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:

СПОСОБЫ ПРОЦЕССУАЛЬНОГО ЗАКРЕПЛЕНИЯ ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ, ОБНАРУЖЕННОЙ В СЕТИ ИНТЕРНЕТ (НА ПРИМЕРЕ УГОЛОВНЫХ ДЕЛ О НЕЗАКОННОМ ОБОРОТЕ НАРКОТИЧЕСКИХ СРЕДСТВ И ПСИХОТРОПНЫХ ВЕЩЕСТВ)

Выполнил:
Слушатель учебной группы НБ 1801
младший лейтенант полиции
Зайцева Светлана 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 — (специальное звание)
(подпись)
Н.А. Юдина — (инициалы, фамилия)

Красноярск 2023

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В современном мире высоких технологий трудно представить человека, который бы не использовал Интернет в личных и служебных целях. Миллионы людей ежедневно посещают свои страницы в социальных сетях, читают новостные ленты, ищут актуальную информацию в поисковых программах. Гаджеты стали неотъемлемой частью жизни благодаря их многофункциональности, надежности, высокой производительности и относительной доступности для потенциального покупателя. Однако помимо рядовых пользователей, преступность также активно использует все возможности, которые нам предоставляет сеть. Банковские операции, переписка по шифрованным каналам связи, сбор персональных данных и другие активно используются при осуществлении нелегального оборота наркотических средств и психотропных веществ (далее – НС и ПВ).

С 1 января 2013 года вступили в силу положения Федерального закона от 01.03.2012 г. № 18-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации». Пункт «б» части 2 статьи 228.1 Уголовного кодекса Российской Федерации (далее – УК РФ) «Сбыт наркотических средств, психотропных веществ или их аналогов, совершенный с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет»)», введение данного квалифицирующего признака напрямую обуславливается широким распространением фактов сбыта наркотических средств и психотропных веществ бесконтактным способом и дополнительно подтверждает актуальность темы исследования.

Согласно статистике, опубликованной на официальном сайте МВД России, за январь-март 2023 года на 57% больше зафиксировано фактов сбыта наркотиков с использованием информационно-

телекоммуникационных технологий относительно аналогичного периода 2022 года[1].

При бесконтактном способе сбыта НС и ПВ используются различные программы для осуществления переписок в сети (мессенджеры), социальные сети, системы электронных кошельков, приложения банков. Также продажа НС и ПВ через ИТС обычно происходит посредством «Darknet», так называемые «темные сайты», которые не доступны через обычные поисковые системы. Такие веб-сайты используются для обеспечения анонимности лиц сбывающих и лиц приобретающих НС и ПВ, что делает их обнаружение труднодоступным для правоохранительных органов. Информация, хранящаяся на ноутбуках, компьютерах, смартфонах и других электронных носителях информации имеет большое доказательственное значение. Однако процесс изъятия информации с электронного носителя уже довольно широко изучен учеными-процессуалистами. Также законодатель в последнее время активно совершенствует Уголовно-процессуальный кодекс (далее – УПК РФ) в данной сфере. Например, ст. 164.1, которая была введена 27.12.2018 г., регулирующая особенности изъятия электронных носителей и копирование с них информации при производстве следственных действий. Но следует учитывать, что огромное количество важной для следствия информации находится непосредственно в сети Интернет на различных серверах и не остается в памяти устройства.

В связи с эти возникает необходимость системного и комплексного исследования способов изъятия и использовании в доказывании сведений, расположенных в сети Интернет по уголовным делам в сфере незаконного оборота наркотиков. Необходимо определить, с помощью каких следственных и иных процессуальных действий можно правомерно получить доступ к интернет-сведениям и конкретизировать процессуальных порядок их изъятия и использовании в качестве доказательств по уголовным делам в

[1] Краткая характеристика состояния преступности в Российской Федерации за январь-март 2023 года // мвд.рф : [Электронный ресурс]. — URL: https://xn--b1aew.xn--p1ai/reports/item/37377025 (дата обращения: 01.05.2023).

сфере незаконного оборота НС и ПВ, а на основе проделанной работы сделать вывод о необходимости внесения изменений в законодательные акты Российской Федерации (далее – РФ). Перечисленные выше обстоятельства послужили поводом выбора данной темы исследования, определили его объект, предмет, цель и задачи.

Актуальность выбранной темы также подтверждается пробелами уголовно-процессуального закона в данной части, и как следствие – отсутствием единого процессуального порядка фиксации информации в сети Интернет и её приобщении в качестве доказательств при расследовании уголовных дел о преступлениях в сфере незаконного оборота НС и ПВ. Единый процессуальный порядок получения и фиксации сведений из сети Интернет должен стать важным инструментом для сотрудников полиции, обеспечивающим соблюдение прав и свобод граждан.

Объектом исследования являются общественные отношения между участниками уголовного процесса, возникающие в процессе производства следственных и иных процессуальных действий, направленных на получение информации из сети Интернет.

Предмет исследования – уголовно-процессуальные нормы, а также положения иных законов, регулирующих производство следственных и иных процессуальных действий, связанных с получением информации из сети Интернет, проблемы, связанные с процессуальным порядком получения сведений из сети Интернет при расследовании преступлений в сфере незаконного оборота НС и ПВ.

Целью дипломной работы является уяснение особенностей практики применения процессуального порядка получения информации из сети Интернет и формирование теоретической базы для разработки рекомендаций по совершенствованию уголовнопроцессуального законодательства в части закрепления способов получения (изъятия) информации, которая содержится в сети Интернет.

Для достижения указанной цели необходимо поставить и решить следующие задачи:

– изучить общие теоретические аспекты оценки доказательственного значения сведений, полученных из сети Интернет по уголовным делам о незаконном обороте наркотических средств и психотропных веществ;

– определить понятие, содержание и систему способов закрепления (фиксации) доказательственной информации, расположенной в сети Интернет;

– выявить особенности и проблемные аспекты процессуального закрепления информации из сети Интернет при производстве следственных действий по уголовным делам о преступлениях в сфере незаконного оборота наркотических средств и психотропных веществ;

– выявить особенности и проблемные аспекты процессуального закрепления информации из сети Интернет при производстве иных процессуальных и непроцессуальных действий по уголовным делам в сфере незаконного оборота наркотиков.

Нормативную базу исследования составили нормативно-правовые акты РФ.

Теоретическую базу исследования составили труды отечественных ученых в области уголовно-процессуального права и криминалистики: К.Б. Калиновского, Р.С. Белкина, А.С. Александрова, Л.В. Головко, Л.А. Головко, В.В. Кальницкого, А.Л. Карлова, Л.Б. Красновой, В.Ю. Стельмах, В.С. Мещерякова, О.М. Ефремовой, В.Ф. Васюкова и др.

Эмпирическую базу исследования составили решения районных судов, судов субъектов РФ, решения Конституционного Суда РФ и Верховного Суда РФ.

При подготовке данной дипломной работы были использованы такие общенаучные и частно-научные методы как анализ нормативно-правовых актов, отнесенных к теме исследования, обобщения отечественной и

зарубежной правоприменительной практики, синтеза, индукции, дедукции, аналогии, а также сравнительно-правовой метод.

Практическая значимость исследования обусловлена отсутствием единой практики и недостаточной правовой регламентацией процессуального порядка получения сведений из сети Интернет при расследовании уголовных дел о преступлениях в сфере незаконного оборота НС и ПВ.

Структура работы обусловлена предметом, целью и задачами исследования. Работа состоит из введения, двух глав, четырех параграфов, заключения и приложений.

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ О ПРОЦЕССУАЛЬНОЙ ФИКСАЦИИ ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ

1.1 Общие теоретические аспекты оценки доказательственного значения сведений, полученных из сети Интернет по уголовным делам о незаконном обороте наркотических средств и психотропных веществ

В настоящее время во всех сферах нашей жизни происходит тотальная компьютеризация. Невозможно представить современного человека, который бы не пользовался смартфоном, планшетом или ноутбуком, не имел свободного выхода в Интернет. Последние несколько лет преступность также активно стала переходить в сеть, используя различные возможности обмена данными. При сбыте НС и ПВ бесконтактным способом, осуществляемым посредством сети Интернет, остаются определенные следы в виде электронной информации, которые могут быть использованы правоохранительными органами в интересах расследования преступлений.

Следует определить понятие «электронная информация». Статья 2 Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» содержит определения «информации» и «электронного документа». Исходя их данных понятий, можно сделать определенный вывод о понимании значения «электронной информации». Электронная информация — это сведения, представленные в электронной форме, т.е. в виде пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по ИТС или обработки в информационных системах.

В науке также можно встретить смежные термины, например одним из таких считается «компьютерная информация». В соответствии с нормами УК РФ, а точнее примечанием к статье 272 УК РФ - «под компьютерной информацией понимаются сведения (сообщения, данные), представленные в

форме электрических сигналов, независимо от средств их хранения, обработки и передачи». Также данный термин закреплен в Соглашении о сотрудничестве государств – участников СНГ в борьбе с преступлениями с сфере информационных технологий. «Компьютерная информация – информация, находящаяся в памяти компьютерной системы, на машинных или на иных носителях в форме, доступной восприятию компьютерной системы, или передающаяся по каналам связи[1]».

[1] Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (Душанбе, 28 сентября 2018 г.) // СПС Гарант.

Основная особенность компьютерной информации – это возможность ее восприятия человеком не с помощью органов чувств, а опосредованно, при помощи компьютерной техники. Анализируя данные определения, можно сделать вывод о невозможности отождествления данных понятий. Электронную и компьютерную информацию следует соотносить как общее и частное, то есть любая компьютерная информация может считаться электронной, но не любая электронная информация считается компьютерной. Данный факт в первую очередь обуславливает стремительное развитие цифровых устройств (сотовые телефоны, планшеты, фото- и видеокамеры). В связи с этим, на наш взгляд, законодателю следует адаптировать нормативно-правовые акты под современную действительность и исключить употребление термина «компьютерная информация». Исходя из этого, далее в работе будет использоваться термин электронная информация.

Электронную информацию, в зависимости от места нахождения на момент получения к ней доступа, можно разделить на две группы:

1. Электронная информация, содержащаяся на электронном носителе информации;
2. Электронная информация, содержащаяся в сети Интернет (интернет-информация).

Понятие «электронный носитель» содержится в Межгосударственном стандарте ГОСТ 2.051-2013. «Электронный носитель – это материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники[1]». Соответственно можно определить понятие «электронного носителя информации» в уголовном процессе. Это материальный носитель, содержащий значимую для производства по уголовному делу сведения, представленные в электронной форме, воспроизводимые при помощи

[1] Межгосударственный стандарт ГОСТ 2.051 – 2013 «Единая система конструкторской документации. Электронные документы. Общие положения» (введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 22.11.2013 N 1628-ст) // СПС Гарант.

программно-технических средств. То есть, источник информации первичен, а носитель информации чаще всего не является её источником, а лишь содержит в себе данные, принятые от источника.

Процессуальный режим получения и использования сведений, расположенных на электронном носителе информации относительно устоялся. Статья 164.1 УПК РФ регулирует особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий. Она определяет основания изъятия электронных носителей информации при расследовании уголовных дел экономической направленности; порядок копирования информации с изымаемого электронного носителя по инициативе его законного владельца или обладателя; также данная статья предлагает процедуру альтернативную изъятию цифрового устройства – копирование информации.

Содержание интернет-информации сводится к синтезу следующих элементов:

– сведения (например, информация о владельцах доменов, базы данных, содержащих конфиденциальную информацию, сведения о сетевых ресурсах);

– условия, предшествующие обнаружению сведений (например, обнаружение уполномоченными должностными лицами органов внутренних в ходе мониторинга Интернет-ресурсов информации, представляющей оперативный интерес);

– действия по фиксации сведений.

Сведения, расположенные в сети Интернет и представляющие интерес для органов следствия, в научной литературе называют электронно-цифровым следом. Под электронно-цифровым следом в научной литературе принято называть криминалистически значимую информацию, выраженную посредством электромагнитных взаимодействий или сигналов в форме, пригодной для обработки с использованием компьютерной техники, в результате создания определенного набора двоичного машинного кода либо

его преобразования, выразившегося в модификации, копировании, удалении или блокировании, зафиксированная на материальном носителе, без которого не может существовать[1].

В научной литературе предлагаются различные классификации цифровых следов. Так можно применить различные основания:

1. В зависимости от формы:

– текстовые;

– графические (например, изображения);

– звуковые (например, голосовые сообщения).

2. В зависимости от способа доступа:

– информация с локальным доступом – возможность обнаружения и фиксации информации через первоначальный носитель;

– информация с удаленным доступом – возможность доступа и фиксации только путем применения специальных средств, например, выхода в Интернет.

3. В зависимости от характера доступа:

– общедоступная информация, доступ к которой неограничен;

– скрытая при помощи специальных программ;

– зашифрованная.

4. В зависимости от происхождения:

– оставленные человеком непосредственно (например, электронные документы);

– опосредованные (например, факт о регистрации человека на определённом сайте).

5. В зависимости от места нахождения:

– находящиеся непосредственно на технических средствах преступника. Данная информация может быть обнаружена при проведении осмотра места преступления;

[1] Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет: дис. … канд. юрид. наук. – М., 2018. С. 34.

– находящиеся на технических средствах потерпевшего (например, программа-вирус);

– находящиеся на технических средствах иных лиц.

Данное основание классификации не исключает возможности нахождения информации одновременно на нескольких устройствах.

Для информации, расположенной в сети Интернет, характерно наличие следующих признаков:

– опосредованность, так как она не может существовать без материального носителя;

– невозможность материального осязания, так как она является идеальной;

– возможность копирования информации в ее первоначальном виде без утраты каких-либо свойств, причем возможно существование большого количества таких копий;

– возможность удаленного доступа к такой информации;

– возможность доступа несколькими субъектами;

– возможность преобразования в иной формат – например из мультимедийного файла создать скриншот;

– невозможность восприятия без использования специальных технических средств;

– сложность в установлении владельца цифровой информации, иногда и вовсе ее невозможность.

Относительно электронной информации, содержащейся в сети Интернет, прямой нормативной регламентации нет, вследствие чего возникает большое количество споров как у теоретиков, так и у правоприменителей. Использование в доказывании информации, обнаруженной в сети Интернет разнится в зависимости от сложившейся практики на конкретной территории.

Согласно УПК РФ, доказательствами по уголовному делу признаются любые сведения, на основе которых определяется наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу.

