Федеральное государственное казенное образовательное учреждение
высшего образования «Сибирский юридический институт
Министерства внутренних дел Российской Федерации»

Кафедра уголовного процесса

Специальность 40.05.01 Правовое обеспечение национальной безопасности, специализация № 1 «Уголовно-правовая» (узкая специализация – предварительное следствие в органах внутренних дел)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
по теме:

СЛЕДСТВЕННЫЕ ДЕЙСТВИЯ, НАПРАВЛЕННЫЕ НА ПОЛУЧЕНИЕ СВЕДЕНИЙ, СОДЕРЖАЩИХСЯ В СЕТИ ИНТЕРНЕТ: УГОЛОВНО-ПРОЦЕССУАЛЬНЫЕ АСПЕКТЫ

Выполнил:
Слушатель учебной группы НБ-1802
младший лейтенант полиции
Донская Полина Дмитриевна

Руководитель:
Старший преподаватель кафедры
уголовного процесса
подполковник полиции
Карлов Андрей Леонидович

Консультант:
Профессор кафедры
криминалистики,
кандидат юридических наук, доцент
полковник полиции
Земцова Светлана Игоревна

Дата защиты:

«22» 06 2023 г.

Оценка: отлично

Председатель ГЭК

полковник юстиции		К.А. Юдаева
(специальное звание)	(подпись)	(инициалы, фамилия)

Красноярск 2023

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования. На сегодняшний день доступ к сети Интернет свободен и практически не ограничен по всему миру. С каждым днем растут пользователи электронной почты, социальных сетей, стало возможным направление писем, просьб, заявлений, ходатайств всуды и другие государственные органы через сеть Интернет. В связи с чем преступная деятельность набирает большие обороты в виртуальной реальности. Так, в январе – феврале 2023 года в России зарегистрированы 93 372 преступлений, совершенных с использованием информационно-телекоммуникационных технологий и в сфере компьютерной информации, что на 17,1 % больше, по сравнению с аналогичным периодом 2022 года.[1] Это объясняется тем, что в настоящее время совеременный мир стал зависим от информационных технологий, что приводит к возникновенияю новых видов преступелний, совершаемых с использованием сети Интернет. Согласно официальной статистике на 30 января 2023 года в мире насчитывается 5,16 миллиардов пользователей сети Интернет, что составляет 64,4% мирового населения.[2]

Законодатель, согласно ст. 2 Федерального закона от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» определил сеть Интернет, как технологическую систему, предназначенную для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

[1] Краткая характеристика состояния преступности в Российской Федерации за январь - февраль 2023 года [Электронный ресурс]: Официальный сайт Министерства внутренних дел Российской Федерации, 2023 МВД России – Режим доступа: https://мвд.рф/reports/item/36479770/ (дата обращения: 15.03.2023).

[2] Чуранов Е.А. Статистика интернета и соцсетей на 2023 год - цифры и тренды в мире и в России [Электронный ресурс]. – Режим доступа: https://www.web-canape.ru/business/statistika-interneta-i-socsetej-na-2023-god-cifry-i-trendy-v-mire-i-v-rossii/ (дата обращения 20.11.2022).

Доступ к сети не требует серьезных усилий и затрат, достаточно иметь вычислительную технику и подключение к информационно-телекоммуникационной сети. Чтобы информация из сети Интернет приобрела доказаетельственное значение, не обязательно чтобы само преступление было совершено в Интернете. Ведь там могут храниться только какие-то данные имеющие значение для уголовного дела. Многие из злоумышленников оставляют огромное количество следов в информационно-телекоммуникационной сети, свидетельствующих о событии преступления, данных о субъекте и много другое, что в последующем может быть использовано в качестве доказательств по уголовному делу. С помощью сети Интернет преступнки могут запутывать следы, тем самым скрывать данные, имеющие доказательственное значение.

На сегодняшний день нет четкого понятия, как называть эти данные, к какому виду доказательств их относить, как их получать, т.е. какие следственные или процессуальные действия использовать для их исследования и дальнейшего изъятия, а также, остается вопрос: как в последующем их процессуально закрпелять? Предлагается называть такие данные электронными доказаетльствами. Уголовно-процессуальное законодательство не содержит понятия эклектронных доказательств, в действующем законе упоминается лишь об электронных носителях информации, под которыми следует понимать материальные носители, используемые для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники.[1] В связи с этим В.Н. Григорьев справедливо указывает, что электронное доказывание на сегодняшний день находится на стадии осмысления и теоретического

[1] Межгосударственный стандарт. Единая система конструкторской документации. Электронные документы. Общие положения. ГОСТ 2.051-2013 от 01.06.2014 г. (утв. приказом Федерального агентства по техническому регулированию и метрологии от 17 октября 2013 г. № 1185-ст) // СПС «Гарант».

обоснования.[1] Данные пробелы по нашему мнению, необходимо устранять путем усовершенствования законодательства. В этой связи являются актуальными вопросы исследования доказательственной информации в сети Интернет и ее процессуального закрпеления.

В практической деятельности сотрудники правоохранительныхорганов сталкиваются со сложностями при выборе следственного действия для правильной фиксации указанной информации. В некоторых случаях, в результате неправильного выбора следственного действия могут ограничиваться права участников уголовного судопроизводства, а также возможны случаи признания доказательств, полученных неверным способом, недопустимыми. Нередко информация о преступлениях хранится на серверах, находящихся в других странах, либо в юрисдикции нескольких провайдеров, что требует сотрудничества между правоохранительными органами разных государств и выполнения определенных процедур, что в свою очередь также порождает немало практических нюансов.

Таким образом, можно констатировать, что актуальность темы исследования обусловленатем, что законодательство и практика нуждаются в точном процессуальном закреплении электронных доказательств, к которым будут относиться сведения из сети Интернет. А также в выделении специализированных следственных действий, которые позволят грамотно исследовать информацию в сети Интернет, имеющую доказательственное значение по уголовному делу.

Целью данной работы является формирование совокупности положений, позволяющих обеспечить правильный выбор следственного действия, направленного на получение информации в сети Интернет, как особого вида сведений, имеющих значение для производства по делу.

---

[1]Григорьев В.Н. Результаты смены парадигмы в исследованиях уголовного процесса / В.Н. Григорьев // Вестник Всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации. 2017. № 2(42). С. 39.

Достижение указанной цели обеспечивается решением следующих **задач**:

– исследовать сведения, содержащиеся в сети Интернет, которые представляют доказательственное значение;

– ознакомиться с характеристикой следственных действий, как средств фиксации сведений в сети Интернет;

– выделить исходные ситуации, в которых возникает необходимость производства следственных действий, направленных на получение и фиксацию сведений в сети Интернет;

– определить критерии выбора следственного действия, направленного на получение сведений в сети Интернет;

– определить пути решения практических и теоретических проблем производства следственных действий, направленных на получение сведений в сети Интернет.

Объектом исследования является совокупность урегулированных уголовно-процессуальных отношений, складывающихся в ходе исследования следственных и процессуальных действий, направленных на поиск и фиксацию информации в сети Интернет, содержащую доказательственное значение по уголовному делу.

Предметом исследования являются: правовая регламентация следственных действий, направленных на поиск информации в сети Интернет, теоретические положения уголовного судопроизводства, а также практика реализации указанных положений, связанных с выбором следственного действия для получения сведений в сети Интернет.

Степень научной разработанности темы выпускной квалификационной работы. Общие вопросы уголовно-процессуального законодательства рассматривались в трудах В.С. Балакшина, Б.Т. Безлепкина, Р.С. Белкина, В. П. Божьева, Л.В. Головко, А.П. Гуляева, А.А. Давлатова, С.И. Земцовой, Н.А. Зигуры, З.З. Зинатуллина, В.В. Кальницкого, Ф.М. Кудина, Е.Р. Россинской, А.В. Смирнова,

В.Т. Тотмина, Л.Т. Ульяновой, И.Я.Фойницкого, С.А.Шейфера, Н.С. Элькинд.

Вопросам, посвященным положениям, направленным на исследование сведений в сети Интернет с помощью следственных действий посвящены работы А.С. Александрова, Н.А. Архиповой, С.П. Безрученко, М.В. Болотова, Я.П. Велиева, С. В. Волкова, С.Н. Воробей, С.П. Ворожбит, В.А. Гаужаевой, Л.В. Головко, В.Н. Григорьева, Е.В. Егоровой, Е.С. Ермаковой, А.А. Жижилевой, О.Л.Журба, С.И. Земцовой, С.В. Зуева, А.Н. Иванова, А.Л. Карлова, А.Н. Колычевой, М.А. Кошелевой, М.Д. Кузьмина, Н.А. Кульмухамбетова, А.С. Мельникова, А.Л. Мишуточкина, С.С. Новикова, А.Н. Першина, Х.Х. Рамалданова, Е.Р. Россинской, С.Б. Россинского, В.Ю. Стельмаха, С.В. Супрун, Ю.А. Тарасова, Телевицкой, М.Н. Федорова, И.С. Федотова, Я.Б. Цабан, Ю.В. Шелегова, Т.К. Шогенова.

Значение разработки проблемы для теории и практики деятельности органов внутренних дел или иных правоохранительных органов состоит в том, что сформулированные в ходе исследования проблемы и положения в дальнейшем могут быть реализованы в целях усовершенствования уголовно-процессуального законодательства и в части изъятия и правомерной фиксации информации в сети Интернет, имеющей значение для уголовного дела, а также в ходе образовательной деятельности.

Теоретическую основу исследования составляют монографические работы, результаты диссертационных исследований, научные статьи и другие публикации, посвященные исследованию электронных доказательств, а также производству следственных действий, направленных на получение сведений в сети Интернет.

Нормативную основу исследования составили положения Конституции Российской Федерации[1], Уголовно-процессуального кодекса Российской Федерации[2], иных федеральные законов и подзаконных актов, постановления Пленума Верховного Суда Российской Федерации, решения Конституционного Суда Российской Федерации, а также иные нормативно-правовые акты, регламентирующие получение информации, содержащейся в сети Интернет.

Эмпирическую основу исследования составили:

- материалы следственной и судебной практики;

- результаты анкетирования 25 следователей;

- результаты интервьюирования сотрудников следственных органов, а также ЭКЦ ГУ МВД России по Красноярскому краю.

Методологическую основу исследования составили общенаучные (анализ, синтез, индукция, дедукция, аналогия и др.) и частно-научные (проблемный, системно-структурный и др.). В качестве основного метода использовался диалектический метод познания. В качестве специальных методов научного познания применялись: историко-правовой, социологический и технико-юридический методы, методы сравнительного правоведения и обобщения следственной и судебной практики, другие методы, позволившие выявить пробелы в законодательной регламентации и практические трудности, возникающие при производстве следственных действий, направленных на получение информации в сети Интернет.

Структура исследования определена целями, задачами и логикой исследования. Выпускная квалификационная работа состоит из введения, двух глав, включающих в себя 4 параграфа, заключения и библиографического списка.

---

[1] Конституция РФ (принята 12 декабря 1993 г. всенародным голосованием, с изм., внесенными Законом РФ о поправках к Конституции РФ от 14 марта 2020 г. № 1-ФКЗ, одобренными в ходе общероссийского голосования 1 июля 2020 г.) // Российская газета.

[2] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 30.12.2021) // Российская газета. 2001. 22 декабря.

ГЛАВА 1. ОБЩАЯ ХАРАКТЕРИСТИКА СВЕДЕНИЙ В СЕТИ ИНТЕРНЕТ И ИХ ПРОЦЕССУАЛЬНАЯ ФИКСАЦИЯ

1.1. Сведения, содержащиеся в сети Интернет и представляющие доказательственное значение.

Доказывание, само по себе являясь подтверждением какого-либо положения, выступает одной из важнейших составляющих уголовно-процессуальной деятельности, предполагающей возможность изъятия (получения, использования) любых сведений, в любых формах, представленных в ст. 74 Уголовно-процессуального кодекса Российской Федерации (далее - УПК РФ). Так, С.В. Зуев, делит указанные сведения на несколько форм:

1) устная (вербальная) форма, к которой относятся показания участников уголовного судопроизводства;

2) письменная (бумажная) форма, к которой относятся протоколы следственных и судебных действий, заключения эксперта и специалиста, иные документы;

3) предметная (объектная) форма, к которой относятся вещественные доказательства.[1]

Однако в период активного развития информационных технологий на протяжении последних 10-15 лет к ранее существовавшему списку добавляется еще одна разновидность сведений - электронные (цифровые), те, которые содержатся в сети Интернет. Данную точку зрения также подтверждает и Я.П. Велиев, который отмечает, что сведения, оставляемые в информационно-телекоммуникационной сети Интернет, способные отображать деятельность лица, подготавливающего или совершившего

[1] Зуев С.В. Электронные доказательства в уголовном судопроизводстве: понятие и значение / С.В. Зуев // Правопорядок: история, теория, практика. 2020. № 3(26). С. 49.

противоправное деяние, являются электронными следами.[1] Ведь как безошибочно отмечает А.Н. Колычева, что сеть Интернет в последнее десятилетие стала важной составной частью нашей повседневной жизнедеятельности, в частности, как источник пополнения информации,как возможность общения со знакомыми или незнакомыми людьми, находящимися на различном удалении другот друга, как инструмент финансовых операций и многое другое.[2]

Ни ст. 74 УПК РФ («Доказательства»), ни ст. 5 УПК РФ («Основные понятия, используемые в настоящем Кодексе») ни другие положения Кодекса не содержат данных об электронных доказательствах, а лишь об электронных носителях информации, как о материальных носителях, которые используются для записи, хранения и воспроизведения информации, в том числе и компьютерной. К таковым можно отнести: флэш-накопители (от англ. Flash– «быстрый, мгновенный»), HD-DVDдиски, жесткие диски и др.

Следует отметить, что мы отделяем компьютерную информацию[3] - сведения, хранящиеся в электронно-цифровой форме, которые находятся в персональных компьютерах, смартфонах и периферийных устройствах от информации, содержащейся в сети Интернет, которая и выступает предметом нашего исследования. Согласно Федеральному закону от 27.07.2006 «Об информации, информационных технологиях и о защите информации»сеть Интернет относится к информационно-коммуникационным сетям, под которыми понимается технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с

[1]Велиев Я.П. Некоторые проблемы, связанные с получением и представлением оперативно значимой информации, содержащейся в электронных документах / Я.П. Велиев // Известия Тульского государственного университета. Экономические и юридические науки. 2022. № 3. С. 55.

