Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Юридический институт
институт

Кафедра уголовного процесса и криминалистики
кафедра

УТВЕРЖДАЮ
Заведующий кафедрой
_____ А.Д. Назаров
подпись инициалы, фамилия
«____» _____ 2020 г.

БАКАЛАВРСКАЯ РАБОТА

40.03.01 – «Юриспруденция»
код – наименование направления

Использование компьютерной информации в качестве доказательств в уголовном процессе
Тема

Руководитель _____ доцент, к.ю.н. А.С. Шагинян
подпись, дата должность, ученая степень инициалы, фамилия

Выпускник _____ П.А. Недбайлов
подпись, дата инициалы, фамилия

Красноярск 2020

СОДЕРЖАНИЕ

Введение 3

1. Понятие компьютерной информации, ее носители. Место в системе доказательств по уголовному делу. 6

1.1. Понятие компьютерной информации. 6

1.2. Носители компьютерной информации как источники доказательств 12

1.3. Место компьютерной информации в системе доказательств по уголовному делу, отграничение от вещественных доказательств и иных документов. 17

2. Использование компьютерной информации в уголовно-процессуальном доказывании. 25

2.1. Собирание компьютерной информации 25

2.2 Особенности проверки и оценки компьютерной информации как доказательства по уголовному делу 47

Заключение 55

Список использованных источников 59

ВВЕДЕНИЕ

Развитие компьютерных и иных информационных технологий не только принесло множество позитивных изменений в жизнь человека, но и оказало влияние на преступность. Появились как новые виды преступлений, так и качественно изменились уже существовавшие. Компьютерная информация все чаще становится как объектом, так и орудием преступного посягательства. Все чаще именно компьютерная информация сохраняет на себе следы преступления. Согласно статистике, представленной на официальном сайте Министерства внутренних дел Российской Федерации[1], за последние несколько лет количество преступлений, связанных с использованием информационно-телекоммуникационных технологий, а также в сфере компьютерной информации выросло в несколько раз. Так, в 2016 г. было зарегистрировано 65 949 преступлений в данной сфере, в 2017 г. – 90 587, в 2018 г. – 174 674, а в 2019 уже 294 409. Тенденцию роста числа компьютерных преступлений можно заметить и в 2020 г., поскольку только за первое полугодье было зарегистрировано порядка 180 498 преступлений.

С развитием технологий должно развиваться и законодательство, поскольку ему необходимо отвечать всем современным потребностям информационного общества. Стремительное внедрение мобильных и компьютерных устройств в повседневную жизнь человека делает необходимым использование компьютерной информации в качестве доказательств по уголовным делам. Более того, использование компьютерной информации как доказательства по уголовному делу необходимо не только при расследовании и рассмотрении преступлений в сфере компьютерной информации, но и при расследовании и рассмотрении иных категорий преступлений.

[1] Официальный сайт Министерства внутренних дел Российской Федерации [Электронный ресурс]. URL:https://xn--b1aew.xn--p1ai/reports/1

Все это позволяет с уверенностью говорить о высокой актуальности выбранной темы на сегодняшний день. Об актуальности говорит и достаточная разработанность темы. Компьютерной информации в уголовном процессе посвящено множество научных работ и статей, данную тему исследовали: А.С. Александров, Ю.М. Батурин, В.Б. Вехов, А.И. Гайдин, Н.А. Зигура, А.В. Кудрявцева, С.И. Кувычков, Т.Э. Кукарникова, М.В. Старичков, А.В. Ткачев, М.А. Ефремова, В.Ф. Васюков, Ю.В. Гаврилин, С.А. Шейфер и другие. Однако в связи с систематическими изменениями законодательства, не все работы остаются актуальными на сегодняшний день.

Объектом исследования является компьютерная информация как доказательство по уголовному делу, а также ее носители. Помимо этого, в данной работе будет исследовано место компьютерной информации в системе доказательств по уголовному делу, а также порядок и особенности ее собирания, проверки и оценки.

Предметом исследования послужили научные работы российских ученых, посвященные компьютерной информации, нормы отечественного уголовного и уголовно-процессуального законодательства, а также международное законодательство, нормативные акты других отраслей права и судебная практика по уголовным делам.

Цель исследования состоит в подробном рассмотрении основных проблем использования компьютерной информации в качестве доказательств по уголовному делу, существующих как в доктрине уголовного процесса, так и в рамках правоприменительной практики.

Задачи выпускной квалификационной работы вытекают из ее цели:

- определить содержание понятия компьютерной информации и установить на каких носителях она может находиться
- определить место компьютерной информации в системе доказательств по уголовным делам, провести разграничение со смежными видами доказательств

- подробно рассмотреть порядок использования компьютерной информации в процессе доказывания, исследовать особенности порядка собирания, проверки и оценки компьютерной информации как доказательства по уголовному делу.

Выбор методов для исследования объясняется спецификой объекта и предмета исследования. Исследование осуществлялось с использованием следующих методов научного познания: общенаучных (общелогический, гипотетический, системный, структурно-функциональный) и специальных (нормативно-логический, историко-правовой, формально-юридический, сравнительно-правовой, и др.).

Структура работы обусловлена предметом, целью и задачами исследования. Работа состоит из введения, двух глав, разбитых на параграфы, заключения и списка используемых источников. Во введении раскрывается актуальность темы, степень ее разработанности, определяются цели, задачи, объект и предмет исследования, формулируется методологическая основа и структура работы. В первой главе рассматривается понятие компьютерной информации, определяются ее носители, анализируются основные подходы к пониманию компьютерной информации как доказательства по уголовному делу, определяется место компьютерной информации в системе доказательств по уголовному делу. Вторая глава посвящена использованию компьютерной информации в уголовно-процессуальном доказывании. Рассматриваются особенности собирания, хранения, проверки и оценки компьютерной информации, теоретические и практические проблемы их проведения. В заключении подводятся итоги исследования, анализируется результат, и формируются окончательные выводы по рассматриваемой теме.

1. Понятие компьютерной информации, ее носители. Место в системе доказательств по уголовному делу

1.1 Понятие компьютерной информации

В современном обществе стремительно развиваются компьютерные технологии, с каждым днем увеличивается поток воспринимаемой людьми компьютерной информации, растет ее юридическое значение. Практически ни одну из сфер деятельности человека невозможно представить без использования компьютерных технологий и компьютерной информации. В связи с этим правовое регулирование использования информации становится приоритетным направлением законодательной деятельности. На сегодняшний день особо остро стоит вопрос использования компьютерной информации в качестве доказательств по уголовному делу.

Изначально потребность в законодательном закреплении понятия компьютерной информации возникла в уголовном праве. В Уголовном кодексе РФ, в его первоначальной редакции, была установлена ответственность за преступления в сфере компьютерной информации, в связи с чем необходимо былоустановить и то, что под ней понимается. Так, в ст. 272 УК РФ было закреплено следующее понятие: компьютерная информация — это «информация на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети»[2].

Однако данное определение имело одну существенную проблему: данным определением устанавливалась зависимость компьютерной информации от средств, на которых она могла находиться, в результате чего под компьютерной информацией понималась информация, содержащаяся на четко определенном перечне технических средств, способных быть ее носителями. Другими словами, в определении не раскрывалось содержание

[2] Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. От 13.06.1996) [Электронный ресурс]. Система Гарант. URL:http://base.garant.ru/3975363

компьютерной информации, ее признаков, оно лишь устанавливало, что компьютерной информацией признается любая информация, содержащаяся на указанных законодателем устройствах.

В современном мире, в силу появления огромного множества устройств, способных быть носителями компьютерной информации, такой подход к определению компьютерной информации стал неактуален, поскольку в таком случае законодателю придется каждый раз включать в определение вновь появившееся техническое устройство. Однако в условиях ограниченного числа устройств, способных содержать компьютерную информацию, подобное определение имело место и было способно отвечать потребностям своего времени. Это подтверждает и то, что подобный подход к раскрытию определения компьютерной информации встречался и в международном законодательстве.

К примеру, подобным образом понятие компьютерная информация трактовалось в Соглашении о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации 2001 г., где было определено, что под компьютерной информацией понимается «информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи»[3].

Однако, как уже отмечалось, с появлением новых технических средств и способов передачи информации, данные определения стали в меньшей степени отвечать реалиям развития информационных технологий и компьютерных устройств. Появилась необходимость отказаться от выбранного ранее подхода, основанного на определении компьютерной информации посредством перечисления всех технических средств, на которых она может находиться, всвязи с чем появилась и необходимость пересмотреть устоявшееся определение компьютерной информации.

---

[3] Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации [Электронный ресурс]. Исполнительный комитет СНГ официальный сайт. URL:http://www.cis.minsk.by/page.php?id=866

7 декабря 2011 года Федеральным законом № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» [4] к ст. 272 УК РФ было добавлено примечание, в котором было закреплено новое определение компьютерной информации. Так, под компьютерной информацией стали пониматься «сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи»[5].

Такие изменения в законодательстве следуют признать положительными. Законодатель учел тенденции развития современного общества, и при закреплении нового определения использовал иной подход, нежели ранее. Теперь в определении не указывается, на каких конкретных носителях может находиться компьютерная информация, а закрепляется лишь один из основных признаков компьютерной информации — существование ее в форме электрических сигналов.

Такой подход используется и некоторыми современными исследователями. Так Я. О. Кучина в своей работе, посвященной анализу понятия компьютерной информации, разделяет позицию законодателя и приходит к выводу, что «компьютерная информация — это вид информации, выраженный в форме электрических сигналов, независимо от средств их хранения, обработки и передачи»[6].