В ходе данной работы нами были изучены более трехсот приговоров по уголовным делам о преступления в сфере незаконного оборота НС и ПВ. Из них были отобраны приговоры (100), содержащих интересующую нас информацию, на их основе и была проведена аналитическая работа по данной теме. Анализ приговоров показал, что наиболее часто в качестве доказательств выступает следующая интернет-информация[1]:

– содержание переписки (95 %);

– фотографии НС и ПВ и участков местности (65 %);

– сведения об использовании сервисов, при помощи которых осуществляется оплата НС и ПВ (электронные кошельки, платежные системы, осуществляющие оборот криптовалюты, приложения банков) (30 %);

– сайты с объявлениями о продаже НС и ПВ (25 %)[2].

С позиции содержания данные сведения, несомненно, имеют большое доказательственное значение, однако для их использования в качестве доказательств по уголовному делу необходимо придать им надлежащую процессуальную форму.

Статья 74 УПК РФ не закрепляет такого самостоятельного вида доказательства как электронная информация, а значит для использования ее в

[1] Здесь и далее по тексту приведены результаты исследования приговоров судов общей юрисдикции о преступлениях в сфере незаконного оборота НС и ПВ, размещенных на сайте «СудАкт» [Электронный ресурс] // Судебные и нормативные акты РФ URL : https://sudact.ru/.

[2] См. Приложение №1.

расследовании необходимо отнести ее к уже имеющимся видам доказательств[1].

Механизм изъятия информации, содержащейся в сети, подразумевает под собой конечное размещение на каком-либо носителе, т.е. следователю (дознавателю) необходимо перенести информацию из виртуального пространства в реальное, чтобы использовать такие данные при формировании доказательственной базы. Поэтому, чаще всего, электронную информацию, обнаруженную в Интернете, относят к вещественным доказательствам по аналогии с электронным носителем информации. В соответствии со статьей 81 УПК РФ вещественными доказательствами могут быть признаны любые предметы (т.е. объекты материального мира):

1. Которые служили орудиями, оборудованием или иными средствами совершения преступлениями или сохранили на себе следы преступления;

2. На которые были направлены преступные действия;

2.1 Деньги, ценности и иное имущество, полученные в результате совершения преступления;

3. Иные предметы и документы, которые могут служить средствами для обнаружения преступления и установления обстоятельств уголовного дела.

Очевидно, что интернет-информация не является предметом (т.е. объектом материального мира), а следовательно отнесение таких сведений к вещественным доказательствам просто невозможно. Также важно отметить, исходя из положений УПК РФ, электронный носитель информации будет считаться вещественным доказательством только в случае, если информация, содержащаяся на носителе и интересующая следователя (дознавателя) появляется на USB-флешке или CD-диске независимо от действий лиц, осуществляющих предварительное расследование (не в ходе следственного

[1] Зазулин А.И. Компьютерная информация в уголовном процессе: сущность и способы закрепления в качестве доказательства по уголовному делу / А.И. Зазулин // Проблемы экономики и юридической практики. 2015. С. 131.

действия и не по инициативе следователя). В ч. 3 ст. 164.1 УПК РФ сказано: «К протоколу прилагаются электронные носители информации, содержащие информацию, скопированную с других электронных носителей информации в ходе производства следственного действия». Следовательно, если уполномоченное лицо в ходе производства следственного действия изымает электронную информацию посредством перемещения на собственный электронный носитель, то такой носитель будет являться частью протокола следственного действия, а именно приложением к нему.

Также основным признаком, определяющим вещественные доказательства, является их невосполнимость в случае утраты, например, такого мнения придерживается Е.В. Брянская[1]. Признак невосполнимости также отсекает отнесение электронной информации к вещественным доказательствам, так как она доступна для многократного копирования. В случае утраты электронного носителя, на которое осуществлялся перенос интернет-информации, в большинстве случаев ее можно легко восстановить.

Исходя из вышеперечисленного, мы не можем в полной мере отнести информацию, обнаруженную в сети Интернет к вещественным доказательствам.

Существует точка зрения, что электронная информация должна быть отнесена к иным документам. Под иными документами, в соответствии с ч. 2 ст. 84 УПК РФ, понимаются сведения, зафиксированные как в письменном, так и в ином виде. К ним могут относиться материалы фото- и киносъемки, аудио- и видеозаписи, и иные носители информации. Содержащиеся в Федеральном законе № 149-ФЗ «Об информации, информационных технологиях и о защите информации» понятия документа и электронного документа также позволяют нам отнести электронную информацию к иным документам. Н.В Лантух приводит перечень признаков иных документов, рассматриваемых в качестве доказательств:

[1] Брянская, Е.В. Аргументирующая силу доказательств при рассмотрении уголовных дел в суде первой инстанции / Е.В. Брянская : Иркутск : Изд-во ИГУ, 2015. С. 158.

1. Сведения исходят от определенного юридического либо физического лица, формулируются, отражаются ими в рамках их должностных полномочий, а в ситуации, если они приводятся гражданином, то в границах его установленной информированности;

2. Заключают в себе значимые для правильного разрешения дела сведения;

3. Иные предметы или документы, которые могут помочь выявить факт преступления и раскрыть обстоятельства происшествия;

4. Представлены согласно установленному процессуальному порядку приобщения документа к делу в виде доказательства[1].

Важно отметить, что п. 4 ст. 84 УПК РФ говорит о том, что документы, обладающие признаками перечисленными в ст. 81 УПК РФ должны быть признаны вещественными доказательствами. Электронный документ может содержать в себе следы преступного воздействия, например измененный определенной программой цифровой код, либо документ, содержащий охраняемую законом тайну, к которому был осуществлен незаконный доступ. Такой документ по своей сути обладает признаками вещественного доказательства, но он все же не является объектом материального мира, поэтому его отнесение к вещественным доказательствам также не представляется возможным.

Исходя из данных положений отнесение электронной информации к иным документам представляется наиболее целесообразным и правильным с точки зрения законодательства.

Ученые-процессуалисты в большинстве своем сходятся в необходимости введения в УПК РФ положений относительно электронных доказательств, а также редакции статьи ст. 74 УПК РФ, т.е. расширения перечня видов доказательств.

[1] Лантух Н.В. Содержание и особенности оценки иных документов как отдельного вида доказательств / Н.В. Лантух // Уголовное судопроизводство России и зарубежных государств: проблемы и перспективы развития: материалы международной научно-практической конференции. - Санкт-Петербург: СПУ МВД России. 2021. С. 243-249.

Н.А. Зигура, А.В. Кудрявцева и Е.А. Гамбарова считают электронную информацию самостоятельным видом доказательств, исходя из ее специфической формы, среды существования, механизма формирования и способа введения ее в качестве доказательств в уголовный процесс[1].

А.С. Александров, придерживается позиции необходимости отражения цифровизации жизни, в частности преступности в нормах УПК РФ. Он считает, что система существующих следственных действий непригодна для расследования «информационных (компьютерных) преступлений» и предлагает дополнить кодекс новым универсальным следственным действием «получение цифровой информации, представленной в электронном виде». Такое следственное действие, по его мнению, объединит в себе целый ряд мероприятий и действий, таких как: выемка, осмотр, контроль и запись телефонных и иных переговоров. Санкция суда при этом будет применяться только в случае, когда такое следственное действие будет нарушать охраняемые законом права человека. Также А.С. Александров приводит достаточно широкий перечень лиц, которые могут быть допущены к проведению такого действия: следователь, оперативный сотрудник, сотрудник службы безопасности организации, адвокат, программист, робот (машина). «Не важно кем и как оно совершается, главное результат[2]».

Оппозиционное мнение приводит Л.В. Головко. Он считает, что «никакого нового «вида» доказательств здесь нет, протокол остается протоколом независимо от формы своего изготовления…[3]». В подобном ключе он высказывается и о том, что доказательственную роль в уголовно-процессуальном доказывании играет не сам материальный носитель, а

---

[1] Зигура Н.А. Компьютерная информация как вид доказательств в уголовном процессе России: монография / Н.А. Зигура, А. В. Кудрявцева. М.: Юрлитинформ, 2011. С. 24.

[2] Александров А.С. Учение о следственных действиях на пороге "цифрового мира" / А.С. Александров // Юридический вестник Самарского университета. 2017. № 4. С. 80-85.

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

непосредственно цифровая информация, содержащаяся на нем. Автор отмечает, что в создании специальных электронных доказательствах нет необходимости. Виртуальный мир подвержен постоянному изменению, но это нисколько не отличает его от реального, который также динамичен. А следовательно, подобно тому, как мы стабилизируем события реального мира (протоколы осмотра или обыска, приложения в виде схем, фотоснимков, видеозаписей, вещдоки и т.д.) такие же доказательственные формы мы можем применять и для фиксации виртуальных событий (протоколы осмотров, заключения экспертов …)[1].

На наш взгляд, каждая позиция относительно необходимости внесения изменений в УПК РФ имеет место быть. Нельзя не согласиться с мнением Л.В. Головко об отсутствии необходимости создания каких-либо новых следственных действий, потому что, по большому счету, они просто будут подменять уже существующие, о чем также утверждает и его оппонент А.С. Александров. Но при этом, на лицо острая необходимость разъяснения для правоприменителей моделей и алгоритмов использования уже существующих следственных действий, используемых при взаимодействии с электронной доказательственной информацией. Важно четко и подробно разъяснить какие именно у лица, осуществляющего предварительное расследование, имеются средства для получения электронных доказательств, определить все нюансы изъятия, осмотра, приобщения, хранения электронной информации.

Таким образом, можно сделать вывод о том, наиболее часто в качестве доказательств по уголовным делам в сфере незаконного оборота НС и ПВ выступает интернет-информация: содержание переписок, фотографии НС и ПВ и участков местности, сведения об использовании сервисов, при помощи которых осуществляется оплата НС и ПВ, сайты с объявлениями о продаже НС и ПВ. В соответствии с действующими уголовно-процессуальными нормами, такие интернет-сведения могут быть оценены лицом,

[1] Там же.

осуществляющим предварительное расследование, только в качестве иного документа, либо протокола следственного действия (в т.ч. приложения к протоколу). Выбор в данном случае будет зависеть именно от средства получения интернет-информации. Если следователь (дознаватель) получает такую информацию посредством истребования (скорее всего в данном случае электронная информация будет предоставлена уже на электронном носителе), то такие сведения будут отнесены к иным документам. В случае если имело место производство следственного действия, соответственно данное доказательство будет отнесено к протоколу следственного действия.

1.2 Понятие, содержание и система способов закрепления (фиксации) доказательственной информации, расположенной в сети Интернет

Сбор доказательственной информации, расположенной в сети Интернет, представляет собой сложный процесс. Это связано с тем, что ИТС развиваются достаточно стремительно, законодательство в настоящее время не охватило в полной мере весь тот необходимый для сбора доказательственной информации, расположенной в сети Интернет, порядок. Это вызывает некоторые трудности в правоприменительной практике. Поэтому, в данном параграфе рассмотрим актуальные вопросы, связанные с фиксацией доказательственной информации, расположенной в сети интернет.

Переходя к рассмотрению данных вопросов, отдельное внимание хотелось бы уделить понятийному аппарату. Во-первых, необходимо раскрыть соотношение понятий «доказательства» и «доказательственная информация». Законодатель в ч. 1 ст. 74 УПК РФ дает определение доказательства, согласно которому «доказательствами по уголовному делу являются любые сведения, на основе которых суд, прокурор, следователь, дознаватель в уголовно-процессуальном порядке устанавливает наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по

уголовному делу, а также иных обстоятельств, имеющих значение для уголовного дела[1]».

В научной литературе отмечается, что невозможно изначально рассматривать доказательства как достоверные сведения, так как они носят вероятностный характер. Поэтому, учеными предлагаются собственные варианты рассматриваемого определения. Так, представляется интересной позиция А.А. Климова и Г.А. Павловец, согласно которой «под доказательствами следует понимать любую собранную, проверенную и оцененную в предусмотренном законом порядке информацию, признанную достоверной, на основании которой орган, ведущий уголовный процесс, устанавливает наличие или отсутствие общественно опасного деяния, предусмотренного уголовным законом, виновность лица, совершившего это деяние, либо его невиновность и иные обстоятельства, имеющие значение для правильного разрешения уголовного дела[2]».

Под доказательственной информацией в свою очередь А.Г. Головач в широком смысле понимает: меру связи доказательства с событием, которое им устанавливается, а в узком – получаемую процессуальным путем при производстве следственных действий информацию о расследуемом событии и связанных с ним обстоятельствах, которая составляет содержание доказательств и служит средством доказывания, и используется в процессе доказывания в ходе расследования и судебного рассмотрения уголовных дел[3].

К.З. Шхагапсоев дает следующее определение: «доказательственная информация – это информация, связанная с событием происшествия и

---

[1] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ // СПС КонсультантПлюс

[2] Климов А.А. Доказательства и доказательственная информация: понятие и соотношение / А.А. Климов // ПРАВО.by научно-практический журнал : [Электронный ресурс]. URL: https://journal.pravo.by/articles/ugolovnoe-pravo-kriminologiya-ugolovno- (дата обращения: 10.03.2023).

[3] Головач А.Г. Производство следственных действий по собиранию материально-фиксированной доказательственной информации в районах вооруженного конфликта: автореф. дисс. … канд. юрид. наук : М.: ВУ Министерства обороны РФ. 2010. С. 20.

связанных с ним обстоятельствах, которая может служить средством доказывания и быть использована в процессе доказывания в ходе доследственной проверки преступления, расследования и судебного рассмотрения уголовных дел[1]».

Рассматривая предложенные определения, мы можем понять, что термин «доказательственная информация» несколько шире по значению, так как может включать в себя не только информацию, являющейся содержанием доказательства, но и любую другую информацию о совершенном преступлении. К тому же, доказательственная информация не обладает признаками доказательств и не всегда обличается в процессуальную форму. Следовательно, невозможно говорить о тождественности рассматриваемых понятий. Многие исследователи (О.Я. Баев, В.А. Ниесов, С.В. Зубенко) считают, что доказательства составляют лишь одну из форм доказательственной информации, так как информация, не облеченная в уголовно-процессуальную форму, не может использоваться для доказывания[2].

Также подробнее следует рассмотреть содержание понятий «фиксация» и «собирание» доказательственной информации. Законодательно установлено, что процесс доказывания состоит из собирания, проверки и оценки доказательств. Сам процесс собирания доказательств представляется достаточно сложным, так как может состоять из более мелких действий. Так, Ю.К. Якимович определяет, что собирание доказательств состоит из следующих элементов: обнаружение, изъятие, фиксация (закрепление), приобщение к делу[3].

---

[1] Шхагапсоев К.З. Понятие доказательственной информации и производства следственных действий по ее проверке в районах вооруженного конфликта / К.З. Шхагапсоев. // Пробелы в российском законодательстве. Юридический журнал. 2017. № 2. С. 186.