[2] Колычева А.Н. Некоторые аспекты фиксации доказательственной информации, хранящейся на ресурсах сети Интернет / А.Н. Колычева // Вестник Удмуртского университета. Серия Экономика и право. 2017. Т. 27. № 2. С. 113.

[3] Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

использованием средств вычислительной техники. Указанные сведения, конечно же, является разновидностью компьютерной информации[1], однако местом хранения такой информации являются не электронно-вычислительные машины (далее – ЭВМ) или машинные носители, а удаленные серверы сети Интернет.

Соответственно сама по себе информация в сети Интернет тоже может быть представлена в различных видах: веб-страницы, веб-сайты, видео- и аудиофайлы, фотографии, текстовые файлы, включая интернет-переписку, а также данные, содержащиеся в различного рода архивных хранилищах (iCloude, GoogleDrive, OneDrive, Dropbox, Mega, Яндекс.Дискит.д.).

Конечно, каждый из них может представлять доказательственное значение. Вместе с тем существует классификация, выделенная А.А. Жижилевой, согласно которой сведения делятся на пассивные и активные. Активные – сознательная деятельность субъекта в информационно-телекоммуникационном пространстве (переписка, ведение блогов, комментарии). Пассивные – совокупность данных, оставленных пользователем непреднамеренно (история посещения сайтов, IP-адрес и т.д.).[2] Тем не менее, все эти сведения, как в совокупности, так и в отдельности могут иметь значение для расследования уголовного дела.

В ходе исследования нами было изучено 35 приговоров, в которых в качестве доказательств фигурировали сведения, размещенные в сети Интернет. В результате можно отметить, что в 17 случаях это были веб-страницы с открытым доступом, в 10 случаях – это данные об интернет-переписке пользователя, включая материалы из социальных сетей и мессенджеров, таких как ВКонтакте, Whatsapp, Telegram и др., фотоснимки

[1]Кульмухамбетова Н.А. Особенности фиксации информации при расследовании преступлений экстремистской направленности в глобальной сети Интернет / Н.А. Кульмухамбетова // Новый юридический вестник. 2019. № 1(8). С. 59.

[2]Жижилева А.А. О некоторых теоретических аспектах использования в криминалистике понятий цифровые, электронные, виртуальные следы / А.А. Жижилева// Вопросы российской юстиции. 2019. № 3. С. 917.

из социальных сетей, в 5 случаях – это облачные хранилища, в 3 случаях – аудиофайлы и фотографии.

Таким образом, к наиболее распространённым видам информации в сети Интернет, можно отнести сведения, содержащиеся на веб-сайтах и веб-страницах. Однако мы считаем, что учитывать только количественный показатель не совсем верно, ведь указанные данные свидетельствует лишь о распространённости такого вида сведений, но в то же время, например, интернет-переписка может иметь большее значение для расследования уголовного дела, так как может содержать информацию, свидетельствующую о направленности умысла лица, либо информацию о местах хранения других доказательств.

Так, например, в приговоре Ленинского районного суда г. Смоленска от 07.07.2015 г. по делу № 1-150/2015[1] в качестве доказательства был признан протокол осмотра документа, а именно осмотр интернет-переписки. В ходе осмотра была установлена объективная сторона преступления (время, место совершения преступления), а также и субъективная сторона. Таким образом, исследование интернет-переписки может помочь установить и преступные связи лица, и данные о предмете преступления, а также многое другое, поэтому ее установление часто имеет большее значение для расследования уголовного дела.

Возникает вопрос, к какому виду доказательств, представленных ст. 74 УПК РФ относятся сведения из сети Интернет?

На сегодняшний день, в правоприменительной практике нет четкой позиции по этому поводу. Так, одни авторы настаивают на введение электронного доказательства, как самостоятельного. Другие, напротив, считают придание самостоятельности нецелесообразным и относят

[1]Приговор Ленинского районного суда г. Смоленска (Смоленская область) от 07 июля 2015 г. № 1-150/2015 по делу № 1-150/2015 [Электронный ресурс] – URL: https://sudact.ru/regular/doc/2zu84yTkqomN/?regular-txt=осмотр+интернет-переписки&regular-case_doc=&regular-lawchunkinfo=&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=&regular-court=&regular-judge=&_=1685249740613&snippet_pos=13018#snippet (датаобращения: 02.04.2023).

сведенияиз сети Интернет, к иным документам, либо же к вещественным доказательствам, тем самым встраивая их в уже существующие «рамки» в уголовно-процессуальном законодательстве.

Разумность выделения отдельного источника доказательствВ.Ю. Стельмах подтверждает тем, что компьютерная информация ограничена виртуальностью и не имеет ни материальных признаков следа, ни идеальных[1], которые присущи уже существующим видам.Как мы указывали ранее, такие следы принято называть электронно-цифровыми.Н.А. Зигура отмечает, что документ и вещественное доказательство доступны непосредственному восприятию органами чувств человека, тогда как цифровая информация для восприятия человеком должна быть соответствующим образом интерпретирована специальным устройством.[2] Именно поэтому некоторые авторы считают целесообразным введение в действующее законодательство ряда изменений и дополнений, касающихся«электронных доказательств». Тем самым, придание самостоятельности сведениям, содержащимся в сети Интернет, исключит ряд проблемных вопросов, касающихся их получения и изъятия.

Если исходить из имеющегося перечня доказательств, то для отнесения сведений из сети Интернет к вещественным доказательствам, для начала необходимо вспомнить, что законодателем выделен ряд оснований, в соответствии с которыми сведения признаются вещественными доказательствами.

Часть 1 ст. 81 УК РФ к таким основаниям относит предметы:

[1] Стельмах В.Ю. Электронная информация в доказывании по уголовным делам: способы получения и место в системе доказательств / В.Ю. Стельмах. - (Дискуссионная трибуна) // Библиотека криминалиста. 2018. № 3 (38). С. 76.

[2]Зигура Н.А. Компьютерная информация как вид доказательств в уголовном процессе России : специальность 12.00.09 "Уголовный процесс" : диссертация на соискание ученой степени кандидата юридических наук / Зигура Надежда Анатольевна. Челябинск, 2010. С. 137.

1) которые служили орудиями, оборудованием или иными средствами совершения преступления или сохранили на себе следы преступления;

2) на которые направлены преступные действия;

3) деньги, ценности и иное имущество, полученные в результате совершения преступления;

4) иные предметы и документы, которые могут служить средствами для обнаружения преступления и установления обстоятельств уголовного дела.

Но ведь и сведения, хранящиеся в сети Интернет, также могут выступать орудием преступления, либо предметом, на который направлены преступные действия, так Л.В. Головко отмечает, что к вещественным доказательствам следует относить не только ножи и пистолеты, но и компьютерную информацию, в том числе и из сети Интернет.[1]Однако, как справедливо отмечает В.А. Лазарева: «вещественное доказательство – это вещь».[2]Действительно, вещественное доказательство, как объект материального мира должно обладать некоторыми физическими свойствами (форма, размер, цвет и т.д.), которыми сведения из сети Интернет обладать не могут.

Дискуссионную позицию занимают также Е.С. Ермакова и Д.М. Джумангалиев, которые приводят в качестве примера приговор Вахитовского районного суда г. Казани от 06 мая 2014 года.[3] Указанным решением осужден гражданин Б., который вел переписку в социальной сети о сбыте сильнодействующих препаратов. Доказательством по данному делу выступала скриншот-страница социальной сети, в которой велась переписка.

---

[1]Головко Л.В. Курс уголовного процесса / Под ред. д.ю.н., проф. Л.В. Головко. - 2-е изд., испр. М.: Статут, 2017. С. 445.

[2]Лазарева В.А. Доказывание в уголовном процессе : Учебник / В.А. Лазарева. – 6-е изд., пер. и доп. – Москва : Издательство Юрайт, 2018.С. 141.

[3] Ермакова Е.С. Электронные доказательства как новое направление в практике расследования преступлений / Е.С. Ермакова, Д.М. Джумангалиева // Молодой ученый. 2018. № 23 (209). С. 85.

В результате скриншот был признан вещественным доказательством. Мы не разделяем данную точку зрения, т.к. согласно ч. 3 ст. 164.1 УПК РФ информация, полученная в ходе следственного действия,будет лишь приложением к протоколу, а признание ее вещественным доказательством категорически невозможно (такой скриншот по существу не будет отличаться от фототаблицы, прилагаемой к протоколу).

Таким образом, к вещественным доказательствам будет относиться лишь материальный носитель, а не сама информация, поэтому сведения из сети Интернет сами по себе вещественными доказательствами не являются.

Отнесение сведений из сети Интернет к иным документам вполне возможно, но в первую очередь нужно определить, что такое электронный документ. Под электронным документом понимается документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.[1]В свою очередь документированная информация – это зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель[2]. Что в данном случае мы понимаем под реквизитами? К реквизитам относятся сведения, позволяющие идентифицировать интернет-страницу, например, установить источник ее происхождения.[3] Общеизвестно, что любая интернет-страница имеет электронный адрес, IP-адрес, которые и выступают в качестве указанных реквизитов. Таким образом, любая интернет-страница может быть отнесена к

[1] Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации"// СПС КонсультантПлюс.

[2] Там же.

[3]Новиков С.С. Электронный документ: понятие и сущность / С.С. Новиков // 2020. № 9-1. С. 154.

электронным документам (в уголовно-процессуальном значении и в целях определения доказательственного значения).

Из положений ст.84 УПК РФ известно, что документы могут содержать сведения, зафиксированные как в письменном, так и ином виде, т.е. в электронном. Подтверждением сказанному может послужить пример из судебной практики, а именно приговор Вахитовского районного суда г. Казани от 06.05.2014 г. по делу № 1-184/2014[1], в рамках которого в качестве доказательства по уголовному делу был признан протокол осмотра электронного документа, содержащий интернет-переписку из социальной сети, свидетельствующую о сбыте сильнодействующих веществ виновным сотруднику УФСКН. Таким образом, отнесение сведений из сети Интернет в качестве иного документа (электронного) считаем вполне допустимым.

По нашему мнению, нет оснований для отнесения сведений из сети Интернет к такому виду доказательств, как заключение эксперта. Само по себе заключение представляет документ, содержащий в себе ход и результаты исследований, проведенных экспертом. Важно отметить, что деятельность эксперта напрямую связана с использованием им специальных знаний, под которыми следует понимать знания не общеизвестные, не общедоступные, не имеющие массового распространения, т.е. знания, которыми располагает ограниченный круг специалистов[2], применяемые для разрешения вопросов, возникающих при расследовании и разрешении уголовных дел.

На сегодняшний день практически вся информация в сети Интернет является общедоступной и для того, чтобы ее получить не требуется обладать специальными знаниями. Еще одной составляющей заключения эксперта является методика экспертного исследования, включающая в себя

---

[1] Приговор Вахитовского районного суда г. Казани (Республика Татарстан) от 06 мая 2014 г. № 1-184/2014 по делу № 1-184/2014 [Электронный ресурс] – URL: https://sudact.ru/regular/doc/WyavwZ7DR958/ (дата обращения: 16.11.2022).

[2]Эйсман А.А. Заключение эксперта. Структура и научное обоснование / Эйсман А.А. Всесоюз. ин-т по изучению причин и разработке мер предупреждения преступности. Москва :Юрид. лит., 1967.С. 89.

рекомендации и обязательные правила, которую он использует при проведении исследования. Однако на сегодняшний день отсутствуют методики для проведения экспертизы в информационно-телекоммуникационной сети Интернет.

Таким образом, мы считаем, что отнесение сведений из сети Интернет к такому виду доказательств, как заключение эксперта невозможно в силу специфики экспертного исследования, а также вследствие недоработки экспертных методик.

Относительно заключения специалиста, как вида доказательств,существует мнение, что в целях осуществления принципа состязательности сторон (ст. 15 УПК РФ), заключение специалиста применяется стороной защиты[1], тогда как заключение эксперта существует для стороны обвинения соответственно.Так и С.А. Шейфер отмечает, что привлечение специалиста является таким способом, который позволит стороне защиты «оспаривать заключение эксперта, представленное стороной обвинения или устанавливать обстоятельства, оправдывающие обвиняемого».[2]То есть фактически, заключение специалиста представлена для стороны защиты, тогда как нас интересует собирание доказательств, выполняемое стороной обвинения. Кроме того специалист при подготовке заключения не исследует предмет с применением различных методик, а всего лишь приводит суждения[3] по уже выявленной информации, которые представляют собой абстрактное мнение, что для применения в нашем случае неуместно, так как нас интересует конкретное исследование информации, которой еще нет, но которую следует установить.

---

[1] Волкова С.В. Рецензия на заключение эксперта как разновидность заключения специалиста в уголовном судопроизводстве / С.В. Волкова, М. В. Бобовкин // Эксперт-криминалист. 2008. № 1. С. 37.

[2]Шейфер С.А. Куда движется российское судопроизводство? (Размышления по поводу векторов развития уголовно-процессуального законодательства) / С.А. Шейфер // Государство и право. 2007. № 1. С. 30.

[3]Рамазанов Т.Б. Заключения и показания эксперта и специалиста как доказательства в уголовном судопроизводстве / Т.Б. Рамазанов // Юридический вестник Дагестанского государственного университета. 2012. № 4. С. 101.

Таким образом, изучив характер и направленность доказательства – заключение специалиста, следует сделать вывод, что его применение для фиксации сведений в сети Интернет является недопустимым.

Для того чтобы исследовать и изымать информацию из сети Интернет имеющую значение для уголовного дела уполномоченные лица проводят следственные действия. Ход и результаты следственных действий фиксируются в свою очередь в письменных актах называемых протоколом следственного действия. Фактически они являются процессуальными документами, как средствами доказывания по уголовному делу.[1]Таким образом, большая часть информации из сети Интернет фиксируется указанным способом, однако бывают случаи и когда такая информация появляется в результате проведения следственного действия, а также путем приобщения иных документов – электронных.