Схожей позиции придерживается и М.А. Ефремова. Однако в своем определении она использует термин «электронно-цифровая форма» вместо «форма электрических сигналов». В связи с чем она считает, что компьютерная информация, по сути своей, представляет сведения (данные, сообщения), которые представлены в электронно-цифровой форме, независимо от средств

---

[4] Федеральный закон от 07.12.2011 N 420-ФЗ "О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации" [Электронный ресурс]. СПС КонсультантПлюс. URL:http://www.consultant.ru/document/cons_doc_LAW_122864

[5] Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 18.02.2020) [Электронный ресурс]. СПС КонсультантПлюс. URL:http://www.consultant.ru/document/cons_doc_LAW_10699

[6] Кучина Я.О. Понятие компьютерной информации и его влияние на квалификацию преступлений, предусмотренных ст. 272 УК РФ. Иркутск: Академический юридический журнал, 2019. N 2. С. 25-34.

их хранения, обработки и передачи. При этом следует отменить, что Ефремова оперирует термином «электронная информация», который, по ее мнению, является шире, нежели понятие «компьютерная информация»[7].

Однако Н.А Зигура и А.В. Кудрявцева скептически отнеслись к данному подходу и новому законодательному определению. По их мнению, «компьютерная информация — это сведения, представленные в электронно-цифровой форме на материальном носителе, создаваемые посредством использования аппаратных и программных средств фиксации, обработки и передачи информации, а также набор команд (программ), предназначенных для использования в электронно-вычислительной машине (ЭВМ), системе ЭВМ или управления ими»[8]. В данном случае, помимо существования компьютерной информации в форме электрических сигналов (электронно-цифровой форме), выделяется еще один сущностный признак компьютерной информации — пригодность ее для обработки и использованиякомпьютерными (электронно-вычислительными) устройствами.

Стоит заметить, что такой термин как «ЭВМ» устарел и на сегодняшний день практически не используется, однако, представляется, что в данном определении его правомерно можно заменить термином «компьютерное устройство», что и сделал М.В. Старичков, который представил более лаконичное определение компьютерной информации, без использования устаревшего термина «ЭВМ». Таким образом, по его мнению, компьютерная информация — «это зафиксированные на материальном носителе сведения (сообщения, данные, команды), представленные в виде, пригодном для обработки с использованием компьютерных устройств, и предназначенные для использования в таких устройствах»[9].

---

[7] Ефремова М.А. К вопросу о понятии компьютерной информации. М.: Российская юстиция, 2012. N 7. С. 50-52.

[8]Зигура Н.А., Кудрявцева А.В. Компьютерная информация как вид доказательств в уголовном процессе России: монография. М.: Юрлитинформ, 2011. С. 30.

[9] Старичков М.В. Понятие «Компьютерная информация» в российском уголовном праве. Иркутск: Вестник Восточно-Сибирского института МВД России, 2014. N 1. С. 18-20.

Обосновывая свою точку зрения М.В. Старичков отмечает, что законодатель слишком широко истолковал понятие компьютерной информации в новом определении. По его мнению, это выражается в следующем: во-первых, компьютерная информация не обязательно должна быть представлена в форме электрических сигналов, в пример тому приводится компьютерная информация на оптических дисках. Информация в данном случае хранится на специальном слое, нанесенном на диске, а считывается она с помощью лазерного излучения. Во-вторых, отмечается, что посредством электрических сигналов возможна передача по сути своей совершенно некомпьютерной информации, примеры тому — телевидение, радио и телефонная связь[8].

Действительно стоит согласиться с тем, что одним из основных признаков компьютерной информации является ее пригодность для обработки и использования компьютерными (электронно-вычислительными) устройствами. Безусловно, компьютерная информация бесполезна без устройства способного воспроизводить ее. Это обусловлено тем, что компьютерная информация, по сути своей, представляет лишь сочетание цифр – единиц и нулей, образующих определенный код. Информация же, которую несет в себе данный код, недоступна для непосредственного восприятия человеком. В связи с чем, для преобразования информации из числового кода в форму пригодную для восприятия и понимания человекомему необходимо компьютерное устройство.

Подводя итог, можно сказать, что развитие информационных технологий побудило законодателя не только нормативно урегулировать понятие компьютерной информации и установить ответственность за преступления в данной сфере, но также заставило его с течением времени привести данное понятие в соответствие с современными требованиями технического развития, а также с тенденциями совершенствования компьютерных устройств.

На сегодняшний день законодатель понимает под компьютерной информацией сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и

передачи. Несмотря на то, что данное определение по большей степени было позитивно встречено научным сообществом, ряд исследователей все же считают такое толкование компьютерной информации слишком широким. Также отмечается, что законодатель не учел одного важного признака компьютерной информации – пригодность для обработки компьютерными устройствами и использования ее в них.

В связи с чем, в данной работе, предлагается внести изменения в понятие компьютерной информации, закрепленное в примечании к ст. 272 УК, включив в него указанный выше признак.

1.2 Носители компьютерной информации как источники доказательств

Рассмотрев различные точки зрения относительно понимания компьютерной информации, представленные в предыдущем параграфе, был сделан вывод, что законодатель, определяя современное содержание понятия компьютерной информации, не очерчивает четкий перечень возможный технических устройств, способных быть носителями компьютерной информации. Однако, в целях наиболее глубокого исследования компьютерной информации как доказательства по уголовному делу, необходимо установить, какие же объекты на сегодняшний день могут являться носителем компьютерной информации?

В нормативно-правовых актах носители компьютерной информации часто называются «электронными носителями информации». Так, термин электронный носитель упоминается в ч. 4 ст. 81 УПК РФ, согласно которой «предметы и документы, изъятые в ходедосудебного производства, но не признанные вещественными доказательствами, включая электронные носители информации, в разумные сроки подлежат возврату лицам, у которых они были изъяты» [10] . Также ст. 82 УПК РФ, определяющая порядок хранения вещественных доказательств, содержит, например, положения о том, что «электронные носители информации хранятся в опечатанном виде в условиях, исключающих возможность ознакомления посторонних лиц с содержащейся в них информацией и обеспечивающих их сохранность и сохранность информации» [11] , а «носители возвращаются их законному владельцу после осмотра и производства другихнеобходимых следственных действий, если это возможно без ущерба для доказывания»[11].

[10] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 18.02.2020) [Электронный ресурс]. СПС КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_34481
[11] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 18.02.2020) [Электронный ресурс]. СПС КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_34481

Несмотря на неоднократные упоминания электронного носителя информации в тексте УПК РФ, чёткого, ясного законодательного определения до сих пор нет. К тому же данный вопрос еще не был предметом обсуждения на Пленуме Верховного Суда Российской Федерации.

В науке уголовно-процессуального права проблематика более разработана. Так, В.Ф. Васюков, А.В. Булыжкин[12] и А.П. Рыжаков[13], а также многие другие, предлагают использовать определение, содержащееся в п. 3.1.9. ГОСТ 2.051-2013 «Единая система конструкторской документации. Электронные документы. Общие положения». Согласно данному ГОСТу, электронный носитель — это «материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники»[14].

Однако стоит отметить, что данное определение достаточно широко толкует понятие электронного носителя, поскольку не содержит основных (отличительных) признаков рассматриваемого объекта. В результате чего под данное определение попадает практически любое техническое устройство (средство вычислительной техники), так как практически любое техническое устройство использует для своей работы запись, хранение и воспроизведение информации. В таком случае к электронным носителям может быть отнесена как любая бытовая техника (стиральные машины, микроволновые печи), так и любые другие устройства, содержащие в себе определенную информацию.

Отсутствие четкого определения электронногоносителя информации порождает серьезные процессуальные проблемы. Так, в судебной практике встречаются абсолютно противоположные позиции, касающиеся вопроса

---

[12] Васюков В. Ф., Булыжкин А. В. Изъятие электронных носителей информации при расследовании преступлений: нерешенные проблемы правового регулирования и правоприменения. М.: Российский следователь, 2016. N 6. С. 5.

[13] Рыжаков А. П. Обыск и выемка: основания и порядок производства. М.: Издательство Дело и Сервис, 2015. С. 135.

[14] Межгосударственный стандарт ГОСТ 2.051-2013 "Единая система конструкторской документации. Электронные документы. Общие положения" (введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 22 ноября 2013 г. N 1628-ст) [Электронный ресурс]. Система Гарант. URL: http://base.garant.ru/70665820

отнесения мобильных телефонов к категории электронных носителей информации.

Некоторое суды не рассматривают мобильные телефоны в качестве таковых[15]. В данном случае это обосновывается тем, что телефоны и любая находящаяся на них информация, по сути своей, не являются электронными носителями, используемыми для записи, хранения и воспроизведения информации, обработанной с помощью компьютерных технологий, поскольку мобильные телефоны — это своего рода предметы быта или же средства связи, которые хоть и содержат определенную информацию, однако получение и использование которой каких-либо специальных познаний не требует[16].

Другие суды, например Верховный суд Удмуртской Республики, признают мобильные устройства в качестве электронных носителей информации. Объясняется это тем, что мобильные телефоны уже сегодня представляют собой достаточно сложное техническое устройство, а уровень развития телефонных технологий позволяет распространить на них режим компьютерного устройства, в связи чем необходимо рассматривать мобильные телефоны как электронные носители информации.

