МИНИСТРЕСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Пермский государственный национальный исследовательский университет»

Юридический факультет

Кафедра уголовного процесса и криминалистики

ОСОБЕННОСТИ ПОЛУЧЕНИЯ ЭЛЕКТРОННОЙ ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ ПО УГОЛОВНЫМ ДЕЛАМ

Выпускная квалификационная работа бакалавра

студентки 4 курса
дневного отделения
направления «Юриспруденция»
Уздяевой Ульяны Дмитриевны
Научный руководитель:
доктор юридических наук,
доцент
Пастухов Павел Сысоевич

Пермь 2020

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В современном мире высокие технологии и информатизация проникли во все сферы жизнедеятельности общества, оказывая на него как позитивное, так и негативное влияние. Негативное проявляется в увеличении количества преступлений, совершенных с использованием различных электронных устройств, улучшения оснащенности преступников, возможности скрываться от правоохранительных органов и препятствовать их деятельности.

Сложности при получении электронной доказательственной информации по уголовным делам обусловлены своеобразием электронных следов, оставляемых на месте совершения преступления, не таким высоким уровнем подготовленности правоохранительных органов, недостаточной нормативной разработкой правил и рекомендаций по работе с такими следами, отсутствием единого подхода к существованию информации в качестве доказательств. Это подтверждается данными отчета о состоянии преступности в России за январь – ноябрь 2019 года, где процент нераскрытых преступлений, связанных с

использованием информационно–телекоммуникационных технологий, составляет 69, 1 %[1].

Степень исследованности данной темы на сегодняшний день недостаточно высокая, однако в силу актуальности появляется все больше отдельных научных статей и монографий. В научных работах отсутствуют общие подходы к пониманию основных категорий в сфере криминалистического и уголовно–процессуального регулирования электронной доказательственной информации.

Теоретическую базу исследования составляют труды таких ученых, как В.А. Мещеряков, В.Б. Вехов, В.Ю. Агибалов,
С.Ю. Скобелин, А.Ю. Семенов, О.С. Кучин, Е.Р. Россинская, А.Г. Волеводз, А.Л. Осипенко, П.С. Пастухов, С.В. Зуев, В.Ф. Васюков, Л.Б. Краснова, А.М. Багмет, Н.Н. Лыткин, Ю.В. Гаврилин, М.И. Воронин, и другие.

Целью исследования является анализ уголовно–процессуального и криминалистического регулирования при собирании электронной доказательственной информации.

Для достижения цели исследования необходимо решить следующие исследовательские задачи: проанализировать сущность понятия электронных следов; рассмотреть вопрос о месте в классификации следов, различных классификаций электронных следов; исследовать информационно–технологические источники электронных следов; проанализировать уголовно–процессуальную формы существования электронной доказательственной

[1] Состояние преступности в России за январь–ноябрь 2019 года. URL : https://мвд.рф/reports/item/19333321/ (дата обращения 22.01.2020).

информации; изучить криминалистические и уголовно–процессуальные особенности обнаружения, собирания, изъятия, фиксации электронных следов; исследовать вопрос использования специальных знаний при получении электронной информации и соблюдения прав и свобод человека; осуществить сравнительно–правовой анализ международных документов по работе с электронной информации как доказательств и разработать меры для совершенствования правового регулирования работы с электронной информацией.

В качестве предмета исследования выступают закономерности следообразования и правовых основ работы с электронной доказательственной информации.

Объектом изучения является действующая совокупность правовых отношений, складывающихся в процессе формирования понятия электронных следов, электронной доказательственной информации, приемов и способов ее обнаружения, изъятия и фиксации.

Методологическую базу исследования составляют общенаучные методы: анализ и синтез, индукция, а также частнонаучные методы: системный, сравнительно–правовой, функциональный, формально–логический.

Практическая значимость настоящего исследования выражается в его комплексном анализе проблемы использования электронной доказательственной информации в уголовном процессе и криминалистике как с точки зрения расследования преступлений, так и с точки зрения эффективного обеспечения прав и свобод человека и гражданина в данной деятельности.

Структура работы. Работа состоит из введения, в котором определяются актуальность темы, цель, задачи, объект, предмет исследования; главы первой – «Теоретические основы исследования электронных следов», состоящая из трех параграфов; главы второй – «Обнаружение, осмотр, изъятие и фиксация электронных следов как доказательств», состоящая из четырех параграфов.

Результаты исследования апробированы при написании следующих статей: Понятие и сущность электронных следов // Материалы XXI Международной научно–практической конференции молодых ученых «Норма. Закон. Законодательство. Право». Пермь. 2019. С. 365–368; Участие специалиста при производстве следственных действий с электронными носителями информации // Вопросы российской юстиции. Екатеринбург. 2019. № 1. С. 679–685; Правовое регулирование использования электронных следов при раскрытии и расследовании преступлений // Трансформация права: Технологии XXI века. Екатеринбург. 2019. С. 626–629; Соблюдение прав и свобод человека и гражданина при получении электронной доказательственной информации // Материалы Всероссийской с международным участием студенческой научно–практической конференции. 2019. С. 110–115; Навигационные системы как источник доказательственной электронной информации // Государство и право: история и современность: материалы VII Региональной науч.–практ. конф. молодых ученых. Пермь. 2019. С. 73–76.

ГЛАВА I. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИССЛЕДОВАНИЯ ЭЛЕКТРОННЫХ СЛЕДОВ

1.1. Понятие и классификация электронных следов

Одной из наиболее молодых и наименее разработанных отраслей криминалистической техники является криминалистическое исследование компьютерной информации или электронных носителей информации. По своей структуре можно отметить некоторую ее схожесть с трасологией, так как центральное место в ней занимает понятие следа. Совершение любого действия, особенно преступного, всегда приводит к изменению в окружающей среде, и до определенного времени такие изменения носили только материальный характер, например, следы пальцев рук, ног, биологические следы и другие. Но в связи с информационно – технологическим развитием, внедрением электронных устройств во все сферы жизнедеятельности общества, имело место появление качественно новых следов осуществления преступления, с одной стороны, также являющихся отражением действительности под воздействием изменений в окружающей среде, но с другой стороны, имеющих особые специфические признаки.

По мнению П.С. Пастухова, в настоящее время количество электронных следов при совершении «бесконтактных» преступлений в сфере компьютерной информации становится больше, чем традиционных[1]. Также в процессе расследования данной группы иногда они играют более значимую и первостепенную роль.

[1] Пастухов П.С. О необходимости развития компьютерной криминалистики // Пермский юридический альманах. 2018. № 1. С. 480.

Несмотря на столь масштабное внедрение электронных следов, они до сих пор не имеют законодательного закрепления. Установление содержания данного понятия является принципиально важным вопросом в целях дальнейшей разработки правил и рекомендаций по поиску, обнаружению, изъятию, исследования и их фиксации.

Многие специалисты предпринимали попытки по определению сущности и содержания понятия электронных следов. Один из первых, кто обратил внимание на необходимость его разработки, был В.А. Мещеряков. Он определяет электронные следы как «любое изменение состояния автоматизированной информационной системы (образованного ею «кибернетического пространства»), связанное с событием преступления и зафиксированное в виде компьютерной информации (то есть информации в виде, пригодном для машинной обработки) на материальном носителе, в том числе в электромагнитом поле»[1]. Несмотря на специфические особенности, присущие электронным следам, а именно, необходимость применения специального оборудования и компьютерных средств, программ при работе, возможность мгновенного и дистанционного изменения, невидимость для глаз человека[2], цифровой вид записи, формирование в искусственно созданной среде[3], сущность электронных следов, в первую очередь, сводится к их основному свойству – отражению действительности. По мнению некоторых ученых, например, А.Н. Колычевой,

[1] Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. М., 2002. С. 104.
[2] Пастухов П.С. О необходимости развития компьютерной криминалистики // Пермский юридический альманах. 2018. № 1. С. 480.
[3] Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе : автореф. дис. ... канд. юрид. наук. Воронеж, 2010. С. 13.

данное понятие сложно для восприятия и нуждается в некоторой доработке[1]. Н.Н. Лыткин под компьютерно–технологическими следами предлагает понимать любые изменения компьютерной информации, относящиеся к преступлению, возникающие в результате уничтожения, копирования, блокирования и модификации[2]. По нашему мнению, такое определение сужает содержание данной группы следов и привязывает к преступлениям в сфере компьютерной информации.

С понятием электронных следов тесно связано такое понятие, как компьютерная информация, под которой понимается элемент искусственной среды, созданный человеком. В Уголовном кодексе РФ содержится легальное определение компьютерной информации, как сведений (сообщений, данных), представленных в форме электронных сигналов, независимо от средств их хранения, обработки и передачи[3]. Как и любой другой вид информации, она состоит из двух элементов: содержания информации — сведений о каком–либо явлении объективной реальности и носителя данных сведений[4]. Можно выделить следующие формы существования компьютерной информации: электромагнитный сигнал, файл, электронное сообщение, электронные денежные средства, электронная подпись, электронный документ, электронный журнал, база данных,

[1] Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет : дис. … канд. юрид. наук. Москва, 2018. С. 22.
[2] Лыткин Н.Н. Использование компьютерно–технических следов в расследовании преступлений против
собственности: дис. … канд. юрид. наук. Москва, 2007. С. 57.
[3] Уголовный кодекс РФ : федеральный закон РФ № 63–ФЗ от 13.06.1996 (ред. от 25.04.2018) // СЗ РФ. 1996, № 25. Ст. 2954.
[4] Яблоков Н. П. Криминалистика : учебник / Н. П. Яблоков. М., 2016. 303 с.

программа для ЭВМ, сайт, страница сайта и др[1]. В то же время данные формы выступают в роли следообразующих и следовоспринимающих объектов при образовании электронных следов.

Некоторые ученые под электронными следами понимают информацию, содержащуюся в электронных устройствах, являющихся носителями цифровой информации[2]. А.Ю. Семенов сразу говорит не просто об информации, а использует термин криминалистически значимая компьютерная информация[3]. В.Б. Вехов дополнил данное определение такими признаками, как электронно–цифровая форма, материальный носитель, возможность передачи по каналам связи с помощью электромагнитных сигналов[4]. А.Н. Колычева также использует понятие криминалистически значимой информации, определяет через пригодную для обработки форму с использованием компьютерной техники, создание с помощью набора двоичного машинного кода либо его преобразования (модификация, копирование, удаление или блокирование)[5].

Но данный подход, скорее всего, в полной мере не отражает сущности следа как основной категории криминалистики. Однако, несмотря на это, в основе механизма образования электронных следов лежат электромагнитное взаимодействия двух и более

---

[1] Вехов В. Б., Смагоринский Б. П., Ковалев С. А. Электронные следы в системе криминалистики // Судебная экспертиза. 2016. № 2 (46). С. 11.

[2] Скобелин С. Ю. Использование специальных знаний при работе с электронными следами // Российский следователь. 2014. № 20. С. 32.

[3] Семенов А. Ю. Некоторые аспекты выявления, изъятия и исследования следов, возникающих при совершении преступлений в сфере компьютерной информации // Сибирский юридический вестник. 2004. №1. С. 54.

[4] Вехов В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки. Волгоград: ВА МВД России, 2008. С. 83.

[5] Колычева А.Н. Указ. соч. С. 34.

материальных объектов – объективных форм существования компьютерной информации[1]. То есть, не информация, а ее отражение все же является непосредственно электронным следом, но она принимает непосредственное участие в их образовании.

Ученое сообщество разделилось в решении вопроса о месте электронных следов. Мы солидарны с точкой зрения авторов, полагающих, что электронные следы не могут быть отнесены ни к материальным, ни к идеальным следам и занимают самостоятельное место в классификации следов[2]. Но многими учеными такая позиция не разделяется. Так, например, О.С. Кучин электронные следы относит к материальным, обуславливая свою позицию тем, что они хранятся в памяти машины, но обладают при этом некоторыми признаками идеальных следов ввиду не воспринимаемости человеческим глазом[3]. Е.Р. Россинская также относит их к материальным следам, так как электронные следы зафиксированы на материальных носителях и не могут существовать отдельно[4]. Сторонники изменений в классификации следов, аргументируя свою позицию, отмечают, что на современном этапе развития технических устройств существуют такие средства, непосредственное наличие которых необязательно для получения информации. Например, по такому принципу действует облачное хранилище, из которого можно извлечь информацию без материального носителя. Подобного мнения

[1] Вехов В. Б., Смагоринский Б. П., Ковалев С. А. Указ. соч. С. 11.
[2] Мещеряков В.А. Указ. соч. С. 104.
[3] Кучин О. С. Электронные носители информации в криминалистике: монография / под ред. докт. юрид. наук О.С. Кучина. М., 2017. С. 83.
[4] Россинская Е.Р., Шамаев Г.П. Новый раздел криминалистики: криминалистическое исследование компьютерных средств и систем // Baikal Research Journal. 2015. №1. С. 19.

придерживается и В.Б. Вехов, указывая на то, что недоступность взгляду человека без применения специального оборудования, не ведет к признанию их нематериальными, как например, следы на фотопленке, пальцы рук, также не могут быть замечены без соответствующих инструментов[1]. Но и материальными такие следы признаться могут с трудом ввиду наличия специфических особенностей. Электронные следы отличаются и по механизму следообразования, заключающемся в электромагнитном взаимодействии цифрового сигнала, который может быть выявлен с помощью технических средств. К наиболее используемым стандартам обмена информацией в сети относят протоколы передачи данных TCP/IP (Transmission Control Protocol/Internet Protocol)[2].

Электронные следы, их поиск, обнаружение, исследование, фиксацию, иногда связывают только с совершением преступлений в сфере компьютерной информации, однако развитие технических устройств, их внедрение во все сферы жизнедеятельности позволяет утверждать, что такие следы могут быть обнаружены при совершении общественно опасных и противоправных деяний любой направленности.

Одним из часто обсуждаемых вопросов в науке являются различные суждения об использовании того или иного термина и его содержания относительно цифровой информации. По нашему мнению, основной вопрос состоит здесь в определении именно сущности и содержания

[1] Вехов В.Б. Указ. соч. С. 83.
[2] Колычева А.Н. Указ. соч. С. 40.

электронных следов, а применение термина «электронные», «виртуальные», «информационные», «бинарные», «компьютерно – технические» и так далее, не имеет определяющего значения в процессе собирания доказательств.

Таким образом, мы разделяем точку зрения ученых, считающих, что наиболее обоснованно под электронными следами следует понимать любое изменение в окружающей среде, в том числе информационной, связанное с событием преступления и зафиксированное в виде электромагнитных сигналов, сущность которых, в первую очередь состоит в характерном для следов свойстве отражения событий действительности. По нашему мнению, такие следы должны занимать самостоятельное место в классификации между материальными и идеальными следами.

Одним из существенных вопросов при изучении электронных следов является установление оснований для их классификации. Многими учеными не признается или недостаточно высоко оценивается значимость классификации. Полагаем, исследование данного вопроса помогает при определении сущности и признаков электронных следов, также при разработке правил при работе с ними в процессе раскрытия и расследования преступлений.

Например, А.Г. Волеводз выделяет электронные следы по физическому носителю их существования:

1) следы на жестком диске (винчестере), магнитной ленте (стримере), оптическом диске (CD, DVD), на дискете;

2) следы в оперативных запоминающих устройствах (ОЗУ) ЭВМ;

3) следы в ОЗУ периферийных устройств (лазерного принтера, например);

4) следы в ОЗУ компьютерных устройств связи и сетевых устройств;

5) следы в проводных, радио–оптических и других электромагнитных системах и сетях связи[1].

Такая классификация имеет большое значение при разработке нормативных правил собирания, исследования, фиксации электронных следов, в зависимости от конкретных носителей ввиду их физических особенностей, которые на данный момент не содержатся в ныне действующем законодательстве.

Применение данной классификации подтверждает и судебная практика. Так, в исследованных нами 20 приговорах судов Пермского края в делах, связанных с оставлением при совершении преступлений электронных следов, упоминаются такие электронные устройства, как флеш–носители, ноутбуки, мобильные телефоны, и др. Стоит отметить, что наиболее часто встречаются оптические диски[2] (45 %),

[1] Волеводз А.Г. Противодействие компьютерным преступлениям. М., 2002. С. 159 –160.
[2] См. например, Приговор от 19 июля 2018 г. по делу № 1–264/2018 Мотовилихинского районного суда г. Перми // https://www.sudact.ru (дата обращения 22.01.2020); Приговор от 5 июня 2018 г. по делу № 1–104/2018 Лысьвенского городского суда Пермского края // https://www.sudact.ru (дата обращения 22.01.2020); Приговор от 4 июня 2018 г. по делу № 1–145/2018 Индустриального районного суда г. Перми // https://www.sudact.ru (дата обращения 22.01.2020); Приговор от 25 мая 2018 г. по делу № 1–63/2018 Чернушинского районного суда Пермского края // https://www.sudact.ru (дата обращения 22.01.2020); Приговор от 16 февраля 2018 г. по делу № 1–25/2018 Чайковского городского суда Пермского края // https://www.sudact.ru (дата обращения 22.01.2020).