Таким образом, на сегодняшний день в уголовно-процессуальном законодательстве отсутствуют отдельные положения о судьбе электронных доказательств, а также их процессуальное закрепление. Однако уполномоченным лицам приходится адаптироваться к новым реалиям научно-технического прогресса, появления виртуальной информации и относить сведения из сети Интернет к такому виду доказательств, как иные документы или к протоколам следственных действий.

1.2. Характеристика следственных действийкак средств фиксации сведений в сети Интернет.

Собирание доказательств – это элемент процесса доказывания, который характеризуется как деятельность субъектов уголовного процесса по

[1]Шишкин В.С. Особенности протоколов следственных и судебных действий как документального вида доказательств / В.С. Шишкин // Вектор науки Тольяттинского государственного университета. Серия: Юридические науки. 2010. № 3. С. 231.

обнаружению, фиксации и сохранению сведений (информации) о совершенном преступлении.[1]Согласно положениям ст.86 УПК РФ основным способом собирания доказательств являются следственные действия, наряду с иными процессуальными действиями. Следственные действия — это такие способы собирания и проверки доказательств, которые детально регламентированы законом и обеспечены возможностью применения государственного принуждения.[2]Тем временем именно следственные действия являются специализированными действиями, представляющими собой основную деятельность следователя (дознавателя), от которой напрямую зависит результат всего предварительного расследования, поскольку в ходе их производства происходит обнаружение, фиксация, сохранение доказательственной информации, имеющей значение для уголовного дела.[3]Очевидно, что каждое следственное действие имеет различную направленность, а также разные цели.

Таким образом, каждое следственное действие можно охарактеризовать с позиции объекта, на который оно направлено. Данный объект может иметь различные формы, и соответственно для каждой формы сведений (выделенных в предыдущем параграфе) существует самостоятельный набор следственных действий. Так, например, для вербальной формы уполномоченные лица используют допрос, очную ставку, предъявление для опознания.

Аналогично с этим, для фиксации компьютерной информации в сети Интернет также должны быть предусмотрены соответствующие средства. Тем не менее, в современной системе следственных действий мы не встречаем специализированных действий, направленных на получение

[1]Цабан Я.Б. Следственные действия как основной способ собирания доказательств по уголовным делам / Я.Б. Цабан // Символ науки: международный научный журнал. 2015. № 12-2. С. 109.

[2] Смирнов А.В. Уголовный процесс : учебник / А.В. Смирнов, К.Б. Калиновский ; под общ.ред. проф. А.В. Смирнова. — 4-е изд., перераб. и доп. — М. : КНОРУС, 2008. С. 387.

[3]Безлепкин Б.Т. Уголовный процесс в вопросах и ответах [Текст] : учебное пособие / Б.Т. Безлепкин. - Изд. 9-е, перераб. и доп. - Москва : Проспект, 2018. С. 328.

информации, имеющей значение для уголовного дела, в сети Интернет. В таком случае следователю приходится обращаться к перечню, которыйуже существуют в законодательстве.

В рамках выпускной квалификационной работы нами было проведено анкетирование сотрудников следственных органов г. Красноярска и Красноярского края, примерный перечень вопросов для анкетирования содержится в приложении №1. В результате проведенного анкетирования было выявлено, что сведения в сети Интернет чаще всего фиксируются протоколом осмотра предмета или документа, а, как нам уже известно, использование в этих целях протокола осмотра предмета является категорически неверным.

Также было выявлено, что 90% опрошенных не известны случаи фиксирования сведений в сети Интернет в результате проведения проверки показаний на месте. 100% опрошенных не известны случаи осмотра информации в сети Интернет в рамках производства компьютерной экспертизы, что является вполне логичным. Ведь компьютерная экспертиза, проводимая в органах внутренних дел, не допускает выход в сеть Интернет в ходе ее производства (подробнее будет рассмотрено далее в рамках данного параграфа). Результаты анкетирования указаны в приложении № 2.

Таким образом, можно сделать вывод, что на сегодняшний день сотрудники следственных органов в рамах предварительного расследования исследуют доказательства в сети Интернет посредством традиционного следственного действия – осмотр, и практически не прибегают к иным следственным действиям. Вместе с тем, могут возникнуть различные ситуации, например, когда нужно будет установить навык обращения лица с определенными интернет-сведениями, и тогда производство одного лишь осмотра будет недостаточно.

В связи с этим, предлагаем рассмотреть действующую систему следственных действий и указать на возможность фиксации сведений в сети

Интернет, имеющих значение для производства по делу посредством различных следственных действий.

Разумеется, отдельные намеки, касающиеся получения информации из сети Интернет в законодательстве все-таки присутствуют. Так, ч.7 ст.185 УПК РФ содержит положение о том, что следователь по судебному решению может произвести осмотр и выемку сведений, содержащихся в электронных сообщениях или иных передаваемых по сетям электросвязи сообщениях. К электронным сообщениям следует относить информацию, переданную или полученную пользователем информационно-телекоммуникационной сети.[1]

По нашему мнению содержание понятий электронные сообщения и иныесообщения, передаваемые по сетям электросвязи являются идентичными, т.к. согласно ст. 2 Федерального закона от 07 июля 2003 г. 126 «О связи», электросвязь – это любые излучение, передача или прием знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам. То есть фактически можно говорить о том, что такое разделение в статье является излишним. Однако с учетом содержания этого следственного действия, а также его наименования (наложение ареста на почтово-телеграфные отправления, их осмотр и выемка) можно утверждать, что в данной статье, речь идет именно о бандеролях, посылках или других почтово-телеграфных отправлениях, телеграммах или радиограммах, а не о компьютерной информации. Разграничить указанные сведения позволяет и ст. 105.1 УПК РФ («Запрет определенных действий»), в которой законодателем разграничены запреты на отправление и получение почтово-телеграфных отправлений и на использование средств связи и информационно-телекоммуникационной сети «Интернет».[2] Из этого можно сделать вывод, что электронные сообщения не

[1] Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" // СПС КонсультантПлюс.

[2]Никитина Е.В. Проблемы законодательного регулирования следственного действия, направленного на получение доступа к электронным сообщениям /

являются телеграфными отправлениями и не подпадают под объект, указанный в ст. 185 УПК РФ.

Также, с учетом наименования можно сделать вывод, что данное следственное действие имеет непростую структуру, а именно:

1) наложение ареста на почтово-телеграфные отправления;
2) осмотр почтово-телеграфных отправлений;
3) выемкапочтово-телеграфных отправлений.

Тем не менее, в ч. 7 ст. 185 УПК РФ не упоминается о наложении ареста, а лишь об осмотре и выемке, как о двух самостоятельных следственных действия, что, по мнению Е.В. Никитиной и В.С. Раменской является упущением законодателя.[1]

В дополнение к этомуА.Л. Карлов справедливо отмечает: «данное следственное действие подразумевает «задержание» отправления до получения адресатом, тогда как в большинстве случаев следствие интересуетуже полученная адресатом интернет-переписка за предшествующий период».[2]Таким образом, содержание ч.7 ст. 185 УПК РФ не соотносится с характером указанного следственного действия. Но и на этом проблемы не заканчиваются. Исследуя указанную норму можно заметить, что лицо на почтово-телеграфные отправления, которого накладывается арест должно обладать следующими признаками: фамилия, имя, отчество, адрес. В случае наложения ареста на электронные сообщения данное лицо может ввести «вымышленные» фамилию и (или) имя. С.В. Супрун и В.С. Черкасов в своей работе оценивают данное положение как недоработку законодателя и предлагают дополнить статью персональными

Е.В. Никитина, В.С. Раменская // Российское право: образование, практика, наука. 2022. № 2. С. 26.

[1]Там же. С. 27.

[2] Карлов А.Л. К проблеме определения следственного действия для процессуальной фиксации интернет-переписки / А.Л. Карлов // Научно-практический электронный журнал Аллея науки. 2018. Т. 2. № 8(24). С. 558.

признаками субъекта для сети Интернет, такими как IP-адрес, доменное имя и т.п.[1]

В конечном итоге, исследовав содержание и характер указанного следственного действия можно сделать вывод о том, что,несмотря на терминологическую схожесть, в части упоминания в ч. 7 «электронных сообщений», указанное следственное действие нельзя считать подходящим дляфиксации сведений в сети Интернет.

Других положений уголовно-процессуального законодательства конкретно направленных на получение информации в сети законом не предусмотрено. Поэтому должностные лица вынуждены приспосабливаться к тем условиям, которые уже созданы законодателем.

Как мы указывали ранее, выбор следственного действия зависит от вида информации, содержащейся в сети. Осмотр, как одно из самых распространённых следственных действий также применим для фиксации информации в сети Интернет, однако,во-первых, следует определиться с объектом такого осмотра, а во-вторых, законом предусмотрены различные виды осмотра.

С учетом объекта осмотра закон выделяет следующие его виды: осмотр места происшествия; осмотр участков местности и помещений, не являющихся местом происшествия; осмотр жилища; осмотр предметов; осмотр документов; осмотр трупа (ст. 178 УПК РФ); освидетельствование (особый вид следственного осмотра). Несмотря на широкую классификацию видов осмотра, в полной мере подходящего вида для осмотра сведений в сети Интернет на сегодняшний день нет, поскольку информация, содержащаяся в информационно-телекоммуникационной сети,не подпадает под указанные объекты.В данном случае будет использоваться особый (нетрадиционный) вид объекта – сведения независимо от формы их представления, к которым

[1] Супрун С.В. О противоречивом характере новеллы в законодательном регулировании следственного действия "наложение ареста на почтово-телеграфные отправления" / С.В. Супрун, В.С. Черкасов // Вестник Омской юридической академии. 2017. Т. 14, № 1. С. 62.

может относиться электронный файл, веб-страница, интернет-переписка, аудио- и видеофайлы, доступ к которым осуществляется непосредственно через сеть Интернет.

Достаточно распространены случаи, когда следователи подменяют объект осмотра. Так, например, по уголовному делу № 1-25/2020 в качестве доказательства признан протокол осмотра предмета (компьютера), в ходе которого осматривалась веб-страница «Farpost.ru».[1] Мы не согласны с данной позицией правоприминителя, т.к. объектом осмотра является не техническое средство с его свойствами, а веб-страница, которую отнести к предметам нельзя.

Возникает вопрос, каким образом следовало поступить должностному лицу? С учетом того, что на данный момент под документами понимается не только материалы в традиционном (бумажном) виде, но и электронные документы,в качестве наиболее приемлемого варианта мы предлагаем использовать осмотр электронного документа (о свойствах электронного документа мы писали подробнее в предыдущей главе). Именно поэтому для получения информации в сети Интернет, целесообразно применять такой вид осмотра, как осмотр документов. В данном случае возможно привлечение к проведению данного вида осмотра специалиста, обладающего знаниями в сфере интернет-технологий.

Проверка показаний на месте как следственное действие, направленное на фиксацию сведений в сети Интернет также заслуживает внимания в рассматриваемом контексте. Данное следственное действие состоит в уточнении и проверке ранее данных показаний, а также установлении новых обстоятельств по делу.[2]Если рассмотретьнаименование следственного действия (проверка показаний на месте), следует в первую

[1] Приговор Первореченского районного суда г. Владивостока от 12 мая 2020 г № 1-25/2020 по делу № 1-25/2020 [Электронный ресурс] — URL: https://sudact.ru/regular/doc/86EXthrJn2oJ/ (дата обращения: 12.12.2022).

[2] Болотов М.В. Некоторые особенности проведения проверки показаний на месте / М.В. Болотов // Синергия Наук. 2018. № 25. С. 628.

очередьопределить, что необходимо понимать под местом проверки. Согласно теории уголовного процесса таким местом может выступатькак место совершения преступления, так и место, где произошло какое-либо событие, имеющее значение для уголовного дела[1], например, место обнаружения доказательств. Таким образом,привязка данного следственного действия к месту совершения преступления не обязательна.Полагаем, что в современных реалиях местом совершения преступления может выступать виртуальное пространство, если в нем содержатся сведения, имеющие значение для уголовного дела. Например, подозреваемым будет продемонстрировано место нахождения интернет-переписки либо местонахождение какого-либо веб-сайта, с помощью которого осуществлялось преступление.

В качестве альтернативного варианта можно предложить осмотр с участием лица, однако эти следственные действия нельзя смешивать, ввиду наличия существенных особенностей, которые будут подробно описаны в следующей главе.

Далее обратимся к судебной экспертизе, как следственному действию.По нашему мнению требует заслуженного внимания предложение Ю.В. Шелегова и В.Г. Шелегова, о том, что скопированная информации может иметь следы фальсификации или же быть изменена, для этого авторы предлагают предусмотреть обязательный порядок производства экспертизы электронных доказательств.[2]

---

[1] Мельникова А.С. Проверка показаний на месте: значение, особенности, пробелы законодательства / А.С. Мельникова, Е.Е. Колбасина // Юристъ-Правоведъ. 2020. № 4(95). С. 91.

[2]Шелегов Ю.В. К вопросу о проблеме использования доказательственной информации из цифровых источников в уголовно-процессуальном доказывании / Ю.В. Шелегов, В.Г. Шелегов // Деятельность правоохранительных органов в современных условиях : сборник материалов XXIV международной научно-практической конференции, Иркутск, 06–07 июня 2019 года / Восточно-Сибирский институт МВД России. – Иркутск: Восточно-Сибирский институт Министерства внутренних дел Российской Федерации, 2019. С. 183.

Экспертиза представляет собой особое исследование, которое проводится лицом, обладающим специальными знаниями в определённой области.В данном случае специальные знания будут направлены на обращение с компьютерной информацией. В системе Министерства внутренних дел Российской Федерации (далее – МВД РФ) в соответствии с приказом МВД России от 29.06.2005 N 511 (ред. от 30.05.2022) «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации» проводитсяэкспертиза исследования компьютерной информации (компьютерная экспертиза). Возникает вопрос: «Могут ли выступать в качестве объекта исследования сведения, содержащиеся в сети Интернет?».