Судебная практика так же не имеет однозначной позиции и по поводу отнесения лазерных оптических дисков к категории электронных носителей информации. Одни суды признают их в качестве электронных носителей информации[17], другие отказывают в таком признании[18].

Единственный верный способ разрешения данной проблемы заключается в подробном нормативном урегулировании сложившихся правоотношений. Только законодательное закрепление определения «электронного носителя информации», содержащего все сущностные признаки данного объекта, сможет разрешить имеющиеся теоретические и практические разногласия.

---

[15] Приговор Лысьвенского городского суда Пермского края от 16 декабря 2013 г. по делу N 1-4/2014.
[16] Приговор Ленинского районного суда г. Ульяновска от 23 марта 2018 г. по делу № 1-25/18.
[17] Приговор Кинельского районного суда Самарской области от 12 августа 2014 г. по делу N 1-129/2014.
[18] Апелляционное постановление Самарского областного суда от 28 октября 2015 г. по делу N 22-5640/2015.

Ю.В. Гаврилин предлагает следующее определение электронного носителя информации: «это устройство, конструктивно предназначенное для постоянного или временного хранения информации в виде, пригодном для использования в электронных вычислительных машинах, а также для ее передачи по информационно-телекоммуникационным сетям или обработки в информационных системах»[19].

Как отмечалось ранее, термин электронно-вычислительная машина употребляется и встречается все реже, в связи с чем имеет смысл заменить в данном определении термин «ЭВМ» на термин «компьютерное устройство», который в большей степени соответствует современным реалиям.

В конечном итоге, Ю.В. Гаврилин отмечает, что «наиболее обоснованным будет распространение правового режима электронного носителя на следующие материальные носители: съемные носители информации (карты памяти, жесткие диски, лазерные диски), персональные компьютеры и серверы, а также иные технические устройства, которые в первую очередь конструктивно предназначенные для постоянного или временного хранения компьютерной информации»[20] .

Однако, данная точка зрения на электронные носители информации не является единственной в научной литературе. А.В. Ткачев рассматривает данную проблему несколько по-иному. Он предлагает воспользоваться ст. 2 закона РФ «О государственной тайне», которая определяет материальные носители сведений, составляющих государственную тайну как «материальные объекты, в том числе физические поля, в которыхсведения, составляющие государственную тайну, находят свое отображение ввиде символов, образов, сигналов, технических решений и процессов»[20].

Исходя из этого, А.В Ткачев делает вывод, что материальным носителем компьютерной информации является электромагнитное поле, и отмечает, что

---

[19] Гаврилин Ю.В. Электронные носители информации в уголовном судопроизводстве. М.: Труды Академии управления МВД России, 2017. N 4. С. 47.

[20] Федеральный закон от 21.07.1993 г. N 5485-1 (ред. от 29.07.2018) "О государственной тайне"[Электронный ресурс]. СПС КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_2481/

«электромагнитное поле, на котором зафиксировано определенное содержание компьютерной информации, может как находиться в специальном техническом устройстве (в компьютере, периферийном оборудовании, съемном машинном носителе и т.д.), то есть иметь предметную форму, так и передаваться по проводной связи или же вовсе находиться вне технических средств (обмен данными по беспроводной связи)»[21].

Подводя итог, можно сделать вывод, что наиболее теоретически обоснованным будет рассмотрение электронного носителя информации в узком и широком понимании. Материальным носителем компьютерной информации в узком смысле является «устройство, конструктивно предназначенное для постоянного или временного хранения информации в форме, пригодной для использования в компьютерном устройстве, а также для ее передачи и обработке в информационных сетях»[22], а в широком смысле это «физическое (электромагнитное) поле, на котором зафиксировано определенное содержание компьютерной информации»[21].

Однако, как уже отмечалось, теоретических положений недостаточно для решения практический процессуальных проблем, в связи с чем представляется, что есть необходимость закрепления законодательного определения «электронного носителя информации», или же, по крайней мере, толкования в одном из постановлений Пленума Верховного Суда РФ положений, касающихся понятия и особенностей электронных носителей информации.

---

[21] Ткачев А.В. Вопросы использования электронных носителей компьютерной информации в уголовном процессе в качестве доказательств иных документов. Тула: Известия Тульского государственного университета. 2016. N 3. С.438.

[22]Гаврилин Ю.В. Электронные носители информации в уголовном судопроизводстве. М.: Труды Академии управления МВД России, 2017. N 4. С. 47.

1.3 Место компьютерной информации в системе доказательств по уголовному делу, отграничение от вещественных доказательств и иных документов

Как уже было отмечено ранее, современный уровень развития компьютерных технологий вынуждает правоприменителя использовать компьютерную информацию при расследовании и рассмотрении уголовных дел. В связи с чем необходимо рассмотреть компьютерную информацию в качестве доказательства по уголовным делам, выявить ее особенности, определить место в системе доказательств по уголовному делу, а также провести разграничительный анализ с иными видами доказательств.

Часть 1 ст. 74 УПК РФ, устанавливает, что «доказательствами по уголовному делу являются любые сведения, на основе которых суд, прокурор, следователь устанавливает наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для уголовного дела»[23].

Согласно ч. 2 ст. 74 УПК РФ[23] в качестве доказательств допускаются: показания подозреваемого, обвиняемого, потерпевшего и свидетеля, заключение и показания эксперта и специалиста, вещественные доказательства, протоколы следственных и судебных действий, а также иные документы.

Данный перечень видов (источников доказательств) является исчерпывающим, таким образом иные, не предусмотренные данным перечнем сведения, не могут являться доказательствами. Можно заметить, что законодатель нарочно не выделяет компьютерную информацию в качестве отдельного самостоятельного вида доказательств по уголовному делу.

С одной стороны это можно объяснить тем, что данная статья содержалась еще в первоначальной редакции УПК РФ от 2001 г. Очевидно, что

[23] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 18.02.2020) [Электронный ресурс]. СПС КонсультантПлюс.URL: http://www.consultant.ru/document/cons_doc_LAW_34481

в то время нельзя было отметить столь широкого распространения компьютерных технологий, в силу чего, возможно, законодатель не посчитал необходимым выделить компьютерную информацию в качестве самостоятельного вида доказательств.

Однако почему с течением времени не были внесены соответствующие изменения? Таким вопросом задаются многие авторы и настаивают на выделении компьютерной информации в качестве самостоятельного вида доказательства. В данном случае даже предлагается использование такого термина как «цифровое» или «электронное» доказательство. К тому же, Международная организация по цифровым доказательствам уже дала определение данному термину, в котором указывается, что «цифровое доказательство — это информация, сохраненная или переданная в бинарной форме, которая может быть использована в суде»[24].

Однако выделение компьютерной информации в особый вид цифрового (электронного) доказательства должно быть основано на том, что компьютерная информация имеет ряд существенных отличительных признаков, способных отграничить ее от иных видов доказательств, в связи с чем она не может быть охвачена никаким из установленных видов (источников) доказательств.

В таком случае необходимо произвести разграничительный анализ компьютерной информации и иных видов доказательств. Исходя из специфики компьютерной информации, наиболее логичным будет разграничить компьютерную информацию (электронные доказательства) с вещественными доказательствами, и с иными документами. Очевидно, что с показаниями подозреваемого, обвиняемого, потерпевшего и свидетеля, а также заключениями и показаниями эксперта и специалиста компьютерная информация особой связи не имеет.

[24] Официальный сайт Центра судебных экспертиз при институте судебных экспертиз и криминалистики. [Электронный ресурс] URL: https://ceur.ru/library/spravochnik/katalog_kompanijj/item126250

Начнем с разграничения компьютерной информации и иных документов, так как данное разграничение наименее проблематично.

Прежде всего стоит установить содержания понятий документа и электронного документа. Согласно ст. 2 ФЗ РФ «Об информации, информационных технологиях и озащите информации», документ (документированная информация) — это «зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленном законодательством Российской Федерации случаях ее материальный носитель»[25].

Согласно этому же закону, электронный документ является «отдельным видом документа, представленным в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах»[25].

В соответствии со ст. 84 УПК «документы допускаются в качестве доказательств, если изложенные в них сведения имеют значение для установления обстоятельств, подлежащих доказывании. Данные документы могут содержать сведения, зафиксированные как в письменном, так и в ином виде»[26].

Электронный документ, по сути, представляет собой компьютерную информацию, обличенную с соблюдением всех формальных требований в установленную форму. Так как электронный документ, согласно его законодательному определению, является одним из видов документа, то, безусловно, электронный документ может являться доказательством по уголовному делу в качестве иного документа, если имеет значение для установления обстоятельств, подлежащих доказыванию, и при соблюдении требований о документировании и реквизитах (а так же авторства и т.д.).

---

[25]Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 18.03.2019) "Об информации, информационных технологиях и о защите информации" [Электронный ресурс]. СПС КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_61798

[26] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 18.02.2020) [Электронный ресурс]. СПС КонсультантПлюс.URL: http://www.consultant.ru/document/cons_doc_LAW_34481

Таким образом, компьютерная информация, представленная в виде электронного документа, охватывается иными документами как видом доказательств по уголовному процессу, и в данном случае выделение отдельного вида «цифрового доказательства» не требуется.

К тому же, нельзя упускать из виду положения ч. 4 ст. 84 УПК РФ, согласно которым «документы, обладающие признаками, указанными в ч. 1 ст. 81 УПК РФ, (то есть признаками вещественных доказательств) должны признаваться в качестве вещественных доказательств»[27]. В таком случае, если компьютерная информация, представленная в виде электронного документа, служила орудием или иными средствами совершения преступления, сохранила на себе следы преступления, или если на нее были направлены преступные действия, а так же, если она может служить средством для обнаружения преступления и установления обстоятельств уголовного дела, то, по смыслу законодателя, такая компьютерная информация, а вернее такой электронный документбуде признаваться в качестве вещественного доказательства.