сотовые телефоны[1] (25 %), флеш–накопители[2] (15 %), жесткие магнитные диски[3] (10 %), компьютеры (25 %). Сами электронные следы в приговорах отражаются в виде перечисления содержащихся на устройствах файлов и log–файлов. Например, в приговоре от 2 марта 2016 г. по делу № 1–56/2016 протоколом осмотра записи видеонаблюдения были исследованы четыре файла с записью камер видеонаблюдения[4]; в приговоре от 25 мая 2018 г. по делу № 1–63/2018 протоколом осмотра предметов произведен осмотр оптического диска, на котором содержался фрагмент видеозаписи, состоящей из пяти файлов[5]. Приговором от 31 марта 2017 г. по делу № 1–166/2017 установлено, что сведения о датах проведения денежных операций, информация о которых имеется на 5 накопителях на жестких магнитных дисках, указаны в имени log–файла (год, месяц, день)[6]. Также важными информационными объектами с точки зрения доказательственного значения можно назвать IP–адрес, MAC–адрес, кэшированные данные приложений, истории или журналы работы пользователей в компьютерной

[1] См. например, Приговор от 25 сентября 2017 г. по делу № 1–387/2017 Свердловского районного суда г. Перми // https://www.sudact.ru (дата обращения 22.01.2020); Приговор от 10 августа 2017 г. по делу № 1–259/2017 Дзержинского районного суда г. Перми // https://www.sudact.ru (дата обращения 22.01.2020); Приговор от 6 июля 2016 г. по делу № 1–179/2016 Пермского районного суда Пермского края // https://www.sudact.ru (дата обращения 22.01.2020).

[2] См. например, Приговор от 19 июля 2018 г. по делу № 1–264/2018 Мотовилихинского районного суда г. Перми // https://www.sudact.ru (дата обращения 23.01.2020); Приговор от 5 июня 2018 г. по делу № 1–104/2018 Лысьвенского городского суда Пермского края // https://www.sudact.ru (дата обращения 23.01.2020).

[3] См. например, Приговор от 27 сентября 2018 г. по делу № 1–124/2018 Ленинского районного суда г. Перми // https://www.sudact.ru (дата обращения 22.01.2020); Приговор от 24 августа 2015 г. по делу № 1–350/2015 Индустриального районного суда г.Перми // https://www.sudact.ru (дата обращения 22.01.2020).

[4] Приговор от 2 марта 2016 г. по делу № 1–56/2016 Кудымкарского городского суда Пермского края (постоянное судебное присутствие в с. Юсьва) // https://www.sudact.ru (дата обращения 21.01.2020).

[5] Приговор от 25 мая 2018 г. по делу № 1–63/2018 Чернушинского районного суда Пермского края // https://www.sudact.ru (дата обращения 22.01.2020).

[6] Приговор от 31 марта 2017 г. по делу № 1–166/2017 Советского районного суда г. Краснодара (Краснодарский край) // https://www.sudact.ru (дата обращения 23.01.2020).

системе, на сервере, файлы, их физические адреса, имена, детализацию соединений[1].

Таким образом, данное основание для классификации имеет не только доктринальное и научное значение, но и практическое.

А. Ю. Семенов дополнил эту классификацию таким основанием, как место их нахождения, в связи с которым можно выделить:

1) следы на компьютере преступника;

2) следы на "компьютере–жертве"[2].

Данное основание также имеет практическое значение при решении вопроса об установлении сведений о личности либо преступника, либо потерпевшего, составлении портрета человека, оставившего такие следы, о его индивидуальных особенностях, наличии или отсутствии образования в данной сфере, возможном возрасте, круге интересов. Несмотря на то, что электронные следы занимают самостоятельное место в классификации следов, не являясь ни материальными, ни идеальными, они также являются источниками криминалистически значимой информации, необходимой для эффективного расследования и раскрытия преступлений. Некоторые ученые дополняют эту классификацию следами на электронных носителях, чаще компьютере операторов связи, который относится к иным участникам процесса[3].

Следующим основанием выделяют соответствующий состав преступления и статья в УК РФ. Таким образом, отдельно выделяют следы, характерные для совершения преступления, предусмотренного статьей 272, статьей 273 и

[1] Колычева А.Н. Указ. соч. С. 45.
[2] Семенов А.Ю. Указ. соч. с. 53–55.
[3] Колычева А.Н. Указ. соч. С. 39.

статьей 274 УК РФ[1]. Данное основание представляется не совсем рациональным для криминалистического исследования. Само понятие электронных следов связано не только с совершением преступлений в сфере компьютерной информации, но и с другими преступлениями, в которых применяется любой электронный носитель информации, сохраняющий на себе следы.

Некоторые ученые высказывают сомнение по поводу необходимости выделения классификации электронных следов ввиду стремительного развития технологий. Такого мнения, например, придерживается В.Ю. Агибалов и утверждает, что создание статической системы классификации является бесперспективным. По его мнению, это будет способствовать необходимости постоянно совершенствовать классификации без их коренной переделки, систематизации сведений об используемых приемах преобразования информации, формированию перечней типовых сценариев применения программно–аппаратных средств выявления и извлечения виртуальных следов и др[2].

Обоснованно можно сказать, что вопрос о классификации электронных следов является недостаточно изученным в науке ввиду недавнего появления и закрепления хотя бы на доктринальном уровне самого понятия. Несмотря на это, по нашему мнению, такая классификация электронных следов необходима. К наиболее обоснованным и находящим место в судебной практике основаниям для классификации можно отнести следующие: физический носитель, место их

[1] Семенов А.Ю. Указ. соч. С. 53–55.
[2] Агибалов В.Ю. Указ. соч. с. 20.

нахождения. Их выделение способствует более эффективному и динамичному процессу разработки правил при обнаружении, фиксации, исследовании электронных следов. Также возможно будет обозначить особенности осуществления данных действий не в отношении всей группы следов, а в отношении определенной подгруппы, что значительно облегчит эту непростую задачу.

1.2. Информационно-технологические источники электронных следов

Ввиду того уровня информатизации, которое стремительно достигло наше общество в современное время, перечень возможных информационно – технологических источников, мест нахождения электронных следов только увеличивается и как следствие не является исчерпывающим. К таким источникам можно отнести файл, лог–файлы, IP–адрес, MAC – адрес, URL (Uniform Resource Locator), DNS (Domain Name system), IMEI телефона, видеозапись, аудиозапись, программа «Безопасный город», концепция «Умный дом», системы видеорегистрации, видеофиксации, ЕСИиА (Единая система идентификации и аутентификации), навигационная деятельность, геолокация и многие другие. В целях характеристики таких возможных источников остановимся на некоторых их них.

Особо актуальным направлением при расследовании и раскрытии преступлений является использование в следственной практике глобальных навигационных спутниковых систем. Изначально их применение сводилось к решению транспортных, военных задач, картографии и

геодезии[1]. Сейчас такие системы стали использовать повсеместно, и одно из наиболее важных направлений – розыск пропавших лиц, определение точных координат места совершения преступления, нахождения трупа, а также лиц, непосредственно совершивших преступление.

Под системой навигации в соответствии с ФЗ от 14 февраля 2009 г. N 22–ФЗ "О навигационной деятельности" понимают технические средства, устройства и системы, предназначенные для формирования навигационных сигналов, передачи, приема, обработки, хранения и визуализации навигационной информации[2]. Реализация данных систем осуществляется через две основные технологии позиционирования – сеть базовых станций сети GSM, то есть по сигналам абонентом станций сотовой связи, и космические системы глобальной навигации (ГЛОНАСС, GPS) и их подсистемы[3]. Географические координаты могут быть извлечены из различных электронных носителей (мобильные устройства, облачные серверы, планшеты и др.) в том числе из установленных приложений, которые запрашивают данные о местоположении человека, чтобы показывать более точные результаты поиска на карте, построения маршрута и др. Далее эта информация отправляется на сервер компании – поставщика услуг или сохраняется в памяти самого устройства[4].

---

[1] Дусева Н.Ю. Возможности использования навигационных систем в раскрытии и расследовании преступлений // Теория и практика общественного развития. 2012. №12. С. 580.

[2] О навигационной деятельности : федеральный закон от 14 февраля 2009 года № 22–ФЗ // Российская газета. 2009. N 27.

[3] Головчанский А.В. Об использовании средств спутниковой навигации в целях установления и фиксации координат места происшествия // Вестник ВИ МВД России. 2015. №2. С. 64.

[4] Кузовлев В.Ю. Использование возможностей средств навигации в установлении обстоятельств совершения преступлений // Известия ТулГУ. Экономические и юридические науки. 2017. №4–2. С. 160.

В дальнейшем данные могут быть получены следователем путем направления мотивированного запроса оператору связи или в ходе проведения следственных действий, направленных на изъятие электронного устройства и информации, находящейся в нем (при осмотре предмета, назначении судебной экспертизы, осуществлении оперативно–розыскных мероприятий). Однако при реализации этих способов на практике возникают некоторые проблемы. Так, В.Ю. Кузовлев отмечает, что операторы связи получают большое количество запросов от правоохранительных органов, что значительно замедляет процесс получения необходимой информации, которая в некоторых случаях носит неотложный характер. Решение данной проблемы специалист видит в создании системы оперативных запросов, которая уже разработана и внедрена ПАО «Мегафон», с помощью которой сотрудник правоохранительных органов, зарегистрированный в системе, сможет через личный кабинет получить необходимую информацию[1]. Другой способ получения информации о геолокации – непосредственное изъятие данных из электронного носителя в рамках существующих следственных действий, например, осмотра предмета, назначение и проведение экспертизы.

В уголовном процессе данные систем навигации могут выступать в качестве доказательственной или ориентирующей информации. Доказательствами такие сведения являются только в случае, если соответствуют критериям относимости, допустимости и достоверности, и представляют по форме либо иной документ, либо протокол

[1] Кузовлев В.Ю. Там же. С. 160.

соответствующего следственного действия с указанием на использование средств навигации[1]. Что касается достоверности, то, по мнению специалистов, общая погрешность систем геолокации составляет менее 3, 5 %[2]. Некоторые ученые при решении вопроса о допустимости соответствующей информации отмечают следующие проблемы: возможность применения навигационных приборов общего назначения при определении координат места происшествия, также отсутствие каких–либо практических рекомендации по применению данных систем[3].

Об эффективности использования систем навигации свидетельствует и судебная практика. Так, во многих судебных актах упоминается о применении глобальных навигационных спутниковых систем при определении координат места происшествия, особое значение это имеет, когда вблизи нет постоянных ориентиров (лес, поле, тайга)[4]. Также в некоторых решениях прямо указывается на использование систем геолокации при установлении лица, совершившего преступление, маршрута его передвижения, определяемого с помощью средств навигации в сотовом телефоне или транспортном средстве, нахождения орудия преступления[5], отдельные следы преступления[6].

---

[1] Дусева Н.Ю. Технико–криминалистические основы использования глобальной навигационной системы в расследовании и предупреждении преступлений : автореф. канд. юрид. наук. Волгоград, 2015. С. 158.

[2] Якимов А.А. Использование возможностей навигационных спутниковых систем в расследовании преступлений. URL : http://elib.bsu.by/ (дата обращения 20.10.2019).

[3] Головчанский А.В. Указ. соч. С. 64.

[4] Например, приговор № 1–61/2019 от 14 марта 2019 г. по делу № 1–61/2019 Краснотурьинского городского суда // sudact.ru (дата обращения 20.10.2019); Приговор № 1–66/2019 от 27 февраля 2019 г. по делу № 1–66/2019 Адлерского районного суда г. Сочи // sudact.ru (дата обращения 20.10.2019).

[5] Приговор № 1–19/2019 от 11 февраля 2019 г. по делу № 1–19/2019 Октябрьского районного суда г. Грозного // sudact.ru (дата обращения 20.10.2019).

[6] Приговор № 2–34/2018 2–6/2019 от 19 февраля 2019 г. по делу № 2–34/2018 Ростовского областного суда // sudact.ru (дата обращения 20.10.2019).

Таким образом, можно сделать вывод, что навигационные спутниковые системы имеют немаловажное, а иногда и первостепенное значение в процессе раскрытия и расследования преступления, но вопрос их применения нуждается в более детальной разработке, выработке практических рекомендаций, что существенно упростит отыскание необходимой доказательственной информации.

Следующим актуальным направлением среди информационно–технологических источников электронных следов можно выделить аппаратно–программный комплекс «Безопасный город» (АПК «Безопасный город»). Правовым регулированием его использования является Концепция построения и развития аппаратно–программного комплекса «Безопасный город», утвержденная распоряжением Правительства РФ от 03.12.2014 N 2446–р. Целью построения и развития АПК является повышение общего уровня общественной безопасности, правопорядка и безопасности среды обитания за счет существенного улучшения координации деятельности сил и служб, ответственных за решение этих задач, путем внедрения на базе муниципальных образований комплексной информационной системы, обеспечивающей прогнозирование, мониторинг, предупреждение и ликвидацию возможных угроз, а также контроль устранения последствий чрезвычайных ситуаций и правонарушений. Основными элементами АПК «Безопасный город» выступают безопасность населения и муниципальной (коммунальной) инфраструктуры, безопасность на транспорте, экологическая безопасность, координация

работы служб и ведомств и их взаимодействие[1]. Главным координатором программы на федеральном уровне является Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий. На территории Пермского края реализация данного АПК регулируется на уровне постановления Администрации г. Перми от 19 октября 2018 года N 793 «Об утверждении муниципальной программы "Безопасный город"», которое определяет исполнителей, задачи программы, источники финансирования, срок реализации до 2023 года.

По мнению специалистов, несмотря на то, что на 2016 год более чем в 750 населенных пунктах было установлено 177 тысяч камер видеонаблюдения, общая интенсивность и эффективность внедрения АПК существенно снижается[2]. Причинами этого называют недостаточное финансирование программы, отсутствие разграничения компетенции между органами государственной власти субъектов РФ, органами местного самоуправления по данному вопросу, отсутствие четко определенного механизма создания АПК, прав и обязанностей участников процесса, сложности, возникающие в процессе централизации различных информационных, управленческих, мониторинговых систем, отсутствие типовых решений, технических заданий по созданию АПК[3].

---

[1] «Об утверждении Концепции построения и развития аппаратно–программного комплекса «Безопасный город» : распоряжение Правительства РФ от 03.12.2014 N 2446–р // СЗ РФ. 2014. № 50. Ст. 7220.

[2] Елисеев А.В., Агафонов С.И. К вопросу о правоохранительном сегменте АПК «Безопасный город» // Вестник Московского университета МВД России. 2016. №7. С. 140.

[3] Евдокимов А.С. Концепция построения и развития аппаратно–программного Комплекса «Безопасный город»: итоги реализации, организационно–правовые проблемы и нерешенные вопросы // Актуальные проблемы российского права. 2019. №5 (102). С. 75.

Некоторые отмечают, что основная проблема заключается в отсутствии единого правового регулирования применения АПК «Безопасный город», принятая Концепция утверждена распоряжением Правительства РФ и соответственно не имеет нормативного характера[1]. По нашему мнению, здесь необходим комплексный подход при решении данного вопроса, интеграция организационных, технических и правовых мер, которые увеличат эффективность применения программы, в будущем снизят уровень преступности. Полагаем, особенно важно создание технических заданий в целях повсеместного внедрения АПК «Безопасный город» в соответствующих субъектов РФ и ОМСУ, которые носят больше технический характер и направлены на использование систем.

Специалисты приходят к выводу о том, что вместе с видеокамерами могут быть внедрены новые средства обеспечения защиты, например, радиочастотная идентификация объектов, камеры наблюдения со встроенным микрофоном и функцией распознавания лиц, точки трансляции тревожного сигнала, экстренного вызова правоохранительных органов[2]. На данном этапе реализации программы интеллектуальные видеокамеры (определяющие биометрические параметры лица, события, предметы) составляют менее 0, 1 % от существующих[3].

О возможности существования в качестве источника электронных следов АПК «Безопасный город» свидетельствует и судебная практика. Так, в приговоре от 28

[1] Евдокимов А.С. Там же. С. 75.
[2] Желудков М.А. К вопросу о повышении эффективности реализации в России аппаратно–программного комплекса «Безопасный город» при обеспечении защиты от корыстной преступности // Вестник экономической безопасности. 2018. №4. С. 97.
[3] Елисеев А.В., Агафонов С.И. Указ. соч. С. 140.

ноября 2018 г. по делу № 1–383/2018 Бугульминского городского суда (Республика Татарстан) упоминается, что изъят CD диск с видеозаписью с программы «Безопасный город» с соответствующих камер видеонаблюдения и использован в качестве доказательства по факту причинения легкого вреда здоровью человека[1]. В приговоре от 12 марта 2019 г. по делу № 1–42/2019 Рузаевского районного суда (Республика Мордовия) видеозаписью с камер видеонаблюдения по программе «Безопасный город» подтверждается факт угона автомобиля[2]. Приговором от 16 января 2019 г. по делу № 1–3/2019 Соликамского городского суд (Пермский край) установлен факт осуществления патрулирования по программе «Безопасный город»[3].

Еще одним интенсивно применяемым возможным информационно–технологическим источником нахождения электронных следов выступает IMEI телефона. IMEI (International Mobile Equipment Identity) – число (обычно 15–разрядное), идентифицирующее устройство в сети. Применяется в сотовых телефонах сетей GSM, WCDMA и IDEN а также в некоторых спутниковых телефонах. Как правило, IMEI указывается в четырёх местах: в самом аппарате, под аккумуляторной батареей, на упаковке и в гарантийном талоне. Также IMEI используется для слежения за телефоном и блокирования оператором сотовой связи при краже[4].

---

[1] Приговор от 28 ноября 2018 г. по делу № 1–383/2018 Бугульминского городского суда (Республика Татарстан) // sudact.ru (дата обращения 05.01.2020).

[2] Приговор от 12 марта 2019 г. по делу № 1–42/2019 Рузаевского районного суда (Республика Мордовия) // sudact.ru (дата обращения 05.01.2020).

[3] Приговор от 16 января 2019 г. по делу № 1–3/2019 Соликамского городского суд (Пермский край) // sudact.ru (дата обращения 05.01.2020).

[4] Колосова А., Намиот Д. Цифровые сертификаты для владельцев мобильных телефонов // International Journal of Open Information Technologies. 2013. №4. С. 7.