В рамках проведения интервьюирования двух сотрудников экспертно-криминалистического центра ГУ МВД России по Красноярскому краю было установлено, то методики производства компьютерных экспертиз не допускают выход в сеть Интернет, то есть при их проведении представляется возможным исследовать только сведения,содержащиеся в памяти представленного устройства. То есть экспертиза будет проводиться при отключенном от сети Интернет устройстве. Помимо этого при помощи экспертов нами был определен примерный перечень вопросов для производства указанной экспертизы (приложение № 3).

Однако в теории криминалистики, как и в практике можно встретить такой вид компьютерной экспертизы, как компьютерно-сетевая. Данная экспертиза является одним из родов судебной компьютерно-технической экспертизы (далее – СКТЭ), выделенных Е.Р. Россинской.[1]Компьютерно-сетевая экспертиза в своей основе базируется на сетевой информационной технологии и применяется для исследования информационных следов в сети

[1]Россинская Е.Р. Настольная книга судьи. Судебная экспертиза : теория и практика, типичные вопросы и нестандартные ситуации : судебно-экспертные учреждения, назначение экспертизы в суде, типичные экспертные ошибки, заключение эксперта, порядок проведения экспертиз / Е.Р. Россинская, Е.И. Галяшина ; Е.Р. Россинская, Е.И. Галяшина ; Московская гос. юридическая акад. им. О.Е. Кутафина, Ин-т судебных экспертиз. Москва :Проспект, 2012. С. 354.

в том случае, когда отсутствует возможность получения доступа к техническому средству правонарушителя. При подготовке выпускной квалификационной работы удалось обнаружить приговор по уголовному делу[1], в рамках которого была назначена компьютерно-сетевая экспертиза. В ходе экспертизы исследовался интернет-сайт, представляющий собой интернет-магазин по продаже наркотических средств и психотропных веществ на территории Российской Федерации, со всеми его разделами и ссылками, а также с подробным описанием каждого раздела.Исходя из описания в приговоре для фиксации содержания интернет-страницы вполне мог быть проведен её осмотр, однако допускаем, что в заключении эксперт дополнительно сделал выводы о назначении и технических возможностях исследуемого интернет-сайта. Тем не менее, в зависимости от вида совершенного преступления, Е.Р. Россинская предлагает использовать в комплексе все разновидности экспертиз (аппаратно-компьютерная, программно-компьютерная, информационно-компьютерная, компьютерно-сетевая) и назначать в конечном итоге компьютерно-техническую экспертизу.[2]

В соответствии с приказом Минюста России от 27.12.2012 № 237 (ред. от 13.09.2018) «Об утверждении перечня родов (видов) судебныхэкспертиз, выполняемых в федеральных бюджетных судебно-экспертных учрежденияхМинюста России, и Перечня экспертных специальностей, по которым представляетсяправо самостоятельного производства судебных экспертиз в федеральных бюджетныхсудебно-экспертных учреждениях Минюста России»СКТЭ проводятся государственными судебно-экспертными учреждениями Минюста России, а также частными экспертами или сотрудниками негосударственных судебно-экспертных организаций. Таким образом, назначение указанного вида экспертизы для сотрудников ОВД РФ

[1] Приговор Краснодарского краевого суда от 23 июля 2019 г. № 2-28/2019 по делу № 2-28/2019 [Электронный ресурс] — URL: https://sudact.ru/regular/doc/PDXLfJbOWeLu/ (дата обращения: 12.12.2022).

[2]Россинская Е.Р. Указ.соч. С. 121.

является весьма проблематичным, так как сотрудники негосударственных судебно-экспертных организаций зачастую не имеют специального образования, однако позиционируют себя в качестве специалистов в области компьютерно-технической экспертизы.[1] В результате чего проведение такого вида экспертизы негосударственными экспертными организациями влечет за собой множество экспертных ошибок.

Таким образом, широкого распространения факты проведения судебных экспертиз в сети Интернет не получили, вместе с тем, полагаем, что практика в этой части должна измениться в ближайшее время, учитывая, что решение данной проблемы лежит в плоскости организационного и (или) ведомственного регулирования.

Далее перейдем к обыску. Как было отмечено ранее, обыск предусматривает наличие поисковых действий.[2]Проведение обыска возможно в помещении, в котором находится компьютерная система с выходом в локальную сеть Интернет. Для этого следователь должен обладать информацией о том, что при помощи компьютера подозреваемого можно получить имеющую значение для дела информацию, расположенную на удаленном сервере. Однако А.Н. Иванов[3] в своей работе указывает о возможности проведения указанного следственного действия и в кабинете следователя (поиск и копирование информации в сети Интернет). В данном случае лицу в соответствии с положениями ст. 182 УПК РФ разъясняются права и обязанности, а также порядок производства обыска, тем не менее, за компьютер лицо никто не пускает, ему лишь предлагается назвать, например

[1]Россинская Е.Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации / Е.Р. Россинская // Вестник Университета имени О.Е. Кутафина (МГЮА). 2019. № 5(57). С. 39.

[2]Журба Л.К вопросу повышения эффективности поисковых действий при производстве обыска / О.Л. Журба, С.А. Торопов // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2018. Т. 4 (70), № 3. С. 131.

[3] Иванов А.Н. Удалённое исследование компьютерной информации: уголовно - процессуальные и криминалистические проблемы / А.Н. Иванов // Известия Саратовского университета. Новая серия. Серия: Экономика. Управление. Право. 2009. Т. 9, № 2. С. 75.

пароль, IP-адрес, название веб-сайта и т.п. Как мы уже упоминали, при обыске проводятся поисковые действия. Мы полагаем, что в приведенном случае необходимо проводить осмотр, так как обыск предполагает изъятие чего-либо овеществленного (предметы, документы), тогда как осмотр Интернета не позволяет ничего изъять, здесь мы, как и в классическом осмотре обнаруживаем информацию и фиксируем её протоколе (либо при помощи копирования).

В том случае, если для исследования какой-либо информации в сети требуется преодоление защиты (пароля), Ю.А. Телевицкая предлагает применять по аналогии ч. 6 ст. 182 УПК РФ[1], позволяющую вскрывать помещения, если владелец отказывается добровольно их вскрыть, однако далеко не все средства защиты телефонов и других устройств мы можем преодолеть. В таких случаях осмотр памяти телефона и ресурсов сети Интернет невозможен.

Таким образом, можно сделать вывод о том, что ресурсы сети Интернет могут быть зафиксированы в ходе обыска только при условии, что устройство находится в обыскиваемом помещении. А в том случае, если нет необходимости обыскивать помещение, для производства отдельного следственного действия направленного на изъятие информации в сети Интернет должен применяться осмотр.

Заметим, что информация в сети Интернет также может быть получена путем производства выемки предметов и документов, в том числе содержащих охраняемую федеральным законом тайну. Тем не менее, ввиду ряда причин производство указанного следственного действия является весьма затруднительным. Трудность заключается в том, что информация может быть изъята только в компании поставщика услуг (оператора связи)[2], а

[1]Телевицкая Ю.А. Выемка, осмотр и обыск в электронных сетях: понятие и разграничение / Ю.А. Телевицкая // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2022. № 4(60). С. 240.

[2] В соответствии с ч. 2 ст. 63 Федерального закона от 07.07.2003 № 126-ФЗ «О связи» - обязанность по соблюдению тайны связи возлагается на операторов связи.

такие компании не всегда могут располагаться территориально в месте производства предварительного расследования. Поэтому данный способ хоть и затруднителен, но все же имеет место. Однако в этом случае мы имеем опосредованное взаимодействие с сетью Интернет, в связи, с чем такие случаи не подпадают под предмет нашего исследования.Так и уже упоминаемая нами ч. 7 ст. 185 УПК РФ, предполагающая производство выемки электронных сообщений, но фактически в указанном случае мы можем изъять только носитель информации, но не сам файл.

Можно сделать вывод, что выемка предполагает изъятие чего-то предметного из места, в котором ранее оно находилось. То есть последующее местонахождение предмета (документа) должно поменяться, тогда, как при изъятии виртуальной информации все сведения в сети Интернет останутся на своем прежнем месте, ведь удаление информации из сети Интернет в частном порядке, практически невозможно. Таким образом, исследовав характерные черты данного следственного действия, приходим к выводу, что в данном случае также целесообразно проведение осмотра.

Не менее распространены случаи применения следственного эксперимента, в ходе производства которого фиксируются сведения, расположенные на удаленных серверах. Следственный эксперимент проводится в целях проверки и уточнения данных, имеющих значение для уголовного дела (ст. 181 УПК РФ), а в нашем случае реальности наступления последствий в виде совершения преступления в результате каких-либо предшествующих этому действий. Так, С.И. Земцова, О.А. Суров, П.В. Галушин отмечают в качестве цели подробную проверку навыков и преступную осведомленность лица, например – необходимость установить владеет ли он навыками работы с компьютерными программами и пользования сетью Интернет.[1]Кроме того, с использованием сети Интернет

[1]Земцова С.И. Методика расследования незаконного сбыта синтетических наркотических средств, совершенного с использованием интернет-магазинов / С.И. Земцова, О.А. Суров, П.В. Галушин. – Красноярск : Сибирский юридический институт Министерства внутренних дел Российской Федерации, 2019. С. 134.

возможно установить наличие или отсутствие у подозреваемого (обвиняемого) определенных навыков оператора (преступления связанные с незаконным оборотом наркотиков), осуществлять покупку и продажу цифровой валюты, использовать VPN, скачивать необходимые программные продукты.[1]Так, в качестве примера приведем приговор от 28 сентября 2020 г.по делу№ 1-86/2020, в ходе предварительного расследования которого был проведен следственный эксперимент с участием подозреваемого Д.[2] В рамках следственного действия подозреваемый Д. добровольно показал последовательность действий в сети Интернет,а также последующего выводы денежных средств. Таким образом, можно отметить, что в целях уточнения владеет ли лицо определёнными навыками в сети Интернет или нет возможно проведение следственного эксперимента.

На практике встречаются случаи в ходе проведения следственного эксперимента интернет-переписки, однако мы считаем такой подход неверным и рассмотрим его подробнее в следующей главе.

Подводя итог, отметим, что проведение следственного эксперимента в сети Интернет возможно только в целях уточнения умений и навыков лица пользоваться Интернет-ресурсами, а также выполнения лицом определённых действий, которые позволят установить механизм совершенного преступления. В иных же целях проведение следственного эксперимента не допускается с учетом характера и целей следственного действия.

Кроме того можно выделить комплекс оперативно-розыскных мероприятий, которые в своем арсенале, в отличие от следственных действий имеют специализированные мероприятия, направленные на получение информации в сети Интернет. Основным мероприятием, осуществляемым в

[1]Земцова С.И. Развитие научных идей профессора Р.С. Белкина о значении следственного эксперимента в условиях современных нарковызовов с использованием интернет-технологий / С.И. Земцова // Вестник Сибирского юридического института МВД России. 2022. № 2(47). С. 96.

[2] Приговор Пензенского районного суда (Пензенская область) № 1-86/2020 от 28 сентября 2020 г. по делу № 1-86/2020 // URL: https://sudact.ru/regular/doc/4PItzykNNxmu/?regular–txt (дата обращения: 23.01.2023).

сети Интернет оперативными подразделениями, является снятие информации с технических каналов связи, которое состоит в перехвате с помощью специальных технических средств информации, передаваемой проверяемыми лицами по техническим каналам связи. Под техническими каналами связи понимают факсимальные каналы, каналы космической связи, каналы сотовой связи, глобальную сеть Интернет.[1]

Также нельзя не забывать об оперативно-розыскном мероприятии - получение компьютерной информации, которое направлено на поиск и извлечение информации, находящейся в компьютерной системе в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Нами уже было отмечено, что для разного рода цифровых сведений используется свое следственное действие. Так и в ходе выполнения оперативно-розыскных мероприятий законодатель предлагает разделять компьютерную информацию. Например, проектом федерального закона от 6 апреля 2021 года «О внесении изменения в статью 6 Федерального закона «Об оперативно-розыскной деятельности» разработанным по инициативе МВД России, предлагается ввести новое оперативно-розыскное мероприятие – «Исследование компьютерной информации».[2]Необходимость указанного нововведения определяется использованием удаленных рабочих столов, расположенных на серверах за пределами Российской Федерации или на облачных хранилищах.Однако, данное исследование возможно в рамках уже существующих оперативно-розыскных мероприятий. По нашему мнению, данное нововведение может повлечь нарушения прав граждан на

[1]Шогенов Т.К. Вопросы технического обеспечения проведения оперативно-розыскного мероприятия «Снятие информации с технических каналов связи»/ Т.К. Шогенгов// Спецтехника и связь. 2013. №6. С. 28. URL: https://cyberleninka.ru/article/n/voprosy-tehnicheskogo-obespecheniya-provedeniya-operativno-rozysknogo-meropriyatiya-snyatie-informatsii-s-tehnicheskih-kanalov (дата обращения: 26.11.2022).

[2] МВД России предлагает дополнить перечень оперативно-розыскных мероприятий «исследованием компьютерной информации». Официальный сайт Министерства внутренних дел Российской Федерации [Электронный ресурс]. Режим доступа: https://xn--b1aew.xn--p1ai/news/item/24427014 (дата обращения: 21.01.20223).

тайну связи[1] со стороны правоохранительных органов. На самом деле деятельность оперативных сотрудников во многом имеет большую правовую регламентацию получения информации в сети, нежели чем следственная деятельность.

Рассмотрев существующую систему следственных действий, мы сделали вывод, что она далеко не совершенна. Выделение новых следственных действий направленных на исследование информации в сети Интернет необходимо в связи с тем, что такая информация обладает своими индивидуальными свойствами, режимом ее хранения и способами доступа к ней.

В соответствии с указанной проблемой ряд авторов предлагает добавить в систему следственных действий специализированные, которые направлены на получение информации в сети Интернет. Данное нововведение позволит получать информацию в сети, имеющую доказательственное значение по уголовному делу, без ограничения прав участников уголовного судопроизводства, а также с использованием четкой правовой регламентации. А.С. Александрова выдвигает категоричный вывод о том, что действующая система следственных действия полностью непригодна для расследования преступлений в сети Интернет.[2] В таком случае автор предлагает создать одно универсальное следственное действие, которое охватит всю информацию в сети Интернет, имеющую значение для уголовного дела.

