возможность искажения, утечки или фальсификации информации. В таком случае, под «виртуальным агентом» следует понимать аккаунт в социальной сети, искусственную персону, используемую в оперативных целях.

«Виртуальный агент» выступает в качестве условного названия аккаунта, который может быть использован сотрудниками оперативных подразделений для внедрения в виртуальную среду и преодолении настроек приватности закрытых экстремистских и проэкстремистских групп, движений и организаций[1]. «Виртуальный агент» позволяет без посредников получить информацию по вербовке, планируемым акциям экстремистского толка, кругу лиц, причастных к деятельности организации, выходить на контакт с пользователями закрытых экстремистских сообществ. При создании «виртуального агента» необходимо выбрать социальные сети, форумы и иные Интернет-ресурсы, используемые лицами, причисляющими себя к проэкстремистским движениям, организациям и субкультурам. Наиболее часто данной категорией лиц используются социальные сети «В Контакте», «Одноклассники», создаются «закрытые» группы общения и

[1] См.: Мешалкин С. Н., Горностаева И. В., Федоткин А.И. Указ. соч. С. 26

переписки на Интернет-ресурсе «Skype», мессенджерах «Viber» и «WhatsApp», различные тематические форумы, а также Интернет-ресурсы, ориентированные на определенный регион. «Виртуальный агент» должен быть ориентирован на ту среду, в которую планируется его внедрение. При подборе контента для наполнения аккаунта должен использоваться фото-, аудио-, видеоматериал, который соответствует понятиям, пользуется популярностью и характерен к использованию в той или иной экстремистской среде. Так, при создании «виртуального агента» лица, причисляющего себя к националистической среде, необходимо подобрать фотографии лица славянской внешности, спортивного телосложения. Желательно, чтобы фотографий было несколько, и по ним невозможно было определить место фотосъемки, также должна соответствовать принятой и модной в националистической среде одежда[1].

«Виртуальные агенты», находясь в закрытых сообществах, обладают свободным доступом к внутренней переписке, к создаваемым «встречам», принимают рассылку о предстоящих мероприятиях. Наиболее важно, что в адрес этих конфидентов могут поступить предложения от радикально настроенных лиц о совершении акций экстремистского и террористического толка.

Использование глобальной сети Интернет как площадки для размещения экстремистских материалов влечет за собой необходимость мониторинга колоссальных объемов информации требует привлечения современных технологий и в оперативную деятельность, в том числе, использование компьютерных устройств и программных систем для автоматизации поиска таких материалов.

Так, на XX международной выставки средств обеспечения безопасности «Интерполитех-2016» в Москве был представлен аппаратно-

[1] См.: там же

программный комплекс "Фоб", разработанный по заявке Экспертно-криминалистического центра МВД России, представляющий собой компьютер с периферийным оборудованием и устройство ввода-вывода. Программное обеспечение включает в себя в том числе информационно-поисковую систему, предназначенную для поиска экстремистских материалов. Комплекс позволяет исследовать материалы содержащие текстовые сообщения, а также изображения, видеоряд, или звук, в том числе и в сочетании. Система может находить дубликаты ранее исследованных изображений, узнавать и отождествлять использованные символы, проводить проверку по стоп-кадрам, система оборудована средствами распознавания текста в изображении или видеозаписи. По данным МВД, комплекс "Фоб" в 2016 году прошел этап опытной эксплуатации и поставлен на снабжение территориальных экспертно-криминалистических подразделений[1].

Возможности автоматизированной проверки больших объемов информации в сети Интернет уже были продемонстрированы на практике.

Использование аппаратно-программных средств для автоматизации процесса поиска экстремистских материалов в пространстве социальных сетей позволяет в значительной степени облегчить мониторинг сети Интернет на предмет наличия таких материалов. Однако, необходимо учитывать необходимость соблюдения прав человека и гражданина при внедрении таких средств, в частности права на уважение частной и семейной жизни[2].

---

[1] См. об этом подробнее: МВД России создало робота для проверки публикаций на экстремизм [Электронный ресурс] – Режим доступа: https://ria.ru/society/20161018/1479503249.html – Загл. с экрана. (дата обращения: 20.05.2022)

[2] См.:Европейская конвенция по правам человека (измененная и дополненная Протоколами № 11 и № 14, в сопровождении Дополнительного протокола и Протоколов № 4, 6, 7, 12 и 13) // Официальный интернет-портал Европейского суда по

Так, Европейский суд по правам человека в деле Роман Захаров против России вынес единогласное решение о том, что Система технических средств для обеспечения функций оперативно-разыскных мероприятий (СОРМ) не удовлетворяет требованию о наличии «эффективных и адекватных гарантий против риска превышения полномочий и произвола, присущие каждой системе скрытого наблюдения, которые наиболее высоки в системе, предоставляющей специальным службам и правоохранительным органам прямой доступ с использованием специальных аппаратных средств к любому сообщению на мобильном телефоне» [1].

Оперативно-розыскная длительность в пространстве компьютерных сетей связана с необходимостью проведения оперативно-розыскных мероприятий в киберпространстве для обнаружения и фиксации цифровых следов. 6 июля 2016 года статья 6 Федерального закона «Об оперативно-розыскной деятельности», перечислявшая возможные оперативно-розыскные мероприятия и не изменявшаяся с начала 1999 года, дополнилась новым оперативно-розыскным мероприятием, под названием «Получение компьютерной информации»[2]. Как новое оперативно-розыскное мероприятие получение компьютерной информации связано с неясностью методики его проведения, поскольку и до его появления компьютерная информация могла быть получена посредством других оперативно-розыскных мероприятий. У субъектов оперативно-розыскной деятельности могут возникнуть вопросы о том, что такое компьютерная информация, чем

правам человека – Режим доступа: https://www.echr.coe.int/Documents/Convention_RUS.pdf Статья 8

[1] См. об этом подробнее: The European Court of Human Rights CASE OF ROMAN ZAKHAROV v. RUSSIA // Официальный интернет-портал Европейского суда по правам человека [Электронный ресурс] – Режим доступа: http://hudoc.echr.coe.int/eng?i=001-159324

[2] См.: Федеральный закон «Об оперативно-розыскной деятельности» № 144-ФЗ от 12 августа 1995 г. (ред. от 02.08.2019) // СПС «Консультант Плюс». Ст. 6

данное оперативно-розыскное мероприятие отличается от снятия информации с технических каналов связи.

Оценивая вложенное законодателем в понятие «получение компьютерной информации» содержание, необходимо отметить, что название данного оперативно-розыскного мероприятия отражает форму полученной информации, в то время как другие оперативно-розыскные мероприятия названы в соответствии со способом получения оперативно-розыскной информации[1]. Каждое из перечисленных в федеральном законе об оперативно-розыскной деятельности оперативно розыскное мероприятие предназначено для получения оперативно-розыскной информации в той или иной форме (письменной или устной, видеозаписи, аудиозаписи, или фотоизображения). Некоторые из оперативно-розыскных мероприятий предполагают возможность получение информации в виде компьютерных файлов (Такие оперативно-розыскные мероприятия как снятие информации с технических каналов связи, наведение справок, сбор образцов для сравнительного исследования, исследование предметов и документов, обследование помещений, зданий, сооружений, участков местности и транспортных средств, а также наблюдение).

Для понимания сущности нового оперативно-розыскного мероприятия необходимо определить значение понятия «Компьютерная информация». Федеральным законом от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» в статье 2 представлено общее понятие информации — это «сведения (сообщения,

[1] См. об этом подробнее: Осипенко А. Л. Новое оперативно-розыскное мероприятие «Получение компьютерной информации»: содержание и основы осуществления/ Осипенко А. Л. // Вестник ВИ МВД России. - 2016. - №3. - С. 85

данные), независимо от формы их представления»[1]. Понятие компьютерной информации на уровне законодательства закреплено только в гл. 28 УК РФ, где в примечании 1 к статье 272 обозначено, что «под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи»[2]. Таким образом, наиболее подходящей представляется следующая формулировка: получение компьютерной информации – это оперативно-техническое мероприятие, направленное на сбор сведений, циркулирующих в компьютерном устройстве или сети таких устройств, а также содержащиеся на различных носителях цифровой информации с последующей их фиксацией для решения оперативно-розыскных задач[3].

Однако, сохраняется проблема разграничения данного оперативно-розыскного мероприятия с другими видами. Так, представленный вариант разграничения «получения компьютерной информации» и «снятия информации с технических каналов связи» на основании того, что «снятие информации с технических каналов связи направлено на получение компьютерных файлов», в то время как «получение компьютерной информации позволяет получить обезличенные компьютерные данные, находящиеся в закодированной форме, такая информация представляется в оцифрованной форме, благодаря чему массивы сведений могут храниться в

[1] 10. Федеральный закон «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27.07.2006 (ред. от 03.04.2020) // СПС «Консультант Плюс». Ст. 2

[2] См.: УК РФ Ст. 272 прим. 1

[3] См. об этом подробнее: Дубоносов Е.С. Оперативно-розыскное мероприятие «Получение компьютерной информации»: содержание и проблемы проведения/ Дубоносов Е.С. // Известия ТулГУ. Экономические и юридические науки. – 2017. – №2-2. – С.26

сжатом виде»[1], не проводит достаточно четкого разделения между данными видами оперативно-розыскных мероприятий, поскольку компьютерные файлы также находятся в закодированной оцифрованной форме. Отмечая проблемы практической реализации оперативно-розыскного мероприятия «получение компьютерной информации», необходимо выделить следующее: недостаток специалистов в области информационных технологий в оперативных подразделениях, а также недостаточность системы специальной подготовке по использованию информационных систем; сложности систематизации массива компьютерной информации; проблемой обеспечения охраняемых конституционных прав граждан, требующей дополнения уголовно-процессуального законодательства; проблемой преодоления средств криптографической защиты, все чаще используемой при работе с компьютерной информацией[2].

Во время доследственной проверки преступлений экстремистского характера важное значение имеет оптимальное взаимодействие между субъектом расследования, сотрудниками специализированных подразделений, прежде всего Центра по противодействию экстремизму и отдела «К», экспертными службами и профильными специалистами в области компьютерной техники, лингвистики, психологии, религии в целях получения наиболее полной криминалистически значимой информации о совершенном преступлении.

---

[1] См.: Меньшова П.Э. К вопросу о нормативном регулировании и применении оперативно-разыскного мероприятия «получение компьютерной информации»/ Меньшова П.Э.// Научно-методический электронный журнал «Концепт». – 2017. – Т. 39. – С. 877.

[2] См. подробнее: Дубоносов, Е. С. Оперативно-розыскное мероприятие "получение компьютерной информации": содержание и проблемы проведения / Е. С. Дубоносов // Известия Тульского государственного университета. Экономические и юридические науки. – 2017. – № 2-2. – С. 24-30.

Необходимость взаимодействия следователей с сотрудниками подразделений по противодействию экстремизму при расследовании уголовных дел о преступлениях экстремистской направленности обусловливается следующими основными причинами, заключающимся в общей трудоемкости расследования преступлений экстремистской направленности, заключающейся в необходимости установления направленности преступной деятельности (политическая, идеологическая, расовая, национальная или религиозная ненависть или вражда либо ненависть или вражда в отношении какой-либо социальной группы), а также необходимостью проведения по уголовным делам большого количества следственных, розыскных и иных процессуальных действий (нередко требуется осуществить одновременно множество таких действий),необходимостью использования в доказывании результатов оперативно-розыскной деятельности, необходимостью проведения оперативно-розыскных мероприятий, а также возможным оказанием преступниками противодействия предварительному следствию.

Таким образом, возбуждение уголовного дела по преступлениям экстремистской направленности, совершаемым в пространстве социальных сетей, основывается на, прежде всего, результатах оперативно-розыскной деятельности и мониторинге социальных сетей, в частности. Мониторинг целесообразно осуществлять с использованием «виртуального агента», предоставляющего большие возможности контроля. Областями мониторинга являются популярные группы региона и группы региональных СМИ. Совершение преступлений в цифровой среде позволяет использовать аппаратно-программные комплексы для автоматизации работы с колоссальными объемами информации, существующей в глобальной сети Интернет, постоянно растущей и меняющейся. Такие средства в значительной степени помогают в поиске экстремистских материалов,

автоматически их фиксируя. Оперативно-розыскное мероприятие «получение компьютерной информации» предназначено непосредственно для оперативно-розыскной деятельности в цифровой среде. Вместе с тем, на данный момент существуют проблемы практической реализации данного оперативно-розыскного мероприятия, выражающиеся в отсутствии непосредственной методики проведения, неготовности кадрового состава оперативных подразделений к работе в цифровой среде, заменимости данного оперативно-розыскного мероприятия другими видами, что выражается в низкой эффективности его применения. В ходе осуществления доследственной проверки необходимо применение специальных знаний в виде лингвистической экспертизы, позволяющей получить начальную точку расследования. При этом необходимо отметить важность оптимального взаимодействия между субъектом расследования, сотрудниками специализированных подразделений, прежде всего Центра по противодействию экстремизму и отдела «К», экспертными службами и профильными специалистами в области компьютерной техники, лингвистики, психологии, религии. По завершению доследственной проверки возникает необходимость организации расследования и выбора тактики проведения отдельных следственных действий, что обуславливается спецификой экстремистских преступлений в пространстве социальных сетей.

2.2. Использование криминалистической информации из социальных сетей при подготовке и проведении отдельных следственных действий при расследовании преступлений экстремистской направленности

В условиях развития информационного общества экстремизм перерос рамки регионального и национального масштаба. Интерес исследователей к проблемам современного международного кибертерроризма и формам его проявления связан с изменившейся политической ситуацией в мире, возросшей активностью экстремистских и террористических организаций на международной арене. Существует необходимость объединения усилий представителей общественности и государственных институтов, правоохранительных органов на национальном и мировом уровне в борьбе с экстремизмом

Основными источниками идей экстремизма и ресурсами вербовки являются социальные сети. Именно в социальных сетях, в так называемых «закрытых группах», проводится идеологическая подготовка пользователей сети. Основной «мишенью» создателей этих групп являются молодые люди (наиболее активные пользователи социальных сетей), мигранты (социальный статус и положение в обществе зависят от окружения и среды, в которой они пребывают, оказавшись на территории нашей страны)

Электронная среда как место совершения преступлений экстремистской направленности в социальных сетях оказывает влияние и на непосредственно расследование такого преступления, поскольку наряду с традиционными доказательствами, такими, как протокол явки с повинной; показания свидетелей, подозреваемых (обвиняемых), указываемыми некоторыми авторами как основные по преступлениям экстремистской

направленности[1], возникает необходимость в использовании информации из пространства сети Интернет и социальных сетей, в частности. Кроме того, нередко достаточно сложно провести границу между выражением права свободу мысли и слова, и завуалированным экстремизмом, что, как правило, определяется при помощи лингвистической (или комплексной совместно с другими отраслями знаний) судебной экспертизы.

Так, постановлением Исакогорского районного суда г. Архангельска от 22.08.2016 N1-102/2016 уголовное дело в отношении подсудимого, обвиняемого в совершении преступлений, предусмотренных ст. 282 ч. 1, 280 ч. 2 УК РФ, возвращено прокурору города Архангельска для устранения препятствий его рассмотрения судом, заключавшихся в том, что в комментарии к новостной статье под заголовком «За антихристианские высказывания молодой архангелогородец отработает срок», начинавшегося со слов «Пойми, глупец, мы разные с тобою...», а также в комментарии к новостной статье под заголовком «В Архангельске вынесен обвинительный приговор гражданину Таджикистана, оправдывающему террористическую деятельность», начинавшегося со слов «Дааа! Сколько надо ещё...» в обвинении не было приведено конкретное содержание высказываний подсудимого, так и не было не раскрыто их содержание иным образом, которые по мнению стороны обвинения образуют объективную сторону преступления, предусмотренного ст. 282 ч. 1 УК РФ, не описан способ и другие обстоятельства совершения деяния[2]**.**

Расследование любого преступления осуществляется по следующей схеме информационно-аналитической деятельности субъекта расследования:

---

[1] См.: Валеев А.Х., Самойлов А.Ю. Особенности расследования преступлений экстремистской направленности / Валеев А.Х., Самойлов А.Ю.// Евразийский юридический журнал. - 2012. - № 9 (52). - С.128

[2] См. об этом подробнее: Постановление Исакогорского районного суд г. Архангельска от 22 августа 2016 года N 1-102/2016 [Электронный ресурс]. Доступ из справ.-правовой системы «Судебные и нормативные акты РФ» (СудАкт).

1. поиск и получение криминалистически значимой информации;

2. фиксация и закрепление криминалистически значимой информации;

3. исследование полученной криминалистически значимой информации;

4. формулирование вероятного умозаключения (криминалистической версии);

5. проверка выдвинутой криминалистической версии;

6. поиск и получение новой криминалистически значимой информации;

7. преобразование полученной криминалистически значимой информации в целях ее автоматизированного накопления и последующего многократного использования[1].

Характерные особенности работы в виртуальном пространстве в ходе информационно-аналитической деятельности субъекта расследования проявят себя, прежде всего, на этапе поиска, получения, фиксации и закрепления криминалистически значимой информации.

Как уже указывалась ранее, необходимо не просто зафиксировать факт совершения преступления в социальной сети. Необходимо установить связи нехарактерные для «традиционных преступлений», такие как: связи между аккаунтом, разместившим информацию являющуюся (предположительно) экстремистской и лицом, использующим этот аккаунт, путем установления IP-адреса, обращавшегося к аккаунту, а также получить информацию, свидетельствующую об исключении возможности обращения к данному

[1] См.: Давыдов В.О. Исследование криминалистически значимой информации в ходе расследования экстремистских преступлений, совершенных с использованием компьютерных сетей. / Давыдов В.О. // Известия Тульского государственного университета. Экономические и юридические науки. - 2013. - № 4. - С.58

аккаунту третьих лиц, что также подтверждается путем сопоставления перечней IP-адресов, обращавшихся к аккаунту.

В данной ситуации существенной сложностью может стать установление местонахождения злоумышленника, поскольку его действия не ограничены пространством, и он может находиться как в любой точке России, так и за рубежом.

Результаты расследования преступлений экстремистской направленности находятся в полной зависимости от качества и полноты следственных действий, проводимых по уголовному делу[1]. Наиболее распространенными следственными действиями по категории экстремистских преступлений являются[2]:

1. осмотр места происшествия;
2. допросы потерпевших;
3. допросы свидетелей;
4. проведение обыска, выемки.

Отмечается, что осмотр места происшествия как первоначальное следственное действие необходим во всех тех случаях, когда по обстоятельствам дела возникает предположение о том, что там могут быть обнаружены вещественные доказательства, изменения в окружающей обстановке, иные следы преступления. Их изучение дает возможность следователю установить характер события, а подчас форму вины субъекта, мотив преступления и др.[3]

---

[1] См. об этом подробнее: Мешков В.М. Роль и значение фактора времени в ситуационном подходе, применяемом при расследовании преступлений//Ситуационный подход в юридической науке и практике: современные возможности и перспективы развития: материалы Международной научно-практической конференции, посвященной 15-летию научной школы криминалистической ситуалогии БФУ им. И. Канта. 2017. С. 44–51.

[2] См.: Валеев А. Х., Данилко А.Н., Кудрявцев А. В. Указ. соч. С.14

[3] См.: Бирюков С.Ю., Скориков Д.Г., Шинкарук В.М. Особенности расследования преступлений экстремистской направленности: учебное пособие /

Отсутствие осмотра места происшествия или низкое его качество по делам о преступлениях экстремистской направленности влечет за собой невозможность или значительно усложняет процесс доказывания, такое положение относится к преступлениям экстремистской направленности, предусмотренным п. «л» ч. 2 ст. 105 УК РФ, п. «е» ч. 2 ст. 111 УК РФ, п. «е» ч. 2 ст. 112 УК РФ, п. «б» ч. 2 ст. 115 УК РФ, п. «б» ч. 2 ст. 116 УК РФ, п. «з» ч. 2 ст. 117 УК РФ, ч. 2 ст. 119 УК РФ, где имеет место и наличие конкретного потерпевшего, так и свидетелей преступления.

Однако, при расследовании преступления в пространстве сети Интернет осмотр места происшествия в его привычном понимании иррелевантен, поскольку физически преступник находился в месте, которое на момент проверки, либо возбуждения уголовного дела еще не установлено, использовал неустановленное устройство, так и само значение местонахождения злоумышленника не имеет такого значения, какое оно имеет при расследовании насильственных преступлений экстремистской направленности.

Необходимо отметить, что уголовно-процессуальных законодательством Российской Федерации предусмотрен не только осмотре места происшествия, но и местности, жилища, а также любого иного помещения, если это удовлетворяет целям обнаружения следов совершенного преступления, или выяснения других обстоятельств, имеющих значение для уголовного дела[1], однако в отличии от осмотра места происшествия данные осмотры могут быть произведены только после возбуждения уголовного дела[2]. Осмотр жилища подозреваемого (обвиняемого) позволяет получить информацию о его отношении к

Бирюков С.Ю., Скориков Д.Г., Шинкарук В.М. - Волгоград: ВА МВД России, 2013. - С.40

[1] См.: УПК РФ ч.1 ст. 176

[2] См.: УПК РФ ч.2 ст. 176

экстремистской организации или сообществу, наличии специальных технических средств для работы в сети Интернет, и иную информацию, имеющую значение для уголовного дела.

Достаточный интерес для расследования преступлений данной категории мог иметь осмотр непосредственно Интернет-страницы, оформляемого протоколом, что характерно для нотариальной практики[1]. Такой осмотр может выступать в качестве отправной точки проведения расследования, доказательством события преступления. Однако, уголовно-процессуальным законодательством не предусмотрена возможность осмотра объектов, находящихся в пространстве глобальной сети Интернет, в результате чего судебная практика в регионах разнится.

С одной стороны, есть полное отрицание возможности следственного осмотра объектов сети Интернет, поскольку такие объекты не удовлетворяют как определению места или иного помещения, будучи программным кодом, так и предмета или документа, поскольку уголовно-процессуальным законодательством предусмотрена их обязательная упаковка, что не применимо к Интернет-странице, что компенсируется возможностью обследования Интернет-страницы в ходе ОРД.

Так, в приговоре Курского гарнизонного военного суда от 18 января 2012 года N 3-2012 в числе доказательств обозначается протокол обследования помещения (предметов документов) от 1 июля 2011 года, в котором указывается, что на персональной странице осужденного в социальной сети «В Контакте», были размещены две видеозаписи экстремистского содержания: «Русский, очнись! Против тебя идет

[1] См. об этом подробнее: Бегичев А.В. Использование протоколов осмотров интернет-сайтов в судебной практике / Бегичев А.В. // Вестник Московского университета МВД России. - 2014. - № 11. - С.209

война!» и «Ой скинхед» [1]*. В качестве следственного действия выступил осмотр предмета, в ходе которого был осмотрен оптический диск, на который были скопированы видеозаписи со страницы осужденного. Таким образом, не имея возможности провести осмотр непосредственно страницы, следователем был проведен осмотр предмета, как типового следственного действия.*

Другим вариантом использования страницы в социальной сети для доказывания является осмотр предмета, содержащего страницу целиком, записанную из глобальной сети Интернет.

Так, в приговоре Ленинского районного суда г. Чебоксары от 12 сентября 2011 года в числе доказательств обозначается протокол осмотра предметов и документов, согласно которому в ходе осмотра оптического носителя информации DVD-RMIREX 4,7 G, записанного в ходе просмотра персональной страницы осужденного в социальной сети «В Контакте», были обнаружены материалы экстремистского характера[2]**.**

С другой стороны, в практике встречаются примеры осмотра Интернет-страницы как ОМП, также осмотра предметов или документов.

Так, в приговоре Новоржевского районного суда Псковской области от 27 мая 2015 года N 1-12/2015 в числе доказательств обозначается протокол осмотра места происшествия, в котором указывается, что на персональной странице осужденного в социальной сети «В Контакте»,

---

[1] См. об этом подробнее: Приговор Курского гарнизонного военного суда от 18 января 2012 года N 3-2012 [Электронный ресурс]. Доступ из справ.-правовой системы «Судебные и нормативные акты РФ» (СудАкт).