IMEI телефона может быть получен в рамках такого следственного действия, как получение информации о соединениях между абонентами и (или) абонентскими устройствами. Специалисты изначально справедливо отнесли данную информацию к другим данным, позволяющим идентифицировать абонентов. Это было подтверждено Постановлением Пленума ВС РФ от 1 июня 2017 г. № 19 «О практике рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением конституционных прав граждан (статья 165 УПК РФ)». В соответствии с п. 12 ПП ВС к другим данным, позволяющим идентифицировать абонентов, могут относиться, в частности, сведения о IMEI–коде абонентского устройства или о местоположении телефонного аппарата относительно базовой станции[1]. Однако вопрос о возможности получения данных о IMEI телефона, как и всей электронной доказательственной информации при производстве следственных действий, которые могут привести к ограничению права человека на неприкосновенность частной жизни, личной и семейной тайны, до сих пор неоднозначно решен в ученом сообществе и среди правоприменителей. Так, по мнению специалистов, данные абонентов сетей электросвязи составляют отдельную группу сведений, носящих конфиденциальный характер, но не относящихся к тайне телефонных переговоров, а их получение от операторов связи для решения задач оперативно – розыскной деятельности и уголовного судопроизводства не требует

[1] «О практике рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением конституционных прав граждан (статья 165 УПК РФ)» : Постановление Пленума Верховного Суда РФ от 01.06.2017 № 19 // Российская газета, № 125.

судебного разрешения[1]. Судебная практика также решает данный вопрос неоднозначно, однако Верховный Суд РФ еще в 2012 году пришел к выводу о необходимости получения судебного решения для определения идентификационных абонентских устройств[2].

В исследованных нами приговорах судов общей юрисдикции Пермского края IMEI код упоминается всегда вместе с телефоном, например, при краже сотового телефона и установлении его местонахождения по IMEI[3], грабежа сумки, где также упоминается полученная от оператора информация об IMEI телефона, детализации телефонных соединений абонентского номера, информация об использовании телефона с соответствующим IMEI[4]. В приговоре Пермского краевого суда № 2–35/2015 от 14 августа 2015 г. установлено, в ходе осмотра компакт–диска, предоставленного оператором связи, на нем содержится детализация соединений с абонентских номеров телефонных аппаратов, с которых осуществлялись звонки в экстренные службы и место их нахождения, имеющих соответствующий IMEI код[5].

Следующим актуальным и пока наименее разработанным направлением среди технологических источников электронных следов является система радиочастотной идентификации объектов (RFID – Radio Frequency

[1] Чечетин А.Е. Правовой режим доступа правоохранительных органов к информации операторов связи // Вестник ВИ МВД России. 2014. №3. С. 99.
[2] Обзор судебной практики по уголовным делам о преступлениях, связанных с незаконным оборотом наркотических средств, психотропных, сильнодействующих и ядовитых веществ. Утвержден Президиумом Верховного Суда РФ 27 июня 2012 года.
[3] Приговор от 29 апреля 2019 г. по делу № 1–116/2019 Ленинского районного суда г. Перми // sudact.ru (дата обращения 06.01.2020).
[4] Приговор от 7 марта 2019 г. по делу № 1–51/2019 Лысьвенского городского суда // sudact.ru (дата обращения 06.01.2020).
[5] Приговор от 14 августа 2015 г. по делу № 2–35/2015 Пермского краевого суда // sudact.ru (дата обращения 06.01.2020).

IDentification). Под этим подразумевается особый вид автоматической регистрации объектов при помощи радиочастотного канала связи по уникальному цифровому коду, считываемому из памяти специализированной микросхемы–транспондера[1]. Такая технология может быть применена для защиты товаров в книжных магазинах, продуктов, вещей в магазинах одежды[2], деревьев при незаконной рубке лесов[3], транспортных средств от угонов и хищения[4]. Кроме того, к задачам, которые могут быть решены с помощью радиочастотной идентификации, можно отнести борьбу с незаконным оборотом оружия, боеприпасов, взрывчатых веществ и взрывных устройств; раскрытие и расследование преступлений, связанных с использованием автомобильного транспорта; организацию исполнения наказаний, не связанных с лишением свободы[5].

К преимуществам использования данной системы специалисты относят их размещение без контакта с субъектом, возможность изменения при отчуждении, считывание на значительно удаленном расстоянии, достаточно высокая устойчивость к воздействию окружающих факторов, уникальность кода. Недостатки могут быть обнаружены в случае механического повреждения, угрозы взлома информационной базы с кодами[6], но они могут

[1] Желудков М.А. Вопросы повышения эффективности информационно–технического обеспечения безопасности собственности от корыстных преступлений // Вестник Казанского юридического института МВД России. 2013. №11. С. 37.
[2] Желудков М.А. Указ. соч. С. 37.
[3] Дусева Н.Ю. Возможности использования навигационных систем в раскрытии и расследовании преступлений // Теория и практика общественного развития. 2012. №12. С. 579.
[4] Желудков М.А. К вопросу о повышении эффективности реализации в России аппаратно–программного комплекса «Безопасный город» при обеспечении защиты от корыстной преступности // Вестник экономической безопасности. 2018. №4. С. 96.
[5] Дусева Н.Ю. Там же. С. 579.
[6] Желудков М.А. К вопросу о повышении эффективности реализации в России аппаратно–программного комплекса «Безопасный город» при обеспечении защиты от

быть исправлены при дальнейшем использовании радиочастотной идентификации и разработке научных и практических рекомендаций. Данные технологии обладают большим потенциалом в части получения объективной информации, дают возможность быстрого получения достоверных сведений об интересующих объектах[1].

Электронная информация, содержащаяся в системах радиочастотной идентификации, еще недостаточно используется в судебной практике ввиду вышеназванных причин. Можно найти лишь немного решений, особенно по уголовным делам, где такие данные используются в качестве доказательств. Так, например, в постановлении от 14 марта 2019 г. по делу № 1–11/2019 Сердобского городского суда (Пензенская область) упоминается электронная информация, которая была получена из чипа с антенной (RFID–радиочастотная идентификация) банковской карты[2]. Стоит отметить, что в рамках этого вопроса доказательственное значение имеет не сам чип или банковская карта, а данные из системы радиочастотной идентификации.

Решением от 15 февраля 2018 г. по делу № 12–46/2018 Железнодорожного районного суда г. Пензы установлено, что в ходе осмотра с применением RFID – оборудования и с используемым программным обеспечением ISOSTART произведена радиочастотная идентификация, в результате

корыстной преступности // Вестник экономической безопасности. 2018. №4. С. 97.

[1] Дусева Н.Ю. Использование современных программно–технических комплексов систем навигации в раскрытии и расследовании преступлений // Современные проблемы науки и образования. 2014. № 4. URL : https://science–education.ru/ru/article/view?id=14294 (дата обращения 06.01.2020).

[2] Постановление от 14 марта 2019 г. по делу № 1–11/2019 Сердобского городского суда (Пензенская область) // sudact.ru (дата обращения 06.01.2020).

которой на 3–х реализуемых изделиях из натурального меха, выявлен факт несоответствия данных[1].

Таким образом, можно сделать вывод, что данная система, несмотря на большой потенциал и возможную эффективность при расследовании преступлений, еще недостаточно используется, что требует дальнейшей разработки организационных, правовых, технических мер вопроса применения радиочастотной идентификации.

Кроме того, можно остановиться на таком часто распространенном технологическом источнике, как MAC–адрес. Под этим понимается уникальный цифровой номер, присвоенный сетевой карте оборудования[2], который в отличие от IP–адреса или виртуального является физическим адресом. MAC–адрес необходим для идентификации пользователя и получателя информации, но при этом может возникнуть ситуация, когда принадлежность адреса конкретному лицу не свидетельствует о том, что источником информации является именно это лицо[3], что может привести к ошибкам в определении обстоятельств, подлежащих установлению по конкретному делу. Определение MAC–адреса пользователя может способствовать более эффективному раскрытию преступлений, где участвует электронный носитель информации, его установление обычно относится к первым этапам расследования таких преступлений.

---

[1] Решение от 15 февраля 2018 г. по делу № 12–46/2018 Железнодорожного районного суда г. Пензы // // sudact.ru (дата обращения 06.01.2020).

[2] Курьянова М.Н., Товба О.Н. Проблемы раскрытия и расследования преступлений, связанных с распространением материалов порнографического характера в сети Интернет // Вестник ВИ МВД России. 2016. №3. С. 123.

[3] Стороженко О.Ю. Система технических средств для обеспечения функций оперативно–розыскных мероприятий: вчера, сегодня, завтра // Вестник КРУ МВД России. 2014. №3 (25). С. 70.

Судебная практика также свидетельствует о частом использовании и упоминании MAC–адресов при рассмотрении уголовных дел. При этом он может быть указан как в качестве характеристики наравне с другими компьютера или иного устройства как вещественного доказательства[1], так и в качестве непосредственной электронной доказательственной информации при осмотре компьютера и заключении при производстве компьютерно–технической экспертизы[2].

Таким образом, можно сделать вывод, что информационно–технологические источники электронных следов многочисленны и будут только увеличиваться в связи с постоянным прогрессом в данной сфере, не подлежит ограничительному толкованию. При рассмотрении этого вопроса имеет значение не сам физический носитель или его характеристики, а то, что может быть извлечено как электронная информация из таких источников.

1.3. Уголовно–процессуальное регулирование при собирании электронной доказательственной информации

Впервые законодательное закрепление понятия электронных носителей информации было осуществлено в 2012 году. Федеральным законом "О внесении изменений в Уголовно–процессуальный кодекс

[1] Приговор от 17 апреля 2019 г. по делу № 1–169/2019 Златоустовского городского суда (Челябинская область) // sudact.ru (дата обращения 06.01.2020); Приговор от 19 июня 2019 г. по делу № 1–183/2019 Краснооктябрьского районного суда г. Волгограда (Волгоградская область) // sudact.ru (дата обращения 06.01.2020).

[2] Приговор от 14 марта 2019 г. по делу № 2–16/2019 Волгоградского областного суда (Волгоградская область) // sudact.ru (дата обращения 06.01.2020); Приговор от 6 февраля 2019 г. по делу № 1–20/2019 Правобережного районного суда г. Магнитогорска (Челябинская область) // sudact.ru (дата обращения 06.01.2020.

Российской Федерации" от 28.07.2012 N 143–ФЗ в действующий УПК РФ были внесены существенные изменения, определившие направление дальнейшего совершенствования законодательства в этой части. Так, были детализированы условия хранения электронных носителей информации, их возвращение законному владельцу после осмотра и производства других необходимых следственных действий, предусмотрена возможность копирования указанной информации с участием законного владельца изъятых электронных носителей информации и (или) его представителя и специалиста в присутствии понятых. Данное право предоставлено в целях обеспечения интересов хозяйствующих субъектов при изъятии сведений, содержащихся на изымаемых носителях, при этом не допускается копирование информации, если это может воспрепятствовать расследованию преступления.

Федеральным законом от 23.06.2016 № 220–ФЗ была введена статья 474.1 УПК РФ, которая предоставила возможность участникам процесса подать ходатайство, заявление, жалобу в виде электронного документа посредством заполнения установленной формы[1]. Положения данной статьи применяются при наличии технической возможности в суде. Это может выступать в качестве одного из первых шагов к переходу на электронный документооборот, что приведет к увеличению состязательности и открытости уголовного процесса.

[1] "О внесении изменений в отдельные законодательные акты Российской Федерации в части применения электронных документов в деятельности органов судебной власти" : федеральный закон от 23.06.2016 N 220–ФЗ // Официальный интернет–портал правовой информации http://www.pravo.gov.ru, 23.06.2016.

При этом на законодательном уровне не было сформулировано понятие электронных носителей информации и не определено его содержание, что значительно затрудняет возможность отнесения тех или иных устройств к электронным носителям информации. Специалисты в основном придерживаются подхода, который установлен в соответствии с ГОСТ 2.051–2013, и определяют электронный носитель как материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники[1]. Однако в теории криминалистики и уголовного процесса по настоящее время существует дискуссия по вопросу определения данного понятия. Например, Ю.В. Гаврилин расширяет определение электронных носителей информации таким признаком, возможность передачи по информационно–телекоммуникационным сетям или обработки в информационных системах[2], то есть распространяет его также на персональные компьютеры и серверы, иные устройства, конструктивно предназначенные для постоянного или временного хранения компьютерной информации, что позволит избежать терминологической чехарды[3]. Установление данной дефиниции имеет существенное и наиболее важное значение при решении судом вопроса о применении норм УПК, касающихся особенности производства следственных действий, например,

[1] ГОСТ 2.051–2013 Единая система конструкторской документации (ЕСКД). Электронные документы. Общие положения (с Поправкой) : М.: Стандартинформ, 2014 год.
[2] Гаврилин Ю.В. Электронные носители информации в уголовном судопроизводстве // Труды Академии управления МВД России. 2017. N 4 (44). С. 47, 48.
[3] Воронин М.И. Электронные доказательства в УПК: быть или не быть? // Lex Russica. 2019. № 7 (152). С. 76.

о привлечении специалиста, понятых, к устройству, как электронному носителю информации. Это будет основным фактором при определении допустимости такого доказательства в дальнейшем. По нашему мнению, понятие электронных носителей информации должно трактоваться так, как оно нормативно установлено, если не на законодательном уровне, то хотя бы на уровне ведомственных актов, то есть в соответствии с вышеуказанным ГОСТом, и закреплено в статье 5 УПК РФ[1], в которой содержатся основные используемые понятия.

Некоторые специалисты отмечают, что введение термина электронный носитель информации в УПК – промежуточный шаг на пути к возможному появлению категории электронных доказательств в уголовном процессе[2]. Данный вопрос является дискуссионным в теории процессуального права и не теряет своей актуальности. Так, основные подходы к его решению состоят в следующем:

1) необходимость введения в УПК нового вида доказательств – электронных – ввиду их специфических особенностей и невозможности существования в рамках традиционных доказательств[3]. У данной точки зрения существует много недостатков, которые заключаются в том, что включение термина еще преждевременно, существует много неразработанных вопросов, например, разграничение по содержанию с такими видами доказательств, как

[1] Воробей С.Н. Проблемы правовой регламентации процессуального порядка изъятия электронных носителей и копирования содержащейся на них информации // Закон и право. 2020. №1. С. 114.
[2] Оконенко Р.И. "Электронные доказательства" и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации: дис канд. юрид. наук. М., 2016. С. 102.
[3] Зигура Н.А., Кудрявцева А.В. Компьютерная информация как вид доказательства в уголовном процессе России: Монография. М., 2011. С. 30.

вещественное и иной документ, в качестве которых чаще всего выступает электронная информация. Также некоторые говорят о несоответствии введения этого термина с уже существующими положениями УПК, так, под доказательствами понимается любые сведения, на основании которых могут быть установлены обстоятельства, подлежащие доказыванию по конкретному делу, то есть, закон не делает исключений для электронной формы существования доказательств[1]. В качестве аргумента ученые приводят то, что если признать за компьютерной информацией отдельный вид доказательств, то необходимо будет признать таковой и показания обычных электронных криминалистических приборов, что, конечно, не соответствует действительности и теории уголовного процесса[2]. Отдельные специалисты высказывают мнение, согласно которому перечень доказательств подлежит расширению за счет допуска показаний (подозреваемого, обвиняемого, свидетеля и др.), заключения эксперта, специалиста в электронно–цифровой форме, электронных вещественных доказательств, электронных следственных и судебных действий[3]. Считаем, что это приведет к неоправданному увеличению перечня видов доказательств, запутанности, так как отличается от уже существующих только электронной формой;

---

[1] Пастухов П.С. «Электронные доказательства» в нормативной системе уголовно–процессуальных доказательств // Пермский юридический альманах. Ежегодный научный журнал. 2019. № 1 // СПС «КонсультантПлюс» (дата обращения 07.01.2020).

[2] Окоменко Р.И. Указ. соч. С. 102.

[3] "Уголовно–юрисдикционная деятельность в условиях цифровизации: Монография" (Голованова Н.А., Гравина А.А., Зайцев О.А. и др.) ("ИЗиСП", "КОНТРАКТ", 2019) // СПС «КонсультантПлюс» (дата обращения 07.01.2020).

2) электронная информация инкорпорируется в УПК путем существования в форме уже содержащихся там доказательств – вещественного и иного документа, специфика которых заключается в том, что здесь играет роль не сам материальный носитель и его свойства, а содержащаяся на нем информация. Мы солидарны с данной точкой зрения, которая заключается в том, что отсутствует необходимость во введении нового института, нужно лишь уточнить в УПК РФ то обстоятельство, что уже существующие доказательства могут быть представлены в виде электронной информации[1]. Данной концепции придерживается в настоящее время большинство ученых, таких, как Р.И. Оконенко, М.И. Воронин, Л.В. Головко, С.В. Зуев, П.С. Пастухов и другие. Сам термин электронные доказательства может быть использован как категория процессуального права для обозначения общей группы носителей, которые содержат в себе доказательственную электронную информацию. По нашему мнению, в этом вопросе правы специалисты, которые отмечают отсутствие необходимости в закреплении закрытого перечня доказательств как анахронизма[2], это могут быть любые сведения, которые соответствуют критериям относимости, допустимости и достоверности.

Важнейшим аспектом при рассмотрении этого вопроса является определение критериев допустимости электронных доказательств, которые будут отличаться от уже существующих для традиционных. По мнению П.С.

[1] Пастухов П.С. «Электронные доказательства» в нормативной системе уголовно–процессуальных доказательств // Пермский юридический альманах. Ежегодный научный журнал. 2019. № 1 // СПС «КонсультантПлюс» (дата обращения 07.01.2020).
[2] Воронин М.И. Указ. соч. С. 77.