Одним из таких нововведений является дополнение системы следственных действий «осмотром сетевых информационных ресурсов»,

[1] В соответствии с ч.1 ст.63 ФЗ от 07.07.2003 № 126-ФЗ «О связи» к тайне связи относятся – тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи.

[2] Александров А.С. Учение о следственных действиях на пороге "цифрового мира" / А.С. Александров // Юридический вестник Самарского университета. 2017. Т. 3, № 4. С. 84.

предложенное А. Н. Першиным.[1] Автор отмечает, что традиционные виды осмотра предусматривают лишь реальное место, а информационные ресурсы содержатся в виртуальном пространстве, без содержания четких границ осматриваемого места либо предмета. Также он указывает на основание производства указанного следственного действия, которым является наличие сведений (фактических данных) о том, что на удаленном сетевом ресурсе размещена информация, имеющая значение для раскрытия, расследования и предупреждения преступления, либо информация, распространение которой в Российской Федерации запрещено. В свою очередь Н.А. Зигура рекомендует выделить еще один вид осмотра – «Осмотр электронного объекта», а также самостоятельное следственное действие – «Контроль электронных отправлений и их копирование».[2]

Нами была рассмотрена ч. 7 ст. 185 УПК РФ, предусматривающая возможность осмотра и выемки электронных сообщений или иных передаваемых по сетям электросвязи сообщений. Однако в ходе подробного исследования мы выявили, что указанное следственное действие не подходит для исследования сведений в сети Интернет. Тем не менее, Е.В. Никитина и В.С. Раменская предлагают внести в уголовно-процессуальное законодательство новое следственное действие, предусмотренное ст. 186.2 УПК РФ «Получение информации об электронных сообщениях, их копирование и осмотр»[3], которое позволит устранить пробелы ст. 186 УПК РФ, а также безошибочно проводить исследование электронных сообщений, в которых может содержаться информация имеющая значение для расследования уголовного дела. Данное следственное действие авторы

[1]Першин А.Н. Осмотр сетевых информационных ресурсов - новый вид следственного действия? / А.Н. Першин // Российский следователь. 2020.№ 1. С. 16.

[2]Зигура Н.А. Компьютерная информация как вид доказательств в уголовном процессе России [Текст] : монография / Н.А. Зигура, А.В. Кудрявцева. - Москва :Юрлитинформ. 2011. С. 166.

[3] Никитина Е.В. Проблемы законодательного регулирования следственного действия, направленного на получение доступа к электронным сообщениям / Е.В. Никитина, В.С. Раменская // Российское право: образование, практика, наука. 2022. № 2. С. 34

предлагают проводить на основании судебного решения через оператора связи. Также авторы устанавливают срок следственного действия, который не должен превышать шести месяцев.

Противоположную позицию выдвигает Л.В. Головко, отмечая отсутствие необходимости дополнения, как ст. 74 УПК РФ новым видом доказательства, так и новым специализированным следственным действием, но не отрицает некоторых изменений, касающихся технического характера уже существующей системы. В своей работе автор отмечает, что действовать в виртуальном мире необходимо также как и в реальном, применяя все те же протоколы следственных действий, заключения экспертов и т.п.[1].

Таким образом, можно сделать вывод, что для исследования в сети Интернет, на сегодняшний день, не существует четко определенных следственных действий, что не скажешь о системе оперативно-розыскных мероприятий. Конечно, некоторыми авторами предлагается дополнить действующее законодательство новыми специализированными следственными действиями, однако пока это не произошло, уполномоченные лица обязаны исследовать, фиксировать, изымать информацию, содержащуюся в сети Интернет теми способами, которые уже существуют.

По нашему мнению, если и вносить изменения в действующую структуру следственных действий, то стоит лишь расширить круг объектов, на которые они направлены, т.е. выделить отдельный вид следственного осмотра – осмотр сведений в сети Интернет.

Как мы уже выяснили, такие сведения могут содержаться в различном виде и иметь различный характер, и для того, чтобы понять в каком случае и каким следственным действием они будут исследоваться, мы предлагаем разграничить такие варианты на исходные ситуации. И в зависимости от того, какая исходная ситуация у нас существует, будут появляться критерии

[1] Головко Л.В. Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция? / Л. В. Головко // Вестник экономической безопасности. 2019. № 1. С. 24.

разграничения указанных нами следственных действий. Предложенную нами схему мы рассмотрим подробно в следующей главе.

ГЛАВА 2. ПРОБЛЕМА ОПРЕДЕЛЕНИЯ СЛЕДСТВЕННОГО ДЕЙСТВИЯ ДЛЯ ФИКСАЦИИ СВЕДЕНИЙ В СЕТИ ИНТЕРНЕТ И ПУТИ ЕЕ РЕШЕНИЯ

2.1. Исходные ситуации, в которых возникает необходимость производства следственных действий, направленных на получение и фиксацию сведений в сети Интернет.

Под исходной ситуацией следует понимать информацию, которая есть у следователя по факту совершения определенного преступления и в соответствии с которой следователю необходимо принять решение о производстве того или иного следственного действия. Выбор следственного действия во многом зависит от исходной ситуации. Данное положение подтверждает и Н.А. Архипова, отмечая, чтоисходная следственная ситуация определяет перспективы предварительного расследования и выбор следственного действия.[1]

По своему характеру исходные ситуации могут иметь различный характер. В ходе исследования выбранной нами темы, мы также выделили ряд исходных ситуаций, связанных с получением информации в сети Интернет, в результате которых следователю необходимо определиться, с помощью какого следственного действия он будет исследовать, и в дальнейшем фиксировать информацию, содержащуюся в информационно-телекоммуникационной сети, а также установили некоторые проблемы, связанные с надлежащей фиксацией такой информации. В выборе следственного действия следователь самостоятелен и поэтому несет за это юридическую ответственность, однако он обязан выбрать такое следственное

[1] Архипова Н.А. Тактика осмотра и выемки электронных сообщений, передаваемых по сетям электросвязи / Н.А. Архипова // Закон и право. 2018. № 6. С. 133.

действие, которое пригодно для извлечения определенной информации.[1] В результате неправильного выбора затрудняется дальнейший ход и развитие предварительного расследования. С.Б. Россинский указывает, что причинами неправильного выбора являются отсутствие четких границ процессуального закона (отсутствие специализированных следственных действий), а также отсутствие криминалистических методик.[2]В конечном итоге в результате неверного выбора следственного действия для конкретной исходной ситуации могут возникнуть негативные последствия в виде нарушения прав участников, а также ненадлежащей фиксации необходимых сведений.

Предлагаем выделить несколько исходных ситуаций, связанных с получением сведений в сети Интернет, обладающими доказательственным значением по уголовному делу.

Ситуация 1: Требуется зафиксировать сведения, находящиеся в открытом, ограниченном или закрытом доступе в сети Интернет.

В данном случае речь идет об информации, содержащейся на какой либо веб-странице или веб-сайте. Из выдвинутой нами исходной ситуации также можно выделить несколько «подситуаций», в зависимости от режима правовой охраны информации. Во-первых, когда требуется зафиксировать сведения, находящиеся в открытом доступе, например информацию на веб-странице, содержащую сведения о похищенном имуществе.[3] Во-вторых, сведения с ограниченным доступом, для доступа к которымнеобходимо пройти авторизацию. В-третьих, сведения, носящие закрытый характер. Таковыми могут признаваться,например веб-страницы содержащие охраняемые государством сведения.

---

[1]Кошелева М.А. Стереотипы выбора следственных действий / М.А. Кошелева // Вектор науки Тольяттинского государственного университета. 2013. № 2(24). С. 290.

[2]Россинский С.Б. Проблемы выбора следственного действия в уголовном судопроизводстве: от теории к практике / С.Б. Россинский // Российская юстиция. 2017. № 8. С. 45.

[3] Приговор Бабаевского районного суда Вологодской области от 15 июля 2020 г. № 1-84/2020 по делу 1-84/2020 [Электронный ресурс] – URL: https://sudact.ru/regular/doc/ONWLUZPkxwWU/ (дата обращения: 17.01.2023).

Ситуация 2:Требуется зафиксировать интернет-переписку, содержащуюся на серверах оператора связи.

Исследование интернет-переписки, может иметь несколько подходов. Так, например, когда лицо, чья переписка будет исследоваться согласно с ее осмотром, а также предоставляет свой электронный носитель (мобильный телефон, ноутбук и т.п.), в таком случае, лицо самостоятельно предоставляет логин и пароль для входа в какую либо социальную сеть для ее дальнейшего просмотра. Такой вариант оформляется протоколом осмотра документа (электронного документа) либо в перспективе - назначением судебной компьютерно-сетевой экспертизы. Фиксация интернет-переписки с сервера оператора связи имеет некоторые сложности. Сложность возникает при доступе к этой переписке. Конечно, нет никаких проблем при свободном доступе к интернет-переписке, тогда мы также оформляем наши действия протоколом осмотра документа. Однако переписка с ограниченным доступом может иметь личный и служебный характер. Переписка служебного характера не относится к тайне связи, охраняемой ст. 13 УПК РФ, поэтому для ее получения судебного решения не требуется.

Рассматривая личную переписку абонента, возникает вопрос, относится ли личная переписка к какому-либо из видов тайн и в каком случае требуется получение судебного решения для ее установления? Мы уже отмечали, что согласно ч. 1 ст. 63 №126-ФЗ«О связи» тайна переписки относится к тайне связи, а согласно ч. 2 указанной нормы обязанность по соблюдению тайны связи возлагается на операторов связи, однако право на тайну связи право признается «неотчуждаемым»[1], соответственно при наличии согласия абонента получение судебного решения не требуется. Таким образом, в рассматриваемой ситуации необходимо получить письменное согласие абонента на просмотр интернет-переписки, а случае его отказа в обязательном порядке получить судебное решение.

[1] Гасанов К.К. Содержание неотчуждаемости основных прав человека / К.К. Гасанов // Вестник Московского университета МВД России. 2012. № 6. С. 8.

Ситуация 3: Лицо при даче показаний о сведениях в сети Интернет не помнит некоторые события, не уверено в правильности изложенного.

Такая ситуация может возникнуть, когда интересующая следствие переписка имела место задолго до задержания лица и его допроса, либо когда следователю необходимы детали (например конкретные даты, время направления сообщений, точное содержание текста), которых лицо запомнить объективно не могло. В то же время самостоятельно, при помощи осмотра, следователь указанные сведения получить не может, так как не знает, где они расположены и не соотносит с обстоятельствами совершенного преступления. Для этого проводиться проверка показаний на месте с помощью, которой лицу предлагается продемонстрировать его действия (механизм преступления, либо же местонахождение интернет-переписки) в сети Интернет.

Ситуация 4: Преступление совершенно в сети Интернет, однако должностное лицо сомневается в способности подозреваемого (обвиняемого) самостоятельно выполнить такие действия.

Предложенная исходная ситуация обладает отличительным признаком, позволяющим отделить ее от других. Данный признак проявляется в сомнении должностного лица, ведущего предварительное расследование. Сомнение выражается в правдивости показаний подозреваемого (обвиняемого) или же, в нашем случае, способности выполнять определенные действия. Известно, что сомнения устраняются посредством следственного эксперимента. Как объективно отмечает А.Л. Мишуточкин: «если отсутствуют сомнения, то и следственный эксперимент проводить нет необходимости».[1]

Подробно о фактах проведения следственного эксперимента в сети Интернет пишут С.И. Земцова, О.А. Суров, П.В. Галушин. В своей работе авторы выделяют ситуации, в ходе которых необходимо провести

[1]Мишуточкин А.Л. Тактика проведения следственного эксперимента при расследовании неочевидных преступлений / А.Л. Мишуточкин // 2020. № 4(26). С. 11.

следственный эксперимент. Первая из них связана с необходимостью установить наличие в сети Интернет страницы (сайта), с помощью которой было совершено преступление, например, возможность покупки наркотика в интернет-магазине. Во-вторых, субъективную сторону преступления, например периодичность посещения интернет-страницы. В-третьих, для установления наличия/отсутствия у лица определенных навыков, например, пользоваться интернет-магазином.[1]

Из этого следует, что для установления перечисленных обстоятельств, а также в целях устранения сомнений у лица, ведущего предварительное расследование по уголовному делу, следует проводить следственный эксперимент.

Ситуация 5: Требуется зафиксировать содержание облачного хранилища, к которому имеется доступ.

Для начала разберемся с понятием облачного хранилища данных – это модель онлайн-хранилища, в котором данные хранятся на многочисленных распределённых в сети серверах,предоставляемых в пользование клиентам, в основном, третьей стороной.[2] В теории и практике уголовно-процессуального права, сведения, содержащиеся на облачных хранилищах, практически не изучены. Тем не менее, они могут содержать в своем хранилище достаточно большой объем информации, имеющей значение для уголовного дела.

Как известно, для доступа к информации, хранящейся на облачном хранилище необходимо пройти идентификацию и аутентификацию (ввод логина и пароля), который зачастую не известен следователю (дознавателю). Тем не менее, возможна ситуация, когда логин и пароль были получены из памяти изъятого устройства. В таком случае мы можем самостоятельно осмотреть информацию, содержащуюся на облачном хранилище. Такой

[1]Земцова С.И. Указ.соч. С. 134.

[2]Растамханова С.Н. "Облачное хранилище данных" в документоведческом аспекте / С.Н. Растамханова, А.Р. Фазлетдинова, Р.Р. Хафизова // Молодой ученый. 2016. № 26(130). С. 82.

осмотр осуществляется с участием лица, так, например, по уголовному делу № 1-81/2019[1] был произведен осмотр Интернет-ресурса «googl.com», а именно видеофайла, содержащегося на облачном хранилище, с участием лица, которое самостоятельного ввело логин и пароль. Мы допускаем, то в данном случае возможно и проведение проверки показаний на месте (критерии разграничения мы подробно изложим в следующем параграфе).