[2] Баев О.Я. Тактические элементы планирования деятельности по собиранию, исследованию и оценке следственной информации / О.Я. Баев // Избранные работы по проблемам криминалистики и уголовного процесса. Москва : ЭКСМО. 2011. С. 49.

[3] Якимович Ю.К. Доказательства и доказывание в уголовном процессе России: учеб. пособ. Томск: Томский гос. ун-т, 2015. С. 21.

Рассматривая данный вопрос, Л.Д. Кокорев и П.П. Кузнецов утверждают, что «собирание доказательств заключается в поиске и обнаружении сведений о фактах, имеющих доказательственное значение[1]». Они считают, что для того, чтобы какие-то сведения и факты были утверждены в статусе доказательств, необходимо их проверить и процессуально закрепить в протоколах.

В.С. Балакшин также исходит из того, что законодательная формулировка «собирание доказательств» носит более общий характер. Вместо нее, по его мнению, необходимо употреблять иную - «собирание фактических данных и их источников».

Исходя из вышесказанного многие исследователи отмечают несоответствие термина «собирание доказательств» существующим ныне реалиям. Поэтому, большинство авторов склонны утверждать, что необходимо преобразование данной стадии процесса доказывания из собирания в формирование доказательств.

Перейдем к рассмотрению понятия фиксации доказательственной информации. Под фиксацией понимается регламентированная законом деятельность следователя и привлеченных или допущенных к участию в ней других лиц по процессуальному закреплению фактических данных в соответствии с уголовно-процессуальным законодательством[2]. Законодатель выделяет следующие способы фиксации:

- составление протокола следственного действия, который может быть написан от руки или изготовлен с помощью технических средств;
- стенографирование,
- фотографирование,
- киносъемка,
- аудио- и видеозапись.

---

[1] Кокорев Л.Д. Уголовный процесс: доказательства и доказывание: монография / Л.Д. Кокорев, Н.П. Кузнецов. Воронеж : Изд-во Воронеж. ун-та, 1995. С. 105-119.

[2] Белоусов А.В. Проблема фиксации доказательств в досудебных стадиях уголовного процесса России: автореф. дис. … кандит. юрид. наук. М., 2001. С. 11.

Данный перечень является традиционным. В научной литературе встречаются различные классификации способов фиксации доказательственной информации:

1. По содержанию уголовно-процессуального закона:

– обязательные способы (например, составление протокола следственного действия или осуществление фотосъемки трупа).

– факультативные (рекомендованные законом).

2. По содержанию свойств субъекта выполнения:

– субъективные, когда результат напрямую зависит от возможностей лица, его производящего (например, от навыков следователя);

– объективные, когда результат зависит от физико-химических процессов.

В связи с активным переходом преступности в ИТС, расследование таких видов преступлений как незаконное приобретение и сбыт НС и ПВ предполагает постоянную фиксацию электронной доказательственной информации. «Следы» таких преступлений остаются в сети, их обнаружение и изъятие возможно только в электронной форме. Ранее мы уже приводили основной перечень сведений, получаемых правоохранительными органами из Интернета при осуществлении расследования преступлений в сфере незаконного оборота НС и ПВ. Такой информацией можно считать: переписки в социальных сетях, информация с личных аккаунтов пользователей, скриншоты, фотографии НС и ПВ, участков местности, сведения о сетевых ресурсах, доменах и их владельцах, сведения об использовании сервисов, при помощи которых осуществляется оплата НС и ПВ, а также вывод данных денежных средств со счета «продавца».

Основными способами фиксации доказательственной информации, расположенной в сети Интернет выступают:

– нотариальное заверение;

– автоматическая фиксация путем применения различных технических средств;

– исследование специалиста и дача им последующего заключения.

Способы фиксации доказательственной информации, расположенной в сети Интернет также принято делить по содержанию способа. Так, выделяют следующие виды:

– процессуальный – фиксация посредством применения протокола;

– технико-криминалистический – применение в качестве способа фиксации графических, предметных и наглядно-образных форм. В их числе, к примеру, изготовление чертежей, графиков, фотосъемка и другие.

Фиксация информации, расположенной в сети Интернет представляет собой достаточно сложный и трудоемкий процесс. Сложность такой фиксации во многом определяется тем, что законодательное толкование допустимых именно для такого рода информации способов фиксации в уголовно-процессуальном праве отсутствует.

Немного иначе ситуация обстоит в гражданском процессе. В рамках гражданского процесса закрепление информации из сети Интернет практикуется уже достаточно давно. Статья 103 Гражданско-процессуального кодекса РФ (далее – ГПК РФ) напрямую говорит о таком виде закрепления доказательственной информации, содержащихся в Сети как осмотр информации, находящейся в ИТС Интернет. Размещенную в сети информацию оформляют в виде нотариально удостоверенного протокола осмотра доказательственной информации. Нотариус фиксирует текстовую, графическую или иную информацию с указанием всех ссылок, к которым он обратился при протоколировании. Также нотариус фиксирует последовательность, в соответствии с которой осуществлялся осмотр и прикладывает распечатанные страницы Интернет-ресурсов. Важно, чтобы нотариус осуществлял осмотр сайта на сертифицированном оборудовании с

использованием лицензионных программ, эти данные также должны быть отражены в протоколе, подписанном нотариусом[1].

При осуществлении нотариального осмотра сайта нотариус руководствуется ст. 71-76 ГПК РФ. Законность досудебного удостоверения нотариусами доказательств в сети Интернет удостоверена Верховным Судом РФ. Пункт 7 Постановления Пленума Верховного Суда РФ от 15.06.2010 № 16 «О практике применения судами Закона Российской Федерации «О средствах массовой информации» сказано, что «в силу части 1 статьи 102 Основ законодательства Российской Федерации о нотариате … нотариусом могут быть обеспеченны необходимые для дела доказательства (в том числе, посредством удостоверения содержания сайта в сети Интернет по состоянию на определенный момент времени)… [2]».

Также в гражданском процессе существуют и некоторые другие способы фиксации интернет-информации, расположенной в сети Интернет. Среди них можно отметить возможность составления усовершенствованного вида протокола - «протокол автоматизированного осмотра доказательств (ПАОД)». Программный комплекс для автоматической фиксации информации в Интернете функционирует с 2014 года и имеет государственную регистрацию в Роспатенте (текущая версия сервиса от 29.10.2018 г. №2018666835). Согласно п. 55 Постановления Пленума ВС №10 от 23.04.2019 распечатки такого формата как ПАОД подлежат оценке судом при рассмотрении дела наравне с прочими доказательствами (статья 67 ГПК РФ, статья 71 АПК РФ)[3].

---

[1] Ярошенко Т.В. Нотариат и защита прав пользователей в сети «Интернет»: проблемные вопросы / Т.В. Ярошенко // Вестник Балтийского федерального университета им. И. Канта. 2015. № 9. С. 47-52.

[2] О практике применения судами Закона Российской Федерации «О средствах массовой информации» : Постановление Пленума Верховного Суда РФ [от 15.06.2010 № 16] // Российская газета. 2010. 17 июня.

[3] О применении части четвертой Гражданского кодекса Российской Федерации : Постановление Пленума Верховного Суда РФ [от 23.04.2019 № 10] // Российская газета. 2019. 6 мая.

Для составления данного вида документа используется онлайн-сервис «ShotApp.ru». Программа позволяет надлежащим образом заверить интернет-информацию без непосредственного обращения к нотариусу. ПАОД имеет все необходимые реквизиты: дату и время составления, регистрационные сведения о сервисе, составляющем данный протокол, данные, которые позволяют удостоверить подлинность данного документа. Несомненным плюсом использования данного сервиса является его скорость, т.е. пользователь может мгновенно зафиксировать информацию и сформировать протокол осмотра менее чем за 1 минуту. Такая оперативность позволяет исключить возможность удаления информации до ее фиксации, в случае если оппонент осведомлен о ваших намерениях и «заметает следы». Также программа хранит сформированный протокол в неизменном виде в течение 5 лет, что позволяет исключить утрату данной информации.

На данный момент нам не удалось обнаружить информацию об использовании данного сервиса в уголовном процессе. Но очевидно, что создание подобной программы, позволяющей следователю (дознавателю) осмотреть интернет-страницу за 1 минуту, а также досконально зафиксировать информацию, содержащуюся на интернет-ресурсе, значительно облегчит формирование доказательственной базы при расследовании уголовного дела, позволит обеспечить достоверность полученных сведений и их полноту.

Информация, расположенная в сети Интернет обладает свойством изменчивости. Злоумышленники способны быстро модифицировать такого рода информацию, а также сокрыть следы ее существования путем удаления из всемирной паутины. Поэтому использование сервиса «ShotApp.ru» позволило бы также участникам уголовного процесса самостоятельно и моментально фиксировать интернет-сведения, которые в дальнейшем могут иметь значение для уголовного дела.

Интернет-информация – основной источник доказательств по уголовным делам в сфере незаконного оборота НС и ПВ. Такой информацией

является: переписки в социальных сетях, информация с личных аккаунтов пользователей, скриншоты, фотографии НС и ПВ, участков местности, сведения о сетевых ресурсах, доменах и их владельцах, сведения об использовании сервисов, при помощи которых осуществляется оплата НС и ПВ, а также вывод данных денежных средств со счета «продавца». В соответствии с действующими уголовно-процессуальными нормами, уполномоченными лицами, может производиться фиксация интернет-сведений посредством следственных и иных процессуальных действий. Сведения, изъятые из сети, могут быть оценены следователем (дознавателем) как иной документ или протокол следственного действия (в т.ч. приложение к протоколу следственного действия). Применение некоторых способов фиксации интернет-информации, используемых в гражданском процессе, например «протокола автоматизированного осмотра доказательств», облегчило бы формирование доказательственной базы при расследовании уголовного дела, обеспечило бы достоверность полученных сведений и их полноту, позволило бы также участникам уголовного процесса самостоятельно и моментально фиксировать интернет-сведения, которые в дальнейшем могут иметь значение для уголовного дела.

ГЛАВА 2. ПРОЦЕССУАЛЬНЫЕ ПРАВИЛА И ПОРЯДОК ЗАКРЕПЛЕНИЯ ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ, ОБНАРУЖЕННОЙ В СЕТИ ИНТЕРНЕТ, ПРИ РАССЛЕДОВАНИИ НАРКОПРЕСТУПЛЕНИЙ

2.1 Особенности и проблемные аспекты процессуального закрепления информации из сети Интернет при производстве следственных действий по уголовным делам о преступлениях в сфере незаконного оборота наркотических средств и психотропных веществ

В соответствии со ст. 86 УПК РФ собирание доказательств осуществляется должностным лицом путем производства следственных и иных процессуальных действий. Составление протокола следственного действия как способ фиксации доказательственной информации, обнаруженной в сети Интернет, считается самым распространенным. Данное высказывание также подтверждается анализом приговоров судов общей юрисдикции по делам о незаконном обороте НС и ПВ (92 %)[1].

Особую актуальность вопрос о фиксации сведений в сети Интернет приобрел с 1 января 2013 года, когда были внесены изменения в ч. 2 ст. 228.1 УК РФ[2]. Таким образом, «Сбыт наркотических средств, психотропных веществ или их аналогов, совершенный с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет»)» стал самостоятельным квалифицирующим признаком состава преступления.

В науке наиболее эффективным методом преодоления сложных ситуаций расследования считается ситуационно обусловленный алгоритм. Ситуационный подход в криминалистике – это один из ведущих методов концепций, который позволяет разрабатывать алгоритмы расследования

[1] См. Приложение №2.

[2] Федеральный закон от 01.03.2012 г. № 18-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // СПС Гарант.

преступлений, совершенных в сложных криминальных ситуациях. Исследованием ситуационного подхода активно занимались Р.С. Белкин, Т.С. Волчецкая, С.Э. Воронин, Д.В. Ким и другие. Предлагаем в данном параграфе рассмотреть процессуальные проблемы закрепления интернет-сведений посредством составления протокола следственного действия, применив ситуационный подход.

Существуют различные исходные ситуации при фиксации доказательственной информации, расположенной в сети Интернет:

1. Изъято устройство (сотовый телефон, ПК), при помощи которого лицо осуществляло преступную деятельность в сфере незаконного оборота НС и ПВ;

1.1 Следственные органы располагают данными, при помощи которых осуществлялась аутентификация и идентификация пользователя;

1.2 У следственных органов отсутствует информация о данных, при помощи которых осуществлялась аутентификация и идентификация пользователя;

2. Органы следствия не располагают устройством, с использованием которого подозреваемый выходил в сеть.

2.1 Известно, что необходимые сведения находятся в общедоступном Интернете;

2.2 Доступ к информации, интересующей органы предварительного расследования затруднен (информация находится в теневом интернете «darknet»).

Ситуация 1. У следователя (дознавателя) имеется изъятое ранее электронное устройство, при помощи которого подозреваемый (обвиняемый) осуществлял преступную деятельность в сфере незаконного оборота НС и ПВ. При этом также имеется информация о паролях и логинах пользователя (допрос лица, осмотр предмета – сотового телефона, ПК; данные ОРД).

Часто информация о нахождении какой-либо информации в сети Интернет появляется в уголовном деле посредством проведения допроса

лица, причастного к совершению преступления в сфере незаконного оборота НС и ПВ. В 67 % изученных приговоров[1] протокол допроса лица – владельца устройства, участника следственного действия, иного лица, имеющего отношение к расследуемому уголовному делу, является средством подтверждения наличия сведений, уже полученных в ходе проведения осмотров. Наиболее часто встречающиеся данные, которые устанавливаются в ходе допроса: кому принадлежит устройство, какие на нем установлены программы, для чего они использовались, с какими лицами велась переписка и посредством каких мессенджеров, какие сайты посещало лицо и иные интересующие следствие вопросы.

Так, согласно приговору Московского областного суда от 10 августа 2020 г. № 2-61/2020 обвиняемые Киселев и Боев совершили незаконное производство наркотических средств группой лиц по предварительному сговору, в особо крупном размере. Киселев в протоколе допроса подтверждает, что именно ему принадлежат изъятые в ходе следственных действий и оперативно-розыскных мероприятий (далее – ОРМ) устройства, подробно объяснил, как он использовал программы «Xabber», «VIPole» для связи с приобретателями наркотиков, каким образом он создавал свою учетную запись в данных программах и так далее[2].

Но, насколько целесообразно учитывать данный протокол в вопросе закрепления интернет-сведений? Целью допроса является получение от лица информации об обстоятельствах, имеющих значение для уголовного дела. Источником информации в данном случае будет являться конкретный человек и его субъективное восприятие отдельных событий. Показания данные лицом в ходе допроса нуждаются в проверке, и подтверждении различными следственными действиями, запросами в различные

[1] См. Приложение №2.