Пастухова, проблема внедрения электронной информации в уголовный процесс заключается в том, что стандарт допустимости доказательств основан на их существовании в письменной форме, что создает препятствия для перевода процессуального документооборота в электронный[1]. До сих пор среди ученых и практиков возникает противоречивое мнение о надежности таких доказательств, несмотря на объективность и их точность, в меньшей мере зависимость от субъекта их получения, специалисты отмечают, что для принятия их в суде требуются большие гарантии, чем для традиционных доказательств[2]. Решением может стать создание единых средств проверки надежности представленных электронных доказательств, установлении их верифицируемости, аутентичности. Многие определяют проверяемость, неизменность электронной информации как основополагающее качество при использовании их в практической деятельности[3]. Специалисты по–разному устанавливают средства проверки электронных доказательств, например, в их качестве могут выступать проведение компьютерно–технической экспертизы, криптостойкая хеш–функция[4] – для подтверждения любой электронной информации, использование единых принципов,

[1] Пастухов П.С. «Электронные доказательства» в нормативной системе уголовно–процессуальных
доказательств // Пермский юридический альманах. Ежегодный научный журнал. 2019. № 1 // СПС
«КонсультантПлюс» (дата обращения 07.01.2020).

[2] Основы теории электронных доказательств: монография / под ред. докт. юрид. наук С.В. Зуева. М.: Юрлитинформ, 2019. С. 79.

[3] Григорьев В.Н., Максимов О.А. Об электронных носителях информации в уголовном судопроизводстве // Вестник ННГУ. 2019. №3. С. 67.

[4] Хеш–функция или функция свёртки — функция, осуществляющая преобразование массива входных данных произвольной длины в (выходную) битовую строку установленной длины, выполняемое определённым алгоритмом. Среди множества существующих хеш–функций принято выделять криптографически стойкие, применяемые в криптографии, так как на них накладываются дополнительные требования.

разработанных международными организациями, которые могут быть включены в текст УПК или бланкетная норма, которая бы к ним отсылала[1]. Некоторые предлагают установить не технические критерии допустимости, а особенности самих электронных носителей, такие, как факт нахождения информации на носителе, создание в ходе расследуемого события, необходимость применения специальных устройств, возможность вносить изменения в содержание без непосредственного воздействия[2], что по нашему мнению, носит слишком общий характер, неэффективно при использовании непосредственно в практической деятельности, такие требования должны носить все–таки технический характер.

Таким образом, полагаем, что основным вопросом при использовании электронных доказательств является установление критериев допустимости или надежности, причем это должны быть именно технические критерии, а не общие принципы, сформулированные с юридической точки зрения. Несмотря на пока еще часто проявляемое недоверие к такой доказательственной информации, они более верифицируемы по сравнению с другими доказательствами, уменьшает субъективные факторы до возможного минимума при их получении, хранении.

Интересной представляется точка зрения, в соответствии с которой может быть создана по аналогии с камерой хранения вещественных доказательств виртуальная комната хранения электронной информации, а также

[1] Пастухов П.С. Средства проверки надежности "электронных" доказательств в ходе производства по уголовному делу // Пробелы в российском законодательстве. 2015. №3. С. 171.
[2] Григорьев В.Н., Максимов О.А. Там же. С. 67.

межведомственные сети с передачей этих данных в суд с проверкой их целостности и неизменности[1]. Сейчас говорить об этом, конечно, преждевременно, но такая возможность может выступать в качестве направления для развития применения электронной информации в уголовном процессе.

ГЛАВА II. ОБНАРУЖЕНИЕ, ОСМОТР, ИЗЪЯТИЕ И ФИКСАЦИЯ ЭЛЕКТРОННЫХ СЛЕДОВ КАК ДОКАЗАТЕЛЬСТВ

2.1. Уголовно–процессуальные и криминалистические особенности получения электронной доказательственной информации

В соответствии со статистическими данными 78 % следователей не учитывают при производстве следственных действий особенности и возможности компьютерной информации, 22 % всех опрошенных ориентируются на

[1] Пастухов П. С. О развитии уголовно–процессуального доказывания с использованием электронных доказательств // Седьмой Пермский конгресс ученых–юристов (г. Пермь, 18–19 нояб. 2016 г.) : сборник научных статей. М. : Статут, 2017. С. 560.

знания специалистов в данном вопросе[1]. Однако в современном мире, где технологии, информатизация проникли во все сферы жизнедеятельности общества, включая возможности людей совершать преступления, так и скрывать их, препятствовать расследованию и раскрытию преступлений, электронные доказательства часто имеют решающее значение по уголовному делу. По мнению А.Л. Осипенко, недостаточное использование электронных следов обусловлено невысокой эффективностью традиционных положений частной криминалистической теории о механизмах следообразования, специфической природой электронных следов[2]. Представляется, что это обусловлено также недостаточной разработкой нормативных и доктринальных правил и рекомендаций по обращению с электронными следами.

Так, в ранее действующих статьях 182, 183 УПК РФ законодатель закрепил стратегически важные правила при работе с электронными следами. При производстве обыска и выемки электронные носители информации изымались с участием специалиста, предусмотрена возможность копирования информации за исключением ситуаций, когда это может воспрепятствовать расследованию преступления либо, по заявлению специалиста, повлечь за собой утрату или изменение информации[3].

---

[1] Зиннуров Ф.К., Хайруллова Э.Т. Особенности работы с электронными носителями как источниками доказательств при проведении следственных действий // Вестник Казанского юридического института МВД России. 2018. №2 (32). С. 275.

[2] Осипенко А.Л., Гайдин А.И. Правовое регулирование и тактические особенности изъятия электронных носителей информации // Вестник ВИ МВД России. 2014. №1. С. 158.

[3] "О внесении изменений в Уголовно–процессуальный кодекс Российской Федерации" : федеральный закон от 28.07.2012 N 143–ФЗ (последняя редакция) // СЗ РФ. 2012, N 31. Ст. 4332.

Далее долгожданные в научном сообществе изменения были внесены только 27 декабря 2018 года и вступили в силу 8 января 2019 года. Федеральным законом № 533–ФЗ была включена новая статья – 164.1 УПК РФ, которая объединила в себе основные положения по обнаружению, исследованию, фиксации электронных следов и получила название – «Особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий». В пояснительной записке цель введения статьи заключалась в улучшении делового климата в РФ, обеспечении гарантий защиты предпринимателей[1], однако некоторые негативно оценили данный факт как ущерб для основного предназначения уголовного судопроизводства, расширения частных начал[2]. Но представляется, что должен быть обеспечен баланс частных и публичных интересов при расследовании преступлений. С юридической точки зрения это было сделано, в том числе, чтобы распространить действие данной нормы на все следственные действия, осуществляемые с использованием электронных устройств. В статью был включена часть, содержащая исключительные обстоятельства, при которых изъятие электронных носителей информации допускается, а именно, когда: 1) вынесено постановление о назначении судебной экспертизы в отношении электронных носителей информации; 2) изъятие производится на основании судебного решения; 3) на

[1] Бондаренко А.А. Изъятие электронных носителей информации при расследовании уголовных дел экономической и общеуголовной направленности, а также по соединенным уголовным делам // "Законодательство и практика", 2019, N 1 // СПС «КонсультантПлюс» (дата обращения 08.01.2020).
[2] Панфилов П.О., Победкин А.В. Очередное обострение конкуренции конституционных ценностей при расследовании преступлений в сфере экономической и предпринимательской деятельности // Вестник Московского университета МВД России. 2020. №1. С. 108.

электронных носителях информации содержится информация, полномочиями на хранение и использование которой владелец электронного носителя информации не обладает, либо которая может быть использована для совершения новых преступлений, либо копирование которой, по заявлению специалиста, может повлечь за собой ее утрату или изменение[1]. Однако данные изменения не внесли достаточной ясности в процесс собирания, изъятия и фиксации электронных следов. Ученые приходят к выводу, что закрепление вышеназванных исключений не способствовали более эффективному их применению на практике. Так, первая названная в статье ситуация, когда выносится постановление о назначении экспертизы, по мнению специалистов, будет возникать крайне редко, так как оно может быть вынесено только после осмотра и изъятия соответствующих носителей[2], а на данной стадии они могут быть еще даже не установлены следователем. Толкование второго исключения может быть затруднено, по мнению А.А. Бондаренко данное положение также фактически работать не будет[3], не установлены случаи, когда судебное решение необходимо получать, а даже при его получении удобнее назначать судебную экспертизу, в постановлении о назначении которой можно будет корректировать объект исследования и круг вопросов, в отличие от решения суда. Что же касается третьей ситуации, то это, полагаем, может привести к неосновательному увеличению пределов

[1] "О внесении изменений в статьи 76.1 и 145.1 Уголовного кодекса Российской Федерации и Уголовно–процессуальный кодекс Российской Федерации" : федеральный закон от 27.12.2018 N 533–ФЗ // "Российская газета", N 295, 29.12.2018.
[2] Васюков В. Ф. Особенности изъятия электронных носителей информации при производстве следственных действий: новеллы законодательства и проблемы правоприменения // Криминалистика: вчера, сегодня, завтра. 2019. №2 (10). С. 10.
[3] Бондаренко А.А. Указ. соч.

производства следственного действия[1] и нарушению прав его участников, которые выражаются в изъятии предметов и информации, не имеющих прямого отношения к уголовному делу. Однако существует противоречивое мнение среди специалистов, с одной стороны, это необходимо в целях предупреждения совершения новых преступлений, с другой стороны, получение электронной доказательственной информации недопустимо на основании предположений и усмотрения должностных лиц. Отдельные ученые указывают на тот факт, что в протоколе должны быть указаны конкретные данные, подтверждающие выводы о необходимости изъятия электронного носителя[2].

Кроме того, ученые отмечают некоторые недоработки и в других частях ст. 164.1 УПК РФ. Например, это касается привлечения понятых при производстве копирования электронной информации, которые по общему правилу выступают в качестве дополнительной гарантии допустимости получаемых доказательств[3], но в этой ситуации не до конца понятно, факт чего они будут подтверждать – заявления ходатайства, копирования как действия, участия специалиста, правильность и полноту копирования[4], а также как именно это будет происходить при большом объеме электронной информации и отсутствия специальной подготовки и необходимых знаний у понятых, чтобы понимать сущность происходящего. Считаем, что данный

[1] Бондаренко А.А. Указ. соч.
[2] Панфилов П.О., Победкин А.В. Очередное обострение конкуренции конституционных ценностей при расследовании преступлений в сфере экономической и предпринимательской деятельности // Вестник Московского университета МВД России. 2020. №1. С. 110.
[3] Григорьев В. Н. Тенденции и проблемы развития законодательства в области информационных технологий, регулирующего уголовное судопроизводство // Академическая мысль. 2019. №3 (8). С. 58.
[4] Бондаренко А.А. Указ. соч.

вопрос нуждается в дальнейшей разработке. Остальные возникающие при применении данной статьи проблемы будут рассмотрены отдельно в следующих параграфах.

Основными путями собирания электронных следов являются сохранение имеющихся сведений о сообщениях, передаваемых по сетям электросвязи («исторические данные»), реализуемое в рамках осмотра, обыска и выемки, и отслеживание сообщений, передаваемых по сетям в реальном масштабе времени (то есть лицо, осуществляющее незаконную деятельность, устанавливается непосредственно во время совершения преступления), которое реализуется в рамках оперативно–розыскных мероприятий[1].

Существенным является вопрос о том следственном действии, в рамках которого производится извлечение данных из электронных носителей информации. По мнению А.М. Багмета, С.Ю. Скобелина, извлечение данных из электронных устройств представляет собой самостоятельное следственное действие, они аргументируют позицию тем, что данное действие соответствует признакам следственного, а именно, обнаружение и изъятие доказательств в ходе такого извлечения, возможность использования электронных устройств в целях фиксирования и закрепления полученных доказательств[2]. В настоящее время извлечение осуществляется в рамках осмотра предмета, назначения и проведения экспертизы, производства оперативно–розыскных мероприятий. Но данное действие по своим целям не совпадает с вышеперечисленными следственными и иными

[1] Волеводз А.Г. Следы преступлений, совершенных в компьютерных сетях // Российский следователь. 2002. № 1. С. 6.
[2] Багмет А.М., Скобелин С.Ю. Извлечение данных из электронных устройств как самостоятельное следственное действие // Право и кибербезопасность. М.: Юрист, 2013, № 2 (3). С. 24.

мероприятиями. Такого же мнения придерживается и С.В. Зуев, который предлагает внести в УПК РФ новые следственные действия – изъятие электронных носителей информации и копирование электронной информации[1]. Несмотря на то, что выделение такого самостоятельного действия не лишено смысла, это может создать затруднительное положение правоприменителя при разграничении соответствующих следственных действий. По нашему мнению, выделение извлечения данных из электронных устройств имеет все основания для закрепления в качестве самостоятельного следственного действия в статье 164.1 УПК РФ. По сути создание законодателем данной статьи в декабре 2018 года можно рассматривать как начальный этап по его отделению.

Несмотря на определенные исключения, например, в одном из приговоров упоминается осмотр записи видеонаблюдения[2], осмотр и прослушивания фонограммы[3], осмотр информации, содержащейся на накопителе жестких магнитных дисках[4], в настоящее время на основании материалов приговоров судов Пермского края можно сделать однозначный вывод о том, что действия с использованием электронных устройств осуществляются в рамках осмотра предмета и оформляются соответствующим протоколом[5].

---

[1] Зуев С.В. Указ. соч. С. 79.
[2] Приговор от 2 марта 2016 г. по делу № 1–56/2016 Кудымкарского городского суда Пермского края (постоянное судебное присутствие в с. Юсьва) // sudact.ru (дата обращения 22.01.2020).
[3] Приговор от 14 января 2016 г. по делу № 1–4/2016 Индустриального районного суда г. Перми // sudact.ru (дата обращения 22.01.2020).
[4] Приговор от 29 октября 2015 г. по делу № 1–287/2015 Ленинского районного суда г. Перми // sudact.ru (дата обращения 24.04.2019).
[5] См. например, Приговор от 19 июля 2018 г. по делу № 1–264/2018 Мотовилихинского районного суда г. Перми // https://www.sudact.ru (дата обращения 24.04.2019); Приговор от 25 мая 2018 г. по делу № 1–63/2018 Чернушинского районного суда Пермского края // https://www.sudact.ru (дата обращения 24.04.2019).

Обнаружение и собирание электронных следов связано с использованием специального оборудования. Особенности применяемых технико–криминалистических средств заключаются в возможности быстро и безопасно восстанавливать и анализировать удаленные и недоступные данные, восстанавливать поврежденную информацию[1]. Так, правоохранительными органами успешно применяется аппаратно–программный комплекс UFED. Данное устройство позволяет полное извлечение таких данных мобильного телефона, как телефонная книга, текстовые сообщения, фотографии, видеоизображения, журналы звонков (исходящих, входящих, пропущенных), звуковые файлы; клонирование идентификатора SIM–карты, анализ содержимого телефона без каких–либо сетевых операций и необходимости «взламывать» SIM–карту, заблокированную PIN–кодом; мобильная судебная лаборатория в полевых условиях, портативное, быстрое и удобное в на месте происшествия[2].

В соответствии с приказом Следственного комитета РФ в 2013 г. все следственные управления СК РФ были обеспечены комплексами UFED. В 2014 г. комплекс применялся 11 752 раза, что на 45 % больше, чем за аналогичный период прошлого года (6566), в результате его использования обнаружено и изъято 9068 информационных следов, имеющих доказательственное значение[3].

---

[1] Пастухов П.С. О необходимости развития компьютерной криминалистики // Пермский юридический альманах. 2018. № 1. С. 481.

[2] UFED System. Универсальное устройство извлечения судебной информации. URL : http://www.rom.by/files/UFED.pdf (дата обращения 27.12.2019).

[3] О работе следователей–криминалистов следственных органов Следственного комитета Российской Федерации в 2014 году : аналитическая справка. Документ официально опубликован не был.

Еще одним уникальным технико–криминалистическим средством является Мобильный Криминалист, который обеспечивает доступ специалиста к общей информации об устройстве, включая контакты, звонки, органайзер, сообщения, фотографии, видео, аудио, данные из более 400 приложений: Apple Maps, Booking.com, Facebook, Google+, PayPal, Safari, Skype, Viber, WhatsApp и так далее, также все удаленные данные с электронного устройства[1]. Мобильный криминалист предназначен также для анализа извлекаемых данных, что имеет особое значение при необходимости оперативно осуществлять расследование. Он позволяет объединять контакты из разных источников, выстраивать все события в хронологическом порядке; осуществлять поиск данных по регулярным выражениям, хеш–наборам, номерам телефонов, паспортов, СНИЛС и другим критериям, строить маршруты передвижения одного или нескольких человек, выявлять самые посещаемые места конкретным субъектом и места общего пребывания нескольких лиц[2].

Зарубежными аналогами данных программ являются XRY Logical – это быстрый метод извлечения, позволяющий получать и восстанавливать данные в режиме онлайн файловой системы с устройства прямо на месте преступления, напрямую связывая их с операционной системой устройства независимо от данной системы[3], а также EnCase Forensic, локальное программное обеспечение для проведения компьютерно–технической экспертизы,

[1] Oxygen Software. URL : http://www.oxygen–forensic.com/ru (дата обращения 29.04.2019).
[2] Бессонов А.А. О некоторых возможностях современной криминалистики в работе с электронными следами // Вестник Университета имени О.Е. Кутафина. 2019. №3 (55). С. 48.
[3] Xry Logical – извлечение данных. URL : https://www.msab.com/products/xry/ (дата обращения 29.04.2019).