Однако, компьютерная информация не всегда представлена в форме электронного документа. В таком случае она уже не может относиться к иным документам как доказательствам по уголовному делу. В связи с чем возникает необходимость выяснить может ли быть компьютерная информация, не представленная в виде электронного, быть вещественным доказательством.

Ч. 1 ст. 81 УПК РФ определяет, что «вещественными доказательствами признаются предметы»[27]. Предмет, по сути своей, это вещь, какой-либо объект материального мира. Содержанием вещественного доказательства являются следы, свойства, признаки, непосредственно запечатлевшиеся на предмете, которые могут быть непосредственно восприняты человеком и обнаружены путем осмотра.

Компьютерная информация, как и информация вообще, не является объектом материального мира, она не осязаема. Да, компьютерная информация

---

[27] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 18.02.2020). СПС КонсультантПлюс.URL: http://www.consultant.ru/document/cons_doc_LAW_34481

выражается вовне посредством ее материального носителя, однако это не позволяет признать ее предметом материального мира, так как она не имеет жесткой привязки к своему материальному носителю, и ее возможно воспроизводить на разных носителях любое количество раз. Помимо этого, информация о вещественном доказательстве, как уже отмечалось, находится в естественном, непосредственно пригодном для восприятия человеком виде, и преобразование ее с помощью компьютерных устройств не требуется. Компьютерная же информация, опосредована через материальный носитель и восприятие ее возможно только посредством технического устройства, например компьютера.

Другими словами, исходя из того, что вещественное доказательство — это предмет, объект материального мира, то и его доказательственное значение определяется его физическими свойствами и расположением в пространстве. Компьютерная информация — это сведения, а вернее содержание сведений. Хоть информация и находится на материальном носителе, поскольку иначе она не может быть признана доказательством, физические характеристики и свойства этого носителя никак не отражают ту информацию, которая на нем записана. Доказательное значение имеет сама информация, ее содержание, а не ее носитель и его физические свойства.

В связи с чем, исходя из теоретических положений, формально компьютерную информацию нельзя отнести к виду вещественных доказательств по уголовному делу.

Данной точки зрения придерживаются Н.А. Зигура и А.В. Кудрявцева, которые отмечают, что «компьютерная информация в любой форме должна быть выделена в отдельный вид доказательств и закреплена процессуально таким же образом, каким это предусмотрено законодателем для закрепления вещественных доказательств — путем принятия постановления о признании в качестве доказательств и приобщения к уголовному делу»[28].

[28]Зигура Н.А., Кудрявцева А.В. Компьютерная информация как вид доказательств в уголовном процессе России: монография. М.: Юрлитинформ, 2011. С. 30–48.

Такую позицию поддерживает и П.С. Пастухов, призывающий законодателя задуматься о выделении электронных носителей информации в отдельный вид (источник) доказательства и определить его как «предмет, содержащий значимую для уголовного дела информацию, созданную не в процессе расследования (раскрытия) уголовного дела, восприятие которой невозможно без использования электронно-вычислительных средств»[29].

Однако, не смотря на наличие различий между компьютерной информацией и вещественными доказательствами, выделение отдельного вида «цифрового доказательства» представляется не совсем верным. Это объясняется тем, что выделение самостоятельных видов доказательств должно быть обусловлено тем, что каждый вид доказательств, помимо своих особых признаков, должен иметь еще свой особый порядок сбора и закрепления.

Таким образом, для выделения компьютерной информации в самостоятельный вид доказательств, необходимо предусмотреть для нее свой особый порядок сбора и закрепления. Установление порядка, тождественного порядку сбора и закрепления вещественных доказательств фактически не придаст никакого процессуального значения выделению компьютерной информации в качестве отдельного вида доказательств. Вместе с тем, предусмотреть существенно иной порядок сбора практически не представляется возможным. Отчасти это связано с тем, что компьютерная информация, по крайней мере при рассмотрении вопроса о признании ее доказательством по уголовному делу, не может существовать отдельно от материального носителя, он является способом выражения компьютерной информации в материальном мире. Поэтому порядок собирания и закрепления такой информации всегда будет опосредован через порядок собирания и закрепления ее носителей – объектов материального мира, а значит через порядок сбора и закрепления вещественных доказательств.

[29] Пастухов П.С. Электронное вещественное доказательство в уголовном судопроизводстве. Томск: Вестник Томского государственного университета. 2015, № 396. С 149–153.

В связи с чем представляется, что в УПК РФ не следует вводить новый вид доказательства («электронное доказательство»), необходимо лишь уточнить понятие «доказательство» указав, что сведения могут быть представлены и в виде электронной информации».

Солидарен с таким подходом и Р.И. Оконенко, который в своем диссертационном исследовании об электронных доказательствах приходит к выводу о том, что цифровые (электронные) доказательства не являются особым видом доказательств, кроме того, он отмечает, что в настоящеевремя и вовсе преждевременно говорить о понятии «электронного доказательства» как о состоявшейся категории позитивного права[30].

Таким образом, выделение самостоятельного вида преждевременно. В тех случаях, когда компьютерная информация обладает признаками вещественного доказательства предусмотренными ч. 1 ст. 81 УПК РФ [31], наиболее рациональным способом придания ей статуса доказательства будет являться признание ее в установленном порядке вещественным доказательством, не смотря на все теоретические различия между ними[32].

Обобщив вышесказанное, и проанализировав место компьютерной информации в уголовно-процессуальном доказывании, можно сделать следующие выводы:

- законодателем компьютерная информация не выделяется в качестве отдельного вида доказательств, что, однако, не препятствует её использованию при рассмотрении и расследовании уголовных дел.

- компьютерная информация может быть:

1) в форме электронного документа и отвечать признакам иного документа.

---

[30]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.

[31] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 18.02.2020) [Электронный ресурс]. СПС КонсультантПлюс.URL: http://www.consultant.ru/document/cons_doc_LAW_34481

[32]Зазулин А.И. Компьютерная информация в уголовном процессе: сущность и способы закрепления в качестве доказательства по уголовному делу. М.: Бизнес в законе. Экономико-юридический журнал, 2015. N 6. С. 132.

2) в форме электронного документа, и обладать признаками вещественного доказательства.

3) в форме, не обладающей признаками электронного документа, однако иметь при этом все признаки вещественного доказательства.

Компьютерная информация первого вида, а именно представленная в форме электронного документа, относится к виду иных документов, так как электронный документ является одним из видов документов вообще.

Компьютерная информация второго вида относится к виду вещественных доказательств в силу прямого указания на это закона.

Компьютерная информация третьего вида не является материальным объектом, и чисто формально не может быть отнесена ни к одному из видов доказательств по уголовному делу. Однако, исходя из своей сущности и специфики, она подразумевает собирание и закрепление ееспособами, предусмотренными для вещественных доказательств, что позволяет распространить на нее правовой режим вещественных доказательств.

Исходя из вышесказанного, следует согласиться с предложением А.И. Зазулина о внесении изменений в ст. 81 УПК РФ и закрепить в ней положения о том, что компьютерная информация может выступать в качестве доказательства по уголовному делу как вещественное доказательство, а также предусмотреть все особенности связанные с ее собиранием, и хранением.

2. Использование компьютерной информации в уголовно-процессуальном доказывании

2.1. Собирание компьютерной информации

Как известно, для вовлечения любого доказательства в уголовный процесс, его, говоря процессуальным языком, необходимо «собрать». Собирание доказательств является важнейшим элементом процесса доказывания по уголовному делу, поскольку нарушение установленного порядка и процедуры собирания доказательств приводит к тому, что собранные таким способом доказательства признаются недопустимыми, и не могут быть использованы в дальнейшем. В связи с чем представляется необходимым подробно рассмотреть порядок собирания компьютерной информации (электронных носителей информации, содержащих на себе компьютерную информацию), его особенности, а так же существующие проблемы и пути их решения.

Сразу стоит оговориться, что компьютерная информация, помимо доказательства, может быть рассмотрена и в качестве непроцессуальных данных, относимых к делу, в связи с чем, также как и другие непроцессуальные данные она может быть использована в качестве различной ориентирующей или тактической информации [33] . Однако данная работа посвящена компьютерной информации как доказательству по уголовному делу, поэтому на данном аспекте компьютерной информации останавливаться не будем.

Собирание компьютерной информации, в силу ее особых признаков, имеет свою специфику. Во-первых, как уже отмечалось ранее, на сегодняшний день законодателем компьютерная информация не выделена в качестве самостоятельного вида доказательства, однако, в зависимости от своих свойств, она может быть отнесена либо квещественным доказательствам, либо к иным

[33]Калиновский К.Б., Маркелова Т.Ю. Доказательственное значение «электронной» информации в российском уголовном процессе. М.: Российский следователь, 2014. N 6. С. 137.

документы. Во-вторых, стоит учитывать особенности материальных носителей таких доказательств — «электронных носителей информации», речь о которых шла в предыдущей главе. И, в-третьих, стоит учитывать то, что важнейшим свойством компьютерной информации является ее пригодность для обработки компьютерными устройствами и использования в них.