[2] Приговор Московского областного суда г. Красногорск от 10.08.2020 № 2-61/2020 [Электронный ресурс] // Судебные и нормативные акты РФ URL : https://sudact.ru/regular/doc/8gaUrkBtCqNr/?regular-txt=&regular-case_doc=2-61%2F2020&regular- (дата обращения: 20.04.2023).

организации, и ОРМ. Мы считаем, что его нельзя в полной мере назвать средством фиксации интернет-информации, так как его используют только в качестве дополнительного подтверждения информации, обнаруженной на изъятом устройстве или в сети Интернет.

Наиболее распространенным следственным действием, при помощи которого можно осуществить фиксацию доказательственной информации является осмотр. В случае обнаружения интернет-информации, представляющих интерес, она может быть скопирована на специальный носитель (CD-диск, USB-носитель) уполномоченным лицом, о чем в протоколе осмотра будет сделана соответствующая запись. Носители информации также будут приобщены к протоколу.

При анализе приговоров судов общей юрисдикции, в которых интернет-информация закреплялась при помощи такого следственного действия как осмотр, в 40 % приговорах[1] использовался именно осмотр предмета, при этом лишь в 6 приговорах было указано о протоколе осмотра документов. Свою позицию по данному вопросу мы подробно изложили в первом параграфе. Согласно нормам уголовно-процессуального законодательства, наиболее целесообразно использовать такой вид следственного действия как осмотр документа.

В 12 % изученных приговоров использовалась такая формулировка как «протокол осмотра интернет-страницы», реже встречалась «протокол осмотра интернет-ресурса» - 8%[2].

Так, в тексте приговора Ленинского районного суда г. Пензы (Пензенская область) от 16 декабря 2019 г. по делу № 1-259/2019 при перечислении имеющихся доказательств, подтверждающих виновность лица по п. «г» ч. 4 ст. 228.1 УК РФ сказано: «Из протокола осмотра интернет-ресурса от 20 мая 2019 года, следует что была осмотрена интернет страница сайта «Hydra», в ходе которого зафиксировано, что в данном Интернет-

[1] См. Приложение №2.
[2] См. Приложение №2.

ресурсе производится незаконный оборот наркотических средств, оборот жидкостей, прекурсоров и приспособлений для синтеза наркотических средств...[1]».

В научной литературе активно обсуждаются тактические вопросы проведения осмотра интернет-ресурса, а также содержание такого протокола. В.Д. Еськов и С.А. Чеботарев отмечают, что протокол осмотра интернет-ресурса должен содержать:

1. Описание технических средств, использовавшихся при осуществлении осмотра;
2. Описание программных средств, использовавшихся при осуществлении осмотра;
3. Указание на провайдера, предоставляющего услуги доступа к сети Интернет;
4. Маршрут доступа к странице в следующем виде: через доменные имена и по IP[2].

Использование формулировки «протокол осмотра интернет-ресурса» в описательной части приговоров суда, а также активного обсуждения тактики проведения и составления протокола осмотра интернет-ресурса в научной литературе позволяет сделать вывод о фактическом расширении перечня видов такого следственного действия как осмотр, несмотря на то что законом такой вид осмотра прямо не предусмотрен.

Также встречаются случаи закрепления интернет-сведений посредством осмотра места происшествия – 2%[3]. Согласно 176 статье УПК РФ целью осмотра места происшествия является обнаружение следов преступления, выяснения других обстоятельств, имеющих значение для

[1] Приговор Ленинского районного суда г. Пензы от 16.12.2019 № 1-259/2019 [Электронный ресурс] // Судебные и нормативные акты РФ URL: https://sudact.ru/regular/doc/Yeyniw1XbblX/?regular-txt=&regular- (дата обращения: 15.04.2023).

[2] Еськов В.Д. Особенности осмотра страниц в сети Интернет / В.Д. Еськов, С.А. Чеботарев // Материалы VI Международной науч. конф. студентов и магистрантов. Симферополь. 2017. С. 39-40.

[3] См. Приложение №2.

уголовного дела. Традиционно местом преступления по общеуголовным преступлениям признают участок местности, в пределах которого были обнаружены следы совершенного преступления. В то же время по исследуемым видам преступлений необходимо говорить, что преступление могло быть совершено не только в месте обнаружения следов преступления, но и в любом другом месте. Если преступление было реализовано посредством компьютерных технологий и использования ресурсов ИТС Интернет, место преступления становится не таким строго определенным, в связи с чем обнаружение и фиксацию важной для следствия информации необходимо осуществлять также и в иных местах[1].

Мы считаем, что в данном случае вполне допустимо признать местом происшествия – интернет-страницу, посредством которой осуществлялась преступная деятельность. Рекомендуется к данному протоколу прикладывать видеозапись «рабочего стола», фиксирующую именно действия на экране устройства (например, при помощи программы для записи экрана «Screen Recorder»), а также фототаблицу, содержащую снимки с экрана «скриншоты», документирующие изображения и текст на осматриваемом ресурсе[2].

Так в приговоре Железнодорожного районного суда г. Пензы от 11.02.2020 № 1-51/2020 указано: «Согласно протоколу осмотра места происшествия от 31 мая 2019 года с фототаблицами … был осуществлен вход на учетную запись Бычкова М.В. на сайте https://hydraruzxpnew4af.onion.bio/, введен логин «sahamili610», пароль (который сообщил Бычков М.В.), открыта страница пользователя «Роман610», создана дата, при выборе вкладки «Мои заказы» открывается

[1] Ялышев С.А. Об особенностях осмотра места происшествия по уголовным преступлениям, совершенным с использованием ресурсов интернет / С.А. Ялышев // Ученые записки Санкт-Петербургского филиала Российской таможенной академии имени В.Б. Бобкова. 2021. № 1. С. 108.

[2] Болвачев М.А. О следственных дейтвиях по делам о преступлениях экстремистской направленности в социальных сетях / М.А. Болвачев // Известия Тульского государственного университета. Экономические и юридические науки. 2022. С. 100.

история заказов пользователя. дата в 19:57 имеется запись о переводе денежных средств в биткоинах за оплату позиции «Вакансия Курьер». При выборе вкладки «Futurama Planet Exspress» осуществляется переход на интернет-ресурс, где в разделе- вкладке «Адреса на модерации» обнаружено описание адресов с закладками с наркотическими средствами…[1]».

Также необходимо рассмотреть вопрос использования «скриншотов» как средства фиксации сведений в сети Интернет. Скриншот – это изображение информации, транслируемой на экран электронного устройства (смартфона, ПК и т.д.), получаемый при помощи определенной комбинации клавиш. На практике такие изображения создаются в ходе производства следственного действия, посредством которого изымается информация с электронного устройства. Изображения распечатываются и приобщаются к протоколу следственного действия в качестве приложений, которые заверяются печатью и удостоверяются подписью следователя. Такое оформление, как правило, не создает вопросов о допустимости.

Н.Ю. Емельянова и Б.Б. Рахмонбердиев приводят классификацию скриншотов в зависимости от того, какая именно информация, находящаяся на электронном устройстве, может быть обнаружена и изъята следователем (дознавателем):

1) скриншоты, полученные из социальных сетей;
2) скриншоты, подтверждения переводов денежных средств;
3) скриншоты, полученные из мессенджеров (переписок);
4) скриншоты – документы[2].

Также не стоит забывать, что скриншоты, как и любые другие доказательства, должны соответствовать требованиям относимости,

[1] Приговор Железнодорожного районного суда г. Пензы от 11.02.2020 по делу № 1-51/2020 [Электронный ресурс] // Судебные и нормативные акты РФ URL : https://sudact.ru/regular/doc/DrXd9RsUQKbK/?regular-txt=&regular-case_doc (дата обращения 20.04.2023).

[2] Емельянова Н.Ю. Проблемы применения отдельных видов доказательств в уголовном судопроизводстве / Н.Ю. Емельянова, Б.Б. Рахмонбердиев // Закон и право. Московский университет МВД России им. В.Я. Кикотя. 2022. № 8. С. 141.

допустимости и достоверности в соответствии с ч. 1 ст. 88 УПК РФ. Предполагается, что для подтверждения достоверности скриншота уполномоченному лицу следует также сохранить изображение и в электронном виде, т.е. посредством перемещения их на электронный носитель информации.

Еще одним распространенным способом фиксации доказательственной информации из сети Интернет является проверка показаний на месте. Согласно статье 194 УПК РФ, при проверке показаний на месте лицо, наглядным образом демонстрирует свои действия или действия других лиц, на месте, связанном с исследуемым событием. Так, при изучении приговоров по уголовным делам о незаконном обороте НС и ПВ, совершенных с использованием сети Интернет, проверка показаний на месте приводится в 22 % изученных приговоров[1].

Например, приговор Серовского районного суда Свердловской области от 09 сентября 2019 года № 1-435/2019, в котором указано на то, что обвиняемый в совершении незаконного приобретения, хранения без цели сбыта наркотического средства в значительном размере, в ходе проверки показаний на месте указал на сайт, а также продемонстрировал порядок действий по приобретению и последующей оплате наркотических средств[2]. Проведение данного следственного действия позволяет более детально установить порядок действий лица в сети Интернет, а также зафиксировать информацию, находящуюся в ИТС.

Однако возникает закономерный теоретический вопрос – как определить «место» производства проверки, если необходимо исследовать информацию в Интернете? Возможность проведения проверки показаний в сети Интернет мало изучена в научной литературе и при этом активно

[1] См. Приложение №2.

[2] Приговор Серовского районного суда Свердловской области от 09.09.2019 № 1-435/2019 [Электронный ресурс] // Судебные и нормативные акты РФ URL : https://sudact.ru/regular/doc/cePnOQEJzKO/?regular- (дата обращения: 20.04.2023).

используется как средство получения доказательств при расследовании наркопреступлений.

В данном случае может быть применена позиция доктора юридических наук А.С. Ялышева о понимании «места» относительно проведения осмотра места происшествия[1]. Интернет-страница является местом, связанным с исследуемым событием и, следовательно в теории местом проведения проверки показаний может считаться адрес интернет-ресурса, на котором осуществлял преступную деятельность подозреваемый (обвиняемый).

На практике же, так как проверка показаний на месте проводится посредством электронного устройства – компьютера следователя (иного лица), имеющего выход в сеть Интернет, местом проведения в данном случае указывается место выхода в Интернет, т.е. помещение, в котором оно будет производится (например, кабинет следователя).

В 93% изученных приговоров[2] судов общей юрисдикции за 2019-2022 гг. сбыт наркотического средства осуществлялся бесконтактным способом, а переговоры между закладчиками, их координаторами, диспетчерами и покупателями велись посредством переписки в мессенджере. А.Л. Карлов, Ю.Л. Пахорукова считают, что важным моментом при проведении процессуальных действий по уголовным делам в сфере незаконного оборота наркотиков является фиксация полученной в ходе данных действий интернет-переписки. Авторы определяют, что интернет-переписка представляет собой «обмен текстовыми сообщениями, а также файлами различного содержания между пользователями посредством сети Интернет[3]».

В своей монографии В.Ю. Стельмах, О.М. Ефремова и В.Ф. Васюкова указывают, что на сообщения, направленные посредством электросвязи в

[1] Ялышев С.А. Указ. соч. С. 108.

[2] См. Приложение №2.

[3] Карлов А.Л. Процессуальная фиксация интернет-переписки в качестве доказательств по уголовным делам о преступлениях в сфере незаконного оборота наркотиков / А.Л. Карлов, Ю.Е. Пахорукова // Вестник Сибирского юридического института МВД России. 2016. №4 (25). С. 112.

открытых мессенджерах (форумы, чаты, соцсети), режим тайны связи не распространяется, поскольку в данном случае отправитель, сознавая открытый характер указанных способов коммуникации, стремится сделать свое сообщение доступным неограниченному кругу лиц. В данном случае должностному лицу и не требуется специальное разрешение, санкционируемое судом, поскольку информация находится в открытом доступе. Но на сообщения, направляемые по закрытым мессенджерам, режим тайны связи должен распространяться поскольку данные средства и способы общения изначально предполагают участие строго определенных лиц. В данном случае необходимо понимать является данная переписка служебной или личной[1].

В случае если личная переписка велась со служебного аккаунта, работодатель имеет право на получение данной переписки в полном объеме, поскольку данные сообщения не относятся к тайне связи. Служебная почта принадлежит конкретной организации и должна использоваться только для выполнения служебных обязанностей[2]. Соответственно данная информация изымается следователем (дознавателем) посредством выемки носителей с данной перепиской либо произвести ее осмотр в присутствии работодателя или его представителя.

А.Л. Карлов и Ю.Е. Пахорукова считают, что, в случае если переписка велась с личного аккаунта, то письменно заверенного в присутствии защитника или адвоката разрешения на ознакомление от лица – владельца интернет-переписки достаточно и судебного санкционирования такие действия не требуют[3]. В случае же если лицо – владелец интернет-переписки не дает согласия на ознакомление следователя (дознавателя) с данными

[1] Стельмах В.Ю. Производство следственных действий, направленных на получение и использование компьютерной / В.Ю. Стельмах, О.М. Ефремова, В.Ф. Васюков. – Москва: МГИМО, 2023. С. 205.

[2] Чтение служебной переписки : [Электронный ресурс]. – URL: Служебная переписка сотрудников (glavbukh.ru) (дата обращения 15.04.2023).

[3] Карлов А.Л., Пахорукова Ю.Е. Указ. соч. С. 113.

переписки, то судебное санкционирование считается обязательным в соответствии с ч. 2 ст. 23 Конституции РФ.

Стоит отметить, что проблемы фиксации интернет-переписки могут быть связаны и с техническими барьерами. Так, в качестве примера рассмотрим материалы уголовного дела № 1-641/202 (42001950012000100) в отношении Г, которая обвинялась в совершении преступлений, предусмотренных ч. 2 ст. 210, ч. 3 ст. 30, пп. «а», «г» ч. 4 ст. 228.1 УК РФ. Согласно материалам дела обвиняема состояла в крупном преступном сообществе по сбыту наркотических средств. Для привлечения новых членов сообщества, рекламы наркотических средств, а также для установления контроля за действиями иных участников была создана программа для обмена сообщениями. Особенностью данной программы являлось анонимность пользователей защиту от прослушивания, шифрование передаваемых текстовых, графических и голосовых сообщений. Стоит отметить, что разные структурные подразделения сообщества использовали разные программы. Помимо этого, существовали и иные меры конспирации:

- специальные требования к компьютерной технике (программу можно было установить не на всех технических средствах);

- использование sim-карт, оформленных на третьих лиц, которые не были осведомлены об этом;

- использование банковских карт, также зарегистрированных на третьих лиц, которые не были осведомлены об этом.