являющееся по сути международным стандартом поиска цифровых улик и предоставления данных в суд. EnCase Forensic позволяет экспертам выявлять потенциальные доказательства путем криминалистического анализа информации, содержащейся на жестком диске, и подготавливать полные отчеты о полученных результатах, сохраняя при этом надежность и целостность полученных доказательств[1].

Для исследования «больших данных» или Big Data, которые все чаще встали использоваться при совершении преступлений, предусмотрены специальные программы для анализа – IBM i2 Analyst's Notebook, «Сегмент–С», «Следопыт» и др. Их задачи сводятся к аналитическому исследованию больших массивов электронной информации. Например, это может быть установление транспортных средств, использованных в серии преступных деяний; выявление мобильных устройств, которые связаны с одним или несколькими событиями; определение лиц из круга общения интересующих следствие подозреваемых, потерпевших и т.д., систему их взаимосвязей и др[2].

Так, после обнаружения электронных следов необходимо осуществить их осмотр, который также характеризуется рядом особенностей по сравнению с другими видами следов. В.Ф. Васюков, А.В. Булыжкин выделяют следующие этапы осмотра электронных носителей информации: 1) внешний осмотр, при котором происходит непосредственное изучение и фиксация наружного строения и состояния аппарата, в рамках которого в протоколе указываются марка, модель,

[1] Cellebrite. URL : https://www.cellebrite.com/en/law–enforcement/investigation/ (дата обращения 29.04.2019).
[2] Бессонов А.А. Указ. соч.

тип, форма аппарата, цвет корпуса, размер и остальные особенности внешнего строения, особые приметы наружного строения (повреждения, наличие дополнительных атрибутов и технических составляющих и др.); 2) конструктивный осмотр, при котором производится осмотр конструкции по частям; 3) осмотр информационной среды, который включает изучение и фиксацию сведений, которые содержатся в самом устройстве[1]. Второй и третий этап осмотра осуществляется уже в рамках дальнейшего назначения судебной экспертизы ввиду недостаточности познаний следователя, который в принципе может осуществить первый этап осмотра в отсутствие специалиста, если это не связано с угрозой потери информации. А.Н. Колычева предлагает подразделять осмотр, связанный с электронными носителями, на осмотр страниц, интернет–сайта, электронной почты, истории сообщений, информации Интернет–соединений абонента и (или) абонентских устройств[2]. Полагаем, что это не имеет здесь существенного значения, так как данные разновидности обладают общими особенностями, связанными с применением электронной информации.

При фиксации вышеуказанных действий все производимое необходимо детально отражать в протоколе, однако только словесное описание может привести к субъективной оценке тех или иных фактов[3]. Это возможно и при производстве остальных следственных действий, но здесь при описании операций, осуществляемых с электронными

[1] Васюков В.Ф., Булыжкин А.В. Указ. соч.
[2] Колычева А.Н. Указ. соч. С. 40.
[3] Васюков, В. Ф. Некоторые вопросы проведения следственных действий, направленных на обнаружение, фиксацию и изъятие электронных сообщений, переданных посредством мобильных абонентских устройств сотовой связи // Российский следователь. 2016. № 23. С. 16.

носителями информации, может возникнуть проблема в самом словесном описании в протоколе ввиду избыточности материала, который должен быть зафиксирован и сложности производимых действий. Данная ситуация может быть решена применением видеосъемки при производстве осмотра, выемки, обыска электронных устройств, при чем в кадре всегда должен находиться экран устройства, освещаться все манипуляции, которые производит с ним следователь или специалист[1].

К средствам допустимой фиксации интернет–информации можно также отнести: распечатанные скриншоты или страницы веб–сайта, формальные реквизиты (URL–адрес сайта, дата обращения, системное время компьютера на момент фиксации информации и др.); сообщение организации, предоставляющей услуги хостинга (размещения) веб–ресурса о контенте (содержимом) сайта, либо сообщение регистратора доменного имени о том, кто является владельцем конкретного имени[2].

Далее после осмотра необходимо надлежащим образом упаковать электронные носители, здесь также можно выделить определенные особенности по сравнению с обычным процессом. Так, все устройства должны опечатываться, в частности все порты, слоты, входы и выходы, чтобы обеспечить сохранность криминалистически значимой информации и невозможность внесения изменений. Но в силу особенностей электронных следов необходимо предусмотреть также и возможный

[1] Кучин О.С. Указ. соч. С. 90.
[2] Бахтеев Д.В. Особенности фиксации и изъятия криминалистически значимой информации, размещенной в сети Интернет // "Российский следователь", 2017, N 21 // СПС «КонсультантПлюс» (дата обращения 08.01.2020).

бесконтактный доступ к данным устройствам, для чего был создан специальный чехол – Мешок Фарадея, блокирующий доступ к носителю информации[1]. В случае отсутствия такого устройства самым надежным является упаковка объектов в пластиковый пакет (мешок) или коробку, при этом горловина пакета прошивается нитью, узел нити оклеивается биркой с пояснительной надписью. Некоторые специалисты указывают, что на подготовительном этапе следственного осмотра, обыска и выемки следователю (дознавателю) необходимо учитывать, какой электронный носитель будет являться объектом следственного действия в целях дальнейшей их упаковки[2]. От того, насколько правильно и грамотно будет упакован обнаруженный носитель информации, зависит результат экспертного исследования. На практике же эксперты–криминалисты сталкиваются с несоблюдением правил упаковки электронных устройств, при котором возможен свободный доступ ко всем разъемам и кнопкам включения/выключения/перезагрузки, что может привести к дальнейшему искажению информации, содержащейся в электронном носителе.

2.2. Использование специальных знаний при получении электронной доказательственной информации

Основными формами участия специалиста в процессе получения электронной доказательственной информации заключаются в справочно–консультационной деятельности, производстве экспертиз, связанными с электронными

[1] Скобелин С.Ю. Указ. соч. С. 33.
[2] Зиннуров Ф.К., Хайруллова Э.Т. Указ. соч. С. 275.

следами и, в отличие от общей теории осуществления следственных действий участие при изъятии электронных носителей информации.

Статья 164.1 УПК, которая была введена в действие в январе 2019 года и призвана разрешить противоречия в науке и правоприменительной практике в отношении привлечения специалиста, закрепила его обязательное императивное участие во всех следственных действиях, связанных с изъятием электронных носителей информации. Однако это не привело к упорядочению судебной практики и выработке единой позиции среди ученых и судей. Так, существует несколько диаметрально противоположных мнений в отношении определения необходимости участия специалиста при обыске и выемке электронных носителей информации. Можно выделить следующие подходы: 1) первая группа ученых, которые допускают возможность привлечения специалиста по усмотрению следователя в зависимости от потребностей производства тех или иных следственных действий, если доступ к информации невозможен. При этом они аргументируют свою позицию ссылкой на ст. 168 УПК РФ, которая закрепляет право следователя привлекать специалиста к производству следственных действий, обуславливает при этом независимость, самостоятельность следователя при раскрытии и расследовании преступлений[1]. Представляется, что данное положение вступает в противоречие с нормой, непосредственно установленной в УПК в отношении привлечения специалиста. Законодатель не оговаривает

[1] Першин А.Н. Электронный носитель информации как новый источник доказательств по уголовным делам // Уголовный процесс. 2015. N 5. С. 50.

какие–либо особые случаи, при которых отсутствует необходимость привлечения специалиста, правило сформулировано им императивно. Данный подход не лишен рациональности, но, возможно, отсутствие в УПК РФ диспозитивности относительно норм о необходимости участия специалиста, обусловлено особой значимостью электронных следов в уголовных делах, связанных с использованием таких устройств, их сложностью и своеобразием, также возможностью потери при ненадлежащей работе с ними.

Стоит отметить, что судебная практика идет по такому же пути, несмотря на законодательное закрепление императивного правила. Так, Апелляционным определением Брянского областного суда от 20 марта 2015 г. по делу № 22–329/2015 было признано законным изъятие электронных носителей информации (телефона обвиняемого) без участия специалиста. Суд аргументировал свою позицию тем, что по смыслу норм уголовно–процессуального закона участие специалиста при производстве выемки электронных носителей информации требуется в тех случаях, когда для этого необходимо использование специальных познаний, связанных с обнаружением и копированием информации с электронных носителей[1]. По сути, суд при вынесении данного определения игнорировал императивные положения УПК РФ в отношении участия специалиста и истолковал ее абсолютно по–своему.

Апелляционным определением Пермского краевого суда от 14 октября 2014 г. по делу № 22–7127/2014 было

[1]Апелляционные определение Брянского областного суда от 20 марта 2015 г. по делу № 22–329/2015 // https://www.sudact.ru (дата обращения 24.04.2019).

установлено, что отсутствие специалиста при выемке электронного носителя информации (флэшкарты) на существо этого следственного действия не повлияло, и его результаты, то есть сам факт изъятия у работника полиции флэшкарты с видеозаписью, поставить под сомнение не могут[1]. Данный довод суда кажется немного необоснованным, так как признание какого–либо доказательства недопустимым ввиду нарушения порядка его получения не зависит от того, повлияет ли этот факт на существо следственного действия.

В большинстве судебных актов участие специалиста при осмотре информации на электронных носителях признается излишним (Апелляционное определение Судебной коллегии по уголовным делам Московского городского суда от 25.10.2016 по делу 10–14375/2016). Более того, протокол подобного осмотра является допустимым доказательством даже в случае отсутствия проведения в дальнейшем соответствующей экспертизы записей компьютера или иного цифрового устройства (Апелляционное определение Судебной коллегии по уголовным делам Московского городского суда от 30.06.2016 по делу 10–99015/2016)[2].

2) следующая группа ученых ставит необходимость участия специалиста в зависимость от типа изымаемого электронного устройства. Например, А.Л. Осипенко, А.И. Гайдин, М.В. Старичков, В.А. Антонов указывают, что при изъятии сотового телефона, флешкарты, фотоаппарата специалист может не участвовать в данном следственном

[1] Апелляционное определение Пермского краевого суда № 22–7127/2014 от 14 октября 2014 г. по делу № 22–7127/2014 // https://www.sudact.ru (дата обращения 24.04.2019).
[2] Зазулин И.Ю. Участие специалиста и производство судебных экспертиз при исследовании компьютерной информации // Правопорядок: история, теория, практика. 2018. № 1 (16). С. 112.

действии[1]. Данный подход несколько схож с предыдущим, так как утверждается, что участие специалиста необходимо только при наличии отдельных обстоятельств. Однако здесь вопрос будет именно в определении группы электронных устройств, которые не нуждаются в таком участии, что, несомненно, создаст спорные ситуации при правоприменении. К тому же, в таком случае необходимо установить те общие признаки, по которым будет решаться вопрос об отнесении устройств к данной группе или закреплять исчерпывающий перечень таких электронных носителей информации, что представляется затруднительным ввиду развития технологий.

3) группа ученых, которые определяют участие специалиста как обязательное при производстве следственных действий с электронными носителями информации в соответствии с императивными положениями УПК РФ[2]. Например, В.Б. Вехов указывает, что привлечение специалиста при производстве обыска в отношении электронных устройств является не правом, а обязанностью следователя[3]. Однако данный подход не воспринимается судебной практикой, суды не соглашаются с признанием доказательств недопустимыми ввиду нарушения порядка их изъятия в отсутствие специалиста. Также сложности возникают при решении вопроса о необходимости привлечения специалиста на стадии подготовки к

[1] Васюков В.Ф., Булыжкин А.В. Некоторые особенности осмотра средств сотовой связи при расследовании уголовных дел // Российский следователь. 2014. N 2. С. 3.
[2] Савицкая И.Г. Участие специалиста в следственных действиях, связанных с изъятием электронных носителей информации // Судебная власть и уголовный процесс. 2016. №2. С. 252.
[3] Вехов В. Б. Работа с электронными доказательствами в условиях изменившегося уголовно–процессуального законодательства // Российский следователь. 2013. № 10. С. 22.

определенному следственному действию, так как следователь заранее при выезде на место совершения преступления не может заранее предусмотреть наличие там электронных носителей информации, за исключением преступлений, явно связанных с данной категорией. По мнению ученых, закрепление такой нормы в качестве обязательной является анахронизмом и может привести к повсеместному отвлечению экспертов от производства компьютерно–технической экспертизы, потребность в которых только увеличивается[1].

Данные социологического исследования практических работников органов предварительного расследования показывают негативное отношение к обязательному участию специалиста при изъятии электронных носителей информации. Анкетирование следователей, проходивших повышение квалификации в Дальневосточном юридическом институте МВД России и на Пятом факультете повышения квалификации Московской академии Следственного комитета РФ (г. Хабаровск) в период с марта по сентябрь 2018 г., показало, что 84 % (70 из 83 следователей) опрошенных считают целесообразным исключение из УПК РФ положения об обязательном участии специалиста при изъятии электронного носителя информации. При этом 16 % (13 человек) решили оставить данное положение без изменений[2].

[1] Васюков В.Ф. Особенности изъятия электронных носителей информации при производстве следственных действий: новеллы законодательства и проблемы правоприменения // Криминалистика: вчера, сегодня, завтра. 2019. №2 (10). С. 10.
[2] Зуев С.В., Черкасов В.С. Новые правила изъятия электронных носителей и копирования информации (статья 1641 УПК РФ): преимущества и недостатки новеллы // Сибирское юридическое обозрение. 2019. №2. С. 194.

Что же касается судебной практики, то, например, в Апелляционном постановлении от 17 октября 2017 г. по делу № 10–83/2017 суд приходит к выводу о необходимости исключить из доказательств CD–диск с записью поскольку при изъятии допущены нарушения требований ч.3.1 ст. 183 УПК РФ, то есть в отсутствии специалиста[1]. Но это лишь незначительная часть актов, где суд принимает такое решение. Специалисты отмечают, что только в 10 % судебных решений отсутствие специалиста было признано существенным нарушением и повлекло признание протоколов следственных действий недопустимыми доказательствами[2]. КС РФ также указывает на обязательность участия специалиста в производстве следственных действий, связанных с изъятием электронных устройств[3], что по идее позволяет сделать вывод о неправомерности решений, где устанавливается обратное.

По нашему мнению, необходим дифференцированный подход в данном вопросе в целях эффективного расследования и раскрытия преступлений, на который указывают и многие специалисты[4]. Представляется, что участие специалиста при изъятии электронных носителей информации обязательно только в случае возникновения необходимости в применении специальных знаний и угрозе

---

[1] Апелляционное постановление от 17 октября 2017 г. по делу № 10–83/2017 Соликамского городского суда (Пермский край) // sudact.ru (дата обращения 09.01.2020).

[2] Крюкова Т. С. Некоторые вопросы изъятия электронных носителей информации в ходе производства следственных действий: анализ судебной практики // Правопорядок: история, теория, практика. 2016. № 4 (11). С. 62.

[3] Об отказе в принятии к рассмотрению жалобы гражданки Сандаковой Ирины Сергеевны на нарушение ее конституционных прав пунктом 5 части второй статьи 29 и частью третьей статьи 182 Уголовно–процессуального кодекса Российской Федерации : определение КС РФ от 26 янв. 2017 г № 204–0. URL: http://legalacts.ru (дата обращения 09.01.2020).

[4] Развитие информационных технологий в уголовном судопроизводстве / под ред. С.В. Зуева. М., 2018. С. 139.

потери хранящейся на носителе информации[1]. К этому же мнению приходят и некоторые региональные суды, так, например, в Апелляционном определении Судебной коллегии по уголовным делам Оренбургского областного суда от 03.11.2016 по делу № 22–4229/2016 суд пришел к выводу, что из смысла ч. 3.1. ст. 183 УПК РФ участие специалиста при производстве выемки электронных носителей информации требуется при наличии нуждаемости в данном специалисте. Например, если при производстве выемки производится копирование информации на другие электронные носители информации, участие специалиста обязательно, так как это связано с риском утраты или изменения информации[2].

В приговорах судах Пермского края только в одном судебном акте из двадцати указывается на участие специалиста в процессе осмотра предметов, а именно компьютеров, связанных локальной сетью[3]. Также участие специалиста отмечается в приговоре Советского районного суда города Казани, в котором был исследован протокол осмотра системного блока[4]. При этом не указывается на какие–то особые обстоятельства его привлечения.

К тому же, участие специалиста во всех случаях изъятия электронных устройств представляется не всегда возможным ввиду оперативности производства следственных действий при раскрытии и расследовании преступлений, однако в случаях, когда информация может быть утеряна, такое

[1] Зазулин И.Ю. Указ. соч. С. 112.
[2] Апелляционное определение Судебной коллегии по уголовным делам Оренбургского областного суда от 03.11.2016 по делу № 22–4229/2016 // https://www.sudact.ru (дата обращения 09.01.2020).
[3] Приговор от 27 сентября 2018 г. по делу № 1–124/2018 Ленинского районного суда г. Перми // sudact.ru (дата обращения 09.01.2020).
[4] Приговор от 3 ноября 2017 г. по делу № 1–20/2017 Советского районного суда города Казани Республики Татарстан // sudact.ru (дата обращения 09.01.2020).

привлечение является необходимым. Это будет способствовать более эффективному использованию электронных следов. При этом необходимо внести изменения в УПК РФ в целях соответствия нормативных положений реально складывающимся условиям. Однако в случае если у следователя есть возможность привлечения специалиста к производству данного следственного действия, то это можно делать независимо от угрозы содержащейся на данных устройствах информации. Данное положение может служить только как рекомендательное и учитываться совместно с вышеприведенным подходом.