Общий порядок собирания доказательств регламентируется ст. 86 УПК РФ, согласно которой «собирание доказательств осуществляется в ходе уголовного судопроизводства дознавателем, следователем, прокурором и судом путем производства следственных и иных процессуальных действий, предусмотренных УПК»[34].

Таким образом, законодателем выделяется только два способа собирания доказательств по уголовному делу – путем проведения следственных действий и путем проведения иных процессуальных действий. Безусловно, что такой порядок распространяется и на собирание компьютерной информации.

Начнем с анализа проведения следственных действий, так как данный способ является основным, и именно он в первую очередь направлен на получение доказательств по уголовному делу.

Как указывалось в предыдущей главе, УПК РФ напрямую предусматривает содержание компьютерной информации на электронных носителях информации. Собирание доказательств в виде электронных носителей информации при производстве по уголовным делам, осуществляется путем проведения таких следственных действий как: осмотра места происшествия, местности, иного помещения, предметов и документов, трупа; обыска; личного обыска; выемки; осмотра и выемки почтово-телеграфной корреспонденции. Регламентируется данные следственные действия соответственно статьями 176, 177, 182, 183, 184, 185 УПК РФ[35].

---

[34] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 18.02.2019) [Электронный ресурс]. СПС КонсультантПлюс.URL: http://www.consultant.ru/document/cons_doc_LAW_34481

[35]Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 18.02.2020)[Электронный ресурс]. СПС КонсультантПлюс. URL:http://www.consultant.ru/document/cons_doc_LAW_34481

Обыск по своей сути направлен на поиск и выявление электронных носителей компьютерной информации. Выемка в первую очередь направлена на фиксацию доказательств. Осмотр электронных носителей может быть двух видов – внешний и содержащейся на них информации. Внешний осмотр меньше связан с компьютерной информацией, в данном случае электронный носитель осматривается как вещественное доказательство, проводится описание их типа и модели, размера, цвета, комплектности, различных индивидуальных особенностей, серийного номера, различных надписей, внешних повреждений. Осмотр содержащейся информации подразумевает исследование посредством использования технических устройств информации содержащейся на электронных носителях информации. В свете чего законодатель в ч. 7 ст. 185 УПК РФ предусмотрел, что «электронные сообщения или иные передаваемые по сетям электросвязи сообщения при наличии достаточных оснований полагать, что они имеют значение для уголовного дела, по решению суда могут быть осмотрены и изъяты в ходе выемки»[36].

На сегодняшний день уголовно-процессуальное законодательство закрепляет два основных способа собирания компьютерной информации путем проведения следственных действий:

1. Изъятие электронных носителей информации у их владельцев с последующим исследованием представленной на них информации.
2. Копирование необходимой компьютерной информации на электронные носители, представленные органами следствия или дознания.

Начнем с изъятия, поскольку на сегодняшний день практически ни одно расследование уголовного дела не обходится без изъятия электронных носителей информации. Необходимость изъятия электронных носителей

[36] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 01.04.2019) [Электронный ресурс]. СПС КонсультантПлюс.URL: http://www.consultant.ru/document/cons_doc_LAW_34481

информации обусловлена несколькими факторами. Во-первых, зачастую компьютерная информация необходимая для расследования уголовного дела может быть скрыта, зашифрована или удалена, и в таком случае изъятие необходимо для восстановления уничтоженной информации, поиска скрытой и расшифровки зашифрованной. Во-вторых, бывают случаи, когда возможности произвести осмотр электронных носителей информации и анализ содержащейся на них компьютерной информации на месте проведения следственного действия нет, в связи с чем необходимо их изъять для дальнейшего их изучения.

Однако процедура изъятия электронных носителей информации имеет некоторые ограничения. Так, согласно общим правилам производства следственных действий, закрепленным в ч. 4.1 ст. 164 УПК РФ, при производстве следственных действий по уголовным делам в сфере предпринимательской деятельности «не допускается необоснованное применение мер, которые могут привести к приостановлению законной деятельности юридических лиц или индивидуальных предпринимателей, в том числе не допускается необоснованное изъятие электронных носителей информации, за исключением случаев, предусмотренных частью первой статьи 164.1 УПК РФ»[37].

Первым исключением, согласно п. 1 ч. 1 ст. 164.1 УПК РФ[37] являются случаи, когда вынесено постановление о назначении судебной экспертизы в отношении электронных носителей информации.

Однако возможность реализации данной нормы спорна, поскольку она прямо противоречит порядку назначения судебной экспертизы, а именно п. 4 ч. 1 ст. 195 УПК РФ[37], согласно которому следователь (дознаватель), не может принять решение о назначении экспертиз и вынести соответствующее постановление без указания объектов, направляемых на исследование. Другими словами, формальным основанием для вынесения постановления о назначении

[37] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 18.02.2020) [Электронный ресурс]. СПС КонсультантПлюс. URL:http://www.consultant.ru/document/cons_doc_LAW_34481

судебной экспертизы является протокол следственного действия, в ходе которого были обнаружены, зафиксированы и изъяты объекты исследования — электронные носители информации.

Данная проблема уже была предметом научного исследования ряда процессуалистов. Так, М.П. Перякина, С.В. Унжакова и Н.Э. Шишкина обращают внимание на то, что, на момент назначения экспертизы, объекты, подлежащие исследованию, уже должны быть изъяты в установленном порядке и указаны в постановлении о назначении экспертизы[38].

Помимо этого, остается не ясным механизм постановки вопросов перед экспертом, ведь при такой постановке вопросов следователю особенно важно опираться на объекты, подлежащие исследованию, поскольку именно от этого зависит то, насколько актуальными и содержательными будут вопросы. Помимо этого, это позволит конкретизировать задачу, поставленную перед экспертом, отчего в совокупности и будет зависеть качество и сроки проведения экспертиз.

Вторым исключением, согласно п. 2 ч. 1 ст. 164.1 УПК РФ[39], являются случаи, когда изъятие электронных носителей информации производится на основании вынесенного судебного решения.

В п. 2 ч. 1 ст. 164 содержится еще три исключения:

1) на электронных носителях информации содержится информация, полномочиями на хранение и использование которой владелец электронного носителя информации не обладает. В данном случае, следователю необходимо устанавливать владельца данной информации и законность полномочий на ее использование и хранение. Изъятие в данном случае предполагается в случаях, когда электронные носителей информации, либо информация на них находятся у владельцав силу совершённых им противоправных действий.

---

[38]Перякина М.П., Унжакова С.В., Шишкина Н. Э. Процессуальные и криминалистические аспекты изъятия электронных носителей информации в свете защиты прав участников уголовного судопроизводства. Иркутск: Сибирский Юридический Вестник, 2019. N 3. С. 82.

[39] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 18.02.2020) [Электронный ресурс]. СПС КонсультантПлюс.URL:http://www.consultant.ru/document/cons_doc_LAW_34481

2) на электронных носителях информации содержится информация, которая может быть использована для совершения новых преступлений. Вывод о наличии данного обстоятельства может быть сделан следователем исходя из оперативно-значимой и доказательственной информации из материалов дела, результатов ОРМ.

3) на электронных носителях информации содержится информация, копирование которой, по заявлению специалиста, может повлечь за собой ее утрату или изменение. В данном случае если специалист, участвующий в следственном действии, приходит к выводу о возможной утрате или изменении информации при ее копировании, он обязан отразить это в заявлении, которое фиксируется в протоколе следственного действия, в ходе которого осуществлялось изъятие. Не соблюдение данной процедуры является основанием признания недопустимыми действий лиц, осуществляющих изъятие электронных носителей информации, и, вследствие чего, признания недопустимыми полученных доказательств.

Помимо ограничений, УПК предусматривает и особый процессуальный порядок изъятия электронных носителей информации. Так законодателем были установлены следующие правила:

1. Обязательное участие специалиста при изъятии электронных носителей информации. Так, согласно ч. 2 ст. 164.1 УПК РФ, «электронные носители информации изымаются в ходе производства следственных действий с участием специалиста»[40]. Однако такое императивное предписание вызывает множество дискуссий в научной литературе, что обостряется и противоречивой судебной практикой.

Так, например, Р. А. Белкин считает, что «законодатель справедливо принял во внимание то обстоятельство, что изъятие электронного носителя

[40]Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 18.02.2020) [Электронный ресурс]. СПС КонсультантПлюс.URL:http://www.consultant.ru/document/cons_doc_LAW_34481

информации в ходе обыска и выемки может представлять собой задачу, требующую профессиональных знаний в области информатики»[41].

П.В. Козловский же, напротив, отмечает, что «обязательное привлечения специалиста для изъятия электронных носителей информации противоречит требованию процессуальной самостоятельности органов расследования»[42].

В.Н. Чернышев и Е.С Лоскутова в своей работе указывают на то, что «участие квалифицированного специалиста при производстве отдельных следственных действий позволит реализовать законное право владельца на получение копии, содержащихся на изымаемом цифровом носителе»[43]. Однако при этом отмечают, что «привлечение сотрудников экспертно-криминалистических подразделений является затруднительным ввиду высокой степени занятости экспертов. Кроме этого, технические подразделения, осуществляющие компьютерные экспертизы, нередко расположены в труднодоступных или отдаленных местах. В связи с чем изъятие электронных средств обоснованно можно производить вотсутствие эксперта-криминалиста»[43].

К тому же отмечается, что на практике действительно сложно найти необходимое количество специалистов для участия в рассматриваемых следственных действиях, учитывая то, что в настоящий момент электронно-технические устройства находят очень широкое применение во всех сферах человеческой деятельности и, соответственно, вопрос о необходимости изъятия электронных носителей информации встаёт очень часто.