[2] См. об этом подробнее: Приговор Ленинского районного суда г. Чебоксары от 12 сентября 2011 года [Электронный ресурс]. Доступ из справ.-правовой системы «Судебные и нормативные акты РФ» (СудАкт).

были обнаружены материалы экстремистского характера, а именно две видеозаписи и две аудиозаписи[1]**.**

Вместе с тем, целесообразно именно проведение осмотра интернет-страницы как осмотра места происшествия, в ходе которого в присутствии понятых, желательно с использованием записи-захвата «рабочего стола», фиксирующей именно действия в программной сфере, производится осмотр интересующего объекта глобальной сети. В протоколе последовательно описываются действия следователя с момента включения Интернет-браузера, с указанием адреса страницы с сети Интернет, имени обладателя страницы в социальной сети, указанием лица, разместившего экстремистский материал, дате и времени публикации, дате последнего посещения пользователем своей страницы, и иной информации об опубликованном материале, которая может иметь значение для расследования преступления. К протоколу целесообразно прилагать фототаблицу, содержащую снимки с экрана (клавиша «PrintScreen»), документирующие изображения и текст на осматриваемом ресурсе.

Допрос свидетелей и потерпевших в ходе расследования преступлений экстремистской направленности, совершенных в пространстве сети Интернет, представляется затруднительным, поскольку объективная сторона преступления находит свою реализацию в киберпространстве, где его действия направлен на неопределенный круг лиц, что исключает личность потерпевшего. Уголовно процессуальным законодательством установлено, что потерпевший – это физическое лицо, которому преступлением был причинен физический, имущественный, моральный вред, а также

---

[1] См. об этом подробнее: Приговор Новоржевского районного суда Псковской области от 27 мая 2015 года

N 1-12/2015 [Электронный ресурс]. Доступ из справ.-правовой системы «Судебные и нормативные акты РФ» (СудАкт).

потерпевшим может быть и юридическое лицо в ситуации, когда вред преступлением был причинен его имуществу и деловой репутации[1].

Так, приговором Гороховецкого районного суда Владимирской области от 27 февраля 2017 года N1-12/2017 в действиях осужденного использовавшего Интернет-сайт социальной сети «В Контакте», разместил на своем аккаунте социальной сети «В Контакте» в блоке «видеозаписи» видеоматериал «Нет толерастии в городе Владимир! Чурки домой», открытый для свободного просмотра всеми пользователями социальной сети «В контакте». Видеоматериал содержал признаки возбуждения вражды, ненависти (розни) по отношению к группам лиц «евреи», «кавказцы», «азиаты» выделенным по национальному признаку, а также признаки унижения человеческого достоинства указанных групп лиц[2].

На примере видно, что публичный не персонифицированный характер публикации исключает саму возможность определения потерпевшего. Если лицо в ходе просмотра веб-страниц увидело опубликованный материал экстремистской направленности, то оно обладает информацией о примерном времени размещения материалов, аккаунте, использованном для размещения материалов и непосредственно страницы, на которой экстремистские материалы, были опубликованы.

Вместе с тем, оценивая роль такого свидетеля как лица, которое может сообщить о совершении преступления, необходимо отметить, что информация о времени и аккаунте-авторе публикации будет отражена в самой публикации, что обусловлено механизмом социальной сети. В таком

---

[1] См.:УПК РФ ч.1 ст. 42

[2] См. об этом подробнее: Приговор Гороховецкого районного суда Владимирской области от 27 февраля 2017 года N1-12/2017 [Электронный ресурс]. Доступ из справ.-правовой системы «Судебные и нормативные акты РФ» (СудАкт).

случае возникает вопрос о целесообразности поиска свидетелей и их последующего допроса.

Так, в приговоре Курского гарнизонного военного суда от 18 января 2012 года N 3-2012, обозначенном ранее, одним из доказательств являлись показаниями свидетеля, который указал в суде, что в 2011 году в социальной сети «В Контакте» на персональной странице осужденного, обнаружил видеоролики, посвященные скинхедам. Свидетель запомнил содержание видеозаписей с названиями «Русский, очнись! Против тебя идёт война!», представлявшие из себя слайд-шоу, с различными изображениями, надписями «Россия для русских», «Слава Руси», «русские идут», сопровождающейся песней в стиле рок националистического характера и видеозапись «Ой скинхед», на которой демонстрировалось избиение человека кавказской внешности, которые находились в свободном доступе для просмотра и копирования в социальной сети «в контакте» [1].

Крайне важными, при расследовании таких преступлений являются такие следственные действия как обыск и выемка, позволяющие получить орудие совершения преступления, уставные документы, регламентирующие деятельность экстремистских организаций, документы организации: протоколы или записи о проведении заседаний, собраний и принятых на них решения и иную информацию, представляющую значение для расследования преступления, документы, содержащие различную информацию о личности лица совершившего преступление, литература, фонограммы, видеозаписи направленные на разжигание национальной, расовой или религиозной ненависти или вражды (проповеди, беседы, обучающие программы), которые могут свидетельствовать о целях и

[1] Приговор Курского гарнизонного военного суда от 18 января 2012 года N 3-2012 [Электронный ресурс]. Доступ из справ.-правовой системы «Судебные и нормативные акты РФ» (СудАкт).

мотивах лица, совершившего преступление, а также предметы, изъятые или запрещенные к гражданскому обороту.

Компьютерное устройство, использованное при совершении преступления, на котором могли сохраниться цифровые следы деятельности злоумышленника в сети Интернет, которые в дальнейшем могут быть обнаружены в ходе осмотра с участием специалиста или экспертного исследования.

Важно отметить, что само проведение обыска или выемки в условиях, когда интересующими объектами являются компьютерные устройства целесообразно привлекать к проведению следственного действия специалиста[1]. Кроме того, при ситуации, когда обыскиваемое лицо не обладает знанием языка уголовного судопроизводства, необходимо обеспечить присутствие переводчика. При этом существует вероятность, что переводчик может в целом или в части поддерживать убеждения лица, совершившего преступление экстремистской направленности. Следовательно, представляется обоснованным применение видеофиксации для того, чтобы при возникновении сомнений в достоверности устного перевода оценить его с участием другого переводчика[2].

В ходе данных следственных действий могут быть обнаружены следующие носители компьютерной информации: персональный компьютер, мобильный телефон, карта памяти, внешний жесткий диск, CD/DVD/BD диски и т.д., что частично позволяет решить проблему обнаружения следов

---

[1] См.: Головин А.Ю. Аристархова Т.А. Особенности проведения отдельных следственных действий при расследовании экстремистских преступлений против прав и законных интересов человека и гражданина / Головин А.Ю. Аристархова Т.А. // Известия Тульского государственного университета. Экономические и юридические науки. -2016. - № 3. - С.38

[2] См.: Лозовский Д.Н. Актуальные вопросы производства отдельных следственных действий по делам экстремистской направленности / Лозовский Д.Н. // Вестник Уральского юридического института МВД России, 2014 С.38

преступлений экстремистской направленности, поскольку обнаружение носителей компьютерной информации не отличается от обнаружения материальных следов-предметов. В таком случае, при обнаружении носителя информации целесообразно обратиться к опыту зарубежных правоохранительных органов, раньше столкнувшихся с преступностью в сфере высоких технологий и сети Интернет[1]:

При обнаружении таких носителей как CD/DVD/BD диски, внешние жесткие диски, карты памяти, или извлеченные из компьютера HDD или SDD накопители достаточно обеспечить их сохранность и невозможность стороннего доступа. Следовательно, обнаруженные носители не подключаются к каким-либо устройствам для их чтения и упаковываются, опечатываются и заверяются[2]. В дальнейшем эти носители могут быть как направлены на компьютерно-техническую экспертизу, так и осмотрены следователем с участием специалиста.

Такие меры предосторожности связаны, в первую очередь, с тем, что на носителе может находиться вредоносное ПО, требующее изучение в особых условиях, а также на носителе могут заданы команды по автоматическому уничтожению содержимого при попытке запустить его обычным способом, либо на носителе могут находиться скрытые и удаленные файлы, обнаружение которых возможно только при применении специального технического или программного оборудования специалистом или экспертом. Факт обнаружения носителя, а также все последующие действия с ним фиксируются в протоколе.

---

[1] См. об этом подробнее: U.S. Department of Justice Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition // [Электронный ресурс] – Режим доступа: https://www.ncjrs.gov/pdffiles1/nij/219941.pdf (дата обращения: 20.05.2022)

[2] См.: УПК РФ Ст. 177. Ч. 3.; Ст. 182. Ч. 10.

Однако, если в ходе следственного действия будет обнаружено программируемое устройство, в том числе, персональный компьютер, ноутбук или мобильный телефон, то действия с таким устройством должны зависеть от его состояния[1].

Так, если устройство включено, то при совершении следственного действия необходимо исключить возможность его отключения кем-либо из участников, поскольку при отключении устройства произойдет потеря всех данных находящихся в ОЗУ устройства. Определить включен ли компьютер можно по цветовым индикаторам на системном блоке персонального компьютера или корпусе ноутбука, звуку вентиляторов системы охлаждения или звуку работающего CD/DVD/BD- привода. Тем не менее, существуют ситуации при которых необходимо немедленно отключить устройство от питания, прежде всего, к таким ситуациям относится процесс удаления информации с устройства, такие процессы на экране могут быть обозначены словами «Удаление», «Форматирование», «Очистка», «Перемещение», или обозначенные английскими словами «format», «delete», «remove» или «wipe».

В частности, браузер I2P, предназначенный для обеспечения анонимности в сети Интернет и доступа к т.н. «darknet» обладает функциями тревожной кнопки, полностью удаляющей всю информацию, связанную с браузером.

Отключение устройства, в таком случае, производиться с целью предотвращения утраты значимой информации[2]. Так же, необходимо обратить внимание на возможность удаленного управления устройством, подключенным к сети Интернет. Если на экране устройства выведена

---

[1] См.: U.S. Department of Justice Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition // [Электронный ресурс] – Режим доступа: https://www.ncjrs.gov/pdffiles1/nij/219941.pdf (дата обращения: 20.05.2022)

[2] См.: там же

информация, имеющая значение для расследования преступления, то необходимо зафиксировать её на фото или видео носитель, а также внести соответствующие сведения в протокол. Если операционная система устройства относится к семейству Microsoft Windows, то имя пользователя, последние открытые файлы и папки, а также все последние действия и иные имеющее значение данные сохраняются в компьютере, что позволяет отключить устройство для дальнейшего изъятия.

Но не рекомендуется отключать устройство если на экране устройства видно, что открыт текстовый документ, открыт доступ к «облачному» хранилищу информации в Интернете, окна мгновенных сообщений или чат-комнаты, программы шифрования данных, или иная выведенная информация криминального или подозрительного вида. В таком случае информация на экране также фиксируется, при необходимости для консультаций вызывается специалист.

Если обнаруженное в ходе следственного действия устройство выключено, то оно изымается по правилам действующего уголовно-процессуального законодательства, упаковывается, опечатывается и заверяется, включение такого устройства происходит уже в ходе осмотра с участием специалиста, либо компьютерно-технической экспертизы[1]. В противном случае включение устройства может инициировать заранее заготовленные команды по удалению, изменению, или шифрованию информации на устройстве, либо иным образом сказаться на состоянии информации.

В случае если поиск цифровых следов сопряжен работой в сети, состоящей из нескольких связанных компьютерных устройств, то изъятие

[1] См. об этом подробнее: Мещеряков В. А. Криминалистические особенности получения компьютерной информации с цифровых носителей при производстве отдельных следственных действий / В. А. Мещеряков, О. Ю. Цурлуй // Эксперт-криминалист. – 2020. – № 2. – С. 15–17

устройства или устройств не производится и возникает необходимость в проведении осмотра компьютерной сети с обязательным участием специалиста, зафиксированы виртуальные следы в таком случае будут в протоколе осмотра.

При расследовании таких преступлений также целесообразно получить от пользователя всю возможную информацию об устройстве: Технические характеристики устройства и его комплектующих. Имена (Логины) и пароли пользователей устройства, e-mail аккаунты пользователей, имеющаяся на устройстве система защиты, программы, работающие в автономном режиме, название интернет провайдера, имеющиеся «облачные» хранилища.

Вместе с тем, необходимо учитывать, что современные средства шифрования информации на компьютерных устройствах могут использовать несколько кодов дешифрования, где только один код дешифрует весь массив информации, в то время как остальные создают имитацию дешифровки или дешифровывают отдельный блок массива информации, выступающий средством отвлечения внимания следователя.

Другим важным следственным действием является выемка у провайдеров и хостинг-провайдеров документов, содержащих сведения об арендаторах мест в сети используемых под web-сайты, web-страницы, форумы или баннеры, о пользователях услугами сети Интернет, способах соединений, о владельцах электронной почты, информацию о плательщиках за арендуемые места, а также статистику соединений по пополнению и обновлению Интернет-ресурсов[1]. Значение данного действия заключается в том, что в условиях использования злоумышленником псевдонима имеется возможность обнаружить фактическое место, с которого осуществлялось

[1] См.: Побегайло А.Э. Борьба с киберпреступностью: учеб. пособие / А.Э. Побегайло; Ун-т прокуратуры Рос. Федерации. – М., 2018. – с.60.

размещение материалов экстремистского характера, что позволяет в дальнейшем найти самого преступника.

В ходе допроса подозреваемого, обвиняемого при расследовании преступления экстремисткой направленности, совершенной с использованием социальных сетей, необходимо учитывать, что допрашиваемые, в большинстве случаев, являются убежденными сторонниками пропагандируемых идей.

Так, приговором Окуловского районного суда Новгородской области от 12.10.2016 N 1-134/2016 было установлено, что осуждённый в разделе «Видеозаписи» на странице социальной сети разместил два видеоролика в открытый доступ, а в разделе «Фотографии» разместил одну фотографию экстремистского содержания для просмотра неограниченного круга лиц, что, как установлено судом, было связано с устойчивой поддержкой экстремистских позиций и националистических взглядов[1].

В зависимости от обстоятельств расследуемого преступления при допросе у подозреваемого, обвиняемого могут подлежать выяснению следующие обстоятельства:

1. является ли допрашиваемый членом какой-либо партии, общественной организации или общественного движения, либо иной группы, в том числе неформального молодежного объединения;

2. если да, то когда и при каких обстоятельствах допрашиваемый вступил в обозначенную группу;

3. что привлекло к участию в деятельности данной группы, какие она преследует цели, какие используются средства для их достижения,

[1] См. об этом подробнее: Приговор Окуловского районного суда Новгородской области от 12.10.2016 N 1-134/2016 [Электронный ресурс]. Доступ из справ.-правовой системы «Судебные и нормативные акты РФ» (СудАкт).

какими лозунгами пользуются, кто является лидером, в чем проявляется конкретная деятельность группы);

4. как были изготовлены материалы экстремистского содержания;

5. с помощью какого оборудования производилось изготовление и распространение материалов экстремистского содержания;

6. какой механизм склонения, вербовки или иного способа вовлечения лиц в совершение экстремистской деятельности;

7. участники, вступившие в организацию;

8. источник поступления материально-технических средств, для поддержания деятельности экстремистской организации;

9. мотивы совершаемых допрашиваемым действий;

10. навыки обращения с компьютерной техникой;

11. способ, средства, методы, логин и пароль для осуществления доступа к информационным базам, банкам данных, компьютерным сетям и веб-страницам;

Вопросы, задаваемые допрашиваемому, не должны существовать в виде жесткого списка и во многом зависят от следственной ситуации, и могут меняться в соответствии с ней.

В ходе расследования уголовных дел экстремистской направленности совершенной с использованием сети Интернет одной из основных проблем выступает установление наличия в действиях направленности на возбуждение ненависти либо вражды, а также на унижение достоинства человека либо группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии, а равно принадлежности к какой-либо социальной группе. Рассматривая подходы, способствующие установлению направленности на возбуждение ненависти или вражду, а также факта призыва к экстремистской деятельности при расследовании преступлений экстремистской направленности необходимо также учитывать

применение специальных знаний в области лингвистики, психологии, этнологии, истории, религиоведении[1].

Таким образом, особенности проведения отдельных следственных действий в ходе расследования преступлений экстремистской направленности в пространстве социальных сетей характеризуются спецификой виртуальной среды, в которой они совершаются, вследствие чего многие из рекомендованных следственных действий, их тактических и организационных особенностей не представляется возможным выполнить, из чего следует, что наиболее целесообразными при расследовании таких преступлений представляются следующие следственные действия:

1. Выемка у провайдеров и хостинг-провайдеров документов, содержащих информацию по действиям преступника в сети Интернет, его фактического адреса, использованных подключениях, IP-адресах.

2. Осмотр помещения, где находилась техника, с помощью которой осуществлялось преступление экстремисткой направленности с использованием сети Интернет.

3. Осмотр использованной техники с фиксацией экстремистских материалов.

4. Обыск у установленного лица по месту жительства, работы и иных хранилищах.

5. Допрос подозреваемого.

6. Назначение лингвистической, компьютерно-технической, или иной судебной экспертизы[2].

---

[1] См.: Бельков В.А. Крутер К.А. Анализ теоретико-практических проблем расследования преступлений экстремистской направленности: пропаганда экстремизма / Бельков В.А. Крутер К.А. // Вестник Казанского юридического института МВД России. - 2017. - № 1(27). - С.101

[2] См. об этом подробнее: Мещеряков, В. А. Особенности специальных знаний, используемых в цифровой криминалистике / В. А. Мещеряков // Известия Тульского

Необходимо отдельно отметить, что недостаточность процессуального урегулирования возможности проведения осмотра Интернет-страницы привела к расхождению судебной практики по порядку использования материалов глобальной сети Интернет в процессе доказывания.

С одной стороны, осмотр Интернет-страниц не проводится, будучи замененный свидетельскими показаниями, осмотром материального носителя, или другим способом.

С другой стороны, Интернет-страница осматривается как место происшествия, либо как предмет или документ, при том, что целесообразнее выделить осмотр объектов глобальной сети интернет в качестве нового места совершения преступления.

государственного университета. Экономические и юридические науки. – 2013. – № 4–2. – С. 88.

2.3. Проблемы использования специальных знаний при расследовании преступлений экстремистской направленности, совершенных с использованием социальных сетей

Социальные сети позволяют насильственным экстремистским группам и отдельным лицам получить большую аудиторию и распространять свои сообщения или идеологические убеждения. Наибольшее беспокойство у правоохранительных органов вызывает саморадикализация. Больше не надо уходить из дома, чтобы встретиться с людьми или группой, которые разделяют те же идеологические убеждения. Нет необходимости харизматичному лидеру или «гуру» вести физическую вербовку и воспитывать последователей или популяризовать определенную позицию или убеждения. Экстремистские идеи или риторика могут быстро распространяться и достичь Интернета при помощи любого, владеющего смартфоном или планшетом. Вместо встречи в местном ресторане или клубе насильственные экстремисты могут «встретиться» в социальных чат-комнатах, дополненных «живыми» видеороликами. Онлайн радиостанции могут вещать постоянно. Могут быть созданы блоги, выражающие особые убеждения экстремистов или поддержку какой-то группы или движения.

Примеров использования внутренними экстремистами и массовыми убийцами Интернета и социальных сетей с рекламированием и предсказанием своих преступлений множество. Правоохранительные органы должны быть в курсе и уметь не только менять угрозы онлайн, выявлять и предотвращать будущие преступления, но и выявлять выходы экстремистов в социальных сетях.

Экстремистская деятельность в социальных сетях обладает характерными сложностями как экстремистской деятельности, так и

цифровой сферы, связи с чем возникает закономерная необходимость использования специальных знаний.

Специальные знания при расследовании уголовных дел исследуемой категории могут быть использованы в двух формах: участие специалиста и назначение, производство экспертиз. Исходя из отмеченного, использование специальных знаний при расследовании рассматриваемого вида преступлений осуществляется в форме:

1) консультаций у специалистов-профессионалов в различных отраслях науки и техники;

2) участия специалистов при производстве следственных действий[1];

3) производства судебных экспертиз[2].

При расследовании преступлений экстремистской направленности, совершенных в сети Интернет, можно выделить две основные группы использования специальных знаний в зависимости от сферы деятельности: Специальные знания в сфере информационных технологий[3] и специальные знания в области лингвистики[4], религии, психологии.

(Специальные знания в сфере информационных технологий.)

---

[1] См. об этом подробнее: Семикаленова А.И., Рядовский И.А. Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики // Актуальные проблемы российского права. 2019. N 6. С. 178 - 185.

[2] См. об этом подробнее: Грибунов О.П. Виды экспертиз, назначаемых при расследовании преступлений в сфере компьютерной информации и высоких технологий / О. П. Грибунов, М. В. Старичков // Криминалистика и судебная экспертиза: прошлое, настоящее и взгляд в будущее : материалы ежегодной международной научно-практической конференции, Санкт-Петербург, 01–02 июня 2017 года / Санкт-Петербургский университет МВД России. – Санкт-Петербург: Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2017. – С. 79

[3] Мещеряков, В. А. Особенности специальных знаний, используемых в цифровой криминалистике / В. А. Мещеряков // Известия Тульского государственного университета. Экономические и юридические науки. – 2013. – № 4–2. – С. 88.

[4] См. об этом подробнее: Подкатилина М.Л. К вопросу о лингвистической экспертизе экстремистских материалов / Подкатилина М.Л. //"Эксперт-криминалист". - 2010. - № 4. - С.22

В статье 164.1 УПК РФ указано, что участие специалиста при изъятии электронных носителей информации обязательно при производстве любых следственных действий. Цифровизация общества и существенное усложнение цифровых устройств привело к тому, что специалисты требуются для оказания помощи в применении технических и программных средств, а также постановке вопросов эксперту. Причем, осуществлять указанные действия специалист может на любой стадии уголовного процесса. Вместе с тем, стоит отметить, что к числу указанных специалистов в рамках производства следственных действий, связанных с извлечением и фиксацией криминалистически значимой информации из объектов компьютерной техники и электронных устройств, следует отнести именно тех, которые обладают специальными знаниями и профессиональной компетенцией в сфере производства компьютерно-технических экспертиз.

Так, современное криминалистическое оборудование позволяет извлекать информацию, в том числе и удаленную, завуалированную или скрытую с устройств или электронных накопителей любой модели, любой операционной системы, а также устройств, защищенных паролем или даже поврежденных. Это следующие устройства: универсальное устройство извлечения судебной информации (UFED - Universal Forensic Extraction Device), мобильный криминалист, XRY, MOBILedit, Тарантула и др.)[1]. В частности, в Забайкальском крае UFED был использован в 106 проверках по 14 уголовным дела, при том, что в 85 случаях была получена интересующая следствие информация[2]. Похожие результаты наблюдались и в других

[1]См.: Скобелин С.Ю. Указ. соч. С. 32

[2]См.: Рогова И.А., Бурцева Е.В. Практика применения UFED – универсального устройства для криминалистического исследования мобильных устройств / И.А. Рогова, Е.В. Бурцева // Евразийский Союз Ученых. 2015. №7-5(16) С. 98

субъектах РФ[1]. В возможности такого устройства входят получение информации:

- О телефоне (IMEI/ESN);
- Сим-карте (ICCID и IMSI);
- Вызовах, с возможностью нахождения удаленных вызовов (время вызова, имена/номера телефонов);
- Об использовании интернет-браузера;
- Закладках интернет-сайтов; файлах Cookie;
- Записях телефонной книги;
- SMS, MMS и голосовых сообщениях;
- Сообщениях чатов и электронной почты;
- Изображениях; видео- и аудиофайлах;
- Местоположении (определяемое по сети WiFi, ретрансляторам мобильной связи или навигационным приложениям), маршрутах перемещения (на платформе Android такие данные могут находиться в приложениях Google Earth и Google Maps), GPS-координатах использования мобильного устройства, а также место сделанного снимка или снятой видеозаписи;
- Введенных в GPS устройствах (навигаторы) местоположения, координатах, избранных расположениях;
- Паролях, журналах вызовов, текстовых сообщениях, контактах в электронной почте, мессенджерах, записях в календаре, медиафайлах, геотегах, приложениях, служебных данных (список IMSI, данные последней сим-карты, коды блокировки);
- Данных журнала, содержащего список действий с телефоном;

[1] См.: там же. С. 99

- **Переписке в различных социальных сетях ("Вконтакте", "Одноклассники", "Twitter", "Facebook"), с помощью таких приложений, как Skype, и др.**

Извлеченная из компьютера или мобильного устройства информация может:

- Напрямую изобличать лицо в совершении преступления, что может выражаться в фото или видеозаписи совершения преступления экстремисткой направленности, сохраненных текстовых сообщениях;

- Косвенно указывать на линию поведения лица, свидетельствующей о возможной причастности его к совершенному преступлению, куда входят закладки на определенных сайтах экстремистского содержания, экстремистская литература в цифровом виде, изображения экстремистской символики;

- Способствовать установлению иных обстоятельств, имеющих значение для дела, таких как время совершения преступления, местонахождение устройства и предположительно его владельца на момент интересующих событий[1].