Следующим спорным вопросом является определение требований, предъявляемых к компетенции такого специалиста. Например, С.В. Зуев полагает, что это может быть специалист средней руки, который должен представлять информацию о наличии диплома о высшем техническом образовании, опыте работы в должности не менее 1 года[1]. Но при этом возникают сомнения относительно уровня необходимого образования такого лица: должно ли быть это только высшее образование или возможно и привлечение специалиста со средним профильным специальным образованием, а также в какой именно должности такое лицо должно получить опыт работы? Данные вопросы остаются нерешенными ни на законодательном, ни ведомственном уровнях. Многие ученые указывают, что в роли таких специалистов могут выступать программисты, сотрудники профильных магазинов и др[2]. Стоит согласиться при решении данного вопроса с А.Л. Осипенко, А.И. Гайдиным, которые

[1] Зуев С.В. Указ соч. С. 79.
[2] Савицкая И.Г. Указ. соч. С. 253.

утверждают, что такой специалист должен разбираться в сложных специфических вопросах (особенностях эксплуатации сетевого оборудования, процедурах шифрования информации и т.п.), иметь достаточные навыки их практического решения (например, владеть методикой применения криминалистических средств выявления и фиксации доказательств)[1]. По мнению П.С. Пастухова, в настоящее время отсутствуют стандарты для аккредитации, сертификации, образования таких специалистов[2]. Представляется, что для практического применения был бы полезен регулярно обновляемый перечень рекомендуемых требований, позволяющих следователю в различных ситуациях определять необходимый уровень квалификации и специализацию привлекаемых к производству следственных действий специалистов[3]. При этом не стоит устанавливать лишь формальные требования к уровню образования такого специалиста, необходимо комплексно подходить к данному вопросу и квалификации такого лица.

Еще в качестве одной проблемы и ученые, и сами сотрудники следственных и оперативных подразделений называют отсутствие необходимой подготовки привлекаемых специалистов. Предлагается, чтобы следователь перед производством следственных действий мог удостовериться в наличии соответствующей компетенции, обладает ли специалист навыками работы при изъятии, фиксации, исследовании электронных носителей информации[4], так как

[1] Осипенко А.Л., Гайдин А.И. Указ. соч. С. 158.
[2] Пастухов П.С. О необходимости развития компьютерной криминалистики // Пермский юридический альманах. 2018. № 1. С. 480.
[3] Осипенко А.Л., Гайдин А.И. Указ. соч. С. 158.
[4] Семикаленова А. И., Рядовский И. А. Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики // Актуальные проблемы российского права. 2019. №6 (103). С. 180.

следователь несет личную ответственность за осуществление расследование. Однако не все следователи на данный момент обладают минимально необходимыми знаниями для определения уровня специалиста. Мы солидарны с точкой зрения, в соответствии с которой в качестве решения этой проблемы некоторые исследователи предлагают расширить информационно–компьютерную составляющую в подготовку будущих следователей и дознавателей либо в рамках основной программы высшего образования либо путем переподготовки или повышения квалификации[1].

Таким образом, можно сделать вывод, что вопросы участия специалиста в производстве следственных действий, связанных с изъятием электронных носителей информации, нуждаются в дальнейшей разработке. Нововведения, которые были осуществлены в 2019 году, в целом оцениваются как положительные в научном сообществе, но императивное участие специалиста не привело к упорядочению судебной практики и выработке единых позиций. Данный вопрос имеет существенное значение, так как может выступать в качестве основания для признания полученных доказательств как недопустимых.

2.3. Проблема соблюдения прав человека и гражданина в процессе получения электронной доказательственной информации

Статья 23 Конституции РФ закрепляет право на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых,

[1] Россинская Е.Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации // Вестник Университета имени О.Е. Кутафина. 2019. №5 (57). С. 33.

телеграфных и иных сообщений[1]. Какое–либо ограничение этого права возможно только на основании судебного решения. Такое же положение установлено и в качестве одного из основополагающих принципов уголовного судопроизводства[2].

Однако действия должностных лиц могут существенно снизить уровень защищенности личности перед государством. Так, любое следственное действие ведет к ограничению прав человека, и в том числе права на личную, семейную тайну. Особенно, когда такое действие связано с электронными носителями, являющимися основным источником информации о жизнедеятельности человека ввиду того уровня распространения высоких технологий, которое достигло наше общество в современное время.

О том, что такое ограничение допускается правоохранительными органами, свидетельствует и судебная практика, а именно жалобы граждан в связи с признанием незаконными действий следователя при проведении осмотра компьютера, телефона и т.д. и извлечение данных из них[3].

Следственное действие, связанное с непосредственным изъятием данных, приводящее к нарушению права на тайну переписки, личную, семейную тайну, которое исходя из толкования норм Конституции РФ и УПК возможно только на основании решения суда, в настоящее время не совпадает ни

---

[1] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6–ФКЗ, от 30.12.2008 N 7–ФКЗ, от 05.02.2014 N 2–ФКЗ, от 21.07.2014 N 11–ФКЗ) // СЗ РФ. 2014, № 31. Ст. 4398.

[2] Уголовно – процессуальный кодекс РФ : федеральный закон РФ № 174–ФЗ от 18.12.2001 (ред. от 06.03.2019) // СЗ РФ. 2001, № 52. Ст. 4921.

[3] См. например, Апелляционное определение Саратовского областного суда № 22–2932 от 24.07.2013 // http://www.samosud.org (дата обращения 12.01.2020); Апелляционное определение Пермского краевого суда № 22–4917 от 16.07.2013 // https://www.sudact.ru (дата обращения 12.01.2020).

с одним другим действием, на производство которого оно необходимо. Однако по характеру умаления прав человека оно не уступает ни получению информации о соединениях между абонентами и (или) абонентскими устройствами, ни наложению ареста на почтовые и телеграфные отправления и др.

Судебная практика разрешает данный вопрос неоднозначно, что свидетельствует об актуальности этой проблемы. Так, в некоторых случаях суд признавал незаконным осмотр следователем содержащейся информации в электронном носителе, ссылаясь на нарушение ст. 8 Конвенции о защите прав человека и основных свобод, положений Конституции РФ[1], нарушение конституционных прав собственности на имущества[2], отсутствие санкции суда[3]. Несмотря на то, что в законодательстве не была закреплена необходимость получения судебного решения, суд всё же пришел к такому выводу, что свидетельствует об особой значимости такого действия, как извлечение информации из электронного устройства. Однако не все суды общей юрисдикции придерживаются данной точки зрения. Так, например, Судебная коллегия по уголовным делам Пермского краевого суда в Апелляционном определении от 16 июля 2013 г. не нашла оснований для удовлетворения жалобы ввиду отсутствия существенных нарушений уголовно–процессуального закона[4]. К таким же выводам

[1] Сергеев М.С. Проблемы соблюдения прав участников уголовного процесса при получении электронной доказательственной информации // ВЭПС. 2017. №2. С. 112.
[2] Апелляционное определение Саратовского областного суда № 22–2932 от 24.07.2013 // http://www.samosud.org (дата обращения: 07.05.2019).
[3] Апелляционное определение Ставропольского краевого суда № 22–733/2014 от 19.02.2014 // https://rospravosudie.com (дата обращения: 07.05.2019).
[4] Апелляционное определение Пермского краевого суда № 22–4917 от 16.07.2013 // https://www.sudact.ru (дата обращения: 07.05.2019).

пришли и Верховный Суд Удмуртской Республики по делу № 22–766/2015[1], Владимирский областной суд по делу № 22–2007–2003[2], что является по существу законным, так как такое положение прямо не закреплено в УПК РФ. Такая противоречивая практика ведет к возникновению сложностей при решении вопроса о необходимости судебного контроля изъятия информации из носителей.

При этом особое значение в данном вопросе имеет Определение КС РФ от 25 января 2018 г. N 189–О об отказе в принятии к рассмотрению жалобы гр. Прозоровского Д.А. на нарушение его конституционных прав статьями 176, 177 и 195 УПК РФ, в котором КС РФ подчеркивает, что предметы, имеющие отношение к уголовному делу, в том числе и электронные носители информации, могут быть изъяты, если для производства осмотра требуется продолжительное время или осмотр на месте затруднен. Таким образом, КС РФ не находит особую значимость электронных устройств как основного источника информации о жизни человека, не проводя разграничение между осмотром материального носителя информации и осмотр самой электронной информации, что имеет существенное значение при решении данного вопроса. Это, по нашему мнению, может только способствовать ухудшению положения участников уголовного процесса, лишая их возможности защитить их конституционные права. КС РФ также ссылается на статью

[1] Апелляционное определение Верховного Суда Удмуртской Республики № 22–766/2015 от 9.04.2015 // https://www.sudact.ru (дата обращения: 07.05.2019).
[2] Апелляционное определение Владимирского областного суда № 22–2007–2003 от 18.06.2013 // https://www.sudact.ru (дата обращения: 07.05.2019).

125 УПК РФ как гарантию обеспечения прав человека и гражданина в данном случае[1].

В этом контексте представляется интересной позиция ЕСПЧ, в соответствии с которой осмотр электронных носителей возможен по разрешению суда; без его получения осмотр возможен в случаях, не терпящих отлагательств, в этом случае обвинение должно после производства осмотра доказать суду данный факт[2].

В научном сообществе специалисты по–разному разрешают данную проблему. Так, например, М.С. Сергеев приходит к выводу, что необходимо осуществление судебного контроля либо при выемке самого электронного устройства, либо только сведений из него, и может реализовываться это путем системы электронного запроса судебного разрешения на проведение данных следственных действий. По его мнению, реализация данной системы и перераспределение нагрузки судей будет возможна путем создания института следственных судей[3]. Однако данный подход кажется не до конца определенным и не решает проблему по существу, также введение этой системы на сегодняшнее время является затруднительным. П.О. Панфилов, А.В. Победкин также указывают на необходимость при решении этого вопроса применения институтов судебного контроля, прокурорского надзора, ходатайств и др[4].

---

[1] Определение Конституционного Суда РФ от 25.01.2018 N 189–О "Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно–процессуального кодекса Российской Федерации" // consultant.ru (дата обращения: 23.09.2019).

[2] Бикмиев Р.Г., Бурганов Р.С. Выемка и осмотр электронных устройств // Уголовное право. 2018. № 1 // СПС КонсультантПлюс (дата обращения 12.01.2020).

[3] Сергеев М.С. Проблемы соблюдения прав участников уголовного процесса при получении электронной доказательственной информации // ВЭПС. 2017. №2. С. 112.

[4] Панфилов П.О., Победкин А.В. Очередное обострение конкуренции конституционных ценностей при расследовании преступлений в сфере экономической и

В.В. Бычков утверждает, что производство извлечения данных возможно только с письменного согласия самого субъекта на обработку информации, так как в соответствии с Федеральным законом от 27.07.2006 N 152–ФЗ "О персональных данных" является персональными данными как любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу[1]. В случае, если такое лицо отказывается дать согласие, то извлечение может быть произведено на основании судебного решения[2]. Представляется, что это является верным решением и не нарушает право человека на неприкосновенность его личной жизни. Но при этом появляется опасность получения такого согласия не на добровольных началах либо дача его лицом, не способным воспринимать обстоятельства действительности.

По мнению Р.И. Оконенко, извлечение информации из электронного устройства по своей сущности является не осмотром, а обыском, так как электронные следы не находятся в свободном доступе, необходимо применять специальные технико–криминалистические средства к их изъятию, и оформлять соответствующим протоколом. Специалист приходит к выводу о необходимости обязательного предварительного судебного контроля такого действия. Но при этом уточняется, что если электронный носитель выступал в качестве способа, орудия совершения

предпринимательской деятельности // Вестник Московского университета МВД России. 2020. №1. С. 111.

[1] . "О персональных данных" : федеральный закон от 27.07.2006 N 152–ФЗ (ред. от 31.12.2017) // "Российская газета", N 165, 29.07.2006.

[2] Бычков В.В. Соблюдение конституционных прав и свобод на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений при проверке сообщений о преступлениях и в ходе их расследования // Российский следователь. 2013. №24. С. 12.

преступления, или без него невозможно его совершение, как например, преступления в сфере компьютерной информации, отсутствует необходимость в получении судебного решения[1]. По нашему мнению, извлечение информации из носителя ограничивает право на неприкосновенность частной жизни независимо от вида преступления, способа его совершения, необходим общий, а не дифференцированный подход к производству данного действия. Можно согласиться с Р.И. Оконенко в том, что только в исключительных случаях в целях обеспечения прав других граждан, интересов общества и государства в качестве неотложной меры возможно их проведение без судебного решения.

Некоторые специалисты предлагают квалифицировать такие действия (изъятие информации и ее использование) следователя или оперативного работника, если они осуществлены в отсутствие судебного решения и повлекли общественно опасные последствия как нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ), злоупотребление (285 УК РФ) или превышение (286 УК РФ) должностных преступлений. Р.Г. Бикмиев, Р.С. Бурганов также приходят к выводу о том, что изъятие самого электронного носителя возможно и без получения судебного решения, осмотр самой содержащейся информации – только на его основании вне зависимости от согласия владельца[2].

[1] Оконенко Р.И. "Электронные доказательства" и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации : дис. ... канд. юрид. наук. Москва, 2016. С. 84–117.

[2] Бикмиев Р.Г., Бурганов Р.С. Выемка и осмотр электронных устройств // Уголовное право. 2018. № 1 // СПС КонсультантПлюс (дата обращения 12.01.2020).

Законодатель только в конце 2018 года внес изменения в УПК РФ, которые отчасти закрепили правила, при которых допускается изъятие электронных носителей, и соответственно, извлечение информации из них. И такое следственное действие возможно только в случаях, когда: 1) вынесено постановление о назначении судебной экспертизы в отношении электронного устройства; 2) получено судебное решение; 3) на них содержится информация, полномочиями на хранение и использование которой владелец электронного носителя информации не обладает, либо которая может быть использована для совершения новых преступлений, либо копирование которой, по заявлению специалиста, может повлечь за собой ее утрату или изменение[1]. Однако применение части 1 статьи 164.1 УПК РФ ограничено и действует только в отношении уголовных дел о преступлениях, предусмотренных соответствующими статьями УК РФ, преимущественно преступлениях в сфере экономики[2], что было сделано в целях защиты положения предпринимателей и уменьшения количества случаев незаконного и необоснованного приостановления хозяйственной деятельности[3]. По нашему мнению, это не совсем удачное решение проблемы, так как нарушает права участников уголовного судопроизводства на неприкосновенность личной жизни, семейную, личную тайну

[1] "О внесении изменений в статьи 76.1 и 145.1 Уголовного кодекса Российской Федерации и Уголовно–процессуальный кодекс Российской Федерации" : федеральный закон от 27.12.2018 N 533–ФЗ // "Российская газета", N 295, 29.12.2018.

[2] Зуев С.В., Черкасов В.С. Новые правила изъятия электронных носителей и копирования информации (статья 164.1 УПК РФ): преимущества и недостатки новеллы // Сибирское юридическое обозрение. 2019. №2. С. 194.

[3] Например, статьями 159 частями первой – четвертой, 159.1 – 159.3, 159.5, 159.6, 160, 165 Уголовного кодекса Российской Федерации, если эти преступления совершены в сфере предпринимательской деятельности, а также статьями 159 частями пятой – седьмой, 171, 171.1, 171.3 – 172.2, 173.1 – 174.1, 176 – 178, 180, 181, 183, 185 – 185.4 и 190 – 199.4 Уголовного кодекса Российской Федерации.

по всем категориям уголовных дел, а не только определенных. Кроме того, положение о том, что извлечение допускается в случае, если содержащаяся информация будет использована для совершения новых преступлений, может быть подвергнуто расширительному толкованию со стороны правоприменителя, так как не до конца понятно, что конкретно включается в ее содержание. Такая норма может привести к отнесению любых сведений к этому пункту, что нарушит права человека. Было бы более рационально определить круг преступлений, по которым возможно данное ограничение права, например, это могут быть наиболее тяжкие и опасные преступления, в частности, преступления террористического характера.

Представляется, что необходимо внести изменения в статью 164.1 УПК РФ и распространить соответствующие нормы на все виды преступлений, также исключить положение из четвертого абзаца части 1 «либо которая может быть использована для совершения новых преступлений» в целях более эффективного обеспечения права на неприкосновенность частной жизни.

По нашему мнению, необходимо обеспечить судебный контроль в отношении всей информации, которая содержится в электронных носителях, так как она включает в себя всю личную и социальную жизнь человека. Это способствует соблюдению права на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, являющегося одним из важнейших конституционных прав.

2.4. Сравнительно-правовой анализ международных документов по работе с электронными доказательствами

Электронные доказательства как категория уголовного процесса не предусмотрена ни одной из стран в качестве самостоятельного вида доказательств. Многие государства упоминают о возможности существования традиционных доказательств в электронной форме. Отмечается, что в европейских судах регулирование электронных доказательств реализуется с помощью общих положений, касающихся всех доказательств[1]. Законы отдельных стран вообще не признают доказательств, полученных электронным способом, что представляется, не соответствует современному состоянию развития информационных технологий и меняющимся тенденциям преступного мира.

Мы солидарны в данном вопросе с учеными, которые настаивают на необходимости разработать на европейском и международном уровне ряд общих директив и рекомендаций, которые бы гарантировали бы эффективное сотрудничество между государствами относительно сбора и сохранения электронных доказательств[2]. Это способствует и внедрению данных положений в российское законодательство, что, несомненно, приведет к увеличению количества и качества расследования преступлений, с одной стороны, и с другой, к соблюдению прав граждан при его осуществлении. С этой целью остановимся на некоторых из международных актов.