Проанализировав различные взгляды авторов в научной литературе, можно выделить несколько основных подходов к решению данной проблемы.

Первый подход сводится к решению вопроса об участии специалиста в зависимости от свойств и типа электронного носителя. В данном случае, если это технически простое устройство, то предлагается наделить следователя

---

[41] Белкин А.Р. Теория доказывания в уголовном судопроизводстве. Ч. 2. М.: Юрайт, 2017. С. 158.

[42]Козловский П. В., Седельников П. В. Участие специалиста в изъятии электронных носителей. Научный вестник Омской академии МВД России. 2014. № 1. С. 18.

[43] Чернышов В. Н., Лоскутова Е. С. Проблемы собирания и использования цифровых доказательств. Тамбов: Социально-экономические явления и процессы, 2017. С. 199-203.

правом самостоятельно изымать его. Так, например, С.Н. Воробей отмечает, что «при изъятии таких электронных носителей, как карт флеш-памяти, CD дисков и иных подобных носителей, нет необходимости в привлечении специалиста, поскольку такие носители используются повсеместно и достаточно просты в обращении»[44].

Интересную точку зрения, в рамках данного подхода, высказали Н.П. Кириллова и С.П. Кушниренко. Так, они указывают на то, что «помощь специалиста (а, соответственно, и его необходимость участия в изъятии электронных носителей информации в процессе осуществления следственных действий) предопределяется тем, что в информацию на некоторых электронных носителях могут быть внесены изменения»[45]. В связи с чем авторы призывают различать электронные носители информации, в которые могут быть внесены изменения, и те, которые могут быть осмотрены и изъяты следователем самостоятельно, в связи с чем предлагают, конкретизировать случаи обязательного участия специалиста. Таким образом «с участием специалиста необходимо изымать встроенные и выносные накопителина жестком магнитном диске, флэш-память и другие аналогичные носители. В то же время изъятие таких электронных носителей информации как CD и DVD диски может быть осуществлено без риска неправильного обращения с объектом, а значит, и без участия специалиста»[46].

Во втором подходе необходимость привлечения специалиста ставится в зависимость от потребности уполномоченных лиц в специальных познаниях.

Так, С.В. Зуев, и В.С. Черкасов называют положения об обязательном привлечении специалиста при изъятии электронных носителей информации анахронизмом, и отмечают, что «следователю необходимо предоставить право привлекать специалиста для изъятия электронных носителей информации

---

[44] Воробей С.Н. Проблемы правовой регламентации процессуального порядка изъятия электронных носителей и копирования содержащейся на них информации. М.: Закон и право, 2020. С. 113.

[45]Кириллова Н.П., Кушниренко С.П. Проблемы осуществления уголовного преследования по делам о преступлениях, совершаемых в сфере высоких информационных технологий. СПБ.: Правоведение. 2013. N 3. С. 83–84.

только тогда, когда для этого действительно требуются специальные умения и знания»[46].

В обоснование своих выводов они указывают то, что современные информационные технологии настолько просты в обращении, что практически не требуют специальных умений и знаний по их применению. Также авторы ссылаются на социологическое исследование практических работников органов предварительного расследования, проходивших повышение квалификации в Дальневосточном юридическом институте МВД России и Московской академии Следственного комитета РФ (г. Хабаровск) в период с марта по сентябрь 2018 г., которое показало, что 84% опрошенных считают целесообразным исключение из УПК РФ положения об обязательном участии специалиста при изъятии электронного носителя информации.

В третьем подходе предлагается учитывать способ, а также саму процедуру изъятия компьютерной информации.

Так, А.Л. Осипенко и А.И. Гайдин в своей статье замечают, что «положения, предусматривающие необходимость участия специалиста в ходе производства следственных действий, были закреплены в соответствующих статьях одновременно с положениями, которые предъявляют требование к специалисту по ходатайству законного владельца или обладателя содержащейся на электронных носителях информации осуществить копирование информации, содержащейся на таких носителях, на другие носители, предоставленные данными лицами»[47].

Таким образом, авторы предполагают, что обязательное участие специалиста надо рассматривать в привязке к обязанности осуществить по ходатайству указанных лиц копирование информации с изымаемых носителей. При таком толковании данных норм, если в ходе изъятия электронных носителей информации при производстве соответствующих следственных

---

[46] Зуев С.В., Черкасов В.С. Новые правила изъятия электронных носителей и копирования информации: преимущества и недостатки новеллы. Омск: Сибирское юридическое обозрение, 2019. N 2. С. 196.

[47] Осипенко А.Л., Гайдин А.И. Правовое регулирование и тактические особенности изъятия электронных носителей информации. Воронеж: Вестник Воронежского института МВД России. 2014. N 1. С.158–159.

действий ходатайство на копирование информации не заявлено, то и присутствие специалиста не требуется.

Несколько иначе свою позицию изложил Ю.В. Гаврилин. Он отмечает, «что помимо случаев, когда заявлено ходатайство о копировании информации с электронных носителей, обязательное участие специалиста необходимо, если в ходе следственного действия проводится непосредственное восприятие и исследование информации, содержащейся на электронном носителе информации»[48] как, например, в случае его осмотра, либо когда происходит копирование информации в порядке ч. 8 ст. 166 УПК РФ.

Также стоит отметить отсутствие единой судебной практики по данному вопросу.

Очевидно, наиболее распространенная позиция судов основывается на буквальном толковании положений УПК РФ, касающихся изъятия электронных носителей информации, исходя из чего суды выводят необходимость участия специалиста в любом случае изъятия электронных носителей в ходе осуществления следственных действий. Примерами таких решений являются Приговор Индустриального районного суда г. Ижевска Удмуртской Республики от 11 июля 2014 г. по делу N 1-201/2014 или Апелляционное постановление Соликамского городского суда Пермского края от 17 октября 2017 г. по делу N 10-83/2017, в котором жалобе защитника был признан в качестве недопустимого доказательства CD-диск, поскольку его изъятие проходило без участия специалиста, что является нарушением требований УПК[49].

Важно отметить, что в аналогичном ключе высказался и Конституционный Суд РФ. В своем постановлении он указал, что при изъятии

[48]Гаврилин Ю.В. Электронные носители информации в уголовном судопроизводстве. М.: Труды Академии управления МВД России, 2017. N4. С. 45-50.
[49]Апелляционное постановление Соликамского городского суда Пермского края от 17 октября 2017 г. N 10-83/2017.

электронных носителей информации в ходе производства обыска электронные носители информации изымаются с участием специалиста[50].

Однако в ряде проанализированных судебных решений вопрос о необходимости привлечения специалиста для участия в изъятии электронных носителей информации решался исходя из того, осуществлялось ли копирование информации, содержащейся на изъятых предметах, на другие электронные носители. И если копирование не производилось, то участие специалиста не требуется. Например в Апелляционном постановлении Приморского краевого суда суд признал правомерным изъятие при производстве обыска электронных носителей (ноутбуков, флеш-накопителей, переносного жесткого диска) без участия специалиста, так как не производилось копирование информации[51].

Казалось бы, такая практика прямо противоречит прямо ч. 1 ст. 75 УПК, согласно которой «доказательства, полученные с нарушением требований УПК, являются недопустимыми»[52].

Однако, данные положения уточняются Пленумом Верховного Суда Российской Федерации в постановлении от 19.12.2017 № 51 «О практике применения законодательства при рассмотрении уголовных дел в суде первой инстанции (общийпорядок судопроизводства)», который в п. 13 указал, что «доказательства признаются недопустимыми, в частности, если были допущены существенные нарушения установленного уголовно-процессуальным законодательством порядка их собирания и закрепления»[53].

Таким образом, данные судебные решения можно признать правомерными, поскольку отсутствие специалиста при изъятии электронных

---

[50]Определение Конституционного Суда РФ от 26 января 2017 г. N 204-О «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».

[51]Апелляционное постановление Приморского краевого суда от 24 сентября 2015 г. N 22-5674/15.

[52]Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 18.02.2020) [Электронный ресурс]. СПС КонсультантПлюс.URL:http://www.consultant.ru/document/cons_doc_LAW_34481

[53] Постановление Пленума Верховного Суда Российской Федерации от 19.12.2017 № 51 «О практике применения законодательства при рассмотрении уголовных дел в суде первой инстанции (общий порядок судопроизводства».

носителей информации в данных случаях не признавалось существенным нарушением уголовно-процессуальных норм, в связи с чем полученные доказательства были признаны допустимыми.

В таком случае возникает закономерный вопрос, когда отсутствие специалиста можно признать существенным нарушением, и каковы критерии существенности в данном случае?

Стоит начать с того, с чем вообще связана необходимость обязательного участия специалиста при изъятии электронных носителей информации. Представляется, что обусловленность участия специалиста потребностью в специальных познаниях, или технической сложностью электронных носителей отражает лишь криминалистический аспект получения доказательств, однако при этом не берутся во внимание уголовно-процессуальные аспекты. Однако именно они отражают правовую потребность в привлечении специалиста.

Так процессуальные гарантии прав участников процесса, в частности право на копирование информации с изымаемых носителей информации и делают участие специалиста обязательным, что подтверждается свежующим: во-первых, как уже отмечалось, положения касающиеся обязательности участия специалиста при изъятии электронных носителей были внесены в закон одновременно с закреплением права на копирование информации, содержащейся на них; во-вторых, само копирование компьютерной информации, обусловленное ходатайством владельцев электронных носителей и обладателей содержащейся на них информации, согласно УПК, может быть осуществлено только специалистом; и, наконец, одним из оснований для отказа в копировании является «заявление специалиста» о возможной утрате или изменении информации, содержащейся на изымаемом электронномносителе.