Однако не всегда удастся получить доступ к облачному хранилищу таким способом. Возможна ситуация, когда нам известно, что лицо пользуется облаком, однако доступа к нему нет. Одной из проблем, связанной с получением таких данных является неготовность провайдеров облачных сервисов к сотрудничеству с правоохранительными органами.[2] Это можно объяснить тем, что данные одного лица могут храниться в одной базе с данными, принадлежащими другому лицу (один сервер содержит данные нескольких клиентов). В то же время ч. 4 ст. 21 УПК РФ содержит положение о том, что требования, поручения и запросы следователя (дознавателя) обязательны для исполнения всеми учреждениями, а умышленное невыполнение этих требований может повлечь наложение санкции в виде штрафа (ст. 17.7. КоАП РФ).

М.Д. Кузьмин выделяет несколько проблем, возникающих при исследовании облачных хранилищ, к которым относятся: отсутствие доступа к информации, недостаток знаний и опыта, а также неопределенная юрисдикция (место) нахождения хранилища.[3]Действительно, информация в

---

[1] Апелляционное постановление Рязанского областного суда № 22-889/2018 22-889/2019 от 14 ноября 2019 г. по делу № 1-81/2019 // Судакт. [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/SxtOHm5tB61r/?regular-txt=выемка+из+облачного+хранилища&regular-case_doc=&regular-lawchunkinfo=&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=&regular-court=&regular-judge=&_=1681460219277&snippet_pos=6814#snippet (дата обращения: 23.03.2023).

[2]Карцхия А.А. "Облачные" технологии: российское и зарубежное законодательство и практика правоприменения / А.А. Карцхия // Мониторинг правоприменения. 2018. № 2(27). С. 38.

[3] Кузьмин М.Д. Проблемы расследований преступлений, совершенных с использованием облачных хранилищ в сети Интернет / М.Д. Кузьмин // 2020. № 1. С. 2.

облачном хранилище обладает виртуальным характером в прямом смысле этого слова, т.е. не имеет привязки к конкретному носителю информации[1] и сама по себе может храниться на множестве серверах, расположенных географически в удаленном расстоянии друг от друга.

С учетом изложенного мы предлагаем производить осмотр облачного хранилища с копированием информации. В то же время С.Н. Воробей отмечает, что информацию из облачных хранилищ необходимо копировать с помощью удаленного проведения выемки или обыска.[2] Мы вынуждены не согласиться с данным мнением, так как уже было отмечено ранее обыск и выемка предполагают изъятие овеществлённого предмета, при этом объект выемки перестает находиться в месте изъятия. Несмотря на то, что облачное хранилище позволяет «вырезать» какой-либо файл, физически он остается в памяти такого хранилища и доступен к восстановлению.

Следует отметить, что облачные хранилища в рамках уголовно-процессуального доказывания на сегодняшний день не имеют четкой регламентации, в связи с этим на практике может возникнуть ряд некоторых проблем, которые требуют правового решения. Вместе с тем, обозначенные в работе средства и сегодня позволяют практическим сотрудникам получать необходимые сведения.

Таким образом, нами были выделены наиболее характерные исходные ситуации, связанные с получением сведений в сети Интернет, обладающими доказательственным значением по уголовному делу. Такие ситуации служат отправной точкой для разрешения конкретных практических проблем, связанных с надлежащим выбором следственного действия.

---

[1]Рамалданов Х.Х. Понятие и сущность цифровизации доказательств и доказывания в уголовном судопроизводстве / Х.Х. Рамалданов // Вестник Волгоградской академии МВД России. 2022. № 1(60). С. 127.

[2]Воробей С.Н. Проблемы правовой регламентации процессуального порядка изъятия электронных носителей и копирования содержащейся на них информации / С.Н. Воробей // Полицейская и следственная деятельность. 2021. № 2. С. 31.

2.2. Критерии выбора следственного действия, направленного на получение сведений в сети Интернет

Практическая деятельность, в отличие от теоретической предполагает необходимость принятия решений, что в свою очередь не возможно без конкретных и точных «границ» между применяемыми механизмами или выделения признаков, позволяющих соотнести их между собой. Такими признаками по нашему мнению выступают критерии принятия решения при отграничении следственных действий в конкретной ситуации.

Критерии выбора следственного действия обусловлены схожей природой некоторых следственных действий, а также их характером. Выбор конкретного следственного действия обусловлен рядом факторов. К указанным факторам мы относим цель следственного действия, доступность и возможность проведения следственного действия в конкретном случае, следственную ситуацию, эффективность, осведомленность.

Рассматривая цель, как критерий выбора следственного действия, отметим, что в зависимости от того, какая информация необходима для расследования уголовного дела, выбирается тот или иной вид следственного действия. Под указанный критерий подпадают такие следственные действия, как проверка показаний на месте и осмотр.

Несомненно, оба следственных действия являются близкими по своему характеру, ведь оба следственных действия проводятся в месте, имеющем отношение к расследуемому событию[1], тем самым можно провести некую аналогию, ведь как уже было отмечено выше, осмотр также позволяет исследовать информацию в сети Интернет.

[1]Остроухова П.А. Тактические особенности проверки показаний на месте / П.А. Остроухова // Современные научные исследования: актуальные вопросы, достижения и инновации : сборник статей XI Международной научно-практической конференции, Пенза, 20 апреля 2020 года / Ответственный редактор: Гуляев Герман Юрьевич. – Пенза: "Наука и Просвещение" (ИП Гуляев Г.Ю.), 2020. С. 209.

Вместе с тем, мы считаем, что проведение проверки показаний на месте будет намного информативнее (ситуация № 3), так как фактически представится возможным совместить в себе два следственных действия – осмотр и допрос, которые сочетаются в проверке показаний на месте, как следственной действии. И, наоборот, при осмотре с участием лица необходимо будет сначала провести осмотр, а затем допрос, так как в протоколе осмотра нельзя фиксировать показания, а лишь действия следователя и все им обнаруженное (ст. 180 УПК РФ). Внесение показаний в протокол осмотра недопустимо по критерию ненадлежащей формы фиксации. Как мы указали в предыдущей главе, именно получение новых доказательств является конечной целью проверки показаний на месте (в том числе в интернет-пространстве). С учетом специфики цели проверки показаний на месте, как следственного действия,отметим, что оказавшись на месте происшествия (месте совершения им ранее действий в сети Интернет) человек лично вспоминает обстоятельства (возвращается в обстановку) и благодаря этому перестает сомневаться в своих показаниях, вспоминает детали произошедшего, в связи, с чем и возникает необходимость зафиксировать его показания.

Таким образом, в том случае, когда лицо точно знает и помнит необходимые следствию сведения, и ему не потребуется никаких уточнений (пояснений), а также мы имеем доступ к информации в сети Интернет, в таком случае, возможно, продублировать показания лица с помощью осмотра электронного документа (интернет-сайта). Если же лицо сомневается, не помнит отдельных обстоятельств, в таком случае целесообразно проводить проверку показаний на месте.

Возможность применения указанного критерия возможна и при разграничении осмотра и обыска. На практике возможна ситуация, когда в ходе осмотра помещения, в котором находится техническое средство (компьютер) с доступом в информационно-телекоммуникационную сеть Интернет, должностные лица производят осмотр компьютера и его

содержимого, включая, например, интернет-переписку. Применение указанного вида осмотра является категорически неверным, ведь в данном случае выполняются поисковые действия, характерные для обыска. Так, В.А. Гаужаева и Д.М. Сафронов указывают, что осмотр не предполагает поисковые действия[1], направленные на выявление скрытых предметов, информации имеющей значение для уголовного дела. В данном случае протокол осмотра должен быть признан недопустимым доказательством, т.к. указанные действия выходят за рамки процессуальных границ, необоснованно ограничивают права человека, в том числе на частную жизнь. Таким образом, осмотреть информацию в сети Интернет при осмотре помещений или жилища нельзя, поскольку в таком случае мы неминуемо допускаем поисковые действия. Исключения составляют случаи, когда такие действия совершает сам пользователь компьютера или иного технического средства.

Однако указанные следственные действия отличаются и по характеристике объекта, в отношении которого они проводятся. Как отмечают А.В. Смирнов и К.Б. Калиновский обыск проводится только в том месте, которое находится у лица в титульном владении (законном, основанном на каком либо праве), например, частный дом или земельный участок, в то время как осмотр может проводиться и в месте, у которого отсутствует законный владелец[2], например – участок леса, общественное место и др. Рассуждая по аналогии, допускаем, что если веб-страница находится в частном владении лица (например, личная страница пользователя), то поиск сведений гипотетически должен обладать признаками обыска, а если нас интересуют сведения, являющиеся

[1]Гаужаева В.А. Сколько нужно следственных действий, направленных на обнаружение, фиксацию и изъятие объектов, имеющих значение для дела? / В.А. Гаужаева, Д.М. Сафронов // Право и государство: теория и практика. 2022. № 2(206). С. 126.

[2] Смирнов А.В. Уголовный процесс : Учебник / А.В. Смирнов, К.Б. Калиновский ; под общей редакцией А.В. Смирнова. – Издание 3-е, переработанное и дополненное. – Москва :Компания КноРус, 2007. С. 400.

общедоступными, то вполне может быть применен осмотр. Предположим, что схожая логика позволяет Ю.А. Телевицкой утверждать, что в том случае, когда известно,какая именно информация находится в сети, накаком ресурсе она отображается, и кто являетсяее обладателем – нужно проводить выемку указанной информации.[1] Но с учетом характера следственных действий и выдвинутых нами предположений, считаем, что уместным будет проведение осмотра сведений, содержащихся в сети Интернет.

Осмотр необходимо отличать и от следственного эксперимента. Мы уже упоминали о том, что на практике существуют случаи, когда в ходе следственного эксперимента фиксируется интернет-переписка. Данное следственное действие проводится путем открытия входящих и исходящих сообщений лицом, участвующим в следственном эксперименте. Так, например С.П. Безрученко в своей работе приводит пример из уголовного дела Индустриального районного суда г. Барнаула № 1-623/2019 от 22.11.2019 г., в рамках которого, в результате производства следственного эксперимента лицом был осуществлен вход в приложение Telegramна аккаунт «*********», где была обнаружена интернет-переписка, содержащая информацию о преступных действиях лица, а именно о местах расположения тайников-закладок на территории г. Барнаул.[2]

Считаем, что с позиции уголовного процесса фиксацию переписки в ходе следственного эксперимента нельзя признать правильной, так как подобные действия противоречат целям следственного эксперимента, как следственного действия. Ведь следственный эксперимент должен

[1]Телевицкая Ю.А. Выемка, осмотр и обыск в электронных сетях: понятие и разграничение / Ю.А. Телевицкая // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2022. № 4(60). С. 240.

[2]Безрученко С.П. К вопросу о проведении следственного эксперимента по делам о незаконном обороте наркотических средств, осуществляемых посредством сети Интернет / С.П. Безрученко // Проблемы совершенствования российского законодательства: сборник тезисов Всероссийской (с международным участием) научной конференции курсантов, слушателей и студентов, Барнаул, 07–09 апреля 2020 года. – Барнаул: Федеральное государственное казенное образовательное учреждение высшего профессионального образования "Барнаульский юридический институт Министерства внутренних дел Российской Федерации", 2021. С. 397.

проводиться для проверки навыков лица, в том случае, если возникает сомнение в совершении лицом каких-либо определенных действий в сети Интернет. Вместе с тем С.А. Шейфер предлагает отличать следственный эксперимент от осмотра наличием в нем познавательной структуры.[1] Несомненно, открытие входящих и исходящих сообщений лицом при производстве следственного эксперимента не содержит познавательной структуры. При данных обстоятельствах предлагаем проводить проверку показаний на месте в интернет-пространстве, которая позволит не только продемонстрировать лицом интернет-переписку, но и зафиксировать его комментарии и показания.

Как уже было отмечено в предыдущем параграфе (ситуация № 1), информация в сети Интернет может иметь различный характер: содержаться в открытом, ограниченном, закрытом доступе. В результате мы можем выделить следующий критерий – режим доступа кинформации.[2] Информация, находящаяся в открытом доступе, исследуетсяв рамках осмотра с последующим фиксированием ее содержания в протоколе. Однакоинформация может иметь и ограниченный вид (например, необходима авторизация), или полностью закрытый вид (например, страница, содержащая охраняемые государством сведения). Исследуя информацию, доступ к которой ограничен, предлагаем назначать компьютерно-сетевую экспертизу, которая поможет преодолеть авторизацию и получить всю информацию, имеющую значение для уголовного дела. Сложнее, конечно же, когда доступ к информации в сети Интернет полностью закрыт. Как уже было отмечено исследование охраняемых государством сведений в соответствии с уголовно-процессуальным

[1] Шейфер, С. А. Следственные действия. Основания, процессуальный порядок и доказательственное значение / С. А. Шейфер ; Самарский государственный университет. – Самара : Самарский государственный университет, 2004. С. 120.

[2]Телевицкая Ю.А. Выемка, осмотр и обыск в электронных сетях: понятие и разграничение / Ю.А. Телевицкая // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2022. № 4(60). С. 241.

законодательством допускается посредством выемки с предварительным получением судебного решения (ч.3 ст.183 УПК РФ).

Таким образом, выбор следственного действия для исследования и фиксации сведений в указанном случае будет напрямую зависеть от характера доступа к этим сведениям.

В результате изложенного, хочется отметить, что выделенные нами критерии помогут облегчить работу следователя (дознавателя), относительно выбора следственных действий, имеющих общие цели, характер и природу. В рамках производства предварительного расследования должностные лица смогут реже допускать процессуальные теоретические и практические ошибки, соблюдать права участников при проведении следственных действий.

ЗАКЛЮЧЕНИЕ

Результаты исследования следственных действий направленных на получение сведений, содержащихся в сети Интернет,позволяют сделать ряд теоретическихвыводови предложений, связанных с грамотным исследованием и фиксацией сведений в информационно-телекоммуникационной сети.

В настоящее время все чаще преступления совершаются в сети Интернет, преступники оставляют в сети все больше следов, которые имеют значение для расследования уголовного дела. Сведения в сети Интернет является разновидностью компьютерной информации, однако местом хранения такой информации являются не электронно-вычислительные машины (далее – ЭВМ) или машинные носители, а удаленные серверы сети Интернет.

Действующее законодательство не содержит данных об электронных доказательствах, в связи, с чем предлагается внести ряд изменений и дополнить ст. 74 УПК РФ новым видом доказательств «Электронное доказательство». Тем не менее, исходя из действующего перечня доказательств, представленного ст. 74 УРК РФ, на сегодняшний день такие доказательства могут признаваться иными документами или протоколами следственных действий.