[1] Григорьев В.Н., Максимов О.А. Об электронных носителях информации в уголовном судопроизводстве // Вестник ННГУ. 2019. №3. С. 67.
[2] Основы теории электронных доказательств: монография / под ред. докт. юрид. наук С.В. Зуева. М.: Юрлитинформ, 2019. С. 81.

Одним из важнейших документов выступает Конвенция о преступности в сфере компьютерной информации (Будапешт, 23 ноября 2001 г.). В качестве основополагающего принципа реализации деятельности по расследованию данных преступлений отмечается надлежащая защита прав человека и свобод, включая права, вытекающие из обязательств, предусмотренные Европейской конвенцией о защите прав человека и основных свобод 1950 года, Международным пактом о гражданских и политических правах 1966 года, а также другими международными договорами, необходимость обеспечения судебного или иного независимого надзора. Конвенция предусматривает общие положения производства обыска и выемки компьютерных данных, сбор в режиме реального времени, пи этом должна быть обеспечена сохранность конкретных данных, их неизменность и аутентичность[1]. Данный документ выступает в качестве общего направления деятельности государства по борьбе с преступлениями в сфере компьютерной информации, однако не предусматривает конкретные рекомендации по изъятию, фиксации, исследованию электронной информации в качестве доказательств.

В качестве еще одного примера можно привести Регламент по получению и сохранению электронных доказательств в уголовных делах, разработанный Европейским парламентом. Он посвящен в большей степени межгосударственному сотрудничеству по вопросам получения и сохранения электронных доказательств, но может быть использован по аналогии и при применении

[1] Конвенция о преступности в сфере компьютерной информации (Будапешт, 23 ноября 2001 г.) ETS N 185 // СПС «КонсультантПлюс» (дата обращения 17.01.2020).

общих положений. Так, под электронными доказательствами понимаются хранящиеся в электронном виде данные, такие как информация о подписчиках, метаданные или данные контента, предоставляемые провайдером[1]. В регламенте обосновывается позиция, согласно которой будет обеспечен прямой доступ в системы хранения электронной информации без участия провайдера, что приведет к необходимости внедрения новых технологий. Это может ограничить права на защиту персональных данных, частную, семейную жизнь, неприкосновенность, безопасность и права самого провайдера как организации на ведение своих дел, но разработка механизма их обеспечения относится к компетенции каждого государства, хотя это и представляется нам наиболее сложным вопросом при решении этой проблемы. Отмечается, что такие запросы могут направлять только уполномоченные лица и при обеспечении верификации электронной информации. Суд все равно установлен как орган, подтверждающий такие запросы, что наводит на мысль о невозможности существования данной системы на современном этапе без судебного контроля как наиболее независимого из всех существующих, что может быть воспринято и в РФ. В качестве одной из проблем в регламенте указана недостаточная эффективность сотрудничества государственных органов и провайдеров при получении и хранении электронных доказательств, что имеет место и в нашей стране, а не только в международном пространстве, однако возможность допуска уполномоченных

[1] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters COM/2018/225 final – 2018/0108 (COD). URL : https://eur–lex.europa.eu/legal–content/EN/ALL/?uri=COM:2018:225:FIN (дата обращения 18.01.2020).

лиц к системе хранения таких данных все равно должна быть ограничена наличием правового основания для такого вмешательства.

В отдельных странах, например, в США вопрос об использовании электронных доказательствах регулируется в первую очередь Федеральными правилами доказывания. Пункт 101 устанавливает, что в случае, когда в тексте говорится о письменных материалах любого вида, то имеется в виду также информация, хранящаяся в электронной форме[1], то есть применяются общие правила для их регулирования.

При рассмотрении более практических вопросов исследования электронных доказательств можно обратиться к Руководству по судебной экспертизе цифровых доказательств (Forensic Examination of Digital Evidence: A Guide for Law Enforcement), которое разработано Министерством юстиции США совместно с Национальным институтом юстиции. Данное руководство предусмотрено больше для экспертов соответствующих учреждений при производстве компьютерно–технических и иных экспертиз и носит рекомендательный характер. Оно закрепило понятие электронных доказательств как сохраненную или переданную информацию в двоичной форме, которая может быть представлена в суде. Такая информация может быть получена на основании ордера или непосредственно от провайдера. Нам представляется интересным положение, согласно которому рекомендуется проверить навыки использования электронных устройств участвующих лиц, что поможет определить риск изменения или утраты

[1] Federal Rules of Evidence. Washington, 2013. URL : https://www.rulesofevidence.org/table–of–contents/ (дата обращения 17.01.2020).

содержащейся электронной информации. Отмечается, что такие доказательства по своей природе могут быть повреждены, изменены или уничтожены при осмотре или неправильном обращении, что обуславливает необходимость применения особых мер предосторожности, которые бы обеспечили защиту и сохранение доказательств[1]. В руководстве наравне с вопросами получения и оценки электронных доказательств, рассматривается вопрос фиксации и протоколирования при проведении экспертизы, но их, по нашему мнению, можно распространить на специалиста, который участвует в следственных действиях с электронными носителями информации. Например, указывается на возможность делать заметки, чтобы обеспечить дублирование действий, документирование выявленных нарушений и любых действий, определение дополнительной информации об авторизованных пользователях, топологии, паролях, операционную систему, версию программного обеспечения, обновления, документирование изменений, внесенных в систему[2]. Таким образом, несмотря на направленность руководства на более практические вопросы, что тоже способствовало бы увеличению эффективности производства судебных экспертиз в РФ, некоторые положения могут быть инкорпорированы и при рассмотрении общих вопросов электронных доказательств.

На территории Великобритании при регулировании вопроса использования электронных доказательств

[1] Forensic Examination of Digital Evidence: A Guide for Law Enforcement. URL: https://www.ncjrs.gov/pdffiles1/nij/199408.pdf (дата обращения 17.01.2020).
[2] Forensic Examination of Digital Evidence: A Guide for Law Enforcement. URL: https://www.ncjrs.gov/pdffiles1/nij/199408.pdf (дата обращения 17.01.2020).

интересным представляется Руководство «The Good Practice Guide for Computer Based Electronic Evidence» [ACPO], которое является комплексным актом, содержащим нормы и правила извлечения информации с электронных носителей, и ориентированным на следователей и других лиц, осуществляющих расследование, адвокатов, иных участников процесса. Руководство закрепляет принципы, которые могут быть переняты и в российскую практику, а именно: запрет на внесение изменений в данные, которые могут быть использованы в суде; специалист должен обладать соответствующей квалификацией, иметь возможность объяснить другим участникам последовательность и сущность его действий; возможность осуществления независимой оценки полученных доказательств; лицо, осуществляющее расследование, несет ответственность за соблюдение закона и реализацию данных принципов[1]. Отмечается необходимость применения к электронным доказательствам общих правил, установленных к документальным доказательствам, за исключением некоторых особенностей их получения, обеспечения сохранности и неизменности. При фиксации электронной информации составители указывают на фото и видеосъемку всех компонентов, если нет возможности, то создание схемы со всеми входами и выходами и др., чтобы потом реконструировать данную систему. Особое внимание уделяется электронным органайзерам и персональным виртуальным помощникам, которые могут иметь значение, и применение их все набирает обороты. В руководстве

[1] The Good Practice Guide for Computer Based Electronic Evidence [ACPO]. URL : https://www.7safe.com/docs/default–source/default–document library/acpo_guidelines_computer_evidence_v4_web.pdf (дата обращения 18.01.2020).

приведены рекомендации по поиску и фиксации отдельных электронных носителей (видео, телефоны, email и др.), указания на действия, производимые перед обыском, брифинг со следственной группой, что и кого необходимо взять с собой, что, несомненно, может и должно быть воспринято российскими следователями, специалистами и иными участниками. Составление такого документа хотя бы на ведомственном уровне способствовало бы определенности в вопросах использования электронной информации как доказательственной, увеличило эффективность расследования преступлений. Именно это направление должно стать одним из преимущественных в современной науке и практике.

ЗАКЛЮЧЕНИЕ

В результате данного исследования представляется возможным сформулировать следующие выводы и предложения:

1. Получение доказательств как категория уголовного процесса и криминалистики является одним из основных и эффективных способов собирания цифровой

доказательственной информации, которое осуществляется путем производства следственных и иных процессуальных действий, направления запросов следователем, дознавателем.

2. Под электронными следами следует понимать любое изменение в информационно–технологической среде, связанное с событием преступления и зафиксированное в виде электромагнитных сигналов, сущность которых, в первую очередь состоит в характерном для следов свойстве отражения событий действительности. К наиболее обоснованным и распространенным в судебной практике основаниям для классификации электронных следов можно отнести следующие: цифровая информация, физический носитель, место их нахождения.

3. Перечень возможных информационно – технологических источников, мест нахождения электронных следов только увеличивается и как следствие не является исчерпывающим, однако для их более эффективного применения необходима разработка технических, организационных и в некоторых случаях правовых рекомендация по их использованию.

4. К таким источникам можно отнести файл, лог – файлы, IP – адрес, MAC – адрес, аккаунты, IMEI телефона, видеозапись, аудиозапись, URL (Uniform Resource Locator), находящиеся в DNS (Domain Name system), в компьютерных системах и сетях, аппаратно–программных комплексах «Безопасный город», «Умный дом», системах видеорегистрации, видеофиксации, ЦОДД, ЦАФАП, ЕСИиА

(Единая система идентификации и аутентификации), навигационная деятельность, геолокация и многие другие.

5. Понятие электронных носителей информации должно трактоваться так, как оно нормативно установлено, если не на законодательном уровне, то хотя бы на уровне ведомственных актов, то есть как материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники, и должно быть закреплено в статье 5 УПК РФ, в которой содержатся основные используемые понятия.

6. Мы солидарны с данной точкой зрения, которая заключается в том, что отсутствует необходимость во введении института электронных доказательств в УПК РФ, нужно лишь уточнить то обстоятельство, что уже существующие доказательства могут быть представлены в виде электронной информации. Основным вопросом при использовании электронных доказательств является установление критериев верифицируемости получаемой информации, причем это должны быть именно технические критерии, а не общие принципы, сформулированные с юридической точки зрения.

7. В целях эффективного раскрытия и расследования преступления, связанных с электронными носителями информации, необходимо разработать методические рекомендации по работе с электронными следами, где могут быть закреплены основные правила осмотра, изъятия, фиксации электронных следов.

8. Нововведения, которые были осуществлены в 2018 году при введении статьи 164.1 УПК РФ, в целом оцениваются как положительные в научном сообществе, но императивное участие специалиста не привело к упорядочению судебной практики и выработке единых позиций. Представляется, что участие специалиста при изъятии электронных носителей информации обязательно только в случае возникновения необходимости в применении специальных знаний и угрозе потери хранящейся на носителе информации.

9. Кроме того, процесс осуществления процессуальных действий может привести к необоснованным ограничениям и нарушениям прав и свобод человека и гражданина. Представляется, что в этих целях необходимо внести изменения в статью 164.1 УПК РФ и распространить закрепленные исключения отношении копирования информации на все виды преступлений, также исключить положение из четвертого абзаца части 1 «либо которая может быть использована для совершения новых преступлений» в целях более эффективного обеспечения права на неприкосновенность частной жизни и недопущения возможного злоупотребления полномочиями со стороны следственных органов.

10. По нашему мнению, необходимо обеспечить судебный контроль в отношении всей информации, которая содержится в электронных носителях, так как она включает в себя охраняемую Конституцией РФ (ст.23) сферу частной жизни человека. Это способствует соблюдению права на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых,

телеграфных и иных сообщений, являющегося одним из важнейших конституционных прав.

11. Мы солидарны в данном вопросе с учеными, которые настаивают на необходимости разработать на европейском и международном уровне ряд общих директив и рекомендаций, которые бы гарантировали бы эффективное сотрудничество между государствами относительно сбора и сохранения электронных доказательств. Это способствует и внедрению данных положений в российское законодательство, что несомненно, приведет к увеличению количества и качества расследования преступлений, с одной стороны, и с другой, к соблюдению прав граждан при его осуществлении (например, на основании проанализированных международных актов это могут быть положения относительно фиксации электронной информации, принципы работы с ней, проверка компетенции участвующего специалиста и др.).

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ И ЛИТЕРАТУРА

I. Специальная литература

1. Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе : автореф. дис. ... канд. юрид. наук. Воронеж, 2010. 24 с.

2. Багмет А.М., Скобелин С.Ю. Извлечение данных из электронных устройств как самостоятельное следственное действие // Право и кибербезопасность. М.: Юрист, 2013, № 2 (3). С. 22 – 27.

3. Бахтеев Д.В. Особенности фиксации и изъятия криминалистически значимой информации, размещенной в сети Интернет // "Российский следователь", 2017, N 21 // СПС «КонсультантПлюс» (дата обращения 08.01.2020).

4. Бессонов А.А. О некоторых возможностях современной криминалистики в работе с электронными следами // Вестник Университета имени О.Е. Кутафина. 2019. №3 (55). С. 46 – 52.

5. Бикмиев Р.Г., Бурганов Р.С. Выемка и осмотр электронных устройств // Уголовное право. 2018. № 1 // СПС КонсультантПлюс (дата обращения 12.01.2020).

6. Бондаренко А.А. Изъятие электронных носителей информации при расследовании уголовных дел экономической и общеуголовной направленности, а также по соединенным уголовным делам // "Законодательство и практика", 2019, N 1 // СПС «КонсультантПлюс» (дата обращения 08.01.2020).

7. Бычков В.В. Соблюдение конституционных прав и свобод на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений при проверке сообщений о преступлениях и в ходе их расследования // Российский следователь. 2013. № 24. С. 10 – 13.

8. Васюков В. Ф. Особенности изъятия электронных носителей информации при производстве следственных действий: новеллы законодательства и проблемы правоприменения // Криминалистика: вчера, сегодня, завтра. 2019. №2 (10). С. 8 – 14.

9. Васюков В.Ф., Булыжкин А.В. Некоторые особенности осмотра средств сотовой связи при расследовании уголовных дел // Российский следователь. 2014. N 2. С. 2 – 4.

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

11. Вехов В. Б. Работа с электронными доказательствами в условиях изменившегося уголовно–процессуального законодательства // Российский следователь. 2013. № 10. С. 22 – 24.

12. Вехов В. Б., Смагоринский Б. П., Ковалев С. А. Электронные следы в системе криминалистики // Судебная экспертиза. 2016. № 2 (46). С. 10 – 19.

13. Вехов В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки. Волгоград: ВА МВД России, 2008. 404 с.

14. Волеводз А.Г. Противодействие компьютерным преступлениям. М., 2002. С. 159 – 160.

15. Волеводз А.Г. Следы преступлений, совершенных в компьютерных сетях // Российский следователь. 2002. № 1. С. 4 – 12.

16. Воробей С.Н. Проблемы правовой регламентации процессуального порядка изъятия электронных носителей и копирования содержащейся на них информации // Закон и право. 2020. №1. С. 112 – 114.

17. Воронин М.И. Электронные доказательства в УПК: быть или не быть? // Lex Russica. 2019. № 7 (152). С. 74 – 84.

18. Гаврилин Ю.В. Электронные носители информации в уголовном судопроизводстве // Труды Академии управления МВД России. 2017. N 4 (44). С. 45 – 50.

19. Головчанский А.В. Об использовании средств спутниковой навигации в целях установления и фиксации координат места происшествия // Вестник ВИ МВД России. 2015. №2. С. 62 – 69.

20. Григорьев В. Н. Тенденции и проблемы развития законодательства в области информационных технологий, регулирующего уголовное судопроизводство // Академическая мысль. 2019. №3 (8). С. 57 – 61.

21. Григорьев В.Н., Максимов О.А. Об электронных носителях информации в уголовном судопроизводстве // Вестник ННГУ. 2019. №3. С. 65 – 71.

22. Дусева Н.Ю. Возможности использования навигационных систем в раскрытии и расследовании преступлений // Теория и практика общественного развития. 2012. №12. С. 578 – 582.

23. Дусева Н.Ю. Использование современных программно–технических комплексов систем навигации в раскрытии и расследовании преступлений // Современные проблемы науки и образования. 2014. № 4. URL : https://science–education.ru/ru/article/view?id=14294 (дата обращения 06.01.2020).

24. Дусева Н.Ю. Технико–криминалистические основы использования глобальной навигационной системы в

расследовании и предупреждении преступлений : автореф. канд. юрид. наук. Волгоград, 2015. 190 с.

25. Евдокимов А.С. Концепция построения и развития аппаратно–программного Комплекса «Безопасный город»: итоги реализации, организационно–правовые проблемы и нерешенные вопросы // Актуальные проблемы российского права. 2019. №5 (102). С. 69 – 77.

26. Елисеев А.В., Агафонов С.И. К вопросу о правоохранительном сегменте АПК «Безопасный город» // Вестник Московского университета МВД России. 2016. №7. С. 139 – 142.

27. Желудков М.А. Вопросы повышения эффективности информационно–технического обеспечения безопасности собственности от корыстных преступлений // Вестник Казанского юридического института МВД России. 2013. №11. С. 36 – 41.

28. Желудков М.А. К вопросу о повышении эффективности реализации в России аппаратно–программного комплекса «Безопасный город» при обеспечении защиты от корыстной преступности // Вестник экономической безопасности. 2018. №4. С. 95 – 100.

29. Зазулин И.Ю. Участие специалиста и производство судебных экспертиз при исследовании компьютерной информации // Правопорядок: история, теория, практика. 2018. № 1 (16). С. 110 – 114.

30. Зигура Н.А., Кудрявцева А.В. Компьютерная информация как вид доказательства в уголовном процессе России: Монография. М., 2011. 176 с.

31. Зиннуров Ф.К., Хайруллова Э.Т. Особенности работы с электронными носителями как источниками доказательств при проведении следственных действий // Вестник Казанского юридического института МВД России. 2018. №2 (32). С. 274 – 278.