Таким образом, не смотря на техническую сложность или простоту устройства, наличие и отсутствие потребности в применение специальных познаний, обязательное участие специалиста при изъятии электронных носителей информации, с правовой (уголовно-процессуальной) точки зрения, обусловлено необходимостью обеспечить реализацию права на копирование

данной информации ее обладателями, а так же владельцами электронных носителей, на которых она содержится. В связи с чем, отсутствие специалиста при изъятии электронных носителей лишает их законного владельца или обладателя содержащейся на них информации потенциальной возможности реализовать данное право.

Исходя из этого, именно объективная вероятность привлечения специалиста для разрешения ходатайства о копировании информации с изымаемых электронных носителей или к самой процедуре копирования должна учитываться как критерий существенности участия специалиста.

Такая позиция позволяет сделать вывод, что подход, избранный законодателем, заключающийся в обязанности участия специалиста при изъятии электронных носителей информации следуют признать верным. Непривлечение специалиста следует рассматривать как нарушение порядка осуществления следственного действия, связанного с изъятием электронных носителей, что с учетом п. 3 ч. 2 ст. 75 УПК РФ ставит вопрос о допустимости полученного доказательства.

Однако, если имели место случаи, когда объективной вероятности привлечения специалиста для копирования информации не было, например при изъятии носителей, которые находились у владельцев в пользовании и были добровольно представлены ими следователю (в такой ситуации данные лица имели возможность скопировать информацию до изъятия), или в случае изъятия электронных носителей, содержащих сведения, не представляющие интерес с точки зренияих копирования, либо же когда копии уже имеются и остаются у них владельцев, то такое нарушение нельзя рассматривать как существенное, а полученные в результате такого следственного действия доказательства могут и должны быть признанны допустимыми.

Так же, как отмечают Н.Н. Цуканов и А.Л. Карлов нельзя рассматривать как существенное нарушение непривлечение специалиста в случаях изъятия электронных носителей, содержащих сведения, полномочиями на хранение и использование которых владелец электронного носителяинформации не

обладает, либо которая может быть использована для совершения новых преступлений, так как в данном случае не может идти речи о праве на копирование, поскольку это является основанием для отказа вкопировании вообще[54].

2. Вторым правилом, регулирующим порядок изъятия электронных носителей информации, является возможность копирования компьютерной информации с изымаемых электронных носителей их владельцами. В данном случае следователь обязан обеспечить законному владельцу изымаемых электронных носителей информации или обладателю содержащейся на них информации возможность реализовать свои права ходатайствовать об изготовлении копий с изымаемых электронных носителей информации и получить такие копии.

Реализация данного права возможна как при непосредственно производстве следственного действия, так и после проведения неотложных следственных действий, в случае невозможности возврата изъятых в ходе производства следственных действий электронных носителей информации.

Так, копирование информации с электронных носителей, предусмотренное ч. 2.1 ст. 82 УПК РФ[38], то есть после производства неотложных следственных действий, возможно только при соблюдении следующих условий:

- копирование осуществляется на другие электронные носители информации, предоставленные законным владельцем изъятыхносителей информации или обладателем содержащейсяна них информации;

- копирование осуществляется с участиемзаконного владельца изъятых носителей информации и (или) обладателя содержащейся на них информациии (или) их представителей;

- копирование осуществляется с участиемспециалиста и понятых;

[54] Цуканов Н.Н., Карлов А.Л. К вопросу об изъятии электроны носителей информации при производстве следственных действий. Барнаул: Алтайский юридический вестник, 2019. N 4. С. 135–140.

- копирование должно происходить в подразделении органа предварительного расследованияили в суде;

- должны обеспечиваться условия, исключающие возможность утраты или изменения копируемой информации;

- не допускается копирование информации, если это может воспрепятствовать расследованию преступления;

- об осуществлении копирования информации и о передаче электронных носителей информации составляется протокол.

В данном случае, не смотря на подробное регулирование, отмечается слабое закрепление прав и процессуальных гарантий лиц, у которых осуществляется изъятие электронных носителей информации.

Как уже отмечалось, в случае невозможности возврата изъятых электронных носителей информации «не допускается копирование информации, если это может воспрепятствовать расследованию преступления...»[55].

При этом, данная норма не содержит четких критериев, подтверждающих возможность наступления указанных последствий при осуществлении копирования.

Отсутствие четких критериев в отдельных случаях способно приводить к безосновательному отказу в копировании. Как отмечает А. В. Шигуров, термин «воспрепятствование расследованию преступления» допускает произвольное толкование, что может привести к нарушениям прав законных владельцев электронных носителей информации[56].

Подобных порядок, за исключением пары различий, закреплен и в ст. 164.1 УПК РФ, регулирующей особенности изъятия электронных носителей информации, непосредственно при производстве следственных действий. Первым отличием является то, что при изъятии электронных носителей во

[55]Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 18.02.202) [Электронный ресурс]. СПС КонсультантПлюс.URL: http://www.consultant.ru/document/cons_doc_LAW_34481

[56]Шигуров А.В. Проблемы регулирования порядка проведения следственных действий, сопровождающихся изъятием электронных носителей информации. М.: Библиотека криминалиста, 2013. С. 140.

время осуществления следственного действия, копирование осуществляется по месту его производства, а не в органе следствия (дознания). Второе отличие заключается в том, что несколько шире раскрываются обстоятельства, при которых копирование не допускается. В данном случае не допускается копирование, если «на 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»[57]. Можно заметить, что данные критерии не допускают произвольного толкования, в связи с чем предлагается использовать их и в ст. 82 УПК РФ.

3. Третьим правилом является обязательно участие понятых при производстве следственных действий направленных на изъятие электронных носителей информации.

Однако данное правило распространяется не на все следственные действия. Так, согласно ч. 1 ст. 170 УПК РФ «в случаях, предусмотренных статьей 182, частью третьей.1 статьи 183, статьями 184 и 193 настоящего Кодекса, следственные действия производятся с участием не менее двух понятых, которые вызываются для удостоверения факта производства следственного действия, его хода и результатов[57]».

Однако в данном случае можно отметить техническую ошибку законодателя, поскольку ч. 3.1 ст. 183 (в которой ранее речь шла об изъятии электронных носителей информации) утратила силу, а ст. 164.1 УПК, введенная на ее замену, содержит положения, только об обязательном участии понятых при копировании информации с изымаемых носителей, не оговаривая порядок участия понятых при их изъятии.

---

[57]Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 18.02.202) [Электронный ресурс]. СПС КонсультантПлюс.URL: http://www.consultant.ru/document/cons_doc_LAW_34481

Соответственно, участие понятых будет обязательно только в случаях проведения обыска и личного обыска, а также в случая удовлетворения ходатайства о копировании информации с электронного носителя информации.

При этом важно отметить, что в данном случае понятые должны обладать определённым объемом знаний в области компьютерных технологий, чтобы понимать суть проводимого следственного действия, иначе их присутствие не будет отвечать целям, для которых они привлекаются в соответствии с УПК РФ.

Вторым способом собирания компьютерной информации, как доказательства по уголовному делу является ее копирование на электронные носители, представленные органами следствия или дознания.

До внесения изменений в УПК Федеральным законом от 27.12.2018 N 533-ФЗ [58] существовала серьезная дискуссия относительно правомерности копирования компьютерной информации без изъятия ее подлинного источника при осуществлении следственных действий. В первую очередь это было связано с тем, что данная процедура копирования информации не была законодательно закреплена. Такое нормативное регулирование порождало серьезную критику со стороны научного сообщества. Положение законодателя усугублялось и тем, что такой способ собирания компьютерной информации зачастую применялся при производстве следственных действий и признавалсяправомерным судебной практикой[59].

Сейчас, наконец, дискуссия по данному поводу прекращена. Это связано с тем, что часть 3 введенной 27.12.2018 в УПК статьи 164.1 прямо предусматривает, что «Следователь в ходе производства следственного действия вправе осуществить копирование информации, содержащейся на электронном носителе информации»[60].

---

[58]Федеральный закон от 27.12.2018 N 533-ФЗ "О внесении изменений в статьи 76.1 и 145.1 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации" [Электронный ресурс]. СПС КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_314650

[59] Определение Верховного суда по делу № 5–012–72сп

[60] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 18.02.2020) [Электронный ресурс]. СПС КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_34481

При этом, помимо законодательного закрепления возможности копирования следователем информации с электронных носителей, была предусмотрена и процедура, в соответствии с которой это копирование должно осуществляться. Так «в протоколе следственного действия должны быть указаны технические средства, примененные при осуществлении копирования информации, порядок их применения, электронные носители информации, к которым эти средства были применены, и полученные результаты. А к протоколу должны прилагаться электронные носители информации, содержащие информацию, скопированную с других электронных носителей информации в ходе производства следственного действия»[59].

Таким образом, законодатель устранил пробел, допущенный им ранее, официально закрепив устоявшуюся до нововведений практику копирования компьютерной информации без изъятия ее непосредственного носителя. Это нововведение можно признать положительным, поскольку зачастую компьютерная информация, в силу специфичности своих характеристик, не может быть непосредственно изъята на электронных носителях, либо же такое изъятие крайне затруднено или вовсе бессмысленно. Также не редки случаи, когда изъятие может повлечь неблагоприятные последствия для других лиц, не причастных к преступлению.