Тем не менее, несмотря на высокую результативность использования UFED, удельный вес уголовных дел, по которым происходит его применение, остается небольшим. Это вызвано как вопросом персональных данных, полученных входе использования устройства[2], так и проблемой

---

[1] См. об этом подробнее: Багмет А.М., Скобелин С.Ю. Извлечение данных из электронных устройств как самостоятельное следственное действие // Право и кибербезопасность. 2013. N 2. С. 24.

[2] См.: Бычков В.В. Соблюдение прав граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений при проверке сообщений о преступлениях и в ходе их расследования / В.В. Бычков // М.:Юрист, 2013.

отнесения мобильных телефонов к компьютерно-техническим экспертизам[1], с чем связаны также и процессуальные проблемы оформления, извлечения и анализа данных с мобильного телефона.

Уголовно-процессуальным законом предоставлена возможность копирования информации с изымаемых электронных носителей информации на другие электронные носители информации, предоставленные законным владельцем изымаемых электронных носителей информации или обладателем содержащейся на них информации. Копирование указанной информации на другие электронные носители информации, предоставленные законным владельцем изъятых электронных носителей информации или обладателем содержащейся на них информации, осуществляется с участием законного владельца изъятых электронных носителей информации или обладателя содержащейся на них информации и (или) их представителей и специалиста в присутствии понятых в подразделении органа предварительного расследования или в суде[2]. В таком случае участие специалиста является обязательным.

Особое внимание необходимо обратить на то, что перед началом осмотра или копирования информации с устройства следует принять меры с помощью специалиста по подготовке техники, которая будет использоваться для считывания и хранения изъятой информации. Необходимо позаботиться и о специальном программном обеспечении, позволяющем совершить копирование и экспресс-анализ информации[3].

---

[1] См.: Рогова И.А., Бурцева Е.В. Практика применения UFED – универсального устройства для криминалистического исследования мобильных устройств. С. 100

[2] См.: УПК РФ Ст. 82. Ч. 2.1

[3] См. об этом подробнее: Михеев А.В. Особенности доказывания публичных призывов к осуществлению экстремистской деятельности в сети Интернет / А.В. Михеев // Российский следователь. 2014. N 9. С. 10

Подобная рекомендация встречается и в зарубежной криминалистике, где указывается на необходимость «Настоящей копии»[1], под которой необходимо понимать точную копию информации с носителя «bit-by-bit», в противном случае, при копировании информации привычным рядовому пользователю способом, не производится копирование удаленных, скрытых системных файлов, временных файлов, которые могут являться источниками искомой информации. В частности, для полного копирования тома может быть использована программа Acronis disk director, способная производить копирование «bit-by-bit» с различных носителей, включая жесткие диски, SSD-накопители, карты памяти и т.д. Кроме того, перед осмотром устройства, содержащего виртуальные следы, также производится резервное копирование информации, что особенно актуально при наличии вероятности автоматического удаления файлов.

Тем не менее, в случае физической удаленности носителя информации его изъятие не представляется возможным, поэтому осмотр происходит опосредованно, через информационно-телекоммуникационную сеть. При этом в качестве инструмента осмотра используется оборудование, подключенное к данной сети (рабочая станция) и находящееся, как правило, в подразделении органа предварительного следствия либо у привлекаемого к расследованию специалиста. Поскольку носитель следовой информации невозможно изъять в натуре, с него снимают копию, максимально отражающую значимые для уголовного дела признаки[2].

К такому следственному действию также привлекаются понятые, также обладающие некоторым объемом знаний в области компьютерных

---

[1] См. об этом подробнее: David Griffith How To Investigate Cybercrime // URL:http://www.policemag.com/channel/technology/articles/2003/11/how-to-investigate-cybercrime.aspx

[2] См.: Старичков М.В. Использование информации из компьютерных сетей в качестве доказательств / М.В. Старичков // Право и кибербезопасность. 2014. N 2. С. 40.

технологий, достаточным для понимания сути проводимого следственного действия[1]. Необходимость обладания специальными знаниями для понятых обусловлена значением их участия в следственных действиях.

Так, в рамках действующего уголовно-процессуального законодательства понятые вызываются для удостоверения факта производства следственного действия, его хода и результатов[2]. Поскольку при выполнении «традиционных» следственных действий достаточно обычного наблюдения за ходом следственного действия, то в случае работы с компьютерными или иными устройствами, необходимо не только наблюдать за ходом следственного действия, но и за происходящим на устройстве, где совершение ошибок, или умышленные действия могут быть не замечены лицами, не обладающими достаточными знаниями в данной сфере.

Другой процессуальной формой использования специальных знаний является производство судебной экспертизы, а именно компьютерно-технической экспертизы. На разрешение эксперту ставятся вопросы общего диагностического характера о наличии в устройстве (включая внешние карты памяти и сим-карты) каких-либо файлов (текстовых, графических, музыкальных, видеофайлов, фотографий, СМС-сообщений, файлов Cookie, web-файлов, вредоносного ПО и др.), и эксперт извлекает весь физический дамп памяти.

Если следователя интересует конкретная информация (как в случае, если подозреваемый, свидетель либо потерпевший указывают на то, что преступные действия субъекта фотографировались или записывались на видео, но фотографии из телефона или компьютера были удалены), то

[1] См.: там же.

[2] См.: УПК РФ Ст. 170. Ч. 1

задаются соответствующие вопросы с указанием временного интервала удаления файлов, возможности их восстановления[1].

Также могут быть поставлены вопросы о служебных данных, имеющихся закладках интернет-страниц, паролей хранящихся в памяти устройств, пользователях, зарегистрированных в Log-файлах, логах сканирования антивирусных программ, имеющихся прокси, I2p, TOR соединений.

Специфический характер экстремистских действий в социальных сетях, или иное косвенное использование социальных сетей в экстремистской деятельности закономерно влечет тесное взаимодействие следователя со специалистом в компьютерной сфере.

Постановление Пленума Верховного Суда РФ от 28.06.2011 N 11 "О судебной практике по уголовным делам о преступлениях экстремистской направленности" предусматривает в необходимых случаях для определения целевой направленности информационных материалов использование специальных знаний в форме лингвистической экспертизы. К такой экспертизе могут привлекаться, помимо лингвистов, и специалисты иной области знаний (психологии, истории, религии). В связи этим представляется целесообразным объединить специальные знания данного вида в единую группу, связанную прежде всего, с лингвистическими экспертизами.

Общая цель лингвистической экспертизы в этом обозначается как «выявление смысловой направленности текстов и используемых пропагандистских приемов», ее выводы нередко становятся основой в процессе квалификации экстремистских материалов: «...определяющим является смысловая функция таких сообщений, то, ради чего, в подтверждение каких взглядов и идей они используются, какие

[1] Скобелин С.Ю. Указ. соч. С. 33

представления и установки и какими средствами пропагандируются, навязываются читателям (слушателям, зрителям)».

Поэтому, представляется целесообразным рассмотреть использование специальных знаний в форме лингвистической судебной экспертизы и следующие характерные особенности, связанные с её подготовкой и назначением: обязательный характер экспертизы, что входит в объект экспертизы, какие вопросы задаются эксперту.

Оценивая Постановление Пленума N 11, необходимо отметить его недостаточность для решения некоторых проблем, возникающих при расследовании преступлений экстремистской направленности[1].

Так, Пленум Верховного Суда Российской Федерации не дал определения таких понятий как «ненависть», «вражда», «социальная группа», а также оставил без однозначного ответа вопрос о том, является ли обязательным производство экспертизы по делам о преступлениях экстремистской направленности, либо вывод о направленности преступления можно сделать на основе заключения, либо показаний специалиста, а может быть, и вовсе на основе иных доказательств или внутреннего убеждения следователя[2].

Также остался без ответа и вопрос о различиях между экстремистскими побуждениями и иными. Так, не является экстремистской пропагандой высказывания лиц с низким культурным уровнем или образованием, из-за чего неспособных адекватно аргументировать свою точку зрения, а также вести дискуссию и сознавать степень социальной ответственности за произнесенные слова.

---

[1] См.: Борисов С.В., Жеребченко А.В. указ. соч. С.104

[2] См. об этом подробнее: Постановление Пленума Верховного Суда РФ от 28.06.2011 N 11 (ред. от 28.10.2021) "О судебной практике по уголовным делам о преступлениях экстремистской направленности"// СПС «Консультант Плюс».

Так же нельзя считать экстремистской пропагандой распространение идей избранности последователей той или иной конфессии. Такие взгляды встречаются практически во всех религиях, однако такая пропаганда является экстремизмом только в том случае, если включает в себя требование изменить объем гражданских прав и обязанностей лица или унижает национальное достоинство той или иной этнорелигиозной группы.

При этом необходимо отметить неоднозначность и толкования самого Федерального закона от 25 июля 2002 г. N 114-ФЗ "О противодействии экстремистской деятельности". Так, в Комментариях к Федеральному закону N 114-ФЗ указана обязательность оценки специалистом (экспертом) материалов при отнесении их к экстремистским, при этом также указано, что не любое исследование, проведенное специалистами (экспертами), суд может расценивать как экспертизу[1], что противоречит формулировке «в необходимых случаях», использованной в постановлении Пленума Верховного Суда РФ N 11. Сложившаяся судебная практика также предполагает проведение экспертизы в отношении любого материала, обнаруженного в пространстве социальных сетей.

Таким образом, лингвистическая или комплексная судебная экспертиза становится обязательной по делам о преступлениях экстремистской направленности, выступая в качестве дополнительного доказательства к числу имеющихся, дополняя обвинительное заключение и приговор суда. Отправляя материалы на лингвистическую экспертизу, следователь решение о преступности деяния фактически оставляет за экспертом. Рассматривая необходимость проведения лингвистических экспертиз целесообразно говорить о среднем и мягком языках вражды, когда у следователя могут возникнуть затруднения в определении значения и

[1] См.: Смушкин А.Б. Комментарий к Федеральному закону от 25 июля 2002 г. N 114-ФЗ "О противодействии экстремистской деятельности" (постатейный) // СПС КонсультантПлюс. - 2015.

направленности материалов. Однако в ситуации жесткого языка вражды, когда имеется прямое выражение ненависти, очевидные призывы к насилию по отношению к другой расе, нации, конфессии. Экспертиза таких материалов представляется излишней.

Рассматривая лингвистические экспертизы необходимо отметить, что существует неопределенность объекта таких экспертиз, особенно в условиях проведения таких экспертиза по материалам сети Интернет. наиболее узкое понятие объекта лингвистических экспертиз: продукты речевой деятельности человека (от отдельного слова до текста в целом или группы текстов), зафиксированные в письменной форме (в том числе устные тексты, записанные с помощью букв)[1]. Такое определение предполагает необходимость стенографирования устного текста, вместе с тем, учитывая, что на такие экспертизы могут направляться видеоролики или аудиозаписи, содержащие необходимый текст в устной форме, фиксация устного текста представляется нецелесообразным, особенно в ситуации, когда в записи существует несколько звуковых дорожек или звуковая дорожка воспроизводится одновременно с текстом, при стенографировании порядок нарушается, что препятствует восприятию текста в целом.

Традиционным определением объекта лингвистической экспертизы является его обозначение как единиц языка и речи, текстов, представленные на любом материальном носителе[2]. Такое определение позволяет оценивать тексты как письменные, так и устные, однако, необходимо отметить, что непосредственно текст характерен для экстремистских материалов в виде самиздата или лозунгов озвученных при массовой аудитории, в то время как

---

[1] См.: Возможности производства судебной экспертизы в государственных судебно-экспертных учреждениях Минюста России. // М., 2004. С. 421.

[2] См.: Россинская Е.Р. Теория и практика судебной экспертизы в гражданском и арбитражном процессе: Научно-практическое пособие / Под ред. д.ю.н., проф. Е.Р. Россинской. - М.: Норма, 2011. - С. 136.

в сети Интернет и социальных сетях, в частности, наиболее характерны продукты так называемого Интернет-творчества, включающих в себя короткие ролики с музыкальным сопровождением, «демотиваторы», изображения с подписями, либо короткие лозунги, оформленные в виде изображения.

Исходя из более широкого толкования объектами экспертизы являются текст, включающий в себя другие продукты речевой деятельности до предложений и слов в отдельности, и (при его наличии) так называемый «антураж», несловесное содержимое материала, которое может оказывать влияние на восприятие текста, изменять характер материала[1]. Таким содержимым могут быть иллюстрации и другие изображения, фотографии, видеоряд, саундтрек и любые другие элементы, вплоть до оформления страницы с текстом. поэтому эксперту всегда необходимо исследовать не только отдельные текстовые единицы, такие как, непосредственно текст публикации или стенограмма видеозаписи, аудиозаписи, но и полностью весь контекст публикации, начиная от названия страницы, на которой опубликован такой материал.

Так, приговором Октябрьского районного суда города Уфы от 10 ноября 2010 года N 1-641/2010 судом было установлено, что подсудимый разместил на видео-хостинге видеозапись экстремистского содержания, на котором были использованы фразы на русском, английском и немецком языках, в частности была использована фраза «Burn and Kill the Beast!» в переводе «Жечь и убивать скотов!», которая в отрыве от видеоряда может быть вариативно истолковано и не является направленной к конкретной расе, национальности или конфессии, однако, фраза сопровождалась изображением оружия, направленного на еврейский

[1] См. об этом подробнее: Подкатилина М.Л. К вопросу о лингвистической экспертизе экстремистских материалов / Подкатилина М.Л. //"Эксперт-криминалист". - 2010. - № 4. - С.20

символ, что характеризуется как призыв именно в отношении определенной нации. Таким образом, для экспертного исследования целесообразно использование всего объема имеющихся материалов для полноты и достоверности экспертизы.

Рассматривая лингвистическую экспертизу немаловажно также отметить проблему постановки вопросов эксперту. Так, в комментариях к ФЗ N114-ФЗ указано, что перед экспертом рекомендуется ставиться следующие вопросы[1]:

– содержатся ли в материалах, представленных на экспертное исследование сведения, включающие в себя призыв к экстремистской деятельности; если да, то в каких именно фрагментах и высказываниях исследуемых материалов они содержатся; какова форма их выражения: вопроса, предположения, утверждения.

– содержатся ли в материалах высказывания, содержащие призыв к насильственному захвату власти.

– содержатся ли в материалах высказывания побудительного характера, направленные призыв к насильственному изменению конституционного строя Российской Федерации.

– имеются ли в материалах высказывания, содержащие подстрекательство на осуществление террористической деятельности в открытой либо скрытой форме.

– имеются ли в материалах высказывания или выражения, публично оправдывающие терроризм;

[1]См. об этом подробнее: Смушкин А.Б. Комментарий к Федеральному закону от 25 июля 2002 г. N 114-ФЗ "О противодействии экстремистской деятельности" (постатейный) // СПС КонсультантПлюс. - 2015.

– имеются ли в материалах высказывания или выражения, направленные на возбуждение расовой, национальной или социальную розни[1];

– имеются ли в материалах слова, высказывания или выражения, призывающие к осуществлению террористической деятельности.

В числе вопросов, предлагаемых к лингвистической экспертизе, встречаются также вопросы о принадлежности материалов к внесенным в список экстремистских.

Однако, в постановлении Пленума ВС РФ прямо указано, что при назначении судебных экспертиз по делам о преступлениях экстремистской направленности не допускается постановка перед экспертом таких вопросов, которые не входят в компетенцию эксперта, вопросов правового характера, связанных с оценкой деяния, разрешение которых относится к исключительной компетенции суда. В частности, вопросы о том, содержатся ли в тексте призывы к осуществлению экстремистской деятельности, о направленности информационных материалов на возбуждение ненависти или вражды перед экспертами поставлены быть не могут.

В действительности, такие вопросы носят юридических характер, поскольку публичные призывы к экстремистской деятельности, либо возбуждение ненависти или вражды образуют составы преступлений соответствующих статей УК, из-за чего возникает ситуация, когда эксперт, отвечая на подобные вопросы подменяет собой функции следователя и суда.

Поэтому необходимо отметить, что в вопросы, сформулированные к эксперту-лингвисту, не рекомендуется включать юридическую термины, такие как «призыв» или «экстремизм». Поэтому понятие экстремистской деятельности как правило распределяется на смысловые компоненты

[1] См.: Алпеева М.А. Отдельные вопросы назначения экспертизы экстремистских материалов, задержанных при пересечении таможенной границы / М.А. Алпеева // Таможенное дело. - 2013. - № 2. - С. 20

термина или его толкований, вследствие чего имеют место выражения, существующие в границах литературного языка[1]. К таким выражениям неюридического характера относятся «информация об исключительности, превосходстве или неполноценности лиц по признаку их расы или национальности», «указание на причинно-следственную связь между неблагоприятным положением в прошлом, настоящем или будущем одной расы, национальности, религии и действиями или фактом существования другой расы, национальности, религии» или «негативная оценка действий отдельных рас, национальностей, конфессий» и другие подобные формулировки.

Однако, разложение понятия экстремистской деятельности на смысловые составляющие при постановке вопросов перед экспертом позволяет удовлетворять требованиям Пленума Верховного Суда РФ, но в сущности эксперт отвечая на такие вопросы отвечает на изначальный вопрос о наличии экстремистского призыва, поскольку негативная оценка расы, национальности, конфессии удовлетворяет понятию среднего или мягкого языка вражды, в зависимости от используемых формулировок, что связано с используемыми законодательством понятиями, входящими в экстремистскую деятельность, такими как пропаганда исключительности, превосходства или наоборот неполноценности по расовому, национальному или религиозному признаку[2].

Меняя понятие «пропаганда» на понятие «информация» сущностных изменений вопроса не происходит. Тем не менее, необходимо отметить, что в вопросах понимания семантического значения, побудительного характера

---

[1] См.: Иссерс О.С. Орлова Н.В. Лингвистические корреляты понятия «вовлечение в экстремистскую деятельность» / Иссерс О.С. Орлова Н.В. // Политическая лингвистика. - 2017. - № 3. - С.132

[2] См.: О противодействии экстремистской деятельности: федеральный закон от 25.07.2002 N 114-ФЗ (ред. от 31.07.2020) [Электронный ресурс]. Доступ из справ.-правовой системы «Консультант Плюс» Ст. 1

юридическая наука и лингвистика находятся в состоянии тесной связи, при которой достаточно сложно определить, где заканчивается специальное знание в области языка и начинается правовая оценка самого деяния, которое носит словесный характер, а потому субъективная, объективная стороны, а также сам объект полностью охватывается одной экспертизой, из-за чего возникает ложная установка на достаточность нахождения субъекта преступления.

Однако, отмечается спорный характер экспертных исследований, поскольку нередко возникает ситуация, когда оценки одного материала разными экспертами являются прямо противоположными[1]. При этом необходимо отметить, что такое расхождение связано в первую очередь не с ошибками, как при проведении криминалистических экспертиз, а с субъективным характером оценки материалов, различием используемых методик, различиями толкования и определения семантики высказываний.

Необходимо также отметить проблему оценки возможности при проведении лингвистических экспертиз, в отличии от большинства других экспертиз формулировка возможности относится не совершению того или иного действия, но возможному последствию от совершенного деяния.

Так, формулировка «*высказывание способно разжечь межрасовую межнациональную, или межрелигиозную ненависть и вражду*» характеризуется асимметричностью, неопровержимостью, но верифицируемостью[2].

Такой ответ предполагает, что он будет истинен при любом количестве людей, на которых высказывание воздействовало вплоть до одного, вместе с тем ответ будет истинен и при отсутствии людей, на

[1] См. об этом подробнее: Бринев К.И. Судебная лингвистическая экспертиза по делам о религиозном экстремизме/ Бринев К.И. // Вестник Томского государственного университета. – 2013. - № 376. - С. 7

[2] См.: там же, С. 9

которых материал воздействовал, поскольку формулировка «возможно» предполагает такую вероятность в будущем.

В таком случае, необходимо оценивать не возможность возбуждения ненависти таким высказыванием, а направленность, наличие призыва в скрытой или открытой форме.

Таким образом, лингвистическая экспертиза материалов в пространстве социальных сетей обладают обязательным в результате сложившейся практики характером, объектом таких экспертиз являются как сам текст в широком смысле, так и сопутствующие элементы (антураж), включающие в себя изображения, видеоряд, аудиозаписи или саундтрек. При формулировке вопросов при назначении экспертизы необходимо избегать юридических конструкций, из-за которых в ходе экспертизы будут формулироваться ответы правового характера.

Так, целесообразной представляется следующая формулировка вопросов:

1. *Выражают ли словесные или изобразительные средства, использованные в материале, унизительные характеристики или отрицательную эмоциональную оценку и негативную установки в отношении какой-либо расовой, этнической, религиозной иной социальной группы, её представителей? Если да, то какой именно, в какой форме?*

2. *Содержится ли в материале информация, направленная на побуждение к действиям против какой-либо расы, нации, конфессии иной социальной группы, её представителей? Если да, то какая именно, в какой форме?*

1. *Имеются ли в спорном речевом произведении высказывания оскорбительного характера по отношению к лицам какой-либо расы, национальности, конфессии или иной социальной группы?*

2. *Носит ли указанный материал характер призыва?*

3. *Создается ли образ врага в указанном материале?*

Экспертиза не может устанавливать виновность лица, поскольку это не может относиться к ведению эксперта, поэтому эксперт-лингвист как лицо, обладающее знаниями в области семантики и лексики, должен установить негативный окрас материалов, оценить слова, используемы для обозначения социальных групп и используемые для их негативной или превозносящей характеристики, при комплексной экспертизе эксперт-психолог должен определить используемые автором публикации методы побуждения к действиям, способы воздействия на читателя, зрителя, слушателя, что в дальнейшем оценивается следователем и судом как доказательство экстремистской направленности материалов.

2.4. Криминалистическая профилактика преступлений экстремистской направленности в социальных сетях

В современном мире практически невозможно избежать постоянного присутствия социальных сетей, и общество одержимо ими. Они повсюду. Смартфоны, компьютеры и планшеты обеспечивают человека или группу круглосуточным безостановочным доступом к Интернету и форумам, что позволяет постоянно обмениваться информацией[1]. Люди уже не сосредоточены на непосредственном общении; вместо этого они полагаются на социальные сети, чтобы встречаться и общаться с членами своей группы интересов.

Проникновение глобальной сети Интернет в общественную жизнь привело к тому, что правоохранительные органы действуют в мире, который не только использует, но и требует присутствия социальных сетей[2]. В таком случае социальные сети не могут рассматриваться как проблема само по себе, необходимо действовать не против Интернета или социальных сетей, а действовать в условиях глобальной сети и её объектов.

Убеждения экстремистов часто имеют глубинные причины в позиции человека или группы по конкретному вопросу. Нередко они относятся скептически к любой точке зрения, которая не поддерживает их собственную, и еще больше склоняются к экстремальному пределу в своих убеждениях. Рациональная беседа или дебаты обычно неэффективны, и прийти к общей точке зрения практически невозможно.