32. Зуев С.В., Черкасов В.С. Новые правила изъятия электронных носителей и копирования информации (статья 1641 УПК РФ): преимущества и недостатки новеллы // Сибирское юридическое обозрение. 2019. №2. С. 193 – 197.

33. Колосова А., Намиот Д. Цифровые сертификаты для владельцев мобильных телефонов // International Journal of Open Information Technologies. 2013. №4. С. 7 – 11.

34. Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет : дис. … канд. юрид. наук. Москва, 2018. 199 с.

35. Крюкова Т. С. Некоторые вопросы изъятия электронных носителей информации в ходе производства следственных действий: анализ судебной практики // Правопорядок: история, теория, практика. 2016. № 4 (11). С. 61 – 63.

36. Кузовлев В.Ю. Использование возможностей средств навигации в установлении обстоятельств совершения преступлений // Известия ТулГУ. Экономические и юридические науки. 2017. №4 – 2. С. 159 – 165.

37. Курьянова М.Н., Товба О.Н. Проблемы раскрытия и расследования преступлений, связанных с распространением материалов порнографического характера в сети Интернет // Вестник ВИ МВД России. 2016. №3. С. 121 – 126.

38. Кучин О. С. Электронные носители информации в криминалистике: монография / под ред. докт. юрид. наук О.С. Кучина. М., 2017. 304 с.

39. Лыткин Н.Н. Использование компьютерно–технических следов в расследовании преступлений против собственности: дис. … канд. юрид. наук. Москва, 2007. 201 с.

40. Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. М., 2002. 407 с.

41. О работе следователей–криминалистов следственных органов Следственного комитета Российской Федерации в 2014 году : аналитическая справка. Документ официально опубликован не был.

42. Оконенко Р.И. "Электронные доказательства" и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации: дис канд. юрид. наук. М., 2016. 158 с.

43. Олиндер Н.В. К вопросу о доказательствах, содержащих цифровую информацию // Юридический вестник Самарского университета. 2017. №3. С. 107 – 110.

44. Осипенко А.Л., Гайдин А.И. Правовое регулирование и тактические особенности изъятия электронных носителей информации // Вестник ВИ МВД России. 2014. №1. С. 156 – 163.

45. Основы теории электронных доказательств: монография / под ред. докт. юрид. наук С.В. Зуева. М.: Юрлитинформ, 2019. 383 с.

46. Панфилов П.О., Победкин А.В. Очередное обострение конкуренции конституционных ценностей при расследовании преступлений в сфере экономической и предпринимательской деятельности // Вестник Московского университета МВД России. 2020. №1. С. 107 – 113.

47. Пастухов П. С. О развитии уголовно–процессуального доказывания с использованием электронных доказательств // Седьмой Пермский конгресс ученых–юристов (г. Пермь, 18–19 нояб. 2016 г.) : сборник научных статей. М. : Статут, 2017. С. 558 – 566.

48. Пастухов П.С. «Электронные доказательства» в нормативной системе уголовно–процессуальных доказательств // Пермский юридический альманах. Ежегодный научный журнал. 2019. № 1 // СПС «КонсультантПлюс» (дата обращения 07.01.2020).

49. Пастухов П.С. О необходимости развития компьютерной криминалистики // Пермский юридический альманах. 2018. № 1. С. 479 – 488.

50. Пастухов П.С. Средства проверки надежности "электронных" доказательств в ходе производства по уголовному делу // Пробелы в российском законодательстве. 2015. №3. С. 170 – 173.

51. Першин А.Н. Электронный носитель информации как новый источник доказательств по уголовным делам // Уголовный процесс. 2015. N 5. С. 48 – 54.

52. Развитие информационных технологий в уголовном судопроизводстве / под ред. С.В. Зуева. М., 2018. 248 с.

53. Россинская Е.Р. Проблемы использования специальных знаний в судебном исследовании компьютерных

преступлений в условиях цифровизации // Вестник Университета имени О.Е. Кутафина. 2019. №5 (57). С. 31 – 44.

54. Россинская Е.Р., Шамаев Г.П. Новый раздел криминалистики: криминалистическое исследование компьютерных средств и систем // Baikal Research Journal. 2015. №1. С. 19 – 24.

55. Савицкая И.Г. Участие специалиста в следственных действиях, связанных с изъятием электронных носителей информации // Судебная власть и уголовный процесс. 2016. №2. С. 250 – 254.

56. Семенов А. Ю. Некоторые аспекты выявления, изъятия и исследования следов, возникающих при совершении преступлений в сфере компьютерной информации // Сибирский юридический вестник. 2004. №1. С. 53 – 55.

57. Семикаленова А. И., Рядовский И. А. Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики // Актуальные проблемы российского права. 2019. №6 (103). С. 178 – 185.

58. Сергеев М.С. Проблемы соблюдения прав участников уголовного процесса при получении электронной доказательственной информации // ВЭПС. 2017. №2. С. 110 – 114.

59. Скобелин С. Ю. Использование специальных знаний при работе с электронными следами // Российский следователь. 2014. № 20. С. 31 – 33.

60. Стороженко О.Ю. Система технических средств для обеспечения функций оперативно–розыскных мероприятий:

вчера, сегодня, завтра // Вестник КРУ МВД России. 2014. №3 (25). С. 69 – 72.

61. Уголовно–юрисдикционная деятельность в условиях цифровизации: Монография (Голованова Н.А., Гравина А.А., Зайцев О.А. и др.) ("ИЗиСП", "КОНТРАКТ", 2019) // СПС «КонсультантПлюс» (дата обращения 07.01.2020).

62. Чечетин А.Е. Правовой режим доступа правоохранительных органов к информации операторов связи // Вестник ВИ МВД России. 2014. №3. С. 98 – 105.

63. Яблоков Н. П. Криминалистика : учебник / Н. П. Яблоков. М., 2016. 303 с.

64. Якимов А.А. Использование возможностей навигационных спутниковых систем в расследовании преступлений. URL : http://elib.bsu.by/ (дата обращения 20.10.2019).

65. Cellebrite. URL : https://www.cellebrite.com/en/law–enforcement/investigation/ (дата обращения 29.04.2019).

66. Federal Rules of Evidence. Washington, 2013. URL : https://www.rulesofevidence.org/table–of–contents/ (дата обращения 17.01.2020).

67. Forensic Examination of Digital Evidence: A Guide for Law Enforcement. URL: https://www.ncjrs.gov/pdffiles1/nij/199408.pdf (дата обращения 17.01.2020).

68. Oxygen Software. URL: http://www.oxygen–forensic.com/ru (дата обращения 29.04.2019).

69. Proposal for a Regulation of the European parliament and of the council on European Production and Preservation Orders for electronic evidence in criminal matters

COM/2018/225 final – 2018/0108 (COD). URL : https://eur–lex.europa.eu/legal–content/EN/ALL/?uri=COM:2018:225:FIN (дата обращения 18.01.2020).

70. The Good Practice Guide for Computer Based Electronic Evidence [ACPO]. URL : https://www.7safe.com/docs/default–source/default–document library/acpo_guidelines_computer_evidence_v4_web.pdf (дата обращения 18.01.2020).

71. UFED System. Универсальное устройство извлечения судебной информации. URL : http://www.rom.by/files/UFED.pdf (дата обращения 27.12.2019).

72. Xry Logical – извлечение данных. URL : https://www.msab.com/products/xry/ (дата обращения 29.04.2019).

II. Правовые акты – источники права

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6–ФКЗ, от 30.12.2008 N 7–ФКЗ, от 05.02.2014 N 2–ФКЗ, от 21.07.2014 N 11–ФКЗ) // СЗ РФ. 2014, № 31. Ст. 4398.

2. Уголовный кодекс РФ : федеральный закон РФ № 63–ФЗ от 13.06.1996 (ред. от 25.04.2018) // СЗ РФ. 1996, № 25. Ст. 2954.

3. Уголовно – процессуальный кодекс РФ : федеральный закон РФ № 174–ФЗ от 18.12.2001 (ред. от 06.03.2019) // СЗ РФ. 2001, № 52. Ст. 4921.

4. О навигационной деятельности : федеральный закон от 14 февраля 2009 года № 22–ФЗ // Российская газета. 2009. N 27.

5. О внесении изменений в отдельные законодательные акты Российской Федерации в части применения электронных документов в деятельности органов судебной власти : федеральный закон от 23.06.2016 N 220–ФЗ // Официальный интернет–портал правовой информации http://www.pravo.gov.ru, 23.06.2016.

6. О внесении изменений в Уголовно–процессуальный кодекс Российской Федерации : федеральный закон от 28.07.2012 N 143–ФЗ (последняя редакция) // СЗ РФ. 2012, N 31. Ст. 4332.

7. О внесении изменений в статьи 76.1 и 145.1 Уголовного кодекса Российской Федерации и Уголовно–процессуальный кодекс Российской Федерации : федеральный закон от 27.12.2018 N 533–ФЗ // "Российская газета", N 295, 29.12.2018.

8. О персональных данных : федеральный закон от 27.07.2006 N 152–ФЗ (ред. от 31.12.2017) // "Российская газета", N 165, 29.07.2006.

9. Об утверждении Концепции построения и развития аппаратно–программного комплекса «Безопасный город» : распоряжение Правительства РФ от 03.12.2014 N 2446–р // Собрание законодательства РФ, 15.12.2014, № 50, ст. 7220.

10. ГОСТ 2.051–2013 Единая система конструкторской документации (ЕСКД). Электронные документы. Общие положения (с Поправкой) : М.: Стандартинформ, 2014 год.

11. Конвенция о преступности в сфере компьютерной информации (Будапешт, 23 ноября 2001 г.) ETS N 185 // СПС «КонсультантПлюс» (дата обращения 17.01.2020).

III. Практика

1. «О практике рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением конституционных прав граждан (статья 165 УПК РФ)» : Постановление Пленума Верховного Суда РФ от 01.06.2017 № 19 // Российская газета, № 125.

2. Обзор судебной практики по уголовным делам о преступлениях, связанных с незаконным оборотом наркотических средств, психотропных, сильнодействующих и ядовитых веществ. Утвержден Президиумом Верховного Суда РФ 27 июня 2012 года // СПС «КонсультантПлюс» (дата обращения 07.01.2020).

3. Об отказе в принятии к рассмотрению жалобы гражданки Сандаковой Ирины Сергеевны на нарушение ее конституционных прав пунктом 5 части второй статьи 29 и частью третьей статьи 182 Уголовно–процессуального кодекса Российской Федерации : определение КС РФ от 26 янв. 2017 г № 204–0. URL: http://legalacts.ru (дата обращения 09.01.2020).

4. Определение Конституционного Суда РФ от 25.01.2018 N 189–О "Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно–процессуального кодекса

Российской Федерации" // consultant.ru (дата обращения: 23.09.2019).

5. Апелляционные определение Брянского областного суда от 20 марта 2015 г. по делу № 22–329/2015 // https://www.sudact.ru (дата обращения 22.12.2019).

6. Апелляционное определение Пермского краевого суда от 14 октября 2014 г. по делу № 22–7127/2014 // https://www.sudact.ru (дата обращения 22.12.2019).

7. Апелляционное определение Судебной коллегии по уголовным делам Оренбургского областного суда от 03.11.2016 по делу № 22–4229/2016 // https://www.sudact.ru (дата обращения 09.01.2020).

8. Апелляционное определение Саратовского областного суда № 22–2932 от 24.07.2013 // http://www.samosud.org (дата обращения 12.01.2020).

9. Апелляционное определение Пермского краевого суда № 22–4917 от 16.07.2013 // https://www.sudact.ru (дата обращения 12.01.2020).

10. Апелляционное определение Ставропольского краевого суда № 22–733/2014 от 19.02.2014 // https://rospravosudie.com (дата обращения: 07.05.2019).

11. Апелляционное определение Верховного Суда Удмуртской Республики № 22–766/2015 от 9.04.2015 // https:// www.sudact.ru (дата обращения: 07.05.2019).

12. Апелляционное определение Владимирского областного суда № 22–2007–2003 от 18.06.2013 // https://www.sudact.ru (дата обращения: 07.05.2019).

13. Апелляционное постановление № 10–83/2017 от 17 октября 2017 г. по делу № 10–83/2017 Соликамского

городского суда (Пермский край) // sudact.ru (дата обращения 09.01.2020).

14. Приговор от 14 августа 2015 г. по делу № 2–35/2015 Пермского краевого суда // sudact.ru (дата обращения 06.01.2020).

15. Приговор от 24 августа 2015 г. по делу № 1–350/2015 Индустриального районного суда г.Перми // https://www.sudact.ru (дата обращения 06.01.2020).

16. Приговор от 29 октября 2015 г. по делу № 1–287/2015 Ленинского районного суда г. Перми // sudact.ru (дата обращения 22.12.2019).

17. Приговор от 14 января 2016 г. по делу № 1–4/2016 Индустриального районного суда г. Перми // sudact.ru (дата обращения 22.12.2019).

18. Приговор от 2 марта 2016 г. по делу № 1–56/2016 Кудымкарского городского суда Пермского края (постоянное судебное присутствие в с. Юсьва) // https://www.sudact.ru (дата обращения 24.04.2019).

19. Приговор от 6 июля 2016 г. по делу № 1–179/2016 Пермского районного суда Пермского края // https://www.sudact.ru (дата обращения 24.04.2019).

20. Приговор от 31 марта 2017 г. по делу № 1–166/2017 Советского районного суда г. Краснодара (Краснодарский край) // https://www.sudact.ru (дата обращения 24.04.2019).

21. Приговор от 10 августа 2017 г. по делу № 1–259/2017 Дзержинского районного суда г. Перми // https://www.sudact.ru (дата обращения 24.04.2019).

22. Приговор от 25 сентября 2017 г. по делу № 1–387/2017 Свердловского районного суда г. Перми // https://www.sudact.ru (дата обращения 24.04.2019).

23. Приговор от 3 ноября 2017 г. по делу № 1–20/2017 Советского районного суда города Казани Республики Татарстан // sudact.ru (дата обращения 09.01.2020).

24. Приговор от 16 февраля 2018 г. по делу № 1–25/2018 Чайковского городского суда Пермского края // https://www.sudact.ru (дата обращения 24.04.2019).

25. Приговор от 25 мая 2018 г. по делу № 1–63/2018 Чернушинского районного суда Пермского края // https://www.sudact.ru (дата обращения 24.04.2019).

26. Приговор от 4 июня 2018 г. по делу № 1–145/2018 Индустриального районного суда г. Перми // https://www.sudact.ru (дата обращения 24.04.2019).

27. Приговор от 5 июня 2018 г. по делу № 1–104/2018 Лысьвенского городского суда Пермского края // https://www.sudact.ru (дата обращения 24.04.2019).

28. Приговор от 19 июля 2018 г. по делу № 1–264/2018 Мотовилихинского районного суда г. Перми // https://www.sudact.ru (дата обращения 24.04.2019).

29. Приговор от 27 сентября 2018 г. по делу № 1–124/2018 Ленинского районного суда г. Перми // sudact.ru (дата обращения 09.01.2020).

30. Приговор от 28 ноября 2018 г. по делу № 1–383/2018 Бугульминского городского суда (Республика Татарстан) // sudact.ru (дата обращения 05.01.2020).

31. Приговор от 16 января 2019 г. по делу № 1–3/2019 Соликамского городского суд (Пермский край) // sudact.ru (дата обращения 05.01.2020).

32. Приговор от 6 февраля 2019 г. по делу № 1–20/2019 Правобережного районного суда г. Магнитогорска (Челябинская область) // sudact.ru (дата обращения 06.01.2020.

33. Приговор от 11 февраля 2019 г. по делу № 1–19/2019 Октябрьского районного суда г. Грозного // sudact.ru (дата обращения 20.10.2019).

34. Приговор от 19 февраля 2019 г. по делу № 2–34/2018 Ростовского областного суда // sudact.ru (дата обращения 20.10.2019).

35. Приговор от 27 февраля 2019 г. по делу № 1–66/2019 Адлерского районного суда г. Сочи // sudact.ru (дата обращения 20.10.2019).

36. Приговор от 7 марта 2019 г. по делу № 1–51/2019 Лысьвенского городского суда // sudact.ru (дата обращения 06.01.2020).

37. Приговор от 12 марта 2019 г. по делу № 1–42/2019 Рузаевского районного суда (Республика Мордовия) // sudact.ru (дата обращения 05.01.2020).

38. Приговор от 14 марта 2019 г. по делу № 1–61/2019 Краснотурьинского городского суда // sudact.ru (дата обращения 20.10.2019).

39. Постановление от 14 марта 2019 г. по делу № 1–11/2019 Сердобского городского суда (Пензенская область) // sudact.ru (дата обращения 06.01.2020).

40. Приговор от 14 марта 2019 г. по делу № 2–16/2019 Волгоградского областного суда (Волгоградская область) // sudact.ru (дата обращения 06.01.2020).

41. Приговор от 17 апреля 2019 г. по делу № 1–169/2019 Златоустовского городского суда (Челябинская область) // sudact.ru (дата обращения 06.01.2020).

42. Приговор от 29 апреля 2019 г. по делу № 1–116/2019 Ленинского районного суда г. Перми // sudact.ru (дата обращения 06.01.2020).

43. Приговор от 19 июня 2019 г. по делу № 1–183/2019 Краснооктябрьского районного суда г. Волгограда (Волгоградская область) // sudact.ru (дата обращения 06.01.2020).

44. Решение от 15 февраля 2018 г. по делу № 12–46/2018 Железнодорожного районного суда г. Пензы // // sudact.ru (дата обращения 06.01.2020).