При расследовании данного уголовного дела сложностью для следственных органов явилось то, что в преступном сообществе действовало обязательное правило – вся переписка удаляется и не подлежит сохранению ни на каких устройствах. Именно поэтому, следствием на момент вынесения

приговора в отношении Г. не были установлены главные лица данного преступного сообщества[1].

Так, в качестве другого примера рассмотрим материалы уголовного дела в отношении Л., обвиняемого в совершении преступлений, предусмотренных п. «г» ч. 4 ст. 228.1, п. «г» ч. 4 ст. 228.1, ч. 2 ст. 228 УК РФ. Согласно материалам дела Л. вступил в преступный сговор с неустановленным лицом через программу мгновенного обмена сообщениями «Telegram». Сам Л. не знал личности данного лица, а знал лишь только его никнейм. Сложностью для следствия стала такая особенность мессенджера, посредством которого общались Л. и его пособник – интернет-переписка удалялась, что послужило причиной невозможности фиксации в материалах дела элементов данной переписки[2].

Как показывают примеры, наркоторговцы используют специальные программы и шифры для того, чтобы скрыть информацию о причастных лица. Порой участники преступного сообщества не знают лично остальных, так как в данных программах используется система анонимных сообщений. Одной из такой программ является программа «Xabber». В данной программе возможна регистрация по номеру телефона, а как мы можем заметить, преступники чаще всего регистрируют сотовые номера на «подставных» лиц.

Компьютерные экспертизы. Следует отметить, что в уголовном процессе допустимо использование не только компьютерно-технической, но и компьютерно-сетевой экспертизы. Е.Р. Россинская отмечает, что объектами данной экспертизы являются подключенные к сети интернет-устройства

[1] Приговор Абаканского городского суда от 15.06.2020 № 1-641/2020 [Электронный ресурс] // Судебные и нормативные акты РФ URL : https://sudact.ru/regular/doc/GbTlHkUPbNLK/ (Дата обращения: 21.04.2023).

[2] Приговор Вологодского городского суда от 19.02.2019 № 1-170/2019 [Электронный ресурс] // Судебные и нормативные акты РФ URL : https://sudact.ru/regular/doc/Vj8SoSfptRlu/ (Дата обращения: 21.04.2023).

различной конфигурации, ресурсы интернет-провайдеров и предоставляемые ими информационные услуги[1].

Анализ уголовных дел показал, что данная экспертиза, как правило, назначается в ситуациях, когда применение ИТС прямо указано законодателем в диспозиции статьи УК РФ, в качестве квалифицирующего признака состава преступления. Для назначения такого вида экспертизы достаточно сложно составить перечень вопросов для эксперта. Специфика данного исследования заключается в том, что по сути эксперту надо оценить информацию из интернет-ресурса, а не отвечать на вопросы. Также фактически у эксперта отсутствует возможность физического осязания объекта исследования, так как информация, расположенная в сети интернет обладает идеальным, а не материальным признаком.

А.А. Бессонов выделяет такой вид криминалистической экспертизы, как «судебная информационно-аналитическая экспертиза, исследующая информацию о соединениях абонентов и (или) абонентских устройств как по отношению к конкретным лицам, так и по массиву телефонных соединений в месте преступления в интересующий следствие период[2]». Данный вид исследования позволяет эксперту на основе изучения и анализа цифровых следов пользователей ИТС составить схему таких пользователей друг с другом, установить номера, IP-адреса и иные идентификационные признаки, позволяющие соотнести действия, совершаемые с помощью того или иного электронного устройства, с конкретным лицом и (или) с некоторой степенью точности установить место нахождения такого лица[3]. Данный вид экспертизы предполагает предоставление эксперту ранее полученных

---

[1] Россинская Е.Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе : монография / Е.Р. Россинская. – М.: Норма: Инфра-М, 2018. С. 200.

[2] Бессонов А.А. Особенности использования специальных знаний при расследовании незаконной добычи рыбных ресурсов / А.А. Бессонов // Эксперт-криминалист. 2015. № 3. С. 3-5.

[3] Сысенко А.Р. Проблемы назначения и производства судебной компьютерно-технической экспертизы / А.Р. Сысенко, И.С. Смирнова, С.Е. Тимошенко // Сибирское юридическое обозрение. 2020. № 4. С. 523-533.

сведений, однако как мы полагаем, некоторые из этих сведений в перспективе он мог бы получать самостоятельно при проведении компьютерно-сетевой экспертизы.

Интервьюирование сотрудника эксперта-криминалиста ЭКЦ ГУ МВД России по Красноярскому краю показало, что компьютерно-сетевая и судебная информационно-аналитическая экспертизы, как правило не применяются на практике в следствие отсутствия соответствующих методик их проведения. Данные экспертизы имеют огромный потенциал, их применение на практике позволило бы облегчить сбор доказательственной информации необходимой для изобличения лиц, осуществляющих незаконный оборот НС и ПВ, а также в значительной степени уменьшило бы срок проведения предварительного расследования.

Но бывают случаи, когда владелец интернет-аккаунта отказывается предоставить аутентификационные данные, а осмотр данных памяти электронного устройства и проведенные ОРМ также не позволили получить их. В данном случае следователь (дознаватель) может установить интернет-сведения, представляющие интерес расследования для уголовного дела посредством проведения выемки сведений у администратора интернет-ресурса, при помощи которого была размещена информация.

Производство выемки регулируется ст. 183 УПК РФ. На практике встречаются случаи проведения выемки электронной информации, представленной сотрудниками компаний – поставщиков определенных услуг. В ходе такой выемки изымаются электронные носители информации с файлами, имеющими значение для уголовного дела. Согласно законодательству РФ, социальные сети обязаны хранить и собирать определенную информацию (местоположение, регистрационные данные, история посещений и данные об устройстве, сообщения, медиафайлы и т.д.). Организация обязана предоставлять информацию государственным органам также по их официальным запросам – при наличии законных оснований.

Одной из существующих проблем использования такого способа изъятия интернет-информации часто является удаленность нахождения серверов организаций. Так, например, при осмотре интернет-ресурса, например, какого-либо сайта, необходимые для следствия страницы будут запечатлены при помощи фото- и видеосъемки. Данные материалы также приобщаются к такому протоколу осмотра. Например, ООО «В Контакте» на данный момент имеют собственные дата-центры только в Москве и Санкт-Петербурге, что делает достаточно затруднительным их взаимодействие с отделами иных субъектов России. Представляется, что в данном случае следователь может воспользоваться одним из следующих способов:

1. Дать соответствующее поручение о производстве отдельных следственных действий либо следователям, которые работают по месту нахождения компании, предоставляющей услуги социальной сети, либо органу дознания в порядке ч. 4 ст. 21 и п. 4 ч. 2 ст. 38 УПК РФ;

2. Дать поручение органу дознания по месту нахождения компании, предоставляющей услуги социальной сети, о проведении ОРМ, направленных на получение указанной информации, в порядке ч. 4 ст. 21 и п. 4 ч. 2 ст. 38 УПК РФ и п. 3 ст. 7 Федерального закона «Об оперативно-розыскной деятельности»;

3. Направить запрос в компанию, предоставляющую услуги социальной сети, о предоставлении такой информации в порядке ч. 4 ст. 21 УПК РФ (при этом по запросу может быть получена далеко не вся необходимая следствию информация)[1].

Второй и третий варианты более детально будут рассмотрены во втором параграфе данной главы.

Что касается удаленности серверов, данный аспект следует рассматривать совместно с проблемой отсутствия международного сотрудничества в рассматриваемой области. Часто преступники для того,

[1] Денисов Е.А. Проблемы изъятия криминалистически значимой информации у компании, предоставляющей услуги социальной сети / Е.А. Денисов // Вестник Московского университета МВД России. 2018. № 2. С. 103.

чтобы усложнить путь установления принадлежности доменов сайтов конкретному лицу, регистрируют их в иностранных государствах. Данное обстоятельство вызывает сложности при необходимости фиксации информации, а также получения доступа к такой информации следственными органами. У РФ имеется множество международных соглашений о взаимной правовой помощи по уголовным делам, в том числе и с Соединенными Штатами Америки от 17.06.1999, однако ввиду сложной геополитической обстановки запросы могут остаться без ответов. Такое положение во многом объясняется тем, что отсутствуют международно-правовые нормы, регулирующие порядок передачи компьютерной и (или) цифровой информации между иностранными государствами[1].

Еще одной проблемой является ограниченный срок хранения истории пользователей самими серверами. Так, например, в России в соответствии с п. 3 ст. 10.1 ФЗ «Об информации, информационных технологиях и о защите информации» организатор распространения информации в сети Интернет обязан хранить переписку российских пользователей в течении шести месяцев, а другую информацию о них (информация о фактах приема, передачи, доставки и обработки голосовой информации, письменного текста, изображений, звуков и т.д.) – в течение года с момента окончания осуществления таки действий.

На практике, не редки случаи выявления преступления и возбуждения уголовного дела по истечению некоторого срока после совершения непосредственно самих преступных действий, даже по ч. 1 ст. 228 УК РФ в соответствии с п. «а» ч. 1 ст. 78 УК РФ предусмотрен срок давности привлечения к уголовной ответственности – 2 года. В таком случае существует реальная возможность утраты важных для следствия сведений ввиду истечения срока хранения интересующей информации сервером. В действующем законодательстве нет указаний на незамедлительность

[1] Россинская Е.Ф. Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров / Е.Ф. Россинская, Т.А. Сааков // Криминалистика: вчера, сегодня, завтра. 2020. № 3 (15). С. 114.

фиксации информации, находящейся в сети, в том числе и при проверке сообщения о преступлении. В соответствии с УПК РФ проверка сообщения о преступлении осуществляется в срок не позднее 3 суток со дня поступления сообщения, с возможностью продления до 10 и 30 суток. За установленный ст. 144 УПК РФ срок информация, содержащаяся в Интернете, может быть утрачена полностью, либо частично изменена, что по своей сути нарушает права участников уголовного судопроизводства.

Так, Е.К. Губарева и Т.А. Калентьева отмечают, что основной проблемой изъятия информации из сети Интернет является то, что виновный может удалить информацию из сети Интернет, в том числе, если ему станет известно о том, что его противоправными действиями заинтересовались следственные органы[1]. В своей работе авторы предлагают внести изменения в кодекс, дополнив ч. 1 ст. 144 УПК РФ указанием на незамедлительность и неотложность осмотра и фиксации информации, которая может быть утрачена за небольшой промежуток времени, при поступлении сообщения о преступлении, в том числе информации, содержащейся в сети Интернет. Мы считаем данное предложение не оправданным, так как данная статья регламентирует общие положения (сроки и порядок) проверки сообщений о преступлении, а не специфику проведения отдельных следственных действий.

Отдельного внимания при изучении данной темы заслуживает возможность извлечения интернет-сведений из облачного хранилища. Понятие «облачного хранилища», а также особенности изъятия информации с него отсутствуют в уголовно-процессуальном законодательстве России. Облачные носители информации представляют собой хранилища данных, предоставляющие независимым друг от друга пользователям услуги по

[1] Губарева Е.К. Особенности фиксации информации, содержащейся в сети Интернет / Е.К. Губарева, Т.А. Калентьева // Вестник Волжского университета им. Татищева. 2019. №2. С. 165.

хранению информации на единой технологической платформе[1]. Отметим, что в случае, если следователь (дознаватель) располагают информацией о логине и пароле, изъятие данных не представляется затруднительным и осуществляется посредством действий, указанных ранее в параграфе при изучении первой ситуации.

Очень часто на сотовых телефонах предусмотрено постоянное автоматическое резервное копирование данных в облачное хранилище. Это нужно в первую очередь для того, чтобы обезопасить владельца от потери важной информации с устройства в случае его поломки или потери к нему доступа. Многие пользователи даже не задумываются о том, что при удалении информации непосредственно из памяти устройства, такие данные могут все еще могут находиться в базе данных хранилища.

Так в приговоре Дзержинского районного суда г. Ярославля от 23.04.2020 г. № 1-84/2020 в перечне доказательств указано: «протокол осмотра предметов (документов) … которым осмотрен сотовый телефон «Honor» с двумя сим-картами сотовых операторов «МТС» № и «Йота» №, в ходе осмотра которого установлено облачное хранилище, зарегистрированное под именем «ФИО1 makov», где сохранены фотографии участка местности с географическими координатами - «тайников» с наркотическим средством, оборудованных…[2]». Следствию удалось обнаружить доказательства преступной деятельности как раз посредством изучения облачного хранилища устройства.

Основные проблемы, связанные с изъятием информации из такого хранилища:

1. Удаленность сервера, на котором хранится информация;

---

[1] Васюков В.Ф. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий / В.Ф. Васюков, В.В. Лукьянова, В.Н. Береснев. – Москва: Академия управления МВД России, 2019. С. 105.

[2] Приговор Дзержинского районного суда г. Ярославля от 23.04.2020 № 1-84/2020 [Электронный ресурс] : Судебные и нормативные акты РФ URL : https://sudact.ru/regular/doc/DIqKzHQMhLZq/?regular- (Дата обращения: 21.04.2023).

2. Возможность получения доступа к хранилищу с любого устройства, посредством авторизации при помощи логина и пароля;

3. Шифрование информации на всех этапах передачи и хранения (у источника, при передаче от пользователя к серверу, при хранении в базе данных).

Экспертами широко используются специальные аппаратно-программные комплексы для обнаружения и извлечения криминалистически значимой информации, в том числе и из облачных хранилищ по логину паролю. Но в условиях постоянного развития информационных технологий, такие устройства как «Мобильный криминалист» считаются достаточно устаревшими и не позволяют извлекать информацию с более современных моделей устройств. Существуют и другие программы позволяющие получить доступ к облаку при отсутствии аутентификационных данных, например «UFED Cloud Analyzer». Но все они на данный момент функционируют на платформе «Windows» (с 2020 года госорганы России в рамках импортозамещения перешли на отечественное программное обеспечение «Astra Linux»), что тоже является своего рода проблемой.

В соответствии с проведенным анализом приговоров по делам в сфере незаконного оборота наркотиков в 40 % случаев[1] фигурируют электронные кошельки и так называемые крипто-кошельки. Они активно используются как сбытчиками, так и приобретателями, так как позволяют анонимно осуществлять транзакции и пополнять счет наличными через различные терминалы. Точнее такая возможность существовала до 3 августа 2020 года.

В соответствии с п. 2.1 ст. 7 ФЗ от 27.06.2011 № 161-ФЗ «О национальной платежной системе», пользователи электронных кошельков для внесения наличных на счет обязаны пройти идентификацию через предоставление паспортных данных и привязать к кошельку банковский счет. Такое нововведение было обусловлено борьбой с финансированием терроризма и распространением наркотиков. Не стоит забывать о

[1] См. Приложение №2.