---

[1] См. об этом подробнее: Попкова Я.А. Блоггинг как специфическая форма социальной активности молодежи// Социальная активность молодежи как необходимое условие развития общества. Материалы международной научно-практической конференции. Под редакцией Г. В. Ковалевой. 2019. С. 351

[2] Финч Р., Флауэрз К. Внутренний насильственный экстремизм и роль социальных сетей (в переводе ФГКУ «ВНИИ МВД России»)/ Финч Р., Флауэрз К. // Полис Чиф. - США. - 2013. - том 80, № 6. - С. 34

Такая саморадикализация через социальные сети позволяет насильственным экстремистским группам и отдельным лицам поддерживать анонимность и ограничить или полностью избавиться от возможной встречи с правоохранительными органами. В результате экстремисты свободно обсуждают грандиозные идеи о применении насилия и строят сложные и хорошо организованные планы, которые могут быть реализованы отдельным лицом или группой[1].

Вместе с тем, учитывая опыт противодействия экстремизму в России и за ее пределами, необходимо сделать вывод о том, что решение проблемы экстремизма не может быть основано исключительно на силовых методах. Они позволяют на некоторое время уменьшить или устранить угрозу проявления экстремизма, однако, эта угроза будет сохраняться, пока идеология экстремизма сохраняет свою привлекательность для последователей и существует возможность свободного ознакомления с ней. В таком случае необходимо отметить, что усилия в сфере противодействия экстремизму должны быть сконцентрированы, в том числе, на профилактике экстремизма[2].

В России в настоящее время преобладает так называемый стихийный тип экстремистской активности. Что, с одной стороны, позволяет оценивать низкий уровень организованности молодежного экстремизма, а с другой –

---

[1] См.: Черных, Н. А. К вопросу о профилактике экстремизма: динамика представлений об экстремизме у молодёжи Борисоглебского городского округа / Н. А. Черных, С. В. Иванкович // Непрерывное образование в современном мире: история, проблемы, перспективы. : Материалы VI Всероссийской с международным участием научно-практической конференции, Борисоглебск, 30 марта 2019 года. – Борисоглебск: Издательство «Перо», 2019. – С. 320-324

[2] См. об этом подробнее: Григорьев А.Н. Проблемы профилактики экстремизма в информационной среде/ Григорьев А.Н. // В сб.: Противодействие терроризму и экстремизму: ситуационный подход (в условиях организации и проведения крупных спортивных мероприятий, с учетом геополитического положения региона и др.): сб. науч. тр. по мат. науч.- практ. конф. –Калининград: изд-во БФУ им. Канта, 2017. – С. 30.

требует специфических форм организации системной профилактической работы[1], так как в стране очень высок уровень стихийного экстремизма, имеющего латентный характер и проявляющегося в редких, но жестоких действиях молодых людей[2].

Необходимость проведения профилактических мер, задачей которых является устранение самих причин и условий, способствующих появлению экстремизма как идеологии находит свое отражение и в федеральном законодательстве, в частности, федеральный закон "О противодействии экстремистской деятельности" относит профилактику экстремизма к основным направлениям противодействия[3].

Основными направлениями профилактики по мнению Т.А. Юмашевой являются[4]:

– Консолидация государственных и негосударственных объединений и организаций по разработке комплекса мер, направленных организацию досуга, пропаганду ЗОЖ, семейное психологическое консультирование молодых людей, просветительская работа по профилактике поведенческих девиаций и асоциальных явлений.

---

[1] См. об этом подробнее: Кобец, П. Н. О радикализме и экстремизме - основе террора и необходимости противодействия экстремизму и терроризму в интенсивно меняющемся мире / П. Н. Кобец // Наука: прошлое, настоящее, будущее : сборник статей Международной научно-практической конференции: в 3 частях, Пермь, 25 июня 2017 года. – Пермь: Общество с ограниченной ответственностью "Аэтерна", 2017. – С. 167-169.

[2] См. об этом подробнее: Экстремизм в условиях прогресса информационно-компьютерных технологий / Е. О. Кубякин, Л. В. Карнаушенко, Е. М. Куликов, Г. А. Городенцев ; Краснодарский ун-т МВД России. - Краснодар : Краснодарский ун-т МВД России, 2015. - С. 65

[3] См.: Федеральный закон «О противодействии экстремистской деятельности» № 114-ФЗ от 25.07.2002 (ред. от 30.07.2020) // СПС «Консультант Плюс».Ст. 3.

[4] Цит. по: Новикова Г.А., Новикова Л.А. Профилактика экстремистских проявлений в молодежной среде: Методические рекомендации/ Новикова Г.А., Новикова Л.А. // Архангельск, 2014. 46 с.

– Взаимодействие с родителями. Поскольку молодые люди, склонные к принятию экстремистских моделей поведения, проживают в неблагополучных семьях, способствующих развитию таких идей. вследствие чего, необходимо: расширять знание родителей о проблеме экстремизма, профилактика ошибок в воспитании, использования мер педагогического воздействия, в том числе включение родителей в систему педагогического обучения, а также вовлечение родителей совместно с детьми в активную общественно-полезную деятельность в школе

– Взаимодействие с молодежью, выражающееся в организация досуга, поскольку «внеурочная воспитательная деятельность представляет возможность молодому человеку не только свободу выбора действий, но и создает условия для упражнения и тренировки, определенных эмоционально-волевых и нравственно-поведенческих качеств.»

Молодёжь (от 14 до 30 лет) представляет собой основную группу риска, наиболее подверженную влиянию последователей террористических (экстремистских) взглядов и идей[1]. Особое внимание следует обратить на обучающихся в средних и высших образовательных учреждениях.

Поэтому одним из важнейших факторов профилактики экстремизма является своевременное обнаружение и воспитательная работа с лицами, вовлеченными или находящимися под угрозой вовлечения в экстремистские сообщества[2].

Данная возрастная группа имеет мало «иммунизирующих» к такой пропаганде личностных ресурсов, в частности:

---

[1] См.: Приложение 1

[2] См. об этом подробнее: Черных Н.А., Ермакова О.В., Иванкович С.В. Работа по профилактике экстремизма в молодёжной среде (на примере борисоглебского городского округа) // Психология и педагогика: актуальные проблемы и тенденции развития: материалы IV Международной научно-практической конференции 14-15 ноября 2018 г. / Отв. ред. А.А. Долгова. - ООО «Издательство Ритм», Воронеж, 2018. - С. 118-120

- подверженность чужому влиянию, внушению и манипулированию;
- недостаточная стрессоустойчивость;
- глубокое погружение в интернет-пространство;
- романтизация и героизация антиобщественных и агрессивных действий.

В молодёжной среде легче приживаются радикальные взгляды и убеждения, наиболее быстро происходит накопление и реализация экстремистского потенциала[1].

К группе риска, как правило, относятся:

- дети, внуки и родственники экстремистов или террористов;
- лица из неполных семей;
- лица из асоциальных семей;
- лица с ограниченными физическими возможностями;
- лица из семей с гиперопекой.

Склонность молодежи противопоставлять себя всему миру, «сопротивляться системе» успешно используются идеологами терроризма. Помимо этого, кризис социально-экономической сферы, отсутствие уверенности в завтрашнем дне пугают молодых людей, которые видят решение данных проблем в радикальных, насильственных мерах.

В целях выявления детей, попавших под влияние неформальных молодежных объединений или секты, необходимо обращать внимание на следующие факторы:

---

[1] См.: Макарова, З. С. Влияние информационного экстремизма на сознание молодежи / З. С. Макарова // Организация работы с детьми и молодежью по месту жительства: опыт, проблемы и перспективы развития : Сборник материалов Республиканской конференции по вопросам организации работы с детьми и молодежью по месту жительства, Казань, 30 ноября 2017 года. – Казань: Государственное бюджетное учреждение "Республиканский центр молодежных, инновационных и профилактических программ", 2017. – С. 64-66.

1. Ужесточение манеры поведения к более резкой и грубой формам. Ребенок становится нетерпим к чужой точке зрения. Формируется четкая система «свой-чужой», где «чужой» всегда неправ.
2. Характерное обесчеловечивание «чужих», акцент на том, что представители «чужой» социальной группы не являются людьми, препятствуют нормальному функционированию общества и государства.
3. Резкая смена эмоционально-психологического фона (перепады настроения, спонтанная агрессия и т.д.)
4. Резкое увеличение числа разговоров на политические, религиозные и/или социальные темы, в ходе которых высказываются радикальные суждения с признаками нетерпимости.
5. Неадекватная или агрессивная реакция на повседневные, привычные вещи, проявляет подчеркнутое безразличие к повседневным делам.
6. Изменение круга общения, кардинальное изменение внешнего облика в соответствии с правилами неформального объединения или секты.
7. В элементах одежды и аксессуаров непонятная и нетипичная символика или атрибутика. Особое внимание необходимо обратить на агрессивную и вызывающую символику, такую как, например, поднятый вверх сжатый кулак. *Так, надпись A.C.A.B. («All Coppers Are Bastards» (англ.. «Все менты — убл*дки»)) характерна как для леворадикальных движений, так и для праворадикальных.*
8. Изменение речи подростка. Он использует нетипичные для повседневного общения и нехарактерные для него выражения, слова, термины, жаргонизмы. А также в грубой форме выражает неодобрение к людям другой национальности, религии, любой

другой социальной группы. В речи встречаются устойчивые речевые штампы и конструкции побудительного или пропагандистского толка.

9. Вступление в открытую словесную конфронтацию с педагогом или другими учащимися; отстаивание при этом ценностей, противоречащих интересам общества.
10. Отказ от прежних интересов, проявление апатии в учебном процессе. Проявление интереса к нестандартным вопросам, не относящимся к межличностным отношениям, обучению, художественной литературе, фильмам, компьютерным играм или другим характерным для возраста темам.
11. Явная антигосударственная (в особенности, в отношении правоохранительных органов) и антиобщественная позиция.

Особенные (характерные черты определенной экстремистской (террористической) идеологии:

Праворадикальные движения, скинхеды, неофашисты и т.д. Молодежные фашистские объединения отличаются подражанием немецкому нацизму, при этом агрессия направляется не на славянские народы, а на выходцев из Азии, Кавказа и др.

1. В речи нередко употребляется понятие нации, чистоты крови, расы и т.п. Дается негативная оценка остальным национальностям. Ксенофобия проявляется, в частности, в использовании используя военных метафор («захватчики», «оккупанты», «агенты инородной экспансии» и т.д.) или аналогии с животным миром.
2. Частные проявления могут выражаться в представлениях о наличии некоего «тайного мирового правительства», масонского сообщества, «Сионистского оккупационного правительства».

3. В одежде встречаются кельтские узоры, рунические записи, черепа и оружие, нередко с дополнительным контекстом в виде угрозы. К примеру, футболка с черепом и перекрещёнными бейсбольными битами, и подписью бейсбольный клуб (baseball club). Также достаточно часто встречаются изображения стилизованной свастики или иной сходной символики третьего рейха до степени узнавания, но не полного сходства. Отдельно необходимо отметить такие бренды как "Thor Steinar" ("Тор Штайнар"), Русультрас, Ультраснордик, Svaston.
4. Особое внимание следует обратить на поведение в определенные дни и даты, в частности, 20 апреля (день рождения Адольфа Гитлера), праворадикалы нередко поздравляют друг друга «с праздником», в издевательской манере называют фразу «спасибо деду за победу», в целом, нередко Адольф Гитлер называется «дедом».
5. Часто используется сочетание 1488 в различных вариациях, выражения «от сердца к солнцу» или аналогичные.

Леворадикальные движения, «антифа» находятся на противоположной политической позиции. Основная цель – борьба с фашистами *(важно учитывать, что представители некоторых ветвей данного движения относят к «фашистам» не только представителей правых взглядов, но и любых несогласных)* нередко насильственными методами.

1. В речи нередко употребляют понятия «фашист», «нацист», «Гитлер» в качестве ругательств по отношению к несогласным.
2. Публично выступают против любых форм дискриминации (национализм, расизм, неонацизм, антисемитизм, ксенофобию, гомофобию). Некоторые движения придерживаются «теории

привилегий», в связи с чем сами склонны проявлять дискриминационное поведение к национальному или расовому большинству.

3. Склонность к интерпретации действий «чужих» как той или иной формы дискриминации.
4. Некоторые ответвления активно поддерживают ЛГБТ и используют связанную символику
5. Характерная «актикорпоративная» позиция, критика капитализма, власти денег, иерархии в любой форме.
6. Наиболее примечателен единый символ движения – два параллельных флага: черный и перекрывающий его красный, развивающиеся в левую сторону.

АУЕ - «арестантский уклад един», название и девиз предположительно существующей криминальной субкультуры, 17 августа 2020 Верховный Суд Российской Федерации принял решение о признании движения экстремистским.

1. АУЕ в силу своей специфики редко носит индивидуальный характер. Как правило, это группа подростков.
2. Резкое падение успеваемости.
3. Использует символ – восьмиконечная «тюремная» звезда.
4. Проявляет заинтересованность «воровской романтикой» (фильмы, сериалы, музыка).
5. Употребляет тюремный жаргон (пахан, общак, смотрящий, опущенный), «АУЕ! Ворам свободу!»
6. Занимается вымогательством у других подростков «в общак» за «крышу».
7. Хвастается связями с «криминалитетом»

8. Совместная травля «опущенных», отказавшихся принимать участие в «общаке».
9. Во внешнем виде стремится создать образ «зэка», «гопника», или иного вида уголовника. Тюремная стилистика на футболках, значках.

Ваххабизм. Ваххабизм – это нетрадиционное для мусульман России течение ислама, лидеры которого в качестве одного из приоритетных направлений своей деятельности видят вербовку российской молодежи. Так, на территории РФ функционируют так называемые центры исламской молодежи, где члены террористических организаций (например, «Хизбут-Тахрир», «Рефах», «Аль-Фатх», «ИДУ», «НУР») обучают молодежь основам радикального ислама и осуществляют вовлечение в экстремистские объединения[1]. Помимо этого, учебные центры предоставляют своим учащимся стипендии, что делает обучение крайне привлекательным для молодежи из малообеспеченных семей.

1. Нетерпимость к атеизму и другим религиям (в том числе и в особенности, к мусульманам).
2. Ваххабизм критикует употребление кофе, ношение шелковой одежды, музыку и пение.
3. Активная пропаганда своего религиозного учения среди сверстников.
4. Критика прав человека, как фактора морального разложения.
5. Критика демократии как преступления против Бога.
6. Критика прав женщин и феминизма.

[1] См. об этом подробнее: Проявление экстремизма в молодежной среде. Сайт ГУ МВД России по г. Санкт-Петербургу И Ленинградской области // [Электронный ресурс] – Режим доступа: https://фрунз.78.мвд.рф/news/item/21056956?year=2020&month=9&day=11 (дата обращения: 20.05.2022)

7. Выраженный антисемитский и антизападный настрой.

8. Исключительно негативное отношение к памяти предков (посещение и уход за захоронениями и т.п.)

9. Используют такие понятия как «джихад» (священная война), «кафир» (неверный), «ширка» и «мунафики» (многобожники и вероотступники).

При этом необходимо отличать экстремистские взгляды от юношеского максимализма и проявлений незрелой ретрансляции увиденного в Интернете, а также обычного хулиганства. Ключевое различие проявляется в крайней идеологизированной готовности к совершению радикальных действий. Поэтому необходимо учитывать признаки в совокупности. Но также важно помнить, что попавший под влияние неформальных молодежных объединений или секты может не соответствовать по тем или иным причинам всей совокупности признаков.

Вместе с тем, целесообразно использование и тех преимуществ, которые глобальная сеть может дать. *Так, одна из подсистем аппаратно-программного комплекса «Демон Лапласа» «Ангел хранитель», разрабатываемая НКО, предназначена для фиксации интереса учащихся к изображениям, видеоматериалам и текстам экстремистского содержания, о чем она оповещает родителей. Программный комплекс запоминает типовые формулировки и словосочетания, используемые вербовщиками ИГИЛ, после чего соотносит их с публикациями подростков*[1].

Использовании систем автоматического поиска и фиксации экстремистских материалов позволит находить очаги распространения экстремистской идеологии еще на фазе информационной обработке

[1] См.: Программа «Ангел хранитель» будет отслеживать интерес подростков к ИГИЛ [Электронный ресурс]. – Режим доступа: https://mediastancia.com/news/4066. – Загл. с экрана. (дата обращения: 20.05.2022)

потенциального экстремиста, что позволяет локализовать вербовщика или распространителя разрушительной идеологии.

Наряду с автоматическим мониторингом материалов представляется целесообразным привлечение института школы, как места, в котором происходит первичная социализация личности, связанное с реализацией школой воспитательных функций. Открытый характер страниц в социальной сети, позволяет осуществлять первичный мониторинг учащихся и выявления ситуаций риска.

Так, администрацией Псковской области было предложено проведение регулярного мониторинга учителями страниц школьников в социальных сетях, что позволит определить изменения в поведении подростков[1].

Другой формой профилактики, связанной не с обнаружением проблемы в зачаточном состоянии, но препятствии развитию самой экстремистской идеи. Она находит свое выражение в профилактических занятия в школах и ВУЗах, проведении тематических конференций, распространению идей, противоположных экстремистским в пространстве СМИ и глобальной сети Интернет. Целесообразным является привлечение к профилактической работе лиц, популярных именно в пространстве сети Интернет (администраторов популярных групп в социальных сетях, известных блогеров и авторов популярных каналов на видеохостингах), поскольку в подростковой среде отмечается больший интерес к социальным сетям и интернет-сети, в целом, чем к телевиденью или радио[2].

---

[1] См.: В Пскове советуют учителям вести мониторинг страниц школьников в соцсетях [Электронный ресурс]. – Режим доступа: https://ria.ru/incidents/20161115/1481444181.html?inj=1. – Загл. с экрана. (дата обращения: 20.05.2022)

[2] См. об этом подробнее: Хачукаева, К. И. Социальные сети и профилактика экстремизма среди учащейся молодежи / К. И. Хачукаева, А. Р. Мидаева // Фундаментальные основы инновационного развития науки и образования : сборник статей VI Международной научно-практической конференции : в 3 ч., Пенза, 30

При этом необходимо отметить, что тонкие методы экстремистской пропаганды требую более тонкого подхода в противодействии. *Так, любое действие запретительного характера будет трактоваться идеологами экстремизма как борьбу со свободой слова, попыткой установления полицейского государства или борьбой с инакомыслием.* В таком случае блокировка объектов сети Интернет должна сопровождаться информацией, объясняющей причины запрета доступа, что позволит лишить идеологов экстремизма возможности позиционирования себя как жертвы.

Оценивая предрасположенность к нетерпимости к «другим» лиц с недостаточно развитой эмоциональной сферой, необходимо отметить целесообразность поддержки мероприятий, образовательных программ, направленных на развитие эмпатии, как способности к сопереживанию, что несколько расходится с отечественной культурой воспитания ребенка, что предполагает определенные эмоциональные запреты на чрезмерное эмпатическое сопереживание («будь мужчиной, не плачь, не кричи, успокойся»), что влечет за собой риск формирования бескомпромиссного мировоззрения, которое достаточно быстро может радикализироваться.

Необходимо отметить также и влияние социальных факторов на формирование экстремистских идей, когда ситуация затянувшегося кризиса, видимой лицом несправедливости, формирования образа «врага» на основе обид, перенесённых от лиц, которые могут быть объединены по тому или иному признаку, влечет радикализацию взглядов и оценку насилия как единственного способа решения проблемы. В таком случае, деятельность, направленная на стабилизацию социальной обстановки, борьба с этнической преступностью также будут выполнять профилактические функции. Тем самым, лишая идеологов экстремизма возможности использования ситуации в своих интересах.

декабря 2019 года. – Пенза: "Наука и Просвещение" (ИП Гуляев Г.Ю.), 2019. – С. 11-13.

Таким образом, профилактические меры противодействия экстремизму в социальных сетях реализуются как общем порядке, в виде: мероприятий, направленных на повышения общественного благополучия и улучшения социальной обстановки, так и мер направленных на организацию досуга; взаимодействия с родителями и учителями, направленного на раннее предупреждение радикализации подростков; использования пространства социальных сетей для автоматического или индивидуального мониторинга распространения экстремистских идей в подростковой среде; привлечения СМИ и ресурсов сети Интернет для обеспечения противодействия самой экстремистской идеологии; формировании у подростков способности к сопереживанию, как механизма защиты от идей ненависти.

ЗАКЛЮЧЕНИЕ

В результате проведенного исследования мы пришли к следующим результатам и выводам.

На основе исследования, а также с позиции криминалистической науки в диссертации было обоснована необходимость введения в научный оборот понятия социальной сети, под которым предлагается понимать цифровое место человеческой деятельности (в том числе преступной) в глобальной сети Интернет, где лицо формирует социальные отношения с другими пользователями, а также создает, осуществляет поиск и использует информацию.

Было установлено то, что социальные сети как средство распространения информации обладают беспрецедентными возможностями, что также стало фактором широкого распространения социальных сетей.

Социальная сеть как новое пространство человеческой интеракции способна отражать в себе как сам процесс такого взаимодействия, так и его последствия – следы.

В криминалистическом аспекте социальные сети могут выступить достаточно информативным источником криминалистически значимой информации:

- о местоположении лица:
    - о его текущем эмоциональное состоянии (по статусу)
    - о месте работы или учебы
    - другой информации, нашедшей отражение в профиле сети

А также:

- определить маршруты перемещений
- определить интересы, предрасположенности, социальные связи

В результате проведенного исследования были установлены характерные особенности социальной сети как особого «места» социальной интеракции между людьми, связи с чем социальная сеть закономерно становится потенциальным местом совершения преступления. В результате чего в диссертации был предложен анализ цифровых объектов как потенциальных средств совершения преступлений экстремисткой направленности. К числу таких объектов могут быть отнесены отдельные текстовые сообщения, фотографии или иллюстрации, видео- или аудиозаписи.

Подробно описан механизм совершения преступления с использованием социальных сетей.

Особое внимание было уделено изменению ситуационной модели преступления: сеть выступает как место совершения преступления, в то время как средствами будут являться объекты материального мира: компьютерные устройства, которые использовались для доступа к сети Интернет, так и цифровые объекты, посредством которых осуществлялась преступная деятельность непосредственно в сети.

Будучи местом совершения преступления, она содержит значительное количество криминалистически значимой информации в виде цифровых следов. Определить физическое местонахождение данных следов не представляется возможным, более того, не представляется целесообразным.

Проанализирована возможность использования самой архитектуры и функциональных возможностей социальной сети, в частности в целях сокрытия преступления, или самого преступника.

В преступлениях, построенных по типу взаимодействия «человек-человек» инструментарий социальной сети становится средством взаимодействия между злоумышленником и жертвой, благодаря чему она

может сохранить информацию о местонахождении устройств злоумышленника и жертвы.

В результате, в отношении данных преступлений целесообразно расширительно толковать место происшествия, включая в него цифровое пространство и социальные сети, в частности. Поскольку именно там будет находиться интересующая следствие информация в виде переписки, опубликованных материалов, лог-файлов, IP-адресов. Именно там должен начинаться процесс расследования таких преступлений.

Проведенные нами исследования эмпирического материала показали то, что насильственные преступления по экстремистским мотивам в подавляющем большинстве случаев носят спонтанный характер, однако высокая доля таких преступлений совершается под влиянием чтения экстремистских информационных материалов и литературы, размещенных в пространстве сети Интернет. Следовательно, в качестве одной из первопричин насильственных действий становится совершение экстремистского преступления посредством компьютерных сетей.

Функциональные возможности социальных сетей предполагают осуществление массовой рассылки однотипных сообщений на контакт-коммуникационном и масс-коммуникационных уровнях, при условии, что каждое отдельное сообщение остается на уровне межличностного общения. Что требует выявления закономерных связей между различными элементами криминальных ситуаций посредством ситуационного анализа.