Любая интернет-страница является электронным документом (в уголовно-процессуальном значении). Большая часть информации из сети Интернет на сегодняшний день фиксируется в результате производства следственных действий, Таким образом, мы выделяем: 1) вид доказательства –электронный документ; 2) способ получения – осмотр документа.

Рассматривая действующую систему следственных действий мы не находим специализированных, которые направленны конкретно на исследование информации в сети Интернет. Такое упоминание есть в ч. 7 ст.

185 УПК РФ, однако исследовав характер следственного действия, а также его наименование считаем, что указанное следственное действие нельзя считать подходящим для фиксации сведений в сети Интернет.

Чаще всего информация в сети интернет исследуется в рамках традиционного следственного действия – осмотра, и фиксируется в качестве осмотра предметов, что является нарушением, так как предметом должен выступать материальный носитель, на котором такая информация может содержаться. Мы предлагаем фиксировать сведения в сети Интернет в рамках осмотра документов.Менее распространены случаи производства судебной экспертизы сведений из сети Интернет. На исследование информации в сети Интернет направлена компьютерно-сетевая экспертиза, однако данный вид экспертизы используется лишь подразделениями Минюста России или негосударственными экспертными учреждениями. В органах внутренних дел существует лишь такой вид экспертизы, как компьютерная, в рамках которой возможно исследование лишь содержимого памяти сотового телефона без выхода в сеть Интернет.

Конечно, многие авторы предлагают дополнить действующую систему следственных действий специализированными, направленными на получение информации в сети Интернет. Мы считаем такое дополнение излишним, т.к. порядок получения не изменится, в связи с этим предлагаем дополнить действующий перечень новым видом осмотра – осмотр сведений в сети Интернет. Однако пока такого не произошло, сотрудникам следственных органов следует использовать уже существующий перечень следственных действий. Чаще всего информация в сети интернет исследуется в рамках традиционного следственного действия – осмотра, и фиксируется в качестве осмотра предметов, что является нарушением, так как предметом должен выступать материальный носитель, на котором такая информация может содержаться. Вместе с тем считаем нецелесообразным проведение производства обыска или выемки сведений из сети Интернет, так как указанные следственные действия предполагают изъятие чего-либо

овеществленного (предметы, документы), тогда как виртуальная информация не обладает свойствами предмета.

Для того чтобы выбрать конкретный вид следственного действия был выделен ряд исходных ситуаций, а также критерии принятия решения при отграничении следственных действий в конкретной ситуации, которые послужат отправной точкой для разрешения практических проблем, связанных с надлежащим выбором следственного действия.

Подводя итог, хочется отметить, что исследование информации в сети Интерне требует большего внимания со стороны законодателя, что позволит не допускать следственных ошибок и исключит в дальнейшем признание доказательств недопустимыми по уголовному делу. А выделенные нами исходные ситуации, а также критерии разграничения следственных действий помогут правоприменителю использовать уже существующие следственные действия и получать информацию с доказательственным значением при этом соблюдая права участников.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ[1]

Нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации : принята 12 декабря 1993 года всенародным голосованием (с учетом поправок, внесенных законами Российской Федерации о поправках к Конституции Российской Федерации от 30 декабря 2008 г.№ 6-ФКЗ, от 30 декабря 2008 г. № 7-ФКЗ, от 5 февраля 2014 г. № 2-ФКЗ, от 21 июля2014 г. № 11-ФКЗ, с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г.) // Российская газета. – 2020. – 4 июля.

2. О государственной судебно-экспертной деятельности в Российской Федерации : Федеральный закон от 31 мая 2001 г. № 73-ФЗ от 5 апреля2001 г. // Российская газета. – 2001. – 5 июня.

3. О связи : Федеральный закон Российской Федерациот 7 декабря 2003 г. № 126-ФЗ // Российская газета. – 2003. – 7 декабря.

4. О судебной экспертизе по уголовным делам : Постановление Пленума Верховного Суда РФ от 21 декабря 2010 г. № 28, ред. 29.06.2021 // Российская газета. – 2010. – 30 декабря.

5. Об информации, информационных технологиях и о защите информации :Федеральный закон Российской Федерации от 27июля 2006 г. № 149-ФЗ // Российская газета. – 2006. – 27 июля.

6. Об оперативно-розыскной деятельности : Федеральный закон Российской Федерации от 12 августа 1995 г. № 144-ФЗ // Российская газета. – 1995. – 18 августа.

7. Об утверждении Методических рекомендаций по производству судебных экспертиз в государственных судебно-экспертных учреждениях

[1] Здесь и далее приводятся нормативные правовые акты и иные документы в первой редакции. Актуальные редакции нормативно-правовых актов и иных документов использовались по СПС КонсультантПлюс.

системыМинистерства юстиции Российской Федерации : Приказ Минюста России от20 декабря 2002 г. № 346 // СПС «КонсультантПлюс» : [сайт]. – URL:http://http://www.consultant.ru/document/cons_doc_LAW_127383/6855643309efa4963f1a243182d7dc90a1664945/ (дата обращения: 16.02.2023).

8. Уголовный кодексРоссийской Федерации от 13 июня 1996 г. № 63-ФЗ, ред. от 28.04.2023 // Российская газета. – 1996. – 24 мая.

9. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ, ред. от 28.04.2023// Российская газета. – 2001. – 22 декабря.

Монографии, учебники и учебные пособия

10. Балакшин, В.С. Доказательства в теории и практике уголовно-процессуального доказывания / В.С. Балакшин. – Екатеринбург : Изд-во УМЦ УПИ,2004. – 298 с.

11. Безлепкин, Б.Т. Уголовный процесс России : учебное пособие. – 2-еизд., перераб. и доп. / Б.Т. Безлепкин. – Москва : ТК Велби, Изд-во Проспект,2004. – 480 с.

12. Белкин, Р.С. Криминалистическая энциклопедия / Р.С. Белкин. – Москва : БЕК, 1997. – 342 с.

13. Белкин, Р.С. Курс криминалистики : в 3 т. Т. 1 / Р.С. Белкин. – Москва :Юристъ, 1997. – 408 с.

14. Головко, Л. В. Курс уголовного процесса / Под ред. д.ю.н., проф. Л.В. Головко. – 2-е изд., испр. – М.: Статут, 2017. – 666 с.

15. Гуляев, А.П. Комментарий к Уголовно-процессуальному кодексу Российской Федерации / Под общ. ред. В.В. Мозякова. –М., 2002.

16. Давлетов, А.А. Уголовное судопроизводство Российской Федерации. Особенная часть : курс лекций / А.А. Давлетов. – Екатеринбург : ИРА УТК, 2011. – 264 с.

17. Земцова, С.И. Методика расследования незаконного сбыта синтетических наркотических средств, совершенного с использованием интернет-магазинов / С.И. Земцова, О. А. Суров, П. В. Галушин. – Красноярск : Сибирский юридический институт Министерства внутренних дел Российской Федерации, 2019. – 160 с.

18. Зигура, Н.А. Компьютерная информация как вид доказательств в уголовном процессе России : монография / Н.А. Зигура, А.В. Кудрявцева. – Москва : Издательство "Юрлитинформ", 2011. – 176 с.

19. Зинатуллин, З.З. Уголовно-процессуальное доказывание: Концептуальные основы : монография / З.З. Зинатуллин, Т.З. Егорова, Т.З. Зинатуллин. – Ижевск :Детектив-Информ, 2002. – 228 с.

20. Кальницкий, В.В. Следственные действия : учебное пособие / В.В. Кальницкий, Е.Г. Ларин. – Омск :ОмА МВД России, 2015. – 172 с.

21. Кудин, Ф.М. Принуждение в уголовном судопроизводстве/ Ф.М. Кудин. – Красноярск : Изд-во Краснояр. ун-та, 1985. - 135 с.

22. Ожегов, С.И. Толковый словарь русского языка: 80000 слов и фразеологических выражений / С.И. Ожегов, Н.Ю. Шведова. – Москва : ООО «А ТЕМП», 2006. – 938 с.

23. Россинская, Е.Р. Настольная книга судьи. Судебная экспертиза : теория и практика, типичные вопросы и нестандартные ситуации : судебно-экспертные учреждения, назначение экспертизы в суде, типичные экспертные ошибки, заключение эксперта, порядок проведения экспертиз / Е.Р. Россинская, Е.И. Галяшина ; Е.Р. Россинская, Е.И. Галяшина ; Московская гос. юридическая акад. им. О.Е. Кутафина, Ин-т судебных экспертиз. – Москва : Проспект, 2012. – 458 с.

24. Россинская, Е.Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе / Е.Р. Россинская. – 3-е изд. – Москва : Норма, 2014. – 735 с.

25. Смирнов, А.В. Уголовный процесс : учебник / А.В. Смирнов, К.Б. Калиновский ; под общ.ред. проф. А.В. Смирнова. – 4-е изд., перераб. и доп. – М. : КНОРУС, 2008. – 691 с.

26. Томин, В.Т. Уголовный процесс: актуальные проблемы теории и практики. –М.: Юрайт, –2009. –376 с.– Текст : непосредственный.

27. Ульянова, Л.Т. Предмет доказывания и доказательства в уголовном процессе России / Л.Т. Ульянова. – Москва : Городец, 2008. – 173 с.

28. Фойницкий, И.Я. Курс уголовного судопроизводства. Т. 2 / под ред. А.В. Смирнова. – Санкт-Петербург : Альфа, 1996. – 607 с.

29. Шейфер, С.А. Следственные действия. Система и процессуальная форма / С.А. Шейфер. – Москва :Юрлитинформ, 2001. – 206 с

30. Шейфер, С.А. Сущность и способы собирания доказательств в советском уголовном процессе : учебное пособие / С.А. Шейфер. – Москва : ВЮЗИ, 1972. – 130 с.

31. Шейфер, С.А. Собирание доказательств по уголовному делу: проблемы законодательства, теории и практики : монография / С.А. Шейфер. – Москва : Норма, 2015. – 110 с.

32. Шейфер, С.А. Следственные действия. Основания, процессуальный порядок и доказательственное значение / С.А. Шейфер. – Москва :Юрлитинформ, 2004. – 183 с.

33. Элькинд, Н.С. Толкование и применение норм уголовно-процессуального права. – Москва : Юрид. лит., 1967. – 192 с.

Научные публикации и статьи в иных периодических изданиях

34. Александров, А.С. Учение о следственных действиях на пороге "цифрового мира" / А.С. Александров // Юридический вестник Самарского университета. – 2017. – Т. 3, № 4. – С. 80-85.

35. Архипова, Н.А. Тактика осмотра и выемки электронных сообщений, передаваемых по сетям электросвязи / Н.А. Архипова // Закон и право. – 2018. – № 6. – С. 132-135.

36. Безрученко, С.П. К вопросу о проведении следственного эксперимента по делам о незаконном обороте наркотических средств, осуществляемых посредством сети Интернет / С. П. Безрученко// Проблемы совершенствования российского законодательства : сборник тезисов Всероссийской (с международным участием) научной конференции курсантов, слушателей и студентов, Барнаул, 07–09 апреля 2020 года. – Барнаул: Федеральное государственное казенное образовательное учреждение высшего профессионального образования "Барнаульский юридический институт Министерства внутренних дел Российской Федерации", 2021. – С. 397-398.

37. Болотов, М.В. Некоторые особенности проведения проверки показаний на месте / М.В. Болотов // Синергия Наук. – 2018. – № 25. – С. 628.

38. Велиев, Я.П. Некоторые проблемы, связанные с получением и представлением оперативно значимой информации, содержащейся в электронных документах / Я.П. Велиев// Известия Тульского государственного университета. Экономические и юридические науки. – 2022. – № 3. – С. 54-61.

39. Волкова, С.В. Рецензия на заключение эксперта как разновидность заключения специалиста в уголовном судопроизводстве / С.В. Волкова, М.В. Бобовкин // Эксперт-криминалист. – 2008. – № 1. – С. 36-38.

40. Воробей, С.Н. Проблемы правовой регламентации процессуального порядка изъятия электронных носителей и копирования содержащейся на них информации / С.Н. Воробей // Полицейская и следственная деятельность. – 2021. – № 2. – С. 26-31.

41. Гасанов, К.К. Содержание неотчуждаемости основных прав человека / К.К. Гасанов // Вестник Московского университета МВД России. – 2012. –№ 6. –С. 8-11.

42. Гаужаева, В.А. Сколько нужно следственных действий, направленных на обнаружение, фиксацию и изъятие объектов, имеющих значение для дела? / В.А. Гаужаева, Д.М. Сафронов // Право и государство: теория и практика. – 2022. – № 2(206). – С. 125-128.

43. Головко, Л.В. Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция? / Л.В. Головко // Вестник экономической безопасности. – 2019. – № 1. – С. 15-25.

44. Григорьев, В.Н. Результаты смены парадигмы в исследованиях уголовного процесса / В.Н. Григорьев// Вестник Всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации. – 2017. – № 2(42). – С. 38-46.

45. Ермакова, Е.С. Электронные доказательства как новое направление в практике расследования преступлений / Е.С. Ермакова, Д.М. Джумангалиева// Молодой ученый. – 2018.– № 23 (209). – С. 85-87.

46. Жижилева, А.А. О некоторых теоретических аспектах использования в криминалистике понятий цифровые, электронные, виртуальные следы / А.А. Жижилева// Вопросы российской юстиции. – 2019. – № 3. – С. 913-918.

47. Журба, О.Л. К вопросу повышения эффективности поисковых действий при производстве обыска / О.Л. Журба, С.А. Торопов// Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. – 2018. – Т. 4 (70), № 3. – С. 130-138.

48. Земцова, С.И. Развитие научных идей профессора Р.С. Белкина о значении следственного эксперимента в условиях современных нарковызовов с использованием интернет-технологий / С.И. Земцова // Вестник Сибирского юридического института МВД России. – 2022. – № 2(47). – С. 92-97.

49. Зигура, Н.А. Компьютерная информация как вид доказательств в уголовном процессе России : специальность 12.00.09 "Уголовный процесс" : диссертация на соискание ученой степени кандидата юридических наук / Зигура Надежда Анатольевна. – Челябинск, 2010. – 234 с.