персональных данных законопослушных граждан, которые могли попасть в открытый доступ, например, посредством «слива» данных в сеть. При этом все еще имеется возможность создания анонимного электронного кошелька, а значит и получения денежных средств за свою преступную деятельность посредством перевода безналичных денежных средств.

Помимо этого, затрудняется фиксация информации, когда в качестве средства платежа используются биткоины или иная другая криптовалюта. Электронные кошельки легко могут быть зарегистрированы на подставных лиц и достаточно сложно бывает вычислить и зафиксировать информацию о настоящем владельце электронного кошелька.

Так, способ оплаты биткоинами использовал гражданин А, у которого имелся преступный умысел, направленный на незаконный сбыт наркотических средств в крупном размере заранее неопределенному кругу лиц. Однако, следствию удалось вычислить владельца электронного кошелька и установить его причастность к совершению данного преступления[1].

Таким образом, мы видим, что обозначенные проблемные вопросы фиксации интернет-сведений в случаях, когда устройство при помощи, которого лицо осуществляло преступную деятельность в сфере незаконного оборота НС и ПВ изъято, хотя и детально не регламентированы законодательством, но применяя общие положения УПК РФ мы обозначили пути их решения.

Ситуация 2. Органы следствия не располагают устройством, с использованием которого подозреваемый выходил в сеть.

В данном случае изъятие доказательственной интернет-информации может быть осуществлено посредством проведения осмотра документа/ интернет-ресурса (страницы).

[1] Приговор Кировского районного суда г. Екатеринбурга от 04.08.2019 № 1-274/2019 [Электронный ресурс] // Судебные и нормативные акты РФ URL : https://sudact.ru/regular/doc/1iUgGLnSSxWq/ (Дата обращения: 21.04.2023).

Как уже неоднократно было сказано, основной отличительной чертой сведений, находящихся в сети Интернет, является их изменчивость. Данная особенность может затруднить процесс сбора доказательств при расследовании наркопреступлений. Представим ситуацию: следователь производит осмотр интернет-ресурса, посредством которого лицо осуществляло сбыт НС и ПВ. Но на момент осмотра, все объявления о продаже наркотиков были удалены администратором сети, либо сайт вовсе прекратил свое существование. Соответственно доказательственная информация в данном случае не будет получена.

Некоторое время назад в сети очень активно обсуждался сервис «Internet Archive Wayback Machine», позволяющий найти старые и несуществующие на сегодняшний день версии интернет-сайтов. Так называемая машина времени для интернета – это бесплатный онлайн-архив некоммерческой библиотеки «Архив интернета». С помощью поисковых роботов (веб-краулеров) ресурс архивирует происходящие на сайтах изменения. На данный момент ресурс предоставляет доступ к более чем 767 миллиардам сохраненных веб-страниц[1].

Применение данного ресурса при производстве осмотра интернет-страницы позволяет получить точные данные именно на момент совершения преступных действий подозреваемых (обвиняемых) лиц. Таким образом проблема постоянной изменяемости интернет-сведений может быть полностью решена. Стоит отметить, что такой осмотр необходимо проводить при обязательном присутствии специалиста, который сможет подтвердить принцип работы такого сервиса и достоверность предоставляемых им данных[2].

Таже типичной для расследования преступлений в сфере незаконного оборота наркотиков считается ситуация, когда интересующая следствие

[1] Internet archive wayback machine : [Электронный ресурс]. – URL : https://archive.org/web/ (Дата обращения: 15.04.2023).

[2] При подготовке работы не исследовались вопросы возможных ограничений, связанных с использованием иностранных Интернет-ресурсов в служебных целях.

интернет-информация находится в теневом Интернете «Darknet». Даркнет – это общее понятие для сети ресурсов, которые объединены свойством, позволяющим поддерживать абсолютную анонимность своих пользователей, для чего используется несколько ступеней шифрования данных. Получить доступ к теневому Интернету можно посредством Tor (The Onion Router) Browser. Данный браузер можно свободно скачать в Интернете, и, следовательно, получить доступ к ресурсам теневого Интернета. Специфика возбуждения уголовных дел о незаконном обороте НС и ПВ складывается таким образом, что поводом и основанием для возбуждения уголовного дела является рапорт об обнаружении признаков преступления и материалы проверки, собранные оперуполномоченными сотрудниками. Следовательно, в материалах уголовного дела сведения о наличии какой-либо интересующей информации, расположенной в теневом Интернете, появляется не посредством следственных действий, а посредством проведения ОРМ. Однако следователь (дознаватель) может самостоятельно получить необходимую информацию посредством производства уже описанного выше следственного действия – осмотра. Но так как информация находится с Даркнете, целесообразно для осмотра привлечь специалиста, который обладает специальными знаниями в данной области.

Таким образом, использование сервисов, позволяющих получить доступ к «архиву интернета» при проведении осмотра интернет-ресурса, позволило бы решить такую проблему как постоянная изменчивость интернет-информации. Важно еще раз отметить, что при фиксации интернет-сведений, расположенных в сети Интернет очень важно привлекать специалиста, который обладает знаниями в данной области. Данное обстоятельство позволит в будущем избежать признания полученных доказательств недопустимыми.

Уголовно-процессуальное законодательство в сфере закрепления доказательственной интернет-информации посредством производства следственных действий далеко от совершенства и имеет достаточное

количество проблемных вопросов. Например, внесение в УПК РФ такого вида осмотра как «осмотр интернет-ресурса», также как и реальное производство компьютерно-сетевой судебной экспертизы позволило бы правоприменителю более качественно фиксировать цифровые «следы», действуя при этом в рамках УПК РФ. Также необходимо рассмотреть вопрос об использовании различных программ и интернет-ресурсов, которые смогли бы значительно облегчить следователю (дознавателю) деятельность по формированию доказательственной базы. Изучение способов фиксации, которыми вынужден обходиться следователь (дознаватель) при расследовании уголовных дел о преступлениях в сфере незаконного оборота наркотиков лишь подтверждает нашу позицию о необходимости внесения изменений в УПК РФ. Создавать какие-либо новые следственные действия не имеет смысла, так как они лишь будут по своей сути подменять уже имеющиеся. Но при этом, необходимо дать лицу, осуществляющему предварительное расследование четкие алгоритмы использования следственных действий при изъятии интернет-сведений. Такое разъяснение позволит в будущем избежать разногласий в толковании закона.

2.2 Особенности и проблемные аспекты процессуального закрепления информации из сети Интернет при производстве иных процессуальных и непроцессуальных действий по уголовным делам в сфере незаконного оборота наркотиков

Цифровая трансформация механизма совершения преступлений в сфере незаконного оборота НС и ПВ порождает определенные сложности в фиксации доказательственной интернет-информации. В том числе имеется ряд проблем закрепления сведений при производстве иных процессуальных и непроцессуальных действий.

Иные процессуальные действия – это действия должностных лиц следственных органов, направленные на обеспечение истребование, получение доказательств, обеспечение документированного взаимодействия между государственными органами.

УПК РФ не содержит точного перечня иных процессуальных действий. Как отмечает В.С. Балакшин, данные действия могут быть разделены на две группы:

- первая группа – вытекающие из полномочий должностных лиц (например, ходатайство защитника о приобщении к материалам уголовного дела документов, иных предметов на основании положений п. 3 ч. 2 ст. 86 УПК РФ);

- вторая группа – вытекают из обязанности должностных лиц следственных органов обеспечить реализацию процессуальных прав участников судопроизводства (например, приобщение к материалам уголовного дела документов, иных предметов по ходатайству защитника на основании п. 3 ч. 2 ст. 86 УПК РФ)[1].

Стоит отметить, что в рамках данного исследования подлежат рассмотрению только те процессуальные действия, которые по своей сути предполагают получение и закрепление в материалах дела какой-либо интернет-информации.

Переходя к рассмотрению проблемы, стоит отметить что при производстве по уголовным делам, связанным с незаконным оборотом наркотиков, фиксация материалов из сети Интернет при производстве иных процессуальных и непроцессуальных действий осложняется тем, что уголовно-процессуальным законодательством не предусматривается четко регламентированной процедуры такой фиксации, также не содержится правил о возможности сохранения информации в сети Интернет при производстве иных процессуальных и непроцессуальных действий. Именно

[1] Балакшин В.С. Иные процессуальные действия как средства уголовно-процессуального доказывания / В.С. Балакшин // Вестник Оренбургского государственного университета. 2006. №3. С. 27.

поэтому данной проблеме уделяется большое внимание в научной литературе.

Изучением проблемных аспектов фиксации информации, расположенной в сети Интернет при производстве иных процессуальных действий, занималась П.С. Волкопялова. Так, по мнению автора, основными проблемными аспектами выступают:

1. Возможность изменения или удаления представляющей интерес для следствия информации. Так, чаще всего информация о незаконном обороте НС и ПВ распространяется в закрытых сообществах социальных сетей, закрытых каналах в мессенджерах, а также на различных интернет-сайтах. Администраторы данных сайтов могут с легкостью удалить и видоизменить информацию в короткие сроки. Возможность хранения подобной информации по законодательству России имеется только после проведения следственных действий. Однако, возможности моментальной фиксации информации, содержащейся в сети интернет-законодательством, не предусматривается.

2. Сложности с приобщением в качестве доказательства информации, расположенной в сети Интернет, при обращении с соответствующим ходатайством стороны защиты. Так, для достижения данной цели необходимо обратиться с соответствующим ходатайством к следователю и только после его удовлетворения, сторона защиты сможет приобщить информацию данного рода. В соответствии со ст. 159 УПК РФ защитнику «…не может быть отказано в приобщении к материалам уголовного дела доказательств, в том числе заключений специалистов, если обстоятельства, об установлении которых они ходатайствуют, имеют значение для данного уголовного дела и подтверждаются этими доказательствами». Сложность заключается в том, что подобное ходатайство может быть и не удовлетворено следователем или дознавателем, так как они могут счесть данное доказательство не имеющим значение для уголовного дела. Но ч. 4 ст. 159

УПК РФ подчеркивает, что такой отказ может быть обжалован стороной защиты.

Рассмотрим актуальные проблемы фиксации при производстве отдельных процессуальных и непроцессуальных действий.

1. Приобщение к материалам дела документов, справок, содержащих информацию из сети Интернет защитником на основании п. 3 ч. 2 ст. 86 УПК РФ. В качестве такой информации по уголовным делам по незаконному обороту НС и ПВ могут выступать скриншоты, электронные письма, фотографии, которые могут служить обстоятельствами, смягчающими ответственность или обстоятельствами, доказывающими невиновность подзащитного. Например, как было указано в предыдущем примере из судебной практики члены преступного сообщества, регистрировали sim-карты и банковские карты на третьих лиц. В последующем следственные органы могут найти данных лиц, фактически не виновных в совершении преступления. Поэтому, важные элементы интернет-переписки или скриншоты могут служить доказательством невиновности данного лица.

Помимо того обстоятельства, когда интересующие сторону защиты данные могут быть удалены, есть и другое – защитник может представить данные материалы в неверном формате. Как отмечает Н.Р. Мухудинова «адвокату наиболее часто отказывают в приобщении к материалам уголовного дела таких документов, как распечатка электронных писем, неудостоверенные факсимильные сообщения, документы, размещенные в Интернете, анонимные письма, фотографии[1]». Именно поэтому для того, чтобы зафиксировать в материалах дела данного рода информацию защитникам следует должным образом удостоверить данные материалы, для того чтобы данное ходатайство было удовлетворено, а исходные данные не

[1] Путихина Н.В. Приобщение доказательственных сведений, собранных защитником, к материалам дела как способ преобразования их в доказательства / Н.В. Путихина // Вестник Вятского государственного гуманитарного университета. 2015. №6. С. 118.

были утеряны или удалены администраторами интернет-страниц или иными лицами.

2. Направление требований, поручений, запросов следователем. Как было установлено, общение между участниками преступного сообщества осуществляется чаще всего через специальные программы или мессенджеры. В случае, если подозреваемый (обвиняемый) отказывается выдать всю имеющуюся переписку следственным органам, следователю приходиться прибегать к такому процессуальному действию как направление запроса в ту организацию, которая владеет данными мессенджерами для получения данных переписки. Чаще всего компании-владельцы мессенджеров находятся за границей. Например, для получения переписки из «WhatsApp» необходимо обратиться к поставщику «Facebook», офис которого находиться в США. Положения гл. 53 УПК РФ обязывают в таком случае направить запрос о правовой помощи (порядок направления, содержание и форма также регулируется положениями данной главы). При этом необходимо четко указать цели получения данной переписки, так как поставщик может отказать в выдаче данной информации. К тому же, дело усложняется тем, что сроки хранения переписок могут быть ограничены, например, в том же Facebook они составляют 90 дней.

Как отмечает В.Б. Батоев, такое положение дел во многом связано с тем, что Россия не является участницей Конвенции Совета Европы о киберпреступности[1]. Как мы знаем, в связи со сложившейся геополитической ситуацией, Россия прекратила действие на своей территории всех актов Совета Европы. Поэтому, говорить о возможной ратификации указанной Конвенции не приходится.

В качестве иной затруднительной ситуации можно назвать использование sim-карты иностранного оператора для регистрации

[1] Батоев В.Б. Использование мессенджеров в преступной деятельности: проблемы деанонимизации пользователей и дешифрования информации / В.Б. Бытоев // Научное издание «Оперативник (сыщик)». 2017. №2. С. 16.

пользователя в соответствующем мессенджере. В таких случаях получение данных переписок практически невозможно.

Особенная сложность фиксации возникает в связи с тем, что в некоторых мессенджерах имеется функция удаления переписки без возможности восстановления даже через поставщика таких услуг. Таким мессенджером является Telegram. Так, в качестве примера приведем материалы уголовного дела, возбужденного в отношении гражданина Н. Он обвинялся в совершении преступления, предусмотренного ч. 1 ст. 228 УК РФ. Согласно материалам дела Н. в мессенджере Telegram связался с неизвестным лицом. Ник его он не запомнил. Н. обратился с просьбой приобрести наркотическое средство. В ответ получил данные электронного кошелька, а после оплаты получил адрес закладки, которую также в дальнейшем не вспомнил. Данная переписка была удалена, восстановлению не подлежала. Telegram не имел возможности восстановить данную переписку, в связи с чем невозможно было установить личность сбытчика[1].

Другой сложностью с получением информации от интернет-провайдеров можно назвать тот факт, что с недавних пор в мессенджерах «WhatsApp» и «Viber» внедрили шифрование «end-to-end». Это означает, что компании-владельцы мессенджеров не смогут дешифровать переписку, данное право имеется только у пользователей. В связи с чем представляется невозможным обращение следственных органов с соответствующими запросами в адрес интернет-провайдеров и владельцев мессенджеров.