Автором выделены следственные ситуации в зависимости от контентного наполнения экстремистских сообщений в социальных сетях:

1. ситуации, когда экстремистский смысл сообщения никак не скрывается, а разжигающие ненависть и вражду призывы и сведения иди другие экстремистские идеи провозглашаются прямо и открыто, в связи с чем они воспринимаются одинаково всеми субъектами;

2. ситуации, когда смысловая направленность высказываний носит закамуфлированный характер, поэтому нуждается в установлении и выявлении.

Описана специфика влияния социальной сети на общую модель совершаемого преступления:

1. Связь между материалом и профилем ее опубликовавшим.

2. Связь профиля в социальной сети и компьютерного устройства, с которого осуществлялся доступ к профилю.

3. Связь между устройством и злоумышленником.

Такое усложнение связано, прежде всего, с возможностью несанкционированного доступа, как к профилю, так и устройству третьими лицами. Ситуация требует доказательств исключительного доступа подозреваемого к устройству и исключительной связи устройства и профиля социальной сети.

Автором выделены типовые исходные следственные ситуации, возникающие перед субъектом проверки:

1. Установлен факт совершения преступления экстремистской направленности в социальной сети и субъект проверки располагает информацией о личности преступника.

2. Установлен факт совершения преступления экстремистской направленности в сети Интернет, но субъект проверки не располагает информацией о личности преступника.

3. Установлен факт совершения преступления экстремистской направленности в сети Интернет, но субъект проверки не располагает информацией ни о личности преступника, ни о способе совершения преступления.

Сокрытие информации о личности преступника может осуществляться следующими способами:

5. Использование прокси-сервера.
6. Использование анонимайзеров.
7. Использование VPN подключений.
8. Использование Socks-протокола.

Наиболее распространенными следственными действиями по категории экстремистских преступлений являются:

5. Осмотр места происшествия
6. Допросы потерпевших
7. Допросы свидетелей
8. Проведение обыска, выемки

Описана целесообразность проведения осмотра интернет-страницы как осмотра места происшествия, в ходе которого в присутствии понятых, желательно с использованием записи-захвата «рабочего стола», фиксирующей именно действия в программной сфере, производится осмотр интересующего объекта глобальной сети.

В протоколе последовательно описываются действия следователя с момента включения Интернет-браузера, с указанием адреса страницы с сети Интернет, имени обладателя страницы в социальной сети, указанием лица, разместившего экстремистский материал, дате и времени публикации, дате последнего посещения пользователем своей страницы, и иной информации об опубликованном материале, которая может иметь значение для расследования преступления.

К протоколу целесообразно прилагать фототаблицу, содержащую снимки с экрана, документирующие изображения и текст на осматриваемом ресурсе.

В ходе обыска и выемки могут быть обнаружены следующие носители компьютерной информации: персональный компьютер, мобильный телефон, карты памяти, внешний жесткий диск, CD/DVD/BD диски.

При обнаружении таких носителей как CD/DVD/BD диски, внешние жесткие диски, карты памяти, или извлеченные из компьютера HDD или SDD накопители достаточно обеспечить их сохранность и невозможность стороннего доступа. Следовательно, обнаруженные носители не подключаются к каким-либо устройствам для их чтения и упаковываются, опечатываются и заверяются. В дальнейшем эти носители могут быть как направлены на компьютерно-техническую экспертизу, так и осмотрены следователем с участием специалиста.

Однако, если в ходе следственного действия будет обнаружено программируемое устройство, в том числе, персональный компьютер, ноутбук или мобильный телефон, то действия с таким устройством должны зависеть от его состояния.

Так, если устройство включено, то при совершении следственного действия необходимо исключить возможность его отключения кем-либо из участников, поскольку при отключении устройства произойдет потеря всех данных, находящихся в ОЗУ устройства. Определить включен ли компьютер можно по цветовым индикаторам на системном блоке персонального компьютера или корпусе ноутбука, звуку вентиляторов системы охлаждения или звуку работающего CD/DVD/BD- привода.

Тем не менее, существуют ситуации, при которых необходимо немедленно отключить устройство от питания.

Если обнаруженное в ходе следственного действия устройство выключено, то оно изымается по правилам действующего уголовно-процессуального законодательства, упаковывается, опечатывается и заверяется, включение такого устройства происходит уже в ходе осмотра с участием специалиста, либо компьютерно-технической экспертизы.

В случае если поиск цифровых следов сопряжен работой в сети, состоящей из нескольких связанных компьютерных устройств, то изъятие

устройства или устройств не производится и возникает необходимость в проведении осмотра компьютерной сети с обязательным участием специалиста, зафиксированы виртуальные следы в таком случае будут в протоколе осмотра.

При расследовании таких преступлений также целесообразно получить от пользователя всю возможную информацию об устройстве

Вместе с тем, необходимо учитывать, что современные средства шифрования информации на компьютерных устройствах могут использовать несколько кодов дешифрования, где только один код дешифрует весь массив информации, в то время как остальные создают имитацию дешифровки или дешифровывают отдельный блок массива информации, выступающий средством отвлечения внимания следователя.

Другим важным следственным действием является выемка у провайдеров и хостинг-провайдеров документов, содержащих сведения об арендаторах мест в сети, используемых под web-сайты, web-страницы, форумы или баннеры, о пользователях услугами сети Интернет, способах соединений, о владельцах электронной почты, информацию о плательщиках за арендуемые места, а также статистику соединений по пополнению и обновлению Интернет-ресурсов.

В качестве основных автором выделены следующие следственные действия:

1. Выемка у провайдеров и хостинг-провайдеров документов, содержащих информацию по действиям преступника в сети Интернет, его фактического адреса, использованных подключениях, IP-адресах.

2. Осмотр помещения, где находилась техника, с помощью которой осуществлялось преступление экстремисткой направленности с использованием сети Интернет.

3. Осмотр использованной техники с фиксацией экстремистских материалов.

4. Обыск у установленного лица по месту жительства, работы и иных хранилищах.

5. Допрос подозреваемого.

6. Назначение лингвистической, компьютерно-технической, или иной судебной экспертизы.

Автором описаны случаи обнаружения преступлений экстремистской направленности в пространстве социальных сетей:

1. Проведения целевого мониторинга на предмет наличия материалов экстремистской направленности пространства социальных сетей (прежде всего русскоязычных), веб-страниц средств массовой информации, форумов и иных областей сети Интернет, на которых возможно и вероятно размещение экстремистских материалов сотрудниками правоохранительных органов.

2. Получении информации о преступлении от лиц, оказывающих правоохранительным органам содействие на основе конфиденциальности (конфидентов).

3. Получении информации в ходе проведения субъектами оперативно-розыскной деятельности оперативно-розыскных мероприятий.

4. Получении информации в ходе расследования преступления экстремистской направленности, совершенного без использования компьютерных устройств и выхода в сеть Интернет.

5. При поступлении заявления в правоохранительные органы от физических и юридических лиц, представителей общественных организаций, депутатских запросов, а также обращений средств массовой информации.

6. При расследовании преступлений общеуголовной направленности, не связанных с экстремистской деятельностью.

При проведении мониторинга социальных сетей, в частности, целесообразно в качестве приоритетных областей проверок выбирать популярные сообщества, созданные по региональному принципу, группы региональных новостных агентств в социальных сетях, а также на персональные страницы пользователей, где место проживания указано в личных данных, либо регион проживания может быть установлено по фотографиям.

При проведении доследственной проверки оперативно-розыскными подразделениями в следственные органы должны предоставляться сведения:

1. где, когда, какие признаки и какого преступления обнаружены;

2. при каких обстоятельствах имело место их обнаружения;

3. о лице, либо о лицах, совершивших преступление экстремистской направленности;

4. о свидетелях и очевидцах данного преступления;

5. о местонахождении предметов и документов, имеющих значение для дела.

Первой задачей при проведении доследственной проверки является определение характера размещенной информации. Определение характера размещённого материала, особенно в случае, если имеет место использование не жесткого языка вражды, а среднего или мягкого, зависит от результатов применения специальных знаний в виде лингвистической или комплексной лингвистической экспертизы с привлечением экспертов психологов, историков или религиоведов.

Автором описано использование «Виртуального агента» в оперативной деятельности. Его использование позволяет без посредников получить информацию по вербовке, планируемым акциям экстремистского толка, кругу лиц, причастных к деятельности организации, выходить на контакт с пользователями закрытых экстремистских сообществ.

«Виртуальный агент» должен быть ориентирован на ту среду, в которую планируется его внедрение. При подборе контента для наполнения аккаунта должен использоваться фото-, аудио-, видеоматериал, который соответствует понятиям, пользуется популярностью и характерен к использованию в той или иной экстремистской среде.

«Виртуальные агенты», находясь в закрытых сообществах, обладают свободным доступом к внутренней переписке, к создаваемым «встречам», принимают рассылку о предстоящих мероприятиях. Наиболее важно, что в адрес этих конфидентов могут поступить предложения от радикально настроенных лиц о совершении акций экстремистского и террористического толка.

При расследовании преступлений экстремистской направленности, совершенных в сети Интернет, можно выделить две основные группы использования специальных знаний в зависимости от сферы деятельности: Специальные знания в сфере информационных технологий и специальные знания в области лингвистики, религии, психологии.

Современное криминалистическое оборудование позволяет извлекать информацию, в том числе и удаленную, завуалированную или скрытую с устройств или электронных накопителей любой модели, любой операционной системы, а также устройств, защищенных паролем или даже поврежденных. В возможности такого устройства входят получение информации и о переписке в различных социальных сетях.

Другой процессуальной формой использования специальных знаний является производство компьютерно-технической судебной экспертизы. На разрешение эксперту ставятся вопросы общего диагностического характера о наличии в устройстве (включая внешние карты памяти и сим-карты) каких-либо файлов (текстовых, графических, музыкальных, видеозаписей,

фотоизображений, СМС-сообщений, файлов Cookie, web-файлов, вредоносного ПО и др.), и эксперт извлекает весь физический дамп памяти.

Специфический характер экстремистских действий в социальных сетях, или иное косвенное использование социальных сетей в экстремистской деятельности закономерно влечет тесное взаимодействие следователя со специалистом в компьютерной сфере.

Таким образом, лингвистическая или комплексная судебная экспертиза фактически становится обязательной по делам о преступлениях экстремистской направленности, выступая в качестве дополнительного доказательства к числу имеющихся, дополняя обвинительное заключение и приговор суда. Отправляя материалы на лингвистическую экспертизу, следователь решение о преступности деяния фактически оставляет за экспертом.

Рассматривая необходимость проведения лингвистических экспертиз целесообразно говорить о среднем и мягком языках вражды, когда у следователя могут возникнуть затруднения в определении значения и направленности материалов. Однако в ситуации жесткого языка вражды, когда имеется прямое выражение ненависти, очевидные призывы к насилию по отношению к другой расе, нации, конфессии. Экспертиза таких материалов представляется излишней.

Таким образом, лингвистическая экспертиза материалов в пространстве социальных сетей обладают обязательным в результате сложившейся практики характером, объектом таких экспертиз являются как сам текст в широком смысле, так и сопутствующие элементы (антураж), включающие в себя изображения, видеоряд, аудиозаписи или саундтрек. При формулировке вопросов при назначении экспертизы необходимо избегать юридических конструкций, из-за которых в ходе экспертизы будут формулироваться ответы правового характера.

Автором представлены формулировки вопросов эксперту при экспертизе экстремистских материалов в социальных сетях:

1. Выражают ли словесные или изобразительные средства, использованные в материале, унизительные характеристики или отрицательную эмоциональную оценку и негативную установки в отношении какой-либо расовой, этнической, религиозной иной социальной группы, её представителей? Если да, то какой именно, в какой форме?

2. Содержится ли в материале информация, направленная на побуждение к действиям против какой-либо расы, нации, конфессии иной социальной группы, её представителей? Если да, то какая именно, в какой форме?

3. Имеются ли в спорном речевом произведении высказывания оскорбительного характера по отношению к лицам какой-либо расы, национальности, конфессии или иной социальной группы?

4. Носит ли указанный материал характер призыва?

5. *Создается ли образ врага в указанном материале?*

В диссертационном исследовании отмечается, что экспертиза не может устанавливать виновность лица, поскольку это не может относиться к ведению эксперта, поэтому эксперт-лингвист как лицо, обладающее знаниями в области семантики и лексики, должен установить негативный окрас материалов, оценить слова, используемы для обозначения социальных групп и используемые для их негативной или превозносящей характеристики, при комплексной экспертизе эксперт-психолог должен определить используемые автором публикации методы побуждения к действиям, способы воздействия на читателя, зрителя, слушателя, что в дальнейшем оценивается следователем и судом как доказательство экстремистской направленности материалов.

В результате исследования установлено, что молодёжь (от 14 до 30 лет) представляет собой основную группу риска, наиболее подверженную влиянию последователей экстремистских взглядов и идей. Особое внимание следует обратить на обучающихся в средних и высших образовательных учреждениях. Поэтому одним из важнейших факторов профилактики экстремизма является своевременное обнаружение и воспитательная работа с лицами, вовлеченными или находящимися под угрозой вовлечения в экстремистские сообщества.

Данная возрастная группа имеет мало «иммунизирующих» к такой пропаганде личностных ресурсов, в частности:

- подверженность чужому влиянию, внушению и манипулированию;
- недостаточная стрессоустойчивость;
- глубокое погружение в интернет-пространство;
- романтизация и героизация антиобщественных и агрессивных действий.

В молодёжной среде легче приживаются радикальные взгляды и убеждения, наиболее быстро происходит накопление и реализация экстремистского потенциала.

К группе риска, как правило, относятся:

- дети, внуки и родственники экстремистов или террористов;
- лица из неполных семей;
- лица из асоциальных семей;
- лица с ограниченными физическими возможностями;
- лица из семей с гиперопекой.

В исследовании представлены характерные особенности, которые проявляются у лиц, попавших под влияние экстремистской идеологии.

При этом необходимо отметить, что тонкие методы экстремистской пропаганды требую более тонкого подхода в противодействии. *Так, любое действие запретительного характера будет трактоваться идеологами экстремизма как борьбу со свободой слова, попыткой установления полицейского государства или борьбой с инакомыслием.* Следовательно, наибольшее значение в области криминалистической профилактики будет иметь разработка методов, связанных с минимальным возможным негативным откликом.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

I. Нормативно-правовые и иные акты

1. Конституция Российской Федерации от 12 декабря 1993 г. (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // СПС «Консультант Плюс».

2. Европейская конвенция по правам человека (измененная и дополненная Протоколами № 11 и № 14, в сопровождении Дополнительного протокола и Протоколов № 4, 6, 7, 12 и 13) // Официальный интернет-портал Европейского суда по правам человека URL:https://www.echr.coe.int/Documents/Convention_RUS.pdf.

3. The European Court of Human Rights: CASE OF ROMAN ZAKHAROV v. RUSSIA // Официальный интернет-портал Европейского суда по правам человека URL:http://hudoc.echr.coe.int/eng?i=001-159324

4. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 11.06.2022) // СПС «Консультант Плюс».

5. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 25.03.2022) // СПС «Консультант Плюс».

6. Федеральный закон «О полиции» № 3-ФЗ от 07 февраля 2011 г. (ред. от 21.12.2021) // СПС «Консультант Плюс».

7. Федеральный закон «О государственной судебно-экспертной деятельности в Российской Федерации» № 73-ФЗ от 31 мая 2001 г. (в ред. от 01.07.2021)// СПС «Консультант Плюс».

8. Федеральный закон «Об оперативно-розыскной деятельности» № 144-ФЗ от 12 августа 1995 г. (ред. от 01.04.2022) // СПС «Консультант Плюс».

9. Федеральный закон «О противодействии экстремистской деятельности» № 114-ФЗ от 25.07.2002 (ред. от 01.07.2021) // СПС «Консультант Плюс».

10. Федеральный закон «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27.07.2006 (ред. от 30.12.2021) // СПС «Консультант Плюс».

11. Постановление Пленума Верховного Суда РФ от 28.06.2011 N 11 (ред. от 28.10.2021) "О судебной практике по уголовным делам о преступлениях экстремистской направленности"// СПС «Консультант Плюс».

12. Стратегия национальной безопасности Российской Федерации (утв. Указом Президента РФ от 31 декабря 2015 г. № 683) // СПС «Консультант Плюс».

13. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646) // СПС «Консультант Плюс».

14. Стратегия противодействия экстремизму в Российской Федерации до 2025 года (утв. Президентом РФ 28 ноября 2014 г., Пр-2753) // СПС «Консультант Плюс».

15. ГОСТ Р 56824-2015. Национальный стандарт Российской Федерации. Интеллектуальная собственность. Использование охраняемых результатов интеллектуальной деятельности в сети Интернет (утв. и введен в действие Приказом Росстандарта от 03.12.2015 N 2103-ст)

16. Письмо Минпросвещения России от 29.03.2019 N 03-393 "О методических рекомендациях" (вместе с "Методическими рекомендациями по реализации мер, направленных на обеспечение безопасности детей в сети "Интернет")

II. Специальная литература

17. Абазов И.С. Актуальные проблемы молодежного экстремизма в Северо-Кавказском регионе на современном этапе // Новая наука: Стратегии и векторы развития. 2016.№ 9 С.208-210.

18. Абазов, И.С. Особенности проявление экстремизма и терроризма в глобальной сети интернет / И. С. Абазов // Лучшая научная работа 2021 : Сборник статей Международного научно-исследовательского конкурса, Пенза, 30 августа 2021 года. – Пенза: Наука и Просвещение, 2021. – С. 133-136.

19. Авакьян, М. В. Скулшутинг как форма девиантного поведения террористической направленности / М. В. Авакьян // Современные технологии и подходы в юридической науке и образовании : Сборник материалов международного научно-практического форума, Калининград, 27–31 августа 2020 года. – Калининград: Балтийский федеральный университет имени Иммануила Канта, 2021. – С. 368-375.

20. Авласенко, В.А. Личность преступника, члена религиозных сект: криминологический и психологический анализ / В.А. Авласенко // Юридическая психология. - 2011. - №4.

21. Агдавлетова, А. М. Меры профилактики киберэкстремизма среди молодежи / А. М. Агдавлетова // Информационные системы и технологии в образовании, науке и бизнесе (ИСиТ-2014) : Материалы Всероссийской молодежной научно-практической школы, Кемерово, 19–21 июня 2014 года. – Кемерово: Кузбасский государственный технический университет им. Т.Ф. Горбачева, 2014. – С. 13-14.

22. Алексеев, А.П. Криминалистическая характеристика преступлений в сфере авторских и смежных прав / А.П. Алексеев. // Российский следователь: научно-практическое и информационное издание - М.: Юрист. - 2009. - №17.

23. Алиев, Э.Р. Борьба с финансированием терроризма / Э.Р. Алиев // Криминальная экономика и организованная преступность - М.: Российская криминологическая ассоциация, 2007.

24. Андрамонова В.В. Социальные сети в контексте развития современного общества // Современные проблемы науки и образования. – 2015. – № 2-2.

25. Ануфриева, Г. В. Язык общения в социальных сетях / Г. В. Ануфриева // Русская речевая культура и текст : материалы XII Международной научной конференции, Томск, 20–21 мая 2022 года. – Томск: Томский центр научно-технической информации, 2022. – С. 111-117.

26. Аристов, С. К. Регулирование медиапространства как основа безопасной коммуникационной среды / С. К. Аристов, А. А. Ароянц // Коммуникационные процессы: теория и практика : Сборник материалов XVII международной научно-практической очно-заочной конференции, Краснодар, 28 октября 2021 года / Отв. редактор М.Б. Щепакин. – Краснодар: Кубанский государственный технологический университет, 2022. – С. 103-109.

27. Бааль Н. Б. Политический экстремизм российской молодежи и технологии его преодоления: автореф. дис. д-ра политич. наук. Н. Новгород, 2012. 42 с.

28. Бахтеев Д.В. Особенности фиксации и изъятия криминалистически значимой информации, размещенной в сети Интернет // Российский следователь. 2017. N 21. С. 10 - 13.

29. Бегичев А.В. Использование протоколов осмотров интернет-сайтов в судебной практике // Вестник Московского университета МВД России. - 2014. - № 11. - С. 208-212.

30. Белкин Р.С. Курс криминалистики: Криминалистические средства, приемы и рекомендации. В 3-х томах. Т. 3. - М.: Юристъ, 1997. - С. 68.

31. Бикмиев Р.Г., Бурганов Р.С. Собирание электронных доказательств в уголовном судопроизводстве // Информационное право. 2015. N 3. С. 17 - 21.

32. Бирюков С.Ю., Скориков Д.Г., Шинкарук В.М. Особенности расследования преступлений экстремистской направленности: учебное пособие / Бирюков С.Ю., Скориков Д.Г., Шинкарук В.М. - Волгоград: ВА МВД России, 2013. - С.40

33. Блинова, О. А. Религиозный киберэкстремизм: причины и способы борьбы с ним / О. А. Блинова // Религия и общество - 12 : сборник научных статей, Могилев, 12–17 марта 2018 года / Под общей редакцией В.В. Старостенко, О.В. Дьяченко. – Могилев: Могилевский государственный университет имени А.А. Кулешова, 2018. – С. 128-130.

34. Болвачев М.А. О следственных действиях по делам о преступлениях экстремистской направленности в социальных сетях // Известия Тульского государственного университета. Экономические и юридические науки. 2022. N 2. С. 98-105.

35. Болвачев, М. А. Особенности расследования преступлений экстремистской направленности, совершенных с использованием социальных сетей / М. А. Болвачев // Тенденции развития современной юриспруденции : Сборник научных трудов международной студенческой научной конференции Юридического института Балтийского федерального университета им. Иммануила Канта, научное электронное издание, Калининград, 20–22 апреля 2018 года. – Калининград: Балтийский федеральный университет имени Иммануила Канта, 2018. – С. 168-173.

36. Болвачев, М.А. Интернет как инструмент вовлечения молодежи в неформальные объединения террористической направленности / М. А. Болвачев // Современные технологии и подходы в юридической науке и образовании : Сборник материалов международного научно-практического форума, Калининград, 27–31 августа 2020 года. – Калининград: Балтийский федеральный университет имени Иммануила Канта, 2021. – С. 384-388.

37. Болвачев, М.А. К вопросу о понятии места совершения преступления в пространстве социальных сетей / М. А. Болвачев // Уголовно-

процессуальные и криминалистические чтения на Алтае, Барнаул, 10–12 июля 2018 года / Отв. ред. С.И. Давыдов, В.В. Поляков. – Барнаул: Алтайский государственный университет, 2018. – С. 39-43.

38. Болвачев, М.А. Социальная сеть как источник криминалистической информации / М.А. Болвачев // Тенденции развития современной юриспруденции : материалы VII Всероссийской студенческой научно-практической конференции Юридического института Балтийского федерального университета имени Иммануила Канта, Калининград, 19–21 апреля 2019 года / под общ. ред. О. А. Заячковского. – Калининград: Издательство балтийского федерального университета имени Иммануила Канта, 2019. – С. 207-213.

39. Болвачев, М.А. Социальная сеть как объект криминалистического исследования / М.А. Болвачев // Известия Тульского государственного университета. Экономические и юридические науки. – 2020. – № 4. – С. 64-71.

40. Болвачев, М.А. Типовые ситуации преступлений экстремистской направленности в социальных сетях / М. А. Болвачев // Союз криминалистов и криминологов. – 2019. – № 2. – С. 45-50. – DOI 10.31085/2310-8681-2019-2-222-45-50.

41. Борисов С. В., Жеребченко А. В. Возбуждение ненависти, вражды, унижение человеческого достоинства: проблемы установления и реализации уголовной ответственности: моногр. / Отв. ред. С. В. Борисов. М.: Юриспруденция, 2015. 264 с.

42. Бринев К.И. Судебная лингвистическая экспертиза по делам о религиозном экстремизме/ Бринев К.И. // Вестник Томского государственного университета. – 2013. - № 376. - С. 7

43. Бычков В.В., Вехов В.Б. Электронное следообразование преступной деятельности в сети Интернет//Расследование преступлений: проблемы и пути их решения. 2020. № 1 (27). С. 107.