50. Зуев, С.В. Электронные доказательства в уголовном судопроизводстве: понятие и значение / С.В. Зуев // Правопорядок: история, теория, практика. – 2020. – № 3(26). – С. 46-51.

51. Иванов, А.Н. Удалённое исследование компьютерной информации: уголовно - процессуальные и криминалистические проблемы / А.Н. Иванов// Известия Саратовского университета. Новая серия. Серия: Экономика. Управление. Право. – 2009. – Т. 9, № 2. – С. 74-77.

52. Карлов, А.Л. К проблеме определения следственного действия для процессуальной фиксации интернет-переписки / А.Л. Карлов// Научно-практический электронный журнал Аллея науки. – 2018. – Т. 2. – № 8(24). – С. 556-563.

53. Колычева, А.Н. Некоторые аспекты фиксации доказательственной информации, хранящейся на ресурсах сети Интернет / А.Н. Колычева// Вестник Удмуртского университета. Серия Экономика и право. – 2017. – Т. 27. – № 2. – С. 109-113.

54. Кошелева М.А. Стереотипы выбора следственных действий / М.А. Кошелева// Вектор науки Тольяттинского государственного университета. – 2013. – № 2(24). – С. 290-292.

55. Кузьмин, М.Д. Проблемы расследований преступлений, совершенных с использованием облачных хранилищ в сети Интернет / М.Д. Кузьмин // Полицейская деятельность. – 2020. – № 1. – С. 1-5.

56. Кульмухамбетова, Н.А. Особенности фиксации информации при расследовании преступлений экстремистской направленности в глобальной сети Интернет / Н.А. Кульмухамбетова// Новый юридический вестник. – 2019. – № 1(8). – С. 58-60.

57. Мельникова, А.С. Проверка показаний на месте: значение, особенности, пробелы законодательства / А.С. Мельникова, Е.Е. Колбасина// Юристъ-Правоведъ. – 2020. – № 4(95). – С. 91- 95.

58. Мишуточкин, А.Л. Тактика проведения следственного эксперимента при расследовании неочевидных преступлений / А.Л. Мишуточкин//ГлаголЪ правосудия. – 2020. – № 4(26). – С. 10-12.

59. Никитина, Е.В. Проблемы законодательного регулирования следственного действия, направленного на получение доступа к электронным сообщениям / Е.В. Никитина, В.С. Раменская// Российское право: образование, практика, наука. – 2022. – № 2. – С. 25-32.

60. Новиков, С.С. Электронный документ: понятие и сущность / С.С. Новиков// ModernScience. – 2020. – № 9-1. – С. 153-156.

61. Остроухова, П.А. Тактические особенности проверки показаний на месте / П.А. Остроухова// Современные научные исследования: актуальные вопросы, достижения и инновации : сборник статей XI Международной научно-практической конференции, Пенза, 20 апреля 2020 года / Ответственный редактор: Гуляев Герман Юрьевич. – Пенза: "Наука и Просвещение" (ИП Гуляев Г.Ю.), 2020. – С. 209-211.

62. Першин, А.Н. Осмотр сетевых информационных ресурсов - новый вид следственного действия? / А.Н. Першин // Российский следователь. – 2020. – № 1. – С. 13-16.

63. Рамазанов, Т.Б. Заключения и показания эксперта и специалиста как доказательства в уголовном судопроизводстве / Т.Б. Рамазанов// Юридический вестник Дагестанского государственного университета. – 2012. – № 4. – С. 96-101.

64. Рамалданов, Х.Х. Понятие и сущность цифровизации доказательств и доказывания в уголовном судопроизводстве / Х.Х. Рамалданов// Вестник Волгоградской академии МВД России. – 2022. – № 1(60). – С. 121-128.

65. Растамханова, С.Н. "Облачное хранилище данных" в документоведческом аспекте / С.Н. Растамханова, А.Р. Фазлетдинова, Р.Р. Хафизова // Молодой ученый. – 2016. – № 26(130). – С. 81-83.

66. Россинская, Е.Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации / Е.Р. Россинская// Вестник Университета имени О.Е. Кутафина (МГЮА). – 2019. – № 5(57). – С. 31-44.

67. Россинский, С.Б. Проблемы выбора следственного действия в уголовном судопроизводстве: от теории к практике / С.Б. Россинский// Российская юстиция. – 2017. – № 8. – С. 44-47.

68. Стельмах, В.Ю. Электронная информация в доказывании по уголовным делам: способы получения и место в системе доказательств / В.Ю. Стельмах// Библиотека криминалиста. – 2018. – № 3 (38). – С. 93-100.

69. Супрун, С.В. О противоречивом характере новеллы в законодательном регулировании следственного действия "наложение ареста на почтово-телеграфные отправления" / С.В. Супрун, В.С. Черкасов // Вестник Омской юридической академии. – 2017. – Т. 14, № 1. – С. 59-64.

70. Телевицкая, Ю.А. Выемка, осмотр и обыск в электронных сетях: понятие и разграничение / Ю.А. Телевицкая// Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2022. – №4(60). – С. 238-242.

71. Федоров, М.Н. Преступления, совершаемые с помощью глобальной информационной сети Интернет / М.Н. Федоров// Молодой ученый. – 2020. – № 17(307). – С. 243-245.

72. Федотов, И.С. Электронные носители информации: "вещественные доказательства" или "иные документы"? / И.С. Федотов, П.Г. Смагин// Вестник Воронежского государственного университета. Серия: Право. – 2014. – № 3(18). – С. 191-199.

73. Цабан, Я.Б. Следственные действия как основной способ собирания доказательств по уголовным делам / Я.Б. Цабан. // Символ науки: международный научный журнал. – 2015. – № 12-2. – С. 108-110.

74. Шейфер, С.А. Куда движется российское судопроизводство? (Размышления по поводу векторов развития уголовно-процессуального законодательства) / С.А. Шейфер // Государство и право. – 2007. – № 1. – С. 28-37.

75. Шелегов, Ю.В. К вопросу о проблеме использования доказательственной информации из цифровых источников в уголовно-процессуальном доказывании / Ю.В. Шелегов, В.Г. Шелегов // Деятельность правоохранительных органов в современных условиях : сборник материалов XXIV международной научно-практической конференции, Иркутск, 06–07 июня 2019 года / Восточно-Сибирский институт МВД России. – Иркутск: Восточно-Сибирский институт Министерства внутренних дел Российской Федерации, 2019. – С. 182-183.

76. Шогенов, Т.К. Вопросы технического обеспечения проведения оперативно-розыскного мероприятия "Снятие информации с технических каналов связи" / Т.К. Шогенов // Спецтехника и связь. – 2013. – № 6. – С. 28-31.

Интернет-ресурсы

77. МВД России предлагает дополнить перечень оперативно-розыскных мероприятий «исследованием компьютерной информации». Официальный сайт Министерства внутренних дел Российской Федерации. Текст: электронный.– Режим доступа: https://xn--b1aew.xn--p1ai/news/item/24427014 (дата обращения: 21.01.20223).

78. Чуранов, Е.А. Статистика интернета и соцсетей на 2023 год – цифры и тренды в мире и в России. – Текст: электронный. – Режим доступа: https://www.web-canape.ru/business/statistika-interneta-i-socsetej-na-2023-god-cifry-i-trendy-v-mire-i-v-rossii/ (дата обращения 20.11.2022).

Эмпирические материалы

79. Апелляционное постановление Рязанского областного суда № 22-889/2018 22-889/2019 от 14 ноября 2019 г. по делу № 1-81/2019 // Судакт. [Электронныйресурс]. – URL: https://sudact.ru/regular/doc/SxtOHm5tB61r/?regular-txt=выемка+из+облачного+хранилища&regular-case_doc=&regular-lawchunkinfo=&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=&regular-court=&regular-judge=&_=1681460219277&snippet_pos=6814#snippet (датаобращения: 23.03.2023).

80. Приговор Бабаевского районного суда Вологодской области от 15 июля 2020 г. № 1-84/2020 по делу 1-84/2020 [Электронный ресурс] – URL: https://sudact.ru/regular/doc/ONWLUZPkxwWU/ (дата обращения: 17.01.2023).

81. Приговор Вахитовского районного суда г. Казани (Республика Татарстан) от 06 мая 2014 г. № 1-184/2014 по делу № 1-184/2014 [Электронный ресурс] – URL: https://sudact.ru/regular/doc/WyavwZ7DR958/ (дата обращения: 16.11.2022).

82. Приговор Краснодарского краевого суда от 23 июля 2019 г. № 2-28/2019 по делу № 2-28/2019 [Электронный ресурс] – URL: https://sudact.ru/regular/doc/PDXLfJbOWeLu/ (дата обращения: 12.12.2022).

83. Приговор Ленинского районного суда г. Смоленска от 07 июля 2015 г. № 1-150/2015 по делу № 1-150/2015 [Электронный ресурс] – URL: https://sudact.ru/regular/doc/2zu84yTkqomN/?regular-txt=осмотр+интернет-переписки&regular-case_doc=&regular-lawchunkinfo=&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=&regular-court=&regular-judge=&_=1685249740613&snippet_pos=13018#snippet (дата обращения: 02.04.2023).

84. Приговор Пензенского районного суда (Пензенская область) № 1-86/2020 от 28 сентября 2020 г. по делу № 1-86/2020 // URL:

https://sudact.ru/regular/doc/4PItzykNNxmu/?regular–txt (дата обращения: 23.01.2023).

85. Приговор Первореченского районного суда г. Владивостока от 12 мая 2020 г № 1-25/2020 по делу № 1-25/2020 [Электронный ресурс] –URL: https://sudact.ru (дата обращения: 12.12.2022).

Приложение №1

Анкета

Сибирский юридический институт МВД России проводит научное исследование.

Мы с пониманием относимся к режиму Вашей работы и загруженности, однако ответив на несколько приведенных ниже вопросов, Вы поможете нам получить объективную и актуальную информацию, необходимую для разработки практических рекомендаций, которые в свою очередь помогут сэкономить время другим сотрудникам, сталкивающимися с трудностями в практической деятельности.

Анкета анонимна, Ваши ответы будут использованы только в обобщенном виде. Если при ответе на вопрос Вы затрудняетесь дать точные количественные данные, укажите приближенные значения.

Выбранный ответ можете отметить «галочкой» либо иным символом в предназначенной для этого графе, если среди приведенных ответов отсутствует подходящий – укажите свой вариант в пустой графе, при необходимости Вами могут быть отмечены несколько вариантов ответов.

1. **Известны ли Вам случаи, когда в ходе проверки показаний на месте осуществлялся выход в сеть Интернет с фиксацией необходимых сведений?**

1	не известны		
2	известны		
3	затрудняюсь ответить		
4	свой вариант		

2. **Известны ли Вам случаи, когда в ходе осмотра с подключением к сети Интернет фиксировалась переписка?**

1	не известны		
2	известны		
3	затрудняюсь ответить		
4	свой вариант		

3. **Как Вы считаете, в ходе, какого вида из осмотров, существующих в уголовно-процессуальном законодательстве, необходимо фиксировать сведения в сети Интернет?**

1	осмотр предметов		
2	осмотр документов		
3	осмотр электронного документа		
4	осмотр помещения, в котором находится техническое средство		
5	свой вариант		

4. **Известны ли Вам случаи, когда в рамках компьютерной экспертизы производился осмотр информации в сети Интернет?**

1	не известны		
2	известны		
4	затрудняюсь ответить		
5	свой вариант		

_____

(укажите Ваш регион, город)

Сибирский юридический институт благодарит Вас за оказанное содействие и искренность при ответе на вопросы анкеты!

Приложение №2

Результаты анкетирования 25 сотрудников следственных органов г. Красноярска и Красноярского края

1. **Известны ли Вам случаи, когда в ходе проверки показаний на месте осуществлялся выход в сеть Интернет с фиксацией необходимых сведений?**

1	не известны		90%
2	известны		5%
3	затрудняюсь ответить		5%
4	свой вариант		-

2. **Известны ли Вам случаи, когда в ходе осмотра с подключением к сети Интернет фиксировалась переписка?**

1	не известны		55%
2	известны		45%
3	затрудняюсь ответить		20%
4	свой вариант		-

3. **Как Вы считаете, в ходе, какого вида из осмотров, существующих в уголовно-процессуальном законодательстве, необходимо фиксировать сведения в сети Интернет?**

1	осмотр предметов		55%
2	осмотр документов		35%
3	осмотр электронного документа		5%
4	осмотр помещения, в котором находится техническое средство		5%
5	свой вариант		-

4. **Известны ли Вам случаи, когда в рамках компьютерной экспертизы производился осмотр информации в сети Интернет?**

1	не известны		100%
2	известны		-
4	затрудняюсь ответить		-
5	свой вариант		-

Приложение №3

ГУ МВД России по Красноярскому краю

Межмуниципальное управление Министерства внутренних дел Российской Федерации «Красноярское»

Отдел полиции № 6

(Отдел полиции № 6 Межмуниципальное управление МВД России «Красноярское»)

ул. 60 лет Октября, 73, Красноярск, 660079

Ф. 249-06-65, т. 233-47-38

Начальнику ЭКО МУ
МВД России «Красноярское»

подполковнику полиции
В. И. Варламову

Г. Красноярск, пр. Металлургов, 53 «а»

Направляю на исследование сотовый телефон «Oddo» принадлежащий XXXX X.X. изъятый в ходе личного досмотра по уголовному делу №12201040XXXXXXX по факту незаконного сбыта наркотических средств, предусмотренного п. «б» ч. 3 ст. 228.1 УК РФ.

В ходе исследования необходимо установить:

1. Имеется ли в памяти представленного мобильного телефона информация об электронной переписке?
2. Имеется ли в памяти представленного мобильного телефона информация об аудио-видео и графических файлах?
3. Имеется ли в памяти представленного мобильного телефона информация о журнале просмотра Web-страниц?

В соответствии с п. 3 ч. 4 ст. 57 УПК РФ разрешаю частичное или полное уничтожение информации, в объеме необходимом для проведения исследования.

Следователь отдела № X
СУ МУ МВД России «Красноярское»
мл. лейтенант юстиции XXXXXX X.X.