Перечисленные факторы следователь (дознаватель) должен учитывать при определении способов фиксации интернет-сведений, имеющих значение для уголовного дела, а также при проверке и оценке полученных доказательств.

[1] Приговор Железнодорожного районного суда г. Рязани от 20.02.2019 № 1-39/2019 [Электронный ресурс] // Судебные и нормативные акты РФ URL : https://sudact.ru/regular/doc/PBld8YNLTH1n/ (Дата обращения 21.04.2023).

Часто следователи для установления доступа к определенным сайтам, а также для получения информации о таких сайтах обращаются с запросами в специализированные органы. Часто ответы на данные запросы не содержат всей полноты необходимой информации, что также может привести к неполной фиксации информации, расположенной в сети Интернет.

При формировании запроса следователям стоит указывать следующую информацию:

— факт наличия возбужденного уголовного дела (номер, статья УК РФ);

— сведения о каком-либо идентификаторе пользователя в сети Интернет (речь идет о пользователе, т. е. физическом лице, причастном к преступлению. Возможные идентификаторы — фамилия, имя, ID, доменное имя, IP-адрес, никнейм / логин);

— перечень сведений, который необходимо получить;

— срок направления ответа на запрос и адрес;

— разъяснение положений ч. 4 ст. 21 УПК РФ и ст. 17.7 КоАП РФ;

— приложения (например, постановление суда);

— данные следователя, направляющего запрос (должность, звание, ФИО, контактный телефон)[1].

Так, органам, отвечающим на запрос следственных органов следует указывать помимо основной информации также следующую:

— дату и время осуществления поиска сведений об интересующем лице или ином объекте на интернет-ресурсах согласно часовому поясу;

— физическое место (адрес), откуда осуществлялся поиск;

[1] Сидорова К.С. Способы фиксации информации, полученной с использованием ресурсов сети интернет / К.С. Сидорова. // Преемственность и новации в юридической науке : Материалы Всероссийской научной конференции адъюнктов, аспирантов и соискателей. – Омск: Омская академия Министерства внутренних дел Российской Федерации. 2019. № 15. С. 96.

— техническое устройство и его характеристики, с которого осуществлялся выход в интернет и способ (мобильный интернет, посредством Wi-Fi-услуг);

— результаты проверки доступности, осматриваемой интернет-страницы (интернет-сайта);

— трассировку пути до интернет-страницы (интернет-сайта);

— имеющуюся текстовую, графическую информацию;

— размещенные медиафайлы (аудио, видео и др.)[1].

3. По поручению следователей в рамках уже возбужденного уголовного дела могут проводиться и ОРМ. Основным условием использования этих сведений является проведение ОРМ в соответствии с законом, а также исключение какой-либо провокации со стороны оперуполномоченных.

Конституционный Суд РФ в рамках жалобы на ст. 89 «Использование в доказывании результатов оперативно-розыскной деятельности» УПК РФ, указал, что «результаты оперативно-розыскных мероприятий являются не доказательствами, а лишь сведениями об источниках тех фактов, которые, будучи полученными с соблюдением требований Закона об оперативно-розыскной деятельности, могут стать доказательствами только после закрепления их надлежащим процессуальным путем[2]».

В рамках рассмотрения данного пункта стоит также сказать о таком виде ОРМ, как получение компьютерной информации. Р.Р. Мамлеев определяет, что получение компьютерной информации – это «совокупность средств и способов исследования компьютерной системы с целью обнаружения и документирования материальных следов, сопутствующих подготовке или совершению преступлений, которые могут содержаться в

[1] Сидорова К.С. Указ. соч. С. 95.

[2] Об отказе в принятии к рассмотрению жалоб гражданина Давлетова Андрея Юрьевича на нарушение его конституционных прав статьей 89 Уголовно-процессуального кодекса Российской Федерации : определение Конституционного Суда РФ от 19.12.2017 № 2801-О/2017 // СПС КонсультантПлюс.

компьютерной системе в форме электрических сигналов, независимо от средств их хранения, обработки и передачи[1]».

Объектами исследования при проведении данного вида процессуального действия выступают:

1) информационные объекты сети Интернет (сайты с запрещенным контентом);

2) места сетевого общения преступных групп в социальных сетях;

3) каналы коммуникаций ИТС Интернет (мессенджеры, электронная почта, групповой чат др.);

4) средства вычислительной техники, мобильные устройства, носители компьютерной информации, устройства фиксирующие компьютерные данные.

Данное ОРМ должно осуществляться на основании судебного решения и только при наличии определенных условий.

Стоит отметить, что проведение данного мероприятия связано с рядом проблем – отсутствие специалистов, шифрование информации и т.д.

Как отмечают В.В. Павлов, М.А. Золотов, Т.А. Калентьева данный вид ОРМ является одним из самых перспективных при расследовании преступлений, связанных с незаконным оборотом НС и ПВ. Авторы предлагают «в рамках ОРМ «Получение компьютерной информации» предусмотреть возможность для субъекта ОРД на основании судебного решения запросить у Интернет-провайдера необходимую информацию из учетных записей пользователей в социальных сетях, мессенджерах и на сайтах с запрещённым контентом. Зафиксированные данные при необходимости будут легализованы и приобщены к уголовному делу. При условии своевременного проведения мероприятия, информация, находящаяся

[1] Серов А.В. Получение компьютерной информации как самостоятельное оперативно-розыскное мероприятие / А.В. Серов, А.С. Дубинин // Вестник ВИ МВД России. 2018. №3. С. 170.

в этих учетных записях, не подвергается угрозе уничтожения или изменения злоумышленниками[1]».

Способы фиксации информации, полученной в ходе проведения данного мероприятия, выступают предметом дискуссий в научной литературе. Так, Р.Г. Драпезо, В.Н. Шелестюков предлагают следующие способы для дальнейшей легализации в качестве доказательств полученной в ходе данного ОРМ информации:

1. Привлечение к проведению мероприятия специалиста, который поможет получить информацию или технические объекты без повреждения и модификации. В данном случае специалистом будет составлен следующий документ – справка «эксперта», которая будет приобщена к материалам уголовного дела, а сам специалист в дальнейшем может быть допрошен как свидетель.

2. Изъятые предметы (например, технические носители информации) должны быть приобщены следователем в качестве вещественных доказательств в рамках ст. 81 УПК РФ. Также следователь должен провести их осмотр и в протоколе указать тип цифрового устройства, их количество, модель, форм-фактор, технические и индивидуальные особенности. Приобщенные цифровые носители и ЦИ могут быть направлены на производство компьютерно-технической экспертизы с получением по ней экспертного заключения[2].

Интересным явлением в оперативно-розыскной деятельности считается «нетсталкинг — это деятельность, осуществляемая в пределах сети методом поиска, направленная на обнаружение малоизвестных, малодоступных и малопосещаемых объектов с их возможным последующим анализом,

[1] Павлов В.В. Проблема получения и фиксации информации, содержащейся на электронных устройствах лиц, задержанных по делам о незаконном обороте наркотических средств с использованием ресурсов сети Интернет / В.В. Павлов, М.А. Золотов, Т.А. Калентьева // Вестник ВУиТ. 2019. №2. С. 220.

[2] Драпезо Р.Г. Особенности использования результатов оперативно-розыскного мероприятия «получение компьютерной информации» / Р.Г. Драпезо, В.Н. Шелестюков // ЮрФак: изучение права онлайн : [Электронный ресурс]. – URL : https://urfac.ru/?p=986#_ftnref6 (Дата обращения 29.04.2023).

систематизацией и хранением[1]». Как часто происходит, бесконтактные способы распространения НС и ПВ приходятся на систему Darknet. В связи с этим, следственные органы при проверке сообщения о преступлении могут воспользоваться данным способом поиска необходимой информации для ее дальнейшей фиксации.

Применение данного метода, по мнению Р.В. Миронова должно проводиться в несколько этапов:

1. Розыск необходимой информации в сети Интернет (преимущественно в Darknet);

2. Фиксация найденной информации при помощи скриншотов или иных методов фиксации;

3. Анализ полученной информации – анализ полученной в ходе розыскной деятельности информации[2].

Таким образом, уголовно-процессуальное законодательство в сфере закрепления доказательственной интернет-информации посредством производства следственных действий, иных процессуальных и непроцессуальных действий далеко от совершенства и имеет достаточное количество проблемных вопросов. Однако УПК РФ содержит перечень инструментов для фиксации такого рода информации. Существуют различные позиции относительно внесении изменений в кодекс и создания новых следственных, процессуальных и непроцессуальных действий, однако мы придерживаемся мнения об отсутствии такой необходимости. При этом необходима модернизация уже имеющихся способов, а также создание алгоритмов и разъяснений относительно процессуальных особенностей изъятия цифровых «следов» при расследовании уголовных дел о незаконном обороте НС и ПВ.

[1] Миронов Р.В. Нетсталкинг как новая форма розыскной деятельности: проблемы и перспективы / Р.В. Миронов // Молодой ученый. 2019. № 19 (257). С. 228.

[2] Миронов Р.В. Указ. соч. С. 229.

ЗАКЛЮЧЕНИЕ

Подводя итог работе, хочется еще раз обозначить основные выводы, к которым мы пришли в ходе исследования.

Наиболее часто в качестве доказательств по уголовным делам в сфере незаконного оборота НС и ПВ выступает интернет-информация: содержание переписок, фотографии НС и ПВ и участков местности, сведения об использовании сервисов, при помощи которых осуществляется оплата НС и ПВ, сайты с объявлениями о продаже НС и ПВ. В соответствии с действующими уголовно-процессуальными нормами, такие интернет-сведения могут быть оценены лицом, осуществляющим предварительное расследование, только в качестве иного документа, либо протокола следственного действия (в т.ч. приложения к протоколу). Выбор в данном случае будет зависеть именно от средства получения интернет-информации. Если следователь (дознаватель) получает такую информацию посредством истребования (скорее всего в данном случае электронная информация будет предоставлена уже на электронном носителе), то такие сведения будут отнесены к иным документам. В случае если имело место производство следственного действия, соответственно данное доказательство будет отнесено к протоколу следственного действия.

К следственным действиям, посредством которых осуществляется фиксация интернет-сведений относятся: осмотр предметов (документов), осмотр места происшествия, допрос, проверка показаний на месте, выемка. Исследование детально показало, что проблемы при использовании данных следственных действий в уголовно-процессуальном законодательстве существуют. Например, такие как фактическое расширение перечня видов осмотра их подмена и часто выход за рамки правил предписанных УПК РФ. В данном случае законодательное закрепление такого вида следственного осмотра как «осмотр интернет-ресурса» позволило бы правоприменителю более качественно фиксировать цифровые «следы», действуя при этом в

рамках закона. Осмотр места происшествия и проверка показаний на месте имеют одну общую проблему – определение «места» производства такого следственного действия. Анализируя позиции ученых-процессуалистов, мы пришли к мнению о том, что «местом» в данном случае должен считаться унифицированный адрес электронного ресурса. Что касается использования допроса как средства фиксации интернет-сведений, данное следственное действие не может в полной мере считаться средством фиксации доказательственной информации из сети Интернет. Показания лица лишь указывают на существование такой информации. При производстве выемки основными проблемами является: удаленность нахождения серверов интернет-ресурсов, обострившееся в последнее время из-за внешнеполитической обстановки международное взаимодействие, ограниченный срок хранения информации на серверах интернет-ресурсов.

Основная проблема состоит в том, что существующие специальные способы изъятия доказательственной интернет-информации, например такие как компьютерно-сетевая судебная экспертиза и оперативно-розыскное мероприятие получение компьютерной информации, но в полной мере не используются при расследовании преступлений по тем или иным причинам.

Также представляется перспективным использование различных программ и интернет-ресурсов, которые смогли бы значительно облегчить следователю (дознавателю) деятельность по формированию доказательственной базы. Изучение способов фиксации, которыми вынужден обходиться следователь (дознаватель) при расследовании уголовных дел о преступлениях в сфере незаконного оборота наркотиков лишь подтверждает нашу позицию о необходимости внесения изменений в УПК РФ. Создавать какие-либо новые следственные действия не имеет смысла, так как они лишь будут по своей сути подменять уже имеющиеся. Но при этом, необходимо создать четкие алгоритмы использования следственных действий при изъятии интернет-сведений. Такое разъяснение позволит в будущем избежать разногласий в толковании закона.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Нормативные правовые акты и иные официальные документы:

1. Конституция Российской Федерации : принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020 // СПС КонсультантПлюс.

2. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (Душанбе, 28 сентября 2018 г.) // СПС Гарант.

3. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // СПС КонсультантПлюс.

4. Гражданский кодекс Российской Федерации от 30.11.1994 №51-ФЗ // СПС КонсультантПлюс.

5. Уголовно-процессуальный кодекс Российской от 18.12.2001 N 174-ФЗ // СПС КонсультантПлюс.

6. Гражданский процессуальный кодекс Российской Федерации от 14.11.2002 № 138-ФЗ // СПС КонсультантПлюс.

7. Арбитражный процессуальный кодекс Российской Федерации от 24.07.2002 № 95-ФЗ // СПС КонсультантПлюс.

8. Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи» // СПС КонсультантПлюс.

9. Федеральный закон от 07.07.2003 N 126-ФЗ «О связи» // СПС КонсультантПлюс.

10. Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» // СПС КонсультантПлюс.

11. Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС КонсультантПлюс.

12. Федеральный закон от 01.03.2012 г. № 18-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // СПС Гарант.

13. Межгосударственный стандарт ГОСТ 2.051 – 2013 «Единая система конструкторской документации. Электронные документы. Общие положения» (введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 22.11.2013 N 1628-ст) // СПС Гарант.

Монографии, учебники, учебные пособия:

14. Брянская, Е.В. Аргументирующая силу доказательств при рассмотрении уголовных дел в суде первой инстанции / Е.В. Брянская – Иркутск : Изд-во ИГУ, 2015. – 193 с.

15. Васюков, В.Ф. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий / В.Ф. Васюков, В.В. Лукьянова, В.Н. Береснев. – Москва : Академия управления МВД России, 2019. – 204 с.

16. Зигура, Н.А. Компьютерная информация как вид доказательств в уголовном процессе России: монография / Н.А. Зигура, А. В. Кудрявцева. – М.: Юрлитинформ, 2011. – 173 с.

17. Кокорев, Л.Д. Уголовный процесс: доказательства и доказывание: монография / Л.Д. Кокорев, Н.П. Кузнецов. - Воронеж : Изд-во Воронеж. ун-та, 1995. – 268 с.

18. Россинская, Е.Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе : монография / Е.Р. Россинская. – М.: Норма: Инфра-М, 2018. – 576 с.