44. Введенская О.Ю. Особенности следообразования при совершении преступлений посредством сети Интернет / Введенская О.Ю. // Юридическая наука и правоохранительная практика. -2015. - № 4. - С. 209 – 216.

45. Вебер К.С., Пименова А.А. Сравнительный анализ социальных сетей // Вестник Тамбовского университета. Серия: Естественные и технические науки. - 2014. - т.19, вып. 2. - С.634.

46. Вехов В.Б. Дорожка электронных следов: понятие и особенности судебного компьютерно-технического исследования // Уголовное производство: процессуальная теория и криминалистическая практика. Материалы VII Международной научно-практической конференции. Ответственные редакторы М.А. Михайлов, Т.В. Омельченко. 2019. С. 18–20.

47. Вехов В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств её обработки: монография. Волгоград: ВА МВД России, 2008. - 404 с.

48. Вехов В.Б. Получение компьютерной информации от организаторов ее распространения в сети Интернет как процессуальное действие // Расследование преступлений: проблемы и пути их решения. 2018. № 1 (19). С. 105–109.

49. Вехов В.Б., Баюш А.А. Правовой статус судебного эксперта и специалиста в процессуальном законодательстве российской федерации // Актуальные научные исследования в современном мире. 2019. № 10-2 (54). С. 98-101.

50. Возгрин И. А. О соотношении следственных ситуаций и алгоритмов расследования преступлений // Вопросы профилактики преступлений. Л., 1977. С. 63.

51. Волчецкая Т. С. Криминалистическое моделирование в уголовном судопроизводстве : Учебно-методическое пособие / Т. С. Волчецкая, Е. В.

Осипова. – Калининград : Балтийский федеральный университет имени Иммануила Канта, 2020. – 126 с.

52. Волчецкая Т. С. Ситуационный подход в обучении криминалистике // Вестник криминалистики. 2000. Вып. 1. С. 4.

53. Волчецкая Т.С. Роль, этапы и перспективы ситуационного подхода в современной криминалистике // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2016. № 4 (46). С. 9–11

54. Волчецкая Т.С. Современные тенденции развития криминалистики в России и США // Folia Iuridica Universitaits Wratislaviensis. 2015. Vol. 4 (1) - С.150

55. Волчецкая Т.С., Кот Е.А. Криминалистический анализ использования Интернет-ресурсов как места и средства побуждения несовершеннолетних к суициду // Известия Тульского государственного университета. Экономические и юридические науки. 2020. № 3. С. 3–10.

56. Волчецкая Т.С. Криминалистическая ситуалогия: Монография. / Под ред. проф. Н.П. Яблокова. Москва; Калинингр. ун-т. - Калининград,1997.

57. Волчецкая, Т. С. Криминалистическая ситуалогия: современное состояние и перспективы / Т. С. Волчецкая // Ситуационный подход в юридической науке и практике: современные возможности и перспективы развития : Материалы Международной научно-практической конференции, посвященной 15-летию научной школы криминалистической ситуалогии БФУ им. И. Канта, Калининград, 20–22 октября 2017 года. – Калининград: Балтийский федеральный университет имени Иммануила Канта, 2017. – С. 11–16.

58. Волчецкая, Т. С. Научно-методические рекомендации по своевременному выявлению студентов, подверженных воздействию идеологии терроризма. Часть 1 / Т. С. Волчецкая, М. В. Авакьян, Е. В. Осипова // Образовательные технологии (г. Москва). – 2021. – № 3. – С. 97-108.

59. Волчецкая, Т. С. Прикладные аспекты противодействия информационно-мировоззренческим угрозам в цифровом пространстве и особенности их профилактики / Т. С. Волчецкая, М. В. Авакьян // Актуальные проблемы российского права. – 2021. – Т. 16. – № 6(127). – С. 194-201.

60. Волчецкая, Т. С. Современные формы насилия в молодежной среде: степень распространения и меры профилактики / Т. С. Волчецкая, Е. В. Осипова, М. В. Авакьян // Российский юридический журнал. – 2021. – № 5(140). – С. 105-115.

61. Воронин М.И. Электронные доказательства в УПК: быть или не быть? // Lex russica. 2019. N 7. С. 74 - 84.

62. Воронкин А.С. Социальные сети: эволюция, структура, анализ /"Образовательные технологии и общество". - 2014. - № 9. - С.650 - 675.

63. Гармаев Ю.П. Противодействие уголовному преследованию по уголовным делам о киберпреступлениях и средства его преодоления: проблемы теории и дидактики // В сборнике: Цифровые технологии в юриспруденции: генезис и перспективы. Материалы I Международной межвузовской научно-практической конференции. 2020. С. 29–35.

64. Гирфанов Г.Т., Румянцев А.А., Симоненко И.В. Киберпространство: определение, основные понятия и систематизация//Повышение обороноспособности государства. материалы заочной научной конференции. Военный учебный центр. Санкт-Петербург, 2021. С. 35.

65. Гладких А.В. Социальные сети как новое средство совершения преступлений против собственности // Безопасность бизнеса. 2016. N 1. С. 33 - 36.

66. Гладышев В.В. «Социальные сети как инструмент для пропаганды экстремизма». // Национальный центр информационного противодействия терроризму и экстремизму в образовательной среде и сети

интернет. Ростов-на-дону [Электронный ресурс] URL:http://nac.gov.ru/publikacii/stati-knigi-broshyury/gladyshev-v-socialnye-seti-kak-instrument-dlya.html (дата обращения 01.09.2020)

67. Глазков, А. В. Противодействие экстремизму экстремизм глазами молодежи / А. В. Глазков // Право. Экономика. Безопасность. – 2017. – № 3. – С. 54-55.

68. Головин А.Ю., Давыдов В.О. Криминалистическая категория «информационное обеспечение расследования преступлений» // Актуальные проблемы криминалистики и судебной экспертизы. Материалы международной научно-практической конференции. 2020. С. 30–33.

69. Головин, А. Ю. Криминалистическая категория «информационное обеспечение расследования преступлений» / А. Ю. Головин, В. О. Давыдов // Актуальные проблемы криминалистики и судебной экспертизы : Материалы международной научно-практической конференции, Иркутск, 13–14 марта 2020 года. – Иркутск: Восточно-Сибирский институт Министерства внутренних дел Российской Федерации, 2020. – С. 30-33.

70. Головин, А.Ю., Головина, Е.В. Некоторые тактические ошибки производства обыска по делам о преступлениях, сопряженных с использованием средств вычислительной техники / А.Ю. Головин, Е.В. Головина // Раскрытие и расследование преступлений, сопряженных с использованием средств вычислительной техники. Проблемы, тенденции, перспективы - М.: РосНОУ, 2005.

71. Головин, А.Ю., Мусаева, У.А. Электронное информационное поле как объект криминалистического исследования / А.Ю. Головин, У.А. Мусаева // Известия Тульского государственного университета. Серия «Современные проблемы законодательства России, юридических наук и правоохранительной деятельности. Вып.3. - Тула: Изд-во ТулГУ, 2000.

72. Гордиенко, В.В. Актуальные проблемы противодействия экстремизму в России / В.В. Гордиенко // Материалы 12 международной

научно-практической конференции - М.: РИО Академии управления МВД России, 2010.

73. Горошко Т. Обзор судебной практики по трудовым спорам с использованием в качестве доказательств данных из социальных сетей // Трудовое право. 2019. N 6. С. 69 - 82.

74. Гортинский, А.В. Метод эксперимента как один из основных методов судебно-экспертного исследования компьютерной информации // Раскрытие и расследование преступлений, сопряженных с использованием средств вычислительной техники. Проблемы, тенденции, перспективы - М., 2005.

75. Грибунов О. П. Виды экспертиз, назначаемых при расследовании преступлений в сфере компьютерной информации и высоких технологий / О. П. Грибунов, М. В. Старичков // Криминалистика и судебная экспертиза: прошлое, настоящее и взгляд в будущее : материалы ежегодной международной научно-практической конференции, Санкт-Петербург, 01–02 июня 2017 года / Санкт-Петербургский университет МВД России. – Санкт-Петербург: Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2017. – С. 77–83.

76. Григорьев А. Н. Использование в раскрытии и расследовании преступлений информации, полученной из открытых источников / А. Н. Григорьев // Наука и новация: современные проблемы теории и практики права : сборник материалов международной научно-практической конференции в рамках IV Международного Фестиваля науки, Москва, 20–21 февраля 2019 года. – Москва: Московский государственный областной университет, 2019. – С. 58-60.

77. Григорьев А. Н. Получение информации о времени при работе с электронными следами / А. Н. Григорьев, В. М. Мешков // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. – 2017. – № 2(48). – С. 10.

78. Григорьев А.Н., Бодылина Э.А., Информационно-телекоммуникационная сеть Интернет как среда и средство совершения преступлений // Материалы международной научно-практической конференции "Закон и правопорядок в третьем тысячелетии". Калининградский филиал Санкт-Петербургского университета МВД России. 2017. С. 72-73.

79. Григорьев А.Н., Мешков В.М. Получение информации о времени при работе с электронными следами / Григорьев А.Н., Мешков В.М. // Вестник калининградского филиала санкт-петербургского университета МВД России. - 2017. - № 2 (48). - С. 10

80. Гриненко, А.В. Понятие и классификация преступлений экстремистской направленности / А.В. Гриненко // Российская юстиция. - 2012. - № 3.

81. Грушихина В.А. Криминалистическая характеристика преступлений, связанных с распространением материалов экстремистской направленности / Грушихина В.А. // Вестник Иркутского государственного технического университета. - 2015. - № 5. - С.372

82. Губченко (Скребец) Е.С. Общая характеристика экстремизма как угрозы общественной безопасности в Российской Федерации (административно-правовой анализ) // Административное право и процесс. 2019. N 4. С. 76 - 79.

83. Давыдов В.О. Исследование криминалистически значимой информации в ходе расследования экстремистских преступлений, совершенных с использованием компьютерных сетей. / Давыдов В.О. // Известия Тульского государственного университета. Экономические и юридические науки. - 2013. - № 4. - С. 57 - 62.

84. Давыдов В.О. О некоторых аспектах обнаружения признаков преступлений экстремистской направленности, совершаемых с использованием средств социальной компьютерной коммуникации, и

принятия решений в стадии возбуждения уголовного дела / Давыдов В.О. // Актуальные проблемы российского права. - 2014. - № 9 (46). - С. 2008 - 2013.

85. Давыдов В.О., Головин А.Ю. Значение виртуальных следов в расследовании преступлений экстремистского характера // Известия Тульского государственного университета. Экономические и юридические науки. 2016. № 3-2. С. 254-259.

86. Давыдов, В. О. Информация в деятельности по раскрытию и расследованию преступлений: теория, практика, инновации / В. О. Давыдов. – Москва : Издательство "Юрлитинформ", 2021. – 248 с. – (Библиотека криминалиста). – ISBN 978-5-4396-2273-3.

87. Давыдов, В. О. К вопросу об организационных формах расследования транснациональной преступной деятельности экстремистского характера / В. О. Давыдов // Оптимизация деятельности органов предварительного следствия и дознания: правовые, управленческие и криминалистические проблемы : Сборник научных статей Международной научно-практической конференции, Москва, 25–26 мая 2017 года / Под редакцией И.П. Можаевой. – Москва: Академия управления Министерства внутренних дел Российской Федерации, 2017. – С. 137-142.

88. Давыдов, В. О. Когнитивные технологии трансформации социального поведения в механизме преступной деятельности экстремистского и террористического характера: криминалистически значимые сведения / В. О. Давыдов // Вестник Сибирского юридического института МВД России. – 2020. – № 3(40). – С. 108-114.

89. Давыдов, В. О. Методика расследования транснациональной преступной деятельности экстремистского характера / В. О. Давыдов. – Москва : Издательство "Юрлитинформ", 2018. – 440 с.

90. Давыдов, В. О. Научные основы базовой методики расследования преступлений и их развитие в практике борьбы с транснациональным

экстремизмом / В. О. Давыдов. – Москва : Издательство "Юрлитинформ", 2020. – 496 с.

91. Давыдов, В. О. О криминалистических рекомендациях проведения осмотров электронных носителей информации по делам о транснациональных преступлениях экстремистского характера / В. О. Давыдов // Известия Тульского государственного университета. Экономические и юридические науки. – 2017. – № 1-2. – С. 96-101.

92. Давыдов, В. О. О механизме транснациональной преступной деятельности экстремистского характера / В. О. Давыдов, И. В. Тишутина // Предупреждение и расследование преступлений экстремисткой направленности в молодежной среде : Материалы Международной научно-практической конференции, Москва, 21 марта 2019 года / Под общей редакцией А.М. Багмета. – Москва: Московская академия Следственного комитета Российской Федерации, 2019. – С. 97-103.

93. Давыдов, В. О. О некоторых аспектах криминалистической характеристики преступлений, связанных с неправомерным доступом к компьютерной информации / В. О. Давыдов, Е. Д. Малахвей // Известия Тульского государственного университета. Экономические и юридические науки. – 2019. – № 2. – С. 94-100.

94. Давыдов, В. О. О некоторых проблемах Отечественной криминалистики в свете борьбы с современными формами преступной деятельности экстремистского характера / В. О. Давыдов // Известия Тульского государственного университета. Экономические и юридические науки. – 2018. – № 3-2. – С. 61-68.

95. Давыдов, В. О. Современный экстремизм: взгляд криминалиста : Учебное пособие для слушателей магистратуры и аспирантов по кафедре криминалистики / В. О. Давыдов. – Москва : Издательство "Юрлитинформ", 2018. – 584 с.

96. Давыдов, В. О. Цифровые следы в расследовании дистанционного мошенничества / В. О. Давыдов, И. В. Тишутина // Известия Тульского государственного университета. Экономические и юридические науки. – 2020. – № 3. – С. 20-27.

97. Давыдов, В.О. Методика расследования транснациональной преступной деятельности экстремистского характера: монография / В. О. Давыдов ; под научной редакцией доктора юридических наук А. Ю. Головина. - Москва : Юрлитинформ, 2018. - 436 с.

98. Давыдов, В.О. Проверка информации, полученной в ходе расследования экстремистских преступлений, совершенных с использованием компьютерных сетей / В.О. Давыдов // Актуальные проблемы права : Сборник материалов ежегодной международной научно-практической конференции. – Тула : Изд-во ТулГУ, 2013. – С.32-37

99. Давыдов, В.О., Головин, А.Ю. Системный подход как основа криминалистического исследования транснациональной преступной деятельности экстремистского характера / В.О. Давыдов, А.Ю. Головин // Криминалистическое сопровождение расследования преступлений: проблемы и пути решения : Материалы международной научно-практической конференции, посвященной 110-летию со дня рождения И.Ф. Крылова – М. : Изд-во Академии Следственного комитета Российской Федерации, 2016. – С.151-155.

100. Дремлюга Р.И., Крипакова А.В. Преступления в виртуальной реальности: миф или реальность? // Актуальные проблемы российского права. 2019. N 3. С. 161 - 169.

101. Дубоносов Е.С. Оперативно-розыскное мероприятие «Получение компьютерной информации»: содержание и проблемы проведения/ Дубоносов Е.С. // Известия ТулГУ. Экономические и юридические науки. - 2017. - № 2-2. - С. 24 - 30

102. Дубоносов, Е. С. Оперативно-розыскное мероприятие "получение компьютерной информации": содержание и проблемы проведения / Е. С. Дубоносов // Известия Тульского государственного университета. Экономические и юридические науки. – 2017. – № 2-2. – С. 24-30.

103. Иванов Д. В. Виртуализация общества. Версия 2.0. - Спб.: «Петербургское Востоковедение», 2002. - С. 15.

104. Иванова Л.В., Пережогина Г.В. Цифровое пространство как место совершения преступления в условиях глобальных ограничений//Вестник Тюменского государственного университета. Социально-экономические и правовые исследования. 2020. Т. 6. № 4.

105. Игнатова, Т. В. Идентификация пользователей в социальных сетях / Т. В. Игнатова, А. А. Смирнов, В. А. Фролов // Информационное развитие России: состояние, тенденции и перспективы : сборник статей XII всероссийской научно-практической конференции, Орел, 03 декабря 2021 года / Среднерусский институт управления - филиал РАНХиГС. – Орел: Среднерусский институт управления - филиал РАНХиГС, 2022. – С. 113-119.

106. Иссерс О.С. Орлова Н.В. Лингвистические корреляты понятия «вовлечение в экстремистскую деятельность» / Иссерс О.С. Орлова Н.В. // Политическая лингвистика. - 2017. - № 3. - С.132

107. Истомин А.Ф., Лопаткин Д.А. К вопросу об экстремизме // Современное право. 2015. № 7.

108. Калинина, Л. Л. Социальная реклама и ее роль в современном российском обществе / Л. Л. Калинина // Вестник РГГУ. Серия: Экономика. Управление. Право. – 2020. – № 3. – С. 15–24.

109. Карагодин В.Н. Ситуационные особенности раскрытия некоторых видов преступлений, совершаемых с использованием информационных технологий//Материалы научно-практического семинара-совещания. 2017 С. 3–12.

110. Касенова М.Б. Идентификация лиц в Интернете и киберпространство социальных сетей // Юрист. 2014. N 6. С. 32 - 36.

111. Кастельс М. Галактика Интернет: Размышления об Интернете, бизнесе и обществе. Екатеринбург: У-Фактория, 2004

112. Князьков, А. С. Методологические проблемы профилактики молодежного экстремизма в России / А. С. Князьков // Уголовная юстиция. – 2020. – № 16. – С. 114-122.

113. Кобец, П. Н. О радикализме и экстремизме - основе террора и необходимости противодействия экстремизму и терроризму в интенсивно меняющемся мире / П. Н. Кобец // Наука: прошлое, настоящее, будущее : сборник статей Международной научно-практической конференции: в 3 частях, Пермь, 25 июня 2017 года. – Пермь: Общество с ограниченной ответственностью "Аэтерна", 2017. – С. 167-169.

114. Кобец, П.Н. О политической стратегии и опыте Бюро расследований штата Джорджия США относительно использования социальных сетей для получения информации и ведения расследования // Международное уголовное право и международная юстиция. - 2018. — № 6. — С. 17—19.

115. Ковалев Н.Д. Анализ основных тенденций политического экстремизма в России // Политический экстремизм в Российской Федерации и конституционные меры борьбы с ним. М.: Известия, 1998.

116. Коняхин В.П., Асланян Р.Г. Информация как предмет и средство совершения преступлений в сфере экономической деятельности // Российский следователь. 2016. N 8. С. 24 - 27.

117. Криминалистика : учебник / Т. В. Аверьянова, Е. Р. Россинская, Р. С. Белкин, Ю. Г. Корухов. - 4-е изд., перераб. и доп. - Москва : Норма : Инфра-М, 2020. - 928 с.

118. Криминалистика в 5 Т. Том 5. Методика расследования преступлений : Учебник / Н. П. Яблоков, А. А. Беляков, И. В. Александров [и др.]. – 1-е изд. – Москва : Издательство Юрайт, 2020. – 242 с.

119. Криминалистическая профилактика преступлений органами предварительного следствия: методические рекомендации / В.А. Передерий; под ред. А.М. Багмета. – М: Московская академия Следственного комитета Российской Федерации, 2017. - 30 с.

120. Кузнецов, А. А. Понятие, признаки и сущность экстремизма как социального явления (по результатам социологического исследования представлений граждан об экстремизме) / А. А. Кузнецов // Вестник Прикамского социального института. – 2021. – № 2(89). – С. 213-218.

121. Куликов, А. В. Мошенничество в сфере компьютерной информации / А. В. Куликов, Е. А. Гуц // Известия Тульского государственного университета. Экономические и юридические науки. – 2020. – № 1. – С. 81-88.

122. Кушнарев К.А. Феномен «социальные сети»: проблемы и перспективы развития//Ломоносовские чтения на Алтае: фундаментальные проблемы науки и образования. Сборник научных статей международной конференции. Алтайский государственный университет. 2015. С. 262.

123. Ледовая Я.А. Социальные сети как новая среда для междисциплинарных исследований поведения человека / Я.А. Ледовая, Р.В. Тихонов, О.Н. Боголюбова // Вестник Санкт-Петербургского университета / Психология и педагогика. – 2017. – Т. 7–№ 3 – С. 193–210.

124. Лыткина, О. А. Влияние СМИ на молодежную аудиторию / О. А. Лыткина // Афанасьевские чтения. Инновации и традиции педагогической науки - 2022 : Сборник материалов XXII Всероссийской научно-практической конференции, посвященной 105-летию со дня рождения доктора педагогических наук, профессора В.Ф. Афанасьева (Алданского), Якутск, 22 марта 2022 года. – Киров: Межрегиональный центр

инновационных технологий в образовании, 2022. – С. 101-103. – DOI 10.52376/978-5-907541-34-4_101.

125. Майлис Н. П. Использование информационных ресурсов при производстве судебных экспертиз / Н. П. Майлис // Вестник экономической безопасности. – 2021. – № 3. – С. 166–169.

126. Макаренко, И. А. Роль судебной экспертизы в уголовном судопроизводстве / И. А. Макаренко // Вопросы экспертной практики. – 2019. – № S1. – С. 385-388.

127. Макарова, З. С. Влияние информационного экстремизма на сознание молодежи / З. С. Макарова // Организация работы с детьми и молодежью по месту жительства: опыт, проблемы и перспективы развития : Сборник материалов Республиканской конференции по вопросам организации работы с детьми и молодежью по месту жительства, Казань, 30 ноября 2017 года. – Казань: Государственное бюджетное учреждение "Республиканский центр молодежных, инновационных и профилактических программ", 2017. – С. 64-66.

128. Макашова, В. Н. Информационные технологии как фактор распространения идей киберэкстремизма в молодежной среде / В. Н. Макашова, Е. В. Чернова // Современные информационные технологии и ИТ-образование. – 2013. – № 9. – С. 328-335.

129. Макашова, В. Н. Педагогические механизмы профилактики идеологии киберэкстремизма среди студенческой молодежи / В. Н. Макашова, Г. Н. Чусавитина // Современные информационные технологии и ИТ-образование. – 2015. – Т. 11. – № 1. – С. 102-105.

130. Малакаев, О. С. Экстремизм в социальных сетях / О. С. Малакаев // Вестник Института комплексных исследований аридных территорий. – 2018. – № 2(37). – С. 83-86.

131. Малыхина, Н. И. Цифровые следы как объект криминалистического исследования / Н. И. Малыхина // Современные

технологии и подходы в юридической науке и образовании : Сборник материалов международного научно-практического форума, Калининград, 27–31 августа 2020 года. – Калининград: Балтийский федеральный университет имени Иммануила Канта, 2021. – С. 200-205.

132. Марков, А. С. Руководящие указания по кибербезопасности в контексте ISO 27032 / А. С. Марков, В. Л. Цирлов // Вопросы кибербезопасности. – 2014. – № 1(2). – С. 28–35.

133. Маркова Т.В. Щербатых Д.А. Философия социальных сетей // Интерактивная наука. – 2018. DOI 10.21661/r-470385

134. Мартынов А.Н. Криминалистическая характеристика преступлений: проблема структурированности / Мартынов А.Н. // Вестник Южно-Уральского государственного университета. Серия: Право. - 2014. - № 2. - С.52

135. Матвеева, М. С. Экстремизм в молодёжной среде: предупреждение и профилактика / М. С. Матвеева // Современные проблемы права: пути решения : Материалы межвузовской научно-практической конференции, проводимой кафедрой конституционного, административного и уголовного права совместно с Научной комиссией студенческого Совета, Орел, 01 октября 2021 года / Под общей редакцией А.А. Комоско. – Орел: Среднерусский институт управления - филиал РАНХиГС, 2022. – С. 130-135.

136. Матюхин, А. В. Необходимые знания студентам о противодействии экстремизму (учебник "политика противодействия экстремизму" под редакцией А.П. Кошкина) / А. В. Матюхин // Журнал политических исследований. – 2021. – Т. 5. – № 1. – С. 178-184. – DOI 10.12737/2587-6295-2021-5-1-178-184.

137. Махтаев М.Ш. Криминалистическая профилактика: история становления, современные проблемы / М. Ш. Махтаев, Н. П. Яблоков. – Москва : Издательство «Юрлитинформ», 2016. – 288 с.

138. Махтаев М.Ш. Криминалистическое предупреждение преступлений (правонарушений) : учебное пособие для вузов / М.Ш. Махтаев. – Москва : Издательство Юрайт, 2020. – 229 с.

139. Махтаев, М. Ш. Использование сети Интернет для совершения преступлений террористического и экстремистского характера / М. Ш. Махтаев // Законодательство. – 2020. – № 4. – С. 70-75.

140. Мельникова М.С., Яковлев И.П. Понятие «социальная сеть» в социологических теориях и интернет-практиках// Вестник СПбГУ. Сер.9.2014.Вып.1. с 255

141. Мешалкин С. Н., Горностаева И. В., Федоткин А.И. Выявление, предупреждение, раскрытие и расследование преступлений экстремистской направленности, совершаемых в сети Интернет: учебно-методическое пособие. – Домодедово: ВИПК МВД России, 2016. – С.31

142. Мешков В.М. Роль и значение фактора времени в ситуационном подходе, применяемом при расследовании преступлений//Ситуационный подход в юридической науке и практике: современные возможности и перспективы развития: материалы Международной научно-практической конференции, посвященной 15-летию научной школы криминалистической ситуалогии БФУ им. И. Канта. 2017. С. 44–51.

143. Мещеряков В. А. Криминалистические особенности получения компьютерной информации с цифровых носителей при производстве отдельных следственных действий / В. А. Мещеряков, О. Ю. Цурлуй // Эксперт-криминалист. – 2020. – № 2. – С. 15–17.

144. Мещеряков В.А. «Виртуальные следы» под «скальпелем Оккама»//Информационная безопасность регионов. 2009. № 1 (4). С. 33.

145. Мещеряков В.А. Следы цифрового века//Вопросы экспертной практики. 2019. № S1. С. 426.

146. Мещеряков В.А., Цурлуй О.Ю. Криминалистические особенности получения компьютерной информации с цифровых носителей

при производстве отдельных следственных действий // Эксперт-криминалист. 2020. № 2. С. 15–17.

147. Мещеряков, В. А. Государственно-частное партнерство в сфере противодействия киберпреступности: шаг вперед или реальная угроза / В. А. Мещеряков, Е. А. Пидусов // Вестник Воронежского института МВД России. – 2019. – № 3. – С. 161-166.

148. Мещеряков, В. А. Копирование информации с компьютерных носителей при производстве следственных действий / В. А. Мещеряков, О. Ю. Цурлуй // Цифровой след как объект судебной экспертизы : Материалы Международной научно-практической конференции, Москва, 17 января 2020 года. – Москва: РГ-Пресс, 2021. – С. 128-132.

149. Мещеряков, В. А. Криминалистика в цифровой век / В. А. Мещеряков // Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения) : Сборник статей Международной научно-практической конференции, Москва, 18 мая 2018 года. – Москва: Академия управления Министерства внутренних дел Российской Федерации, 2018. – С. 180-185.

150. Мещеряков, В. А. Криминалистические особенности получения компьютерной информации с цифровых носителей при производстве отдельных следственных действий / В. А. Мещеряков, О. Ю. Цурлуй // Эксперт-криминалист. – 2020. – № 2. – С. 15-17.

151. Мещеряков, В. А. Особенности использования специальных знаний в расследовании преступлений, связанных с применением информационных и телекоммуникационных технологий / В. А. Мещеряков // Воронежские криминалистические чтения. – 2017. – № 19. – С. 163-167.

152. Мещеряков, В. А. Особенности специальных знаний, используемых в цифровой криминалистике / В. А. Мещеряков // Известия Тульского государственного университета. Экономические и юридические науки. – 2013. – № 4–2. – С. 88.

153. Мещеряков, В. А. Специальные знания в расследовании преступлений в сфере использования информационных и телекоммуникационных технологий / В. А. Мещеряков // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. – 2016. – № 1. – С. 11-15.

154. Мещеряков, В. А. Формирование дополнительных компетенций экспертов криминалистических экспертиз в сфере исследования информационных систем и компьютерных устройств / В. А. Мещеряков, Ю. М. Баркалов // Вестник Воронежского института МВД России. – 2020. – № 1. – С. 183-188.

155. Мигулева М.В. История определения понятия «киберпространство» // Этносоциум и межнациональная культура. 2018. № 6 (120). С. 41–45.

156. Микаева А.С. Проблемы правового регулирования в сети Интернет и их причины / Микаева А.С. //"Актуальные проблемы российского права". - 2016. - N 9. - С.45

157. Миночкина Я. Язык вражды - открывая ящик Пандоры // Прецеденты Европейского суда по правам человека. 2016. N 10. С. 4 - 13.

158. Морозов И. Л. Политический экстремизм - леворадикальные течения: учеб. пособие для студентов и аспирантов. Волжский: Изд-во ВФ МЭИ, 2002. 70 с.

159. Мухтаров, М.М. Использование социальных сетей для выявления лиц, причастных к экстремистской деятельности / М. М. Мухтаров, У. Е. Ергенбек // Эффективное государство: достижения и новые направления развития: сборник научных трудов по материалам : Сборник научных трудов по материалам I Международной научно-практической конференции, Москва, 31 октября 2017 года. – Москва: Научная общественная организация "Профессиональная наука", 2017. – С. 113-125.

160. Ненашев С.М. Негативные воздействия на пользователей социальных сетей как элемент информационной войны // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2016. № 1. С. 39–45.

161. О противодействии экстремистской деятельности: федеральный закон от 25.07.2002 N 114-ФЗ (ред. от 23.11.2015) [Электронный ресурс]. Доступ из справ.-правовой системы «Консультант Плюс». Ст. 2

162. Олиндер Н.В., Гамбарова Е.А. Проблемные вопросы поиска и восприятия информации о человеке в сети интернет и ее использование при расследовании преступлений // Юридический вестник Самарского университета. 2016. Т.2, №4

163. Осипова, Е. В. Профилактика распространения идеологии экстремизма и терроризма в молодежной среде (на примере образовательных учреждений) / Е. В. Осипова, А. В. Прозоров // Ситуационная обусловленность терроризма и экстремизма как одной из угроз национальной безопасности Российской Федерации : Материалы Международной научно-практической конференции, Калининград, 04–06 декабря 2021 года. – Калининград: Балтийский федеральный университет имени Иммануила Канта, 2021. – С. 67-71.

164. Пастухов П.С. О необходимости развития компьютерной криминалистики / под ред. О.А. Кузнецовой, В.Г. Голубцова, Г.Я. Борисевич, Л.В. Боровых, Ю.В. Васильевой, С.Г. Михайлова, С.Б. Полякова, А.С. Телегина, Т.В. Шершень // Пермский юридический альманах. Ежегодный научный журнал. 2018. N 1. С. 479 - 488.

165. Петросян, М. А. Противодействие терроризму. Глобальная проблема современности / М. А. Петросян // Профилактика экстремизма в XXI веке: теория и практика : Материалы Международной научно-практической конференции, Москва, 21 февраля 2022 года. – Москва:

федеральное государственное бюджетное образовательное учреждение высшего образования "Московский политехнический университет", 2022. – С. 111-115.

166. Печенкин В. Анализ социальных сетей: в ожидании чуда // Журнал «Компьютера». 2005. № 42. С. 15-20.

167. Побегайло А.Э. Борьба с киберпреступностью: учеб. пособие / А.Э. Побегайло; Ун-т прокуратуры Рос. Федерации. – М., 2018. – 184 с.

168. Подкатилина М.Л. К вопросу о лингвистической экспертизе экстремистских материалов / Подкатилина М.Л. //"Эксперт-криминалист". - 2010. - № 4. - С.20

169. Полстовалов, О. В. Криминалистическая профилактика на уровне установления противоправных намерений: научная рефлексия трагедии в Казани / О. В. Полстовалов // Социально-экономическое развитие и качество правовой среды : Сборник докладов VIII Московского юридического форума (XIX Международная научно-практическая конференция): в 5 ч., Москва, 08–10 апреля 2021 года. – Москва: Московский государственный юридический университет имени О.Е. Кутафина (МГЮА), 2021. – С. 205-208.

170. Полстовалов, О. В. Обратная сторона цифровизации уголовного правосудия: новые вызовы для криминалистики и правоприменительной практики / О. В. Полстовалов // Современные технологии и подходы в юридической науке и образовании : Сборник материалов международного научно-практического форума, Калининград, 27–31 августа 2020 года. – Калининград: Балтийский федеральный университет имени Иммануила Канта, 2021. – С. 247-254.

171. Попкова Я.А. Блоггинг как специфическая форма социальной активности молодежи// Социальная активность молодежи как необходимое условие развития общества. Материалы международной научно-практической конференции. Под редакцией Г. В. Ковалевой. 2019. С. 351.

172. Преступность в XXI веке. Приоритетные направления противодействия / Ю. М. Батурин, В. Е. Батюкова, С. Д. Белоцерковский [и др.] ; Институт государства и права РАН. – Москва : Общество с ограниченной ответственностью "Издательство "Юнити-Дана", 2020. – 559 с. – ISBN 978-5-238-03423-2.

173. Пыхтеев, В. С. Деятельность органов прокуратуры по противодействию киберэкстремизму / В. С. Пыхтеев // Актуальные вопросы публичного права : Материалы XVII Всероссийской научной конференции молодых ученых и студентов. В 2-х частях, Екатеринбург, 01–02 ноября 2018 года / Отв. редактор Д.В. Конев. – Екатеринбург: Федеральное государственное бюджетное образовательное учреждение высшего образования "Уральский государственный юридический университет", 2018. – С. 510-515.

174. Расследование преступлений экстремистской направленности, совершенных с использованием информационно-телекоммуникационных технологий : Научно-практическое пособие / А. А. Бессонов, Ф. О. Байрамова, И. В. Гарт [и др.] ; Следственный комитет Российской Федерации. – Москва : Издательство "Юрлитинформ", 2021. – 176 с. – (Библиотека криминалиста). – ISBN 978-5-4396-2150-7.

175. Рогозин, Е. А. Тенденции развития классификационных систем угроз безопасности информации / Е. А. Рогозин, В. А. Мещеряков, А. М. Каднова // Вестник Воронежского института МВД России. – 2020. – № 3. – С. 165-169.

176. Романова, Л. М. Правовое и психологическое сопровождение межличностных отношений подростков, склонных к совершению преступлений террористического и экстремистского характера / Л. М. Романова, А. Р. Трофимчук // Противодействие идеологии экстремистской и террористической деятельности среди молодежи : Сборник научных статей,

Ростов-на-Дону, 15 октября 2021 года. – Ростов-на-Дону: Донской государственный технический университет, 2022. – С. 135-139.

177. Российский праворадикальный экстремизм и социальные сети как пространство его публичного существования / В. В. Кашпур, А. А. Барышев, Ю. О. Мундриевская, Е. В. Щекотин // Противодействие терроризму. Проблемы XXI века - COUNTER-TERRORISM. – 2017. – № 3. – С. 27-33.

178. Россинская Е.Р., Рядовский И.А. Концепция цифровых следов в криминалистике // Аубакировские чтения: материалы Международной научно-практической конференции (19 февраля 2019 г.). Алматы, 2019. С. 6–8.

179. Россинская, Е. Р. Учение о цифровизации судебно-экспертной деятельности и проблемы судебно-экспертной дидактики / Е. Р. Россинская // Правовое государство: теория и практика. – 2020. – № 4–1(62). – С. 88–101.

180. Руденко, О. Ю. Киберэкстремизм в молодёжной среде / О. Ю. Руденко // Сборники конференций НИЦ Социосфера. – 2013. – № 55. – С. 33-35.

181. Рыдченко, К.Д. Административно-правовое обеспечение информационно-психологической безопасности органами внутренних дел Российской Федерации: дис. … канд. юрид. наук : 12.00.14 / К.Д. Рыдченко. — Воронеж, 2011. – С. 166

182. Садыгова Т. С. Социально-психологические функции социальных сетей // Вектор науки ТГУ. - 2012. - №3 (10). - С. 192-194.

183. Семикаленова А.И., Рядовский И.А. Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики // Актуальные проблемы российского права. 2019. N 6. С. 178 - 185.

184. Серобян Г.А., Яковенко А.А. О понятии «киберпространство» в современной научной доктрине//Право и государство: теория и практика. 2019. № 9 (177). С. 104–106.

185. Сигарев А. В., СмирноваМ. С. Законодательство о противодействии экстремизму: время осмысления и реформирования // Рос. юст. 2018. № 11. С. 35—38.

186. Сидорова И.Г. Способы позиционирования интернет-личности в социальной сети // Известия Волгоградского государственного педагогического университета. - 2013.

187. Синергия цифровых технологий и графического моделирования в криминалистическом противодействии распространению идеологии экстремизма и терроризма в молодежной среде / Т. С. Волчецкая, Е. В. Осипова, М. В. Авакьян, А. А. Викторов // Вестник Томского государственного университета. – 2021. – № 471. – С. 215-222.

188. Скобелин С.Ю. Использование цифровых технологий при доказывании преступной деятельности // Российский следователь. 2019. N 3. С. 26 - 28.

189. Славин В. Е. О некоторых вопросах определения места предварительного расследования киберпреступлений / В. Е. Славин, В. О. Головизин, М. В. Сапсай // Наука и бизнес: пути развития. – 2019. – № 12(102). – С. 275–277.

190. Смушкин А.Б. Виртуальные следы в криминалистике / А.Б. Смушкин // Законность. - 2012. - N 8. - С. 43.

191. Соловьев В.С. Преступность в социальных сетях интернета (криминологическое исследование по материалам судебной практики) /Соловьев В.С.// Криминологический журнал Байкальского государственного университета экономики и права. - 2016. - Т. 10, № 1. - С. 60–72.

192. Соловьев В.С. Преступность в социальных сетях Интернета (криминологическое исследование по материалам судебной практики) // Криминологический журнал Байкальского государственного университета экономики и права. 2016. Т. 10. № 1. С. 60–72.

193. Степаненко Д.А., Рудых А.А. Использование открытых информационных технологий для расследования преступлений в отношении несовершеннолетних // Российский следователь. 2019. №4 С. 17

194. Степанова, А. А. Подростковый экстремизм: проблема травли и психологического воздействия на подростков в сети Интернет / А. А. Степанова, В. К. Косьяненко // Особенности реализации молодежной политики в вопросах профилактики экстремизма в городе Новосибирске : Материалы международного научно-практического форума, Новосибирск, 22–26 ноября 2021 года / Под научной редакцией А.С. Поличко. – Новосибирск: Новосибирский государственный педагогический университет, 2022. – С. 117-120.

195. Столбинская, Л. Е. Футбольный фанатизм, переходящий в экстремизм / Л. Е. Столбинская // Особенности реализации молодежной политики в вопросах профилактики экстремизма в городе Новосибирске : Материалы международного научно-практического форума, Новосибирск, 22–26 ноября 2021 года / Под научной редакцией А.С. Поличко. – Новосибирск: Новосибирский государственный педагогический университет, 2022. – С. 121-124.

196. Стороженко О.Ю. Противодействие экстремизму в информационном пространстве социальных сетей // Общество и право. - 2014. - № 2 (48). - С. 158 - 163.

197. Судебно-экспертная деятельность: правовое, теоретическое и организационное обеспечение : Учебник для аспирантуры / Е. Р. Россинская, Е. И. Галяшина, А. М. Зинин [и др.]. – Москва : Издательский Дом «Инфра-М», 2019. – 400 с.

198. Терентьева, Л. В. Понятие киберпространства и очерчивание его территориальных контуров / Л. В. Терентьева // Правовая информатика. – 2018. – № 4. – С. 66–71.

199. Ткачев А.В. Исследование компьютерной информации в криминалистике // Эксперт-криминалист. 2012. N 4. С. 5 - 8.

200. Токарева, В. А. Влияние социальных сетей на мировоззрение современного человека / В. А. Токарева // Традиции и инновации в пространстве современной культуры : Материалы IV Всероссийской научно-практической конференции, Липецк, 14–15 апреля 2022 года. – Липецк: Липецкий государственный педагогический университет имени П.П. Семенова-Тян-Шанского, 2022. – С. 130-134.

201. Трусов А.И. Установление личности гражданина Российской Федерации, совершившего правонарушение // Российская юстиция. 2016. N 9. С. 22 - 25.

202. Федоров А. П. Об опыте Китая по противодействию манипуляционным технологиям в социальных сетях Интернета / А. П. Федоров // Вестник Московского государственного областного университета. – 2018. – № 2. – С. 179–188.

203. Федосеева, К. Д. Предупреждение и профилактика экстремизма и терроризма в поликультурной молодежной среде / К. Д. Федосеева, А. В. Поддубняков // Особенности реализации молодежной политики в вопросах профилактики экстремизма в городе Новосибирске : Материалы международного научно-практического форума, Новосибирск, 22–26 ноября 2021 года / Под научной редакцией А.С. Поличко. – Новосибирск: Новосибирский государственный педагогический университет, 2022. – С. 133-139.

204. Федяшкин, М. В. Понятие и сущность экстремизма. Характеристика возникновения причин и условий экстремизма / М. В. Федяшкин // Студенческий вестник. – 2020. – № 20-5(118). – С. 63-66. – EDN WATPJL.

205. Фещенко П. Н. Место социальной напряженности в причинном комплексе экстремизма и терроризма // Экстремизм: социальные, правовые и криминологические проблемы / под. ред. А. И. Долговой. М., 2010. С. 59-60.

206. Филина Н.В. Политические акценты современных взаимодействий религиозного и светского в обществе //Журнал политических исследований. - 2020. - Т.4. - №3. - С. 24-45.

207. Хан, В. Актуальность терминологических проблем при решении задач противодействия компьютерным преступлениям / В. Хан // Раскрытие и расследование преступлений, сопряженных с использованием средств вычислительной техники. Проблемы, тенденции, перспективы - М.: РосНОУ, 2005.

208. Хафизов, И. Г. Социальная профилактика экстремизма в молодежной среде / И. Г. Хафизов // Поколения y и z в постпандемийной реальности: идентификации, ориентации, поведение : Сборник статей Всероссийской научно-практической конференции, Уфа, 24–26 ноября 2021 года. – Уфа: Башкирский государственный университет, 2022. – С. 153-158.

209. Хачукаева, К. И. Социальные сети и профилактика экстремизма среди учащейся молодежи / К. И. Хачукаева, А. Р. Мидаева // Фундаментальные основы инновационного развития науки и образования : сборник статей VI Международной научно-практической конференции : в 3 ч., Пенза, 30 декабря 2019 года. – Пенза: "Наука и Просвещение" (ИП Гуляев Г.Ю.), 2019. – С. 11-13.

210. Хлус А.М. Средства совершения преступлений как элемент их криминалистической структуры / А.М. Хлус // Российское право: образование, практика, наука, 2018. № 1. - 112 с. - С. 24

211. Холопова Е.Н. Ситуационная экспертиза: понятие, значение и возможности исследования // Ситуационный подход в юридической науке и практике: современные возможности и перспективы развития: Материалы Международной научно-практической конференции, посвященной 15-летию

научной школы криминалистической ситуалогии БФУ им. И. Канта. 2017. С. 232–239.

212. Холопова, Е. Н. Принципы построения структурно-функциональной модели психосемантики экстремизма / Е. Н. Холопова, А. А. Гайворонская // Современные технологии и подходы в юридической науке и образовании : Сборник материалов международного научно-практического форума, Калининград, 27–31 августа 2020 года. – Калининград: Балтийский федеральный университет имени Иммануила Канта, 2021. – С. 333-337.

213. Хорунжий, С. Н. Экспертиза цифрового изображения: род, вид или класс? / С. Н. Хорунжий, В. А. Мещеряков // Вопросы экспертной практики. – 2019. – № S1. – С. 695-698.

214. Цурлуй, О. Ю. Направления развития габитоскопии и портретной экспертизы с учетом информационных технологий и методов искусственного интеллекта / О. Ю. Цурлуй, В. А. Мещеряков // Эксперт-криминалист. – 2021. – № 2. – С. 25-28.

215. Цховребова, И.А. О функциональном назначении криминалистической характеристики преступления / И. А. Цховребова // Сборник материалов 50-х криминалистических чтений - М.: Академия управления МВД России, 2009.

216. Чернова, Е. В. Пропедевтика явлений киберэкстремизма в молодежной среде / Е. В. Чернова // Сборник научных трудов SWorld. – 2013. – Т. 16. – № 2. – С. 44-47.

217. Чернова, Е. В. Формирование толерантного мировоззрения у учащихся для профилактики киберэкстремизма в условиях поликонфессионального и многонационального общества / Е. В. Чернова, Г. З. Гиляжева // Современные информационные технологии и ИТ-образование. – 2014. – № 10. – С. 671-681.

218. Черных Н.А., Ермакова О.В., Иванкович С.В. Работа по профилактике экстремизма в молодёжной среде (на примере

борисоглебского городского округа) // Психология и педагогика: актуальные проблемы и тенденции развития: материалы IV Международной научно-практической конференции 14-15 ноября 2018 г. / Отв. ред. А.А. Долгова. - ООО «Издательство Ритм», Воронеж, 2018. - С. 118-120

219. Черных, Н. А. К вопросу о профилактике экстремизма: динамика представлений об экстремизме у молодёжи Борисоглебского городского округа / Н. А. Черных, С. В. Иванкович // Непрерывное образование в современном мире: история, проблемы, перспективы. : Материалы VI Всероссийской с международным участием научно-практической конференции, Борисоглебск, 30 марта 2019 года. – Борисоглебск: Издательство «Перо», 2019. – С. 320-324.

220. Шевченко Е.С. О криминалистической трактовке понятия "киберпреступность" / Е.С. Шевченко // Информационное право. - 2014. - N 3. - С. 29 - 32.

221. Шипицин А.И. Феномен социальных сетей в современной культуре // Известия Волгоградского государственного педагогического университета. – 2011. – С. 38

222. Щебетенко С.А. Большая пятерка черт личности и активность пользователей в социальной сети «ВКонтакте» //Вестник Южно-Уральского государственного университета. Серия: Психология. - 2013. – Том 6 № 4. - С.73

223. Югова, Д. И. Профилактика молодёжного экстремизма в образовательных учреждениях / Д. И. Югова, С. Н. Добросмыслова // Молодежь и государство: научно-методологические, социально-педагогические и психологические аспекты развития современного образования. Международный и российский опыт : Сборник трудов XI Всероссийской научно-практической конференции с международным участием, Тверь, 18 октября 2021 года / Под редакцией М.А. Крыловой. – Тверь: Тверской государственный университет, 2022. – С. 117-121.

224. Юрасова, Е.Н. Психологические особенности лиц, склонных к экстремизму, терроризму и ксенофобии / Е.Н. Юрасова // Юридическая психология. - №4. - 2008.

225. Яблоков Н.П. Криминалистика: природа, система, методологические основы. 2-е изд. М., 2009. С. 56.

226. Ярощук, И. А. Киберэкстремизм как одна из ключевых проблем современности / И. А. Ярощук // Актуальные проблемы раскрытия и расследования преступлений, совершаемых с использованием интернета : Сборник материалов Всероссийской научно-практической конференции, Белгород, 23 сентября 2021 года / Под редакцией Н.А. Жуковой. – Федеральное государственное автономное образовательное учреждение высшего образования «Белгородский государственный национальный исследовательский университет»: Белгородский государственный национальный исследовательский университет, 2021. – С. 104-107.

III. Авторефераты и диссертации

227. Агибалов В. Ю. Виртуальные следы в криминалистике и уголовном процессе : специальность 12.00.09 «Уголовный процесс» : автореф. дисс. … канд. юрид. наук / Агибалов Владимир Юрьевич. – Воронеж, 2010. – 24 с.