19. Стельмах, В.Ю. Производство следственных действий, направленных на получение и использование компьютерной / В.Ю. Стельмах, О.М. Ефремова, В.Ф. Васюков. – Москва: МГИМО, 2023. – 480 с.

20. Якимович, Ю.К. Доказательства и доказывание в уголовном процессе России: учеб. Пособие / Ю.К. Якимович. – Томск : Томский гос. ун-т, 2015. – 21 с.

Диссертации и авторефераты диссертаций:

21. Колычева, А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет : диссертация на соискание ученой степени кандидата юридических наук / Колычева Алла Николаевна. — Москва, 2018. – 199 с.

22. Головач, А.Г. Производство следственных действий по собиранию материально-фиксированной доказательственной информации в районах вооруженного конфликта : автореф. дисс. … канд. юрид. наук – М.: ВУ Министерства обороны РФ, 2010. – 24 с.

23. Белоусов, А.В. Проблема фиксации доказательств в досудебных стадиях уголовного процесса России: автореф. дис. … кандит. юрид. наук – М.: 2001. – 20 с.

24. Ким, Д.В. Ситуационный подход как методологическая основа предварительного расследования и судебного разбирательства уголовных дел : автореф. дис. … д. юр. наук. – Барнаул: 2006. – 49 с.

Научные публикации и статьи в периодических изданиях:

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

26. Баев, О.Я. Тактические элементы планирования деятельности по собиранию, исследованию и оценке следственной информации / О. Я. Баев // Избранные работы по проблемам криминалистики и уголовного процесса. – Москва : ЭКСМО. – 2011. – С. 49.

27. Баженов, С.В. Оперативно-розыскное мероприятие «Получение компьютерной информации» / С.В. Баженов // Научный вестник Омской академии МВД России. – 2017. – № 2. – С. 31-33.

28. Балакшин, В.С. Иные процессуальные действия как средства уголовно-процессуального доказывания / В.С. Балакшин // Вестник Оренбургского государственного университета. – 2006. – №3. – С. 25-30.

29. Батоев, В.Б. Использование мессенджеров в преступной деятельности: проблемы деанонимизации пользователей и дешифрования информации / В.Б. Бытоев // Научное издание «Оперативник (сыщик)». – 2017. – №2. – С. 16.

30. Болвачев, М.А. О следственных действиях по делам о преступлениях экстремистской направленности в социальных сетях / М.А. Болвачев // Известия Тульского государственного университета. Экономические и юридические науки. – 2022. – С. 98-105.

31. Гамбарова, Е. А. Социальные сети как источник цифровых доказательств / Е. А. Гамбарова // Криминалистическое обеспечение расследования преступлений: проблемы, перспективы и инновации: материалы Международной научно-практической конференции, посвященной 45-летию кафедры криминалистики юридического факультета БГУ. – 2017. – С. 189.

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

33. Губарева, Е.К. Особенности фиксации информации, содержащейся в сети Интернет / Е.К. Губарева, Т.А. Калентьева // Вестник Волжского университета им. Татищева. – 2019. – №2. – С. 161-168.

34. Денисов, Е.А. Проблемы изъятия криминалистически значимой информации у компании, предоставляющей услуги социальной сети / Е.А. Денисов // Вестник Московского университета МВД России. – 2018. – № 2. – С. 101-104.

35. Емельянова, Н.Ю. Проблемы применения отдельных видов доказательств в уголовном судопроизводстве / Н.Ю. Емельянова, Б.Б. Рахмонбердиев // Закон и право. – Московский университет МВД России им. В.Я. Кикотя. – 2022. – № 8. – С. 140-142.

36. Еськов, В.Д. Особенности осмотра страниц в сети Интернет / В.Д. Еськов, С.А. Чеботарев // Симферополь : Материалы VI Международной науч. конф. студентов и магистрантов. – 2017. – С. 39-40.

37. Зазулин, А.И. Компьютерная информация в уголовном процессе: сущность и способы закрепления в качестве доказательства по уголовному делу / А.И. Зазулин // Проблемы экономики и юридической практики. – 2015. – С. 130-133.

38. Карлов, А.Л. Процессуальная фиксация интернет-переписки в качестве доказательств по уголовным делам о преступлениях в сфере незаконного оборота наркотиков / А.Л. Карлов, Ю.Е. Пахорукова // Вестник Сибирского юридического института МВД России. – 2016. – №4 (25). – С. 112.

39. Лантух, Н. В. Содержание и особенности оценки иных документов как отдельного вида доказательств / Н. В. Лантух // Уголовное судопроизводство России и зарубежных государств: проблемы и перспективы развития: материалы международной научно-практической конференции. – Санкт-Петербург : СПУ МВД России. – 2021. – С. 243-249.

40. Миронов, Р.В. Нетсталкинг как новая форма розыскной деятельности: проблемы и перспективы / Р.В. Миронов // Молодой ученый. – 2019. – № 19 (257). – С. 228-229.

41. Павлов, В.В. Проблема получения и фиксации информации, содержащейся на электронных устройствах лиц, задержанных по делам о незаконном обороте наркотических средств с использованием ресурсов сети Интернет / В.В. Павлов, М.А. Золотов, Т.А. Калентьева // Вестник Волжского университета им. В.Н. Татищева. – 2019. – №2. – С. 216-224.

42. Путихина, Н.В. Приобщение доказательственных сведений, собранных защитником, к материалам дела как способ преобразования их в доказательства/ Н.В. Путихина // Вестник Вятского государственного гуманитарного университета. – 2015. – №6. – С. 115-120.

43. Серов, А.В. Получение компьютерной информации как самостоятельное оперативно-розыскное мероприятие / А.В. Серов, А.С. Дубинин // Вестник ВИ МВД России. – 2018. – №3. – С. 170.

44. Сидорова, К.С. Способы фиксации информации, полученной с использованием ресурсов сети интернет / К.С. Сидорова // Преемственность и новации в юридической науке : Материалы Всероссийской научной конференции адъюнктов, аспирантов и соискателей. – Омск : Омская академия Министерства внутренних дел Российской Федерации. – 2019. – № 15. – С. 95-97.

45. Шхагапсоев, К.З. Понятие доказательственной информации и производства следственных действий по ее проверке в районах вооруженного конфликта / К.З. Шхагапсоев // Пробелы в российском законодательстве. Юридический журнал. – 2017. – № 2. – С. 186.

46. Ялышев, С.А. Об особенностях осмотра места происшествия по уголовным преступлениям, совершенным с использованием ресурсов интернет / С.А. Ялышев // Ученые записки Санкт-Петербургского филиала Российской таможенной академии имени В.Б. Бобкова. – 2021. – № 1. – С. 106-110.

47. Ярошенко, Т.В. Нотариат и защита прав пользователей в сети «Интернет»: проблемные вопросы / Т.В. Ярошенко // Вестник Балтийского федерального университета им. И. Канта. – 2015. – № 9. – С. 47-52.

Интернет-ресурсы:

48. Internet archive wayback machine : [Электронный ресурс]. – URL : https://archive.org/web/ (Дата обращения: 15.04.2023).

49. Драпезо, Р.Г. Особенности использования результатов оперативно-розыскного мероприятия «получение компьютерной информации» / Р.Г. Драпезо, В.Н. Шелестюков // ЮрФак: изучение права онлайн : [Электронный ресурс]. – URL : https://urfac.ru/?p=986#_ftnref6 (Дата обращения 29.04.2023).

50. Климов, А.А. Доказательства и доказательственная информация: понятие и соотношение / А.А. Климов // ПРАВО.by научно-практический журнал : [Электронный ресурс]. – URL: https://journal.pravo.by/articles/ugolovnoe-pravo-kriminologiya-ugolovno- (дата обращения: 10.03.2023).

51. Краткая характеристика состояния преступности в Российской Федерации за январь-март 2023 года // мвд.рф : [Электронный ресурс]. – URL: https://xn--b1aew.xn--p1ai/reports/item/37377025 (дата обращения: 01.05.2023).

52. Сервис онлайн фиксации доказательств в сети Интернет : [Электронный ресурс]. – URL: Скриншот сайта для суда, заверить видео в Интернет онлайн (shotapp.ru). (дата обращения: 10.03.2023).

Эмпирические материалы:

53. О практике применения судами Закона Российской Федерации «О средствах массовой информации» : Постановление Пленума Верховного Суда РФ [от 15.06.2010 № 16] // Российская газета. – 2010. – 17 июня.

54. О применении части четвертой Гражданского кодекса Российской Федерации : Постановление Пленума Верховного Суда РФ [от 23.04.2019 № 10] // Российская газета. – 2019. – 6 мая.

55. Об отказе в принятии к рассмотрению жалоб гражданина Давлетова Андрея Юрьевича на нарушение его конституционных прав статьей 89 Уголовно-процессуального кодекса Российской Федерации : Определение Конституционного Суда РФ [от 19.12.2017 № 2801-О/2017] // СПС КонсультантПлюс.

56. Приговор Вологодского городского суда от 19.02.2019 № 1-170/2019 [Электронный ресурс] // Судебные и нормативные акты РФ URL : https://sudact.ru/regular/doc/Vj8SoSfptRlu/ (Дата обращения: 21.04.2023).

57. Приговор Железнодорожного районного суда г. Рязани от 20.02.2019 № 1-39/2019 [Электронный ресурс] // Судебные и нормативные акты РФ URL : https://sudact.ru/regular/doc/PBld8YNLTH1n/ (Дата обращения 21.04.2023).

58. Приговор Ленинского районного суда г. Пензы от 16.12.2019 № 1-259/2019 [Электронный ресурс] // Судебные и нормативные акты РФ URL: https://sudact.ru/regular/doc/Yeyniw1XbblX/?regular-txt=&regular- (дата обращения: 15.04.2023).

59. Приговор Железнодорожного районного суда г. Пензы от 11.02.2020 по делу № 1-51/2020 [Электронный ресурс] // Судебные и нормативные акты РФ URL : https://sudact.ru/regular/doc/DrXd9RsUQKbK/?regular-txt=&regular-case_doc (дата обращения 20.04.2023).

60. Приговор Дзержинского районного суда г. Ярославля от 23.04.2020 № 1-84/2020 [Электронный ресурс] : Судебные и нормативные акты РФ URL : https://sudact.ru/regular/doc/DIqKzHQMhLZq/?regular- (Дата обращения: 21.04.2023).

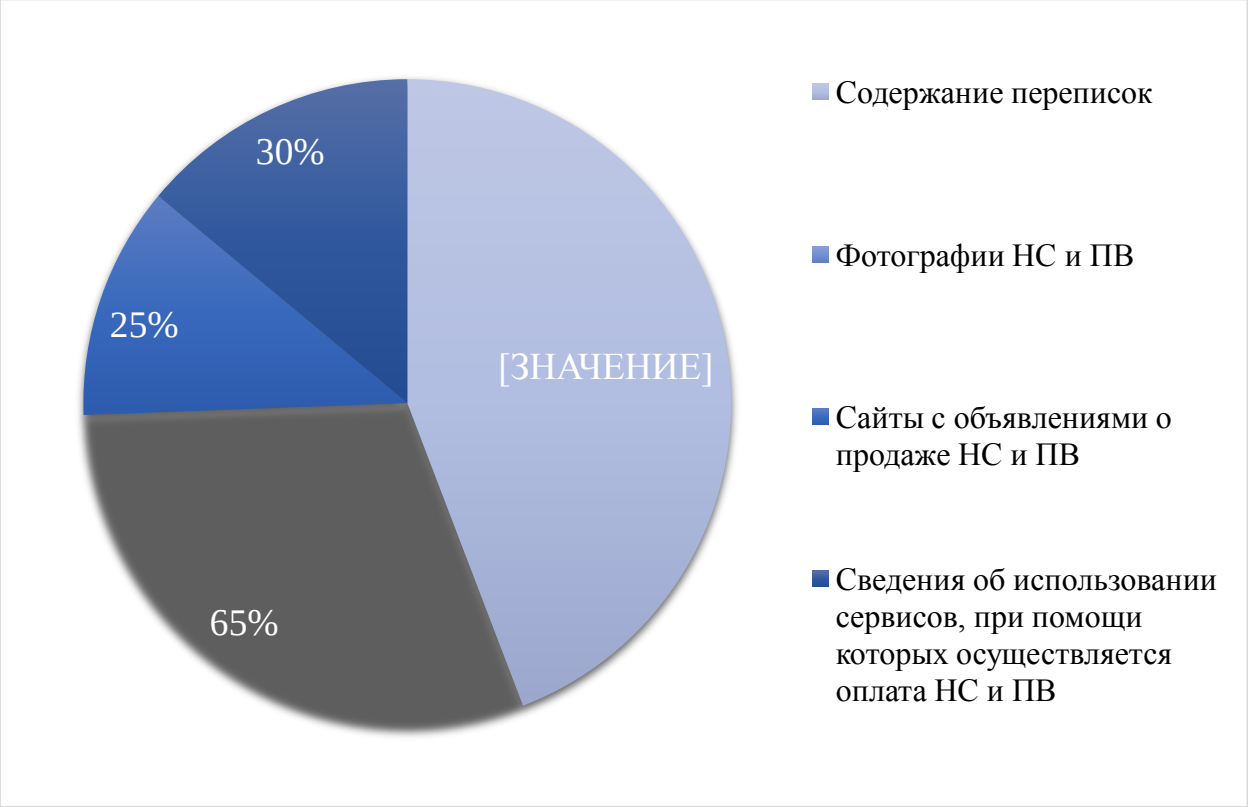
61. Приговор Абаканского городского суда от 15.06.2020 № 1-641/2020 [Электронный ресурс] // Судебные и нормативные акты РФ URL : https://sudact.ru/regular/doc/GbTlHkUPbNLK/ (Дата обращения: 21.04.2023).

62. Приговор Московского областного суда г. Красногорск от 10.08.2020 № 2-61/2020 [Электронный ресурс] // Судебные и нормативные акты РФ URL : https://sudact.ru/regular/doc/8gaUrkBtCqNr/?regular-txt=&regular-case_doc=2-61%2F2020&regular- (дата обращения: 20.04.2023).

63. Приговор Серовского районного суда Свердловской области от 09.09.2019 № 1-435/2019 [Электронный ресурс] // Судебные и нормативные акты РФ URL : https://sudact.ru/regular/doc/cePnOQEJzKO/?regular- (дата обращения: 20.04.2023).

Приложение №1

Интернет-информация, используемая в качестве доказательств по уголовным делам о преступлениях в сфере незаконного оборота НС и ПВ (на основании проведенного анализа приговоров судов общей юрисдикции по делам о незаконном обороте НС и ПВ).



Приложение №2

Следственные действия, используемые в качестве способа фиксации интернет-сведений ПВ (на основании проведенного анализа приговоров судов общей юрисдикции по делам о незаконном обороте НС и ПВ).