228. Безбогова М. С. Социальные сети как фактор формирования социальных установок современной молодежи : автореферат дисс. ... канд. психол. наук : 19.00.05 / Безбогова Марина Сергеевна; [Место защиты: Гос. ун-т упр.]. - Москва, 2017. - 25 с.

229. Брун О.Н. Развитие теорий социальных сетей: от локального к глобальному социуму : дисс. ... канд. социол. наук : 22.00.01 / Брун Ольга Евгеньевна; [Место защиты: Моск. гос. ин-т междунар. отношений]. - Москва, 2012. - 154 с.

230. Будыльский Д.В. Автоматизация мониторинга общественного мнения на основе интеллектуального анализа сообщений в социальных сетях: дисс. ... канд. тех. наук: 05.13.10 / Будыльский Дмитрий Викторович; [Место защиты: Брянский государственный технический университет]. - Брянск, 2015.- 169 с.

231. Вехов В.Б. Криминалистическая характеристика и совершенствование практики расследования и предупреждения преступлений, совершаемых с использованием средств компьютерной техники: автореф. дис. ... канд. юрид. наук. Волгоград, 1995. С. 15.

232. Вехов, В.Б. Криминалистическая характеристика и совершенствование практики расследования и предупреждения преступлений, совершаемых с использованием средств компьютерной техники: автореф. дис. ... канд. юрид. наук. Волгоград, 1995. - 27 с.

233. Волчецкая Т. С. Ситуационное моделирование в расследовании преступлений: автореф. дис. …канд. юрид. наук. М.: МГУ им. М.В. Ломоносова, 1991. – 23 с.

234. Волчецкая Т.С. Криминалистическая ситуалогия: дисс. …д-ра юрид. наук. М.: МГУ им. М.В. Ломоносова, 1997. – 395 с.

235. Волчецкая Т.С. Ситуационное моделирование в расследовании преступлений: дисс. … канд. юрид. наук. М., 1991. – 173 с.

236. Давыдов, В.О. Информационное обеспечение раскрытия и расследования преступлений экстремистской направленности, совершенных с использованием компьютерных сетей: автореф. дисс. … канд. юрид. наук. Ростов-н/Д., 2013. – 42 с.

237. Давыдов, В.О. Методика расследования транснациональной преступной деятельности экстремистского характера : дисс. ... д-ра юрид. наук : 12.00.12 / Давыдов Владимир Олегович; [Место защиты: Рост. юрид. ин-т МВД РФ]. - Ростов-на-Дону, 2018. - 607 с.

238. Давыдов, В.О. Информационное обеспечение раскрытия и расследования преступлений экстремистской направленности, совершенных с использованием компьютерных сетей : дисс. ... канд. юрид. наук : 12.00.12 / Давыдов Владимир Олегович; [Место защиты: Рост. юрид. ин-т МВД РФ].- Тула, 2013.- 264 с.

239. Иванов И.И. Криминалистическая превенция: комплексное исследование генезиса, состояния, перспектив: автореф. дисс. … д-ра юрид. наук. М., 2004. С. 206.

240. Кулешов, Р.В. Теоретико-методологические основы раскрытия и расследования преступлений в сфере экстремистской и террористической деятельности : дисс. ... д-а юрид. наук : 12.00.12 / Кулешов Роман Владимирович; [Место защиты: Рост. юрид. ин-т МВД РФ]. - Ростов-на-Дону, 2017. - 545 с.

241. Лещенко А. М. Социальные сети как механизм конструирования коммуникации в современном обществе: автореферат дисс. ... канд. философ. наук : 09.00.11 / Лещенко Александр Михайлович; [Место защиты: Пятигорский государственный гуманитарно-технологический университет]. - Пятигорск, 2011. - 25 с.

242. Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации: автореф. дисс. … д-ра юрид. наук — Воронеж, 2001. — 39 с.

243. Милашев В.А. Проблемы тактики поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ: автореф. дисс. ... канд. юрид. наук, 2004. 24 с.

244. Мусаева, У .А. Розыскная деятельность следователя по делам о преступлениях в сфере компьютерной информации: дисс. … канд. юрид. наук / У.А. Мусаева - Тула, 2001.

245. Мыльников, Б.А. Противодействие преступлениям экстремистской направленности: криминологический и уголовно-правовой аспекты: дисс. ... канд. юрид. наук / Б.А. Мыльников - М., 2005.

246. Новиков, Д.В. Этнорелигиозный экстремизм на Северном Кавказе: методы противодействия (политико-правовой аспект): дисс. ... канд. юрид. наук / Д.В. Новиков - Ростов-на-Дону, 2002.

247. Поминов, С.Н. Организация деятельности органов внутренних дел в сфере противодействия проявлениям религиозного экстремизма: автореф. дисс. ... канд. юрид. наук / С.Н. Поминов - М., 2007.

248. Семикаленова, А.И. Судебная программно-техническая экспертиза: организационные, правовые и методические аспекты: дисс. ... канд. юрид. наук / А.И. Семикаленова - М., 2004.

249. Скворцова, Т.А. Религиозный экстремизм в контексте государственно-правового обеспечения национальной безопасности современной России: дисс. ... канд. юрид. наук / Т.А. Скворцова - Ростов-на-Дону, 2004.

250. Филиппов, С.С. Информационное обеспечение советской физической культуры: дисс. … д-ра пед. наук / С.С. Филиппов. - Л, 1991.

251. Хлебушкин А.Г. Преступный экстремизм: понятие, виды, проблемы криминализации и пенализации: автореф. дисс. ... канд. юрид. наук / А.Г. Хлебушкин - Саратов, 2007.

252. Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: дис. … канд. юрид. наук. М., 2016. С. 10.

253. Юрков А.А. Виртуальная компьютерная реальность: негативные и позитивные формы межсубъектных взаимосвязей: автореф. дис. ... канд. юрид. наук. Москва, 2013. – 24 с.

IV.Иностранаая литература

254. Amy Shuen. Web 2.0: A Strategy Guide. — O'Reilly, 2008. — 272 p. — ISBN 978-0-596-52996-3.

255. J. A. Barnes Class and committees in a norwegian island parish [Электронный ресурс] URL:http://pierremerckle.fr/wp-content/uploads/2012/03/Barnes.pdf

256. Jennifer Golbeck Introduction to Social Media Investigation: A Hands-on Approach // Elsevier, ISBN: 9780128016565, 2015, 305 c.

257. Tim O'Reilly What Is Web 2.0 Design Patterns and Business Models for the Next Generation of Software [Электронный ресурс] URL: https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=3

V. Интернет – ресурсы

258. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. [Электронный ресурс] URL:http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf (дата обращения: 20.05.2022)

259. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. [Электронный ресурс].URL:http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf – Загл. с экрана. (дата обращения: 20.05.2022)

260. The State of Broadband: Broadband catalyzing sustainable development. [Электронный ресурс] URL:https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.18-2017-PDF-E.pdf – Загл. с экрана. (дата обращения: 20.05.2022).

261. The Use of the Internet for Terrorist Purposes. [Электронный ресурс]. –

URL:http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf (дата обращения: 20.05.2022)

262. Бессонов А. А. О некоторых возможностях современной криминалистики в работе с электронными следами // Вестник Университета имени О.Е. Кутафина. 2019. №3 (55). URL: https://cyberleninka.ru/article/n/o-nekotoryh-vozmozhnostyah-sovremennoy-kriminalistiki-v-rabote-s-elektronnymi-sledami (дата обращения 23.07.2020).

263. Бондаренко Ю.А., Кизилов Г.М. Проблемы выявления и использования следов преступлений, оставляемых в сети «Darknet»// Юридический вестник Кубанского государственного университета. 2019, № 5. С. 97–101. [Электронный ресурс]. Режим доступа: https://online-science.ru/m/products/law_sciense/gid5181/pg0/ (дата обращения 16.02.2021).

264. Всё о Вконтакте 2020 [Электронный ресурс]. Режим доступа: https://online-vkontakte.ru/2018/10/skolko-lyudej-zaregistrirovano-v-vk.html (дата обращения 19.08.2021).

265. Вся статистика Интернета и соцсетей на 2021 год – цифры и тренды в мире и в России. [Электронный ресурс]. URL: https://www.web-canape.ru/business/vsya-statistika-interneta-i-socsetej-na-2021-god-cifry-i-trendy-v-mire-i-v-rossii/ (дата обращения: 08.11.2021).

266. Вся статистика Интернета на 2020 год — цифры и тренды в мире и в России [Электронный ресурс]. – Режим доступа: URL: https://www.web-canape.ru/business/internet-2020-globalnaya-statistika-i-trendy/(дата обращения 19.11.2021).

267. Жизнь без интернета: рай или апокалипсис? [Электронный ресурс] URL: https://wciom.ru/index.php?id=236&uid=9681 – Загл. с экрана. (дата обращения: 20.05.2022)

268. Одоевский В.Ф. "Повести и рассказы", ГИХЛ, 1959. [Электронный ресурс] URL: http://az.lib.ru/o/odoewskij_w_f/text_0490.shtml – Загл. с экрана (дата обращения: 20.05.2022).

269. Социальные сети и цензура: за и против. [Электронный ресурс] URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/socialnye-seti-i-cenzura-za-i-protiv – Загл. с экрана (дата обращения: 20.05.2022).

270. Федеральный список экстремистских материалов. [Электронный ресурс]. URL: http://minjust.ru/extremist-materials (дата обращения: 20.05.2022).

V. Эмпирические материалы

271. Уголовные дела из Архива Центрального районного суда г. Калининграда (2014 -2022 гг)

272. Уголовные дела из Архива Ленинградского районного суда г. Калининграда (2013 -2019 гг)

273. Уголовные дела из Архива Московского районного суда г. Калининграда (2012 -2022 гг)

274. Уголовные дела из Архива Приволжского районного суда г. Казани (2014 -2020 гг)

275. Уголовные дела из Архива Вахитовского районного суда г. Казани (2013 -2016 гг)

276. (Уголовные дела из Архива Пресненского районного суда г. Москвы (2012 -2020 гг)

277. Уголовные дела из Архива Чертановского районного суда г. Москвы (2013 -2021 гг)

278. Уголовные дела из Архива Октябрьского районного суда г. Ставрополя (2019 -2021 гг)

279. Уголовные дела из Архива Химкинского Городского суда Московской Области (2012 -2022 гг)

280. Уголовные дела из Архива Ленинского районного суда г. Махачкала (2014 -2020 гг)

281. Приговор Ленинского районного суда г. Чебоксары от 12 сентября 2011 года [Электронный ресурс]. Доступ из справ.-правовой системы «Судебные и нормативные акты РФ» (СудАкт).

282. Приговор Курского гарнизонного военного суда от 18 января 2012 года N 3-2012 [Электронный ресурс]. Доступ из справ.-правовой системы «Судебные и нормативные акты РФ» (СудАкт).

283. Приговор Новоржевского районного суда Псковской области от 27 мая 2015 года N 1-12/2015[Электронный ресурс]. Доступ из справ.-правовой системы «Судебные и нормативные акты РФ» (СудАкт).

284. Постановление Исакогорского районного суд г. Архангельска от 22 августа 2016 года N 1-102/2016 [Электронный ресурс]. Доступ из справ.-правовой системы «Судебные и нормативные акты РФ» (СудАкт).

285. Приговор Окуловского районного суда Новгородской области от 12 октября 2016 N 1-134/2016 [Электронный ресурс]. Доступ из справ.-правовой системы «Судебные и нормативные акты РФ» (СудАкт).

286. Приговор Гороховецкого районного суда Владимирской области от 27 февраля 2017 года N1-12/2017[Электронный ресурс]. Доступ из справ.-правовой системы «Судебные и нормативные акты РФ» (СудАкт).

287. Постановление Октябрьского районного суда г. Томска от 06 марта 2017 года N1-151/2017[Электронный ресурс]. Доступ из справ.-правовой системы «Судебные и нормативные акты РФ» (СудАкт).

288. Постановление Октябрьского районного суда г. Саратова от 27 февраля 2017 года N1-28/2017[Электронный ресурс]. Доступ из справ.-правовой системы «Судебные и нормативные акты РФ» (СудАкт).

Приложение № 1

СВОДНАЯ АНАЛИТИЧЕСКАЯ ТАБЛИЦА

изучения судебно-следственной практики по преступлениям экстремистской направленности, совершенных с использованием социальных сетей.
за период с 2012 по первый квартал 2022 года.

В рамках диссертационного исследования изучено 132 материала репрезентативной выборки по преступлениям экстремистской направленности, совершенных с использованием социальных сетей за период за период с 2012 по первый квартал 2022 года, рассмотренных судами первой инстанции, г. Москвы, Московской, Калининградской областей, Ставропольского края, Республик Дагестан, Татарстан по следующим направлениям:

1) обнаружение характерных особенностей преступлений экстремистской направленности, совершенных с использованием социальных сетей.
2) выявление типовых следственных ситуаций, алгоритмов их разрешения.
3) определение типичных следственных действий по указанным преступлениям.
4) выявления проблем, возникающих при использовании специальных знаний в ходе расследования указанной категории преступлений.

Общий анализ материалов позволил выявить следующее:

№	Сведения	Количество	%
1	**Статус дел:**	**132**	**100%**
	рассмотрено судом, вынесен обвинительный приговор	55	41.67%
	возбуждено уголовное дело	77	58.33%
	вынесено постановление о применении принудительных мер воспитательного воздействия	-	-
	вынесено постановление о прекращении уголовного дела и уголовного преследования в связи с деятельным раскаянием	-	-
	вынесено постановление об отказе в возбуждении уголовного дела	15	11.36%
2	**Преступление совершено:**		
	в одиночку	103	78.03%
	группой лиц	29	21.97%
3	**Преступление обнаружено:**		
	при проведения целевого мониторинга	82	62.12%
	при получении информации от конфидентов	3	2.27%
	при получении информации в ходе оперативно-розыскных мероприятий	8	6.06%
	при получении информации в ходе расследования преступления экстремистской направленности, совершенного без использования компьютерных устройств и выхода в сеть Интернет	15	11.36%
	при поступлении заявления о преступлении	9	6.82%
	при расследовании преступлений общеуголовной направленности	15	11.36%
4	**Преступление совершено:**		
	с использованием личного аккаунта	76	57.58%
	с использованием псевдонима	56	42.42%

5	**Пол злоумышленника:**		
	женский	14	10.61%
	мужской	118	89.39%
6	**Возраст злоумышленника:**		
	до 18 лет	1	0.76%
	18–30 лет	96	72.72%
	30 лет и более	35	26.52%
7	**Социальная сеть, использованная для совершения преступления:**		
	ВКонтакте	98	74.24%
	Одноклассники	26	19.7%
	Facebook	5	3.79%
	Twitter	3	2.27%
	другие	-	-
8	**Злоумышленник использовал средства анонимизации:**		
	да	48	36.36%
	нет	84	63.64%
9	**Средствами анонимизации являлись:**		
	прокси-сервер	6	4.55%
	анонимайзер	16	12.12%
	VPN-подключение	25	18.94%
	Socks-протокол	1	0.76%
10	**По делу назначались судебные экспертизы:**		
	компьютерно-техническая судебная экспертиза	130	98.48%
	лингвистическая судебная экспертиза	132	100%
	Из них: комплексная лингвистическая судебная экспертиза	48	36.36%
	психолого-психиатрическая судебная экспертиза	-	-

11	**Комплексная лингвистическая экспертиза включала экспертов*:**		
	Лингвистов	48	100%
	Психологов	30	22.73%
	Историков	7	5.3%
	Религиоведов	21	15.91%
	Антропологов	-	-
	Философов	-	-
	Политологов	-	-
	Другие	-	-
	*в соответствии с п.23. Постановления Пленума Верховного Суда РФ от 28.06.2011 N 11 (ред. от 28.10.2021) "О судебной практике по уголовным делам о преступлениях экстремистской направленности"		
12	**Следственные действия, произведенные по делу:**		
	осмотр места происшествия	132	100%
	следственный эксперимент	-	-
	проверка показаний на месте	-	-
	обыск	122	92.42%
	выемка	64	48.48%
	осмотр электронных устройств	120	90.91%
	осмотр предметов	25	18.94%
	допрос подозреваемого	117	88.64%
	допрос свидетеля	13	9.85%
	допрос потерпевшего	-	-
13	**Проводились оперативно-розыскные мероприятия:**		
	да	132	100%
	нет	-	-

Приложение № 2

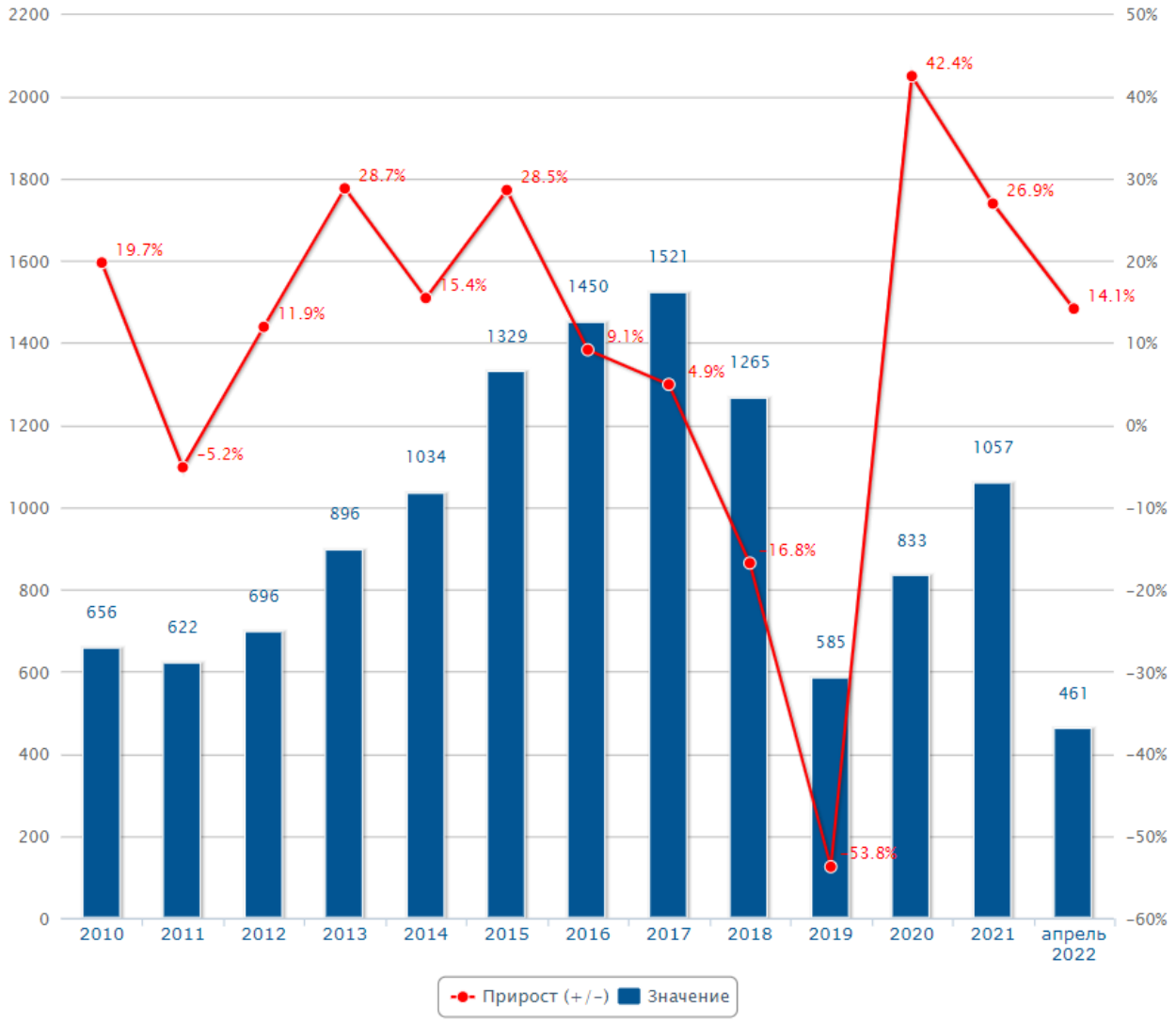

Схема 1. Динамика зарегистрированных преступлений экстремистской направленности[1]

[1] Информационно-аналитический портал правовой статистики Генеральной прокуратуры Российской Федерации

Приложение № 3

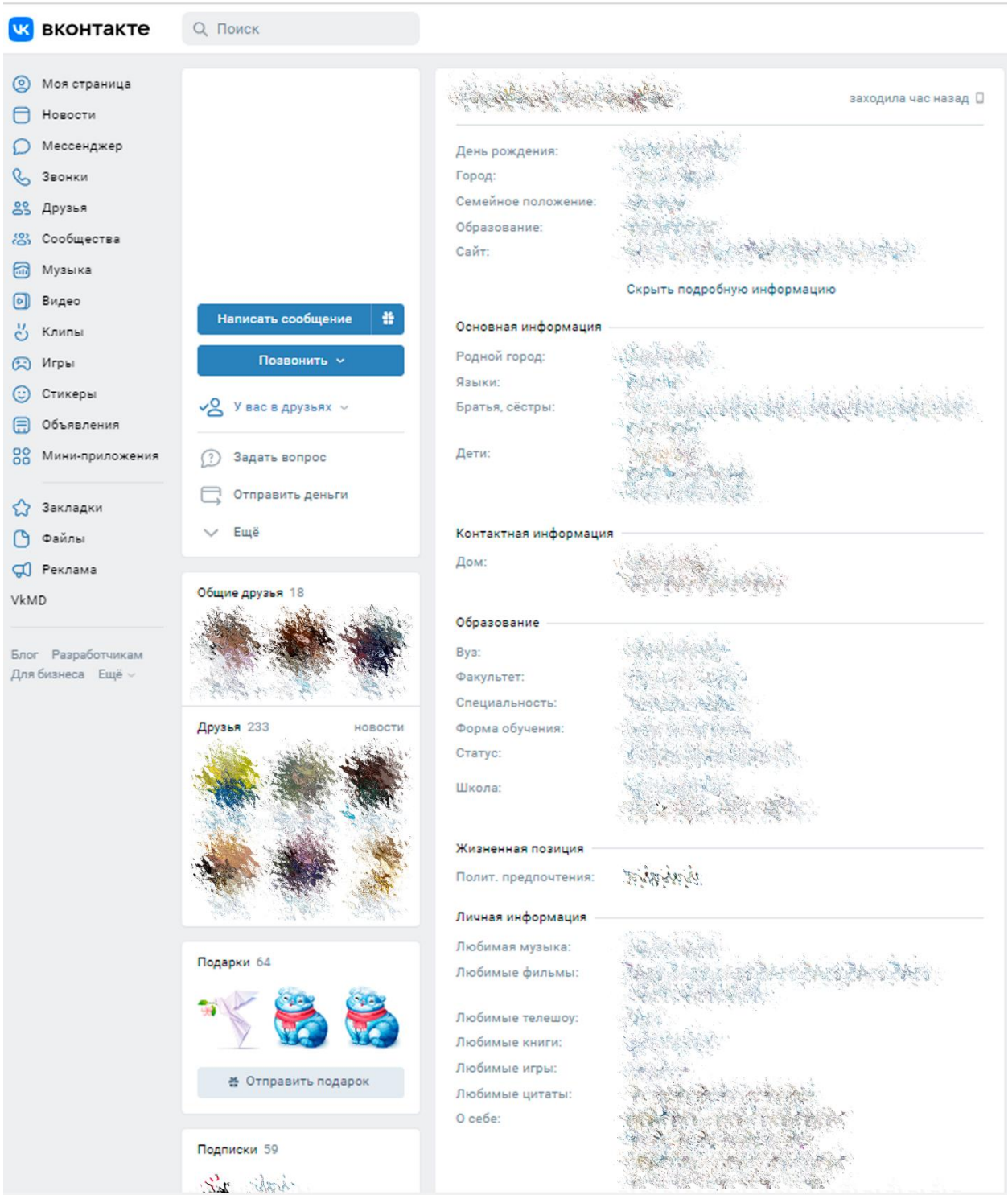

Рис. 1. Содержание страницы социальной сети (на примере социальной сети «В контакте»)