Однако, в процедуре копирования компьютерной информации с электронных носителей, не смотря на все свои положительные стороны, и, порой, неизбежность применения, можно выделить и ряд недостатков. Во-первых, при совершении копирования всегда есть риск нарушить сохранность компьютерной информации (компьютерного устройства, на котором эта информация находится) в первоначальном виде. Можно отметить, что при копировании каких-либо файлов как минимум изменяется дата и время последней операции с объектом, а средства и способы, позволяющие производить копирование без таких изменений не всегда возможно применить.

Во-вторых, если компьютерная информация только копируется, а электронные носители не изымаются, то впоследствии это может дать лицу

возможность избавиться от них, и отрицать факт принадлежности ему этих электронных носителей информации.

Казалось бы, наличие данных проблем при осуществлении компьютерной информации вызывает необходимость привлечения специалиста для участия в осуществлении данных действий. К тому же участие специалиста признано обязательным в случае, когда копирование производится с изымаемых носителей информации на электронные носители, предоставленные законным владельцем изымаемых электронных носителей или обладателем содержащейся на них информации, по их ходатайству.

Однако ч. 3 ст. 164.1 [61] не содержит прямого указания на участие специалиста, в связи с чем можно прийти к выводу, что законодатель не посчитал обязательным участие специалиста при осуществлении данных действий, и формально такого предписания нет.

Данная позиция законодателя критикуется, так некоторые исследователи, такие как К.И. Сутягин, С.В. Зуев и Ю.А. Извеков отмечают, что «в каждом случае копирования компьютерной информации в ходе производства следственного действияобязательно необходимо привлечение специалистов в области компьютерной техники и информатизации»[62]. Это обосновывается тем, чторабота с компьютерной информацией имеет свою специфику, и в определенных случаях копирование компьютерной информации требует наличия специальных знаний, чтобы не допустить утрату или изменение информации, а также потерю ею доказательственного значения, в случае неосторожного доступа к такого рода информации следователем, не обладающим соответствующими знаниями данной области.

Однако, данные меры стоит признать чрезмерными. Как уже отмечалось ранее, обязательное участие специалиста при работе с электронными носителями информации обуславливается необходимостью обеспечить

[61]Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 18.02.2020) [Электронный ресурс]. СПС КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_34481

[62]Сутягин К. И., Зуев С. В., Извеков Ю. А. Электронное копирование информации как самостоятельное следственное действие. Следователь. 2003. № 4. С. 15.

потенциальную возможность реализации права на копирование данной информации ее обладателями, а так же владельцами электронных носителей, на которых она содержится. Поскольку вопрос о предоставлении копии владельцу или обладателю без изъятия самих носителей информации не возникает, то и участие специалиста являться обязательным не будет.

Так же в настоящее время особо актуальными в качестве доказательств по уголовному делу являются электронные сообщения, передаваемые при помощи мобильных устройств.

В сфере этого законодатель в ч. 7 ст. 185 УПК РФ предусмотрел, что «электронные сообщения или иные передаваемые по сетям электросвязи сообщения при наличии достаточных оснований полагать, что они имеют значение для уголовного дела, по решению суда могут быть осмотрены и изъяты в ходе выемки»[63].

Однако, как быть, если необходимая компьютерная информация не содержится непосредственно на электронном носителе информации, а представляет собой сведения в сети интернет, будь то переписка в социальных сетях, интернет-страницы, аккаунты в социальных сетях, и т.д. Такую информацию не всегда возможно изъять вместе с конкретным носителем, и уж тем более не всегда возможно произвести ее копирование.

Порядок изъятия такой информации законодательно не урегулирован, в связи с чем следует признать, что выделение только двух способов собирания компьютерной информации, таких как изъятие электронных носителей и копирование компьютерной информации с них недостаточно.

Однако очевидно, что использование такой информации необходимо при расследовании и рассмотрении уголовных дел. В таком случае, необходимо рассмотреть в каком же порядке собирается и фиксируется данная информация.

Одним из наиболее очевидных выходов из данной ситуации является адаптация уже имеющихся положений касающихся производства следственных

---

[63]Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 01.04.2019) [Электронный ресурс]. СПС КонсультантПлюс.URL: http://www.consultant.ru/document/cons_doc_LAW_34481

действий применительно к такому виду компьютерной информации. В данном случае, одним из способов собирания компьютерной информации, помимо ее копирования и изъятия электронных носителей информации, на которых она расположена, будет являться составление протокола следственного действия, с приложением к нему материалов фото- или видеосъемки, на которых должна отражаться все необходимая для дела информация. Например, так может осуществляться фотосъемка переписки в социальных сетях, или видеосъемка страницы интернет-сайта.

В дополнении к этому, возможно проведение допроса, в протоколе которого могут быть отражены подтверждения или опровержения наличия данной информации в сети интернет. Так, например, понятой, или иной участник уголовного процесса может подтвердить или опровергнуть факт обнаружения определенной информации в сети интернет во время проведения следственного действия.

Помимо адаптации уже имеющихся законодательных положений, предлагается и иной выход из ситуации, так Ю.В. Гаврилин и А.В. Победкин предлагают «регламентировать процедуру изъятия доказательственной информации, находящейсяна соответствующих страницах интернет-сайтов (сайтов социальных сетей, блогов, электронной почты, иных интернет-сервисов), путем введения в УПК РФ самостоятельноговида осмотра – дистанционного осмотра информационных ресурсов, который будет производиться в помещении следственного органа (органа дознания)».[64]

Как уже отмечалось, собирание доказательств осуществляется путем производства и иных процессуальных действий, предусмотренных УПК РФ, таких как истребования документови предметов, запрос, либо путемпринятия предметов, представленных подозреваемым, обвиняемым, а также потерпевшим, гражданским истцом, гражданским ответчиком их представителями.

---

[64] Гаврилин Ю.В., Победкин А.В. Собирание доказательств в виде сведений на электронных носителях в уголовном судопроизводстве России: необходимо совершенствование процессуальной формы. Труды академии МВД Росиии, 2018. С. 111-112.

Таким образом, законодатель выделил два основных способа собирания компьютерной информации: копирование представляющей интерес компьютерной информации на электронные носители предоставленные органами следствия или дознания и изъятие электронных носителей информации у их владельцев с последующим исследованием представленной на них информации.

Изъятие имеет обширное процессуальное регулирования, однако законодательные положения достаточно спорны и вызывают ряд дискуссий, в частности касающихся обязательного участия специалиста при изъятииэлектронных носителей информации. В данной работе разделяется позиция законодателя относительно обязательного участия специалиста, поскольку отсутствие специалиста при изъятии электронных носителей лишает их законного владельца или обладателя содержащейся на них информации потенциальной возможности реализовать право на ее копирование.

На сегодняшний день очевидно, что выделенных законодателем способов недостаточно для собирания всех видов имеющей значения для дела компьютерной информации. В связи с чем на практике приходится адаптировать уже имеющиеся положения о проведении следственных действий применительно к компьютерной информации. Однако научным сообществом предлагается иной подход — введение в УПК РФ самостоятельноговида осмотра — дистанционного осмотра информационных ресурсов.

2.2 Особенности проверки и оценки компьютерной информации как доказательства по уголовному делу

Далее имеет смысл проанализировать проверку компьютерной информации как одного из важнейших элементов процесса доказывания. Проверке доказательств посвящена ст. 87 УПК РФ. Согласно данной статье «проверка доказательств производится дознавателем, следователем, прокурором, судом путем сопоставления их с другими доказательствами, имеющимися в уголовном деле, а также установления их источников, получения иных доказательств, подтверждающих или опровергающих проверяемое доказательство»[65]. Суть проверки доказательств заключается в установлениисвойств доказательств, источника их происхождения, а также достоверности сведений, составляющих доказательство, при этом устанавливается достоверность как отдельно взятых сведений, так и всего содержания доказательства в целом.

Данный раздел не будет полностью охватывать порядок и правовое регулирование проверки доказательств. В данной работе представляется важным отметить особенности и специфику проверки именно компьютерной информации, используемой в качестве доказательств по уголовному делу.

Специфика компьютерной информации обуславливает и определенные сложности, связанные с ее проверкой. В связи с тем, что на электронных носителях информации зачастую содержится огромное количество файлов, а необходимая для использования в процессе доказывания информация может быть скрыта, зашифрована или вовсе уничтожена, для обнаружения или

[65]Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 18.02.2020)[Электронный ресурс]. СПС КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_34481

восстановления такой информации требуются специальные познания в области информационных технологий, а так же применение специального программного обеспечения.

Одной из основных особенностей проверки компьютерной информации является частая необходимость обращения к помощи специалиста в ходе работы с такими доказательствами. Согласно ст. 80 УПК РФ «специалист в проверке доказательств может участвовать путем дачи заключения либо путем дачи показаний, по поставленным перед ним вопросам»[66]. Так, заключением являются представленные в письменном виде суждения по вопросам, поставленным перед специалистом сторонами, а показания представляют собой сведения, сообщенные специалистом на допросе об обстоятельствах, требующих специальных познаний, а также разъяснения своего мнения. В данном случае, важно правильно формулировать вопросы перед специалистом, использовать вопросы проверочного, а не оценочного характера.

Следующие особенности связаны с проверкой самих электронных носителей доказательств. Важно сохранять в первоначальном виде подлинники электронных носителей информации. Это обусловлено тем, что в последствии путем сравнения с ними возможно будет установить внесениеизменений в компьютерную информацию или компьютерные объекты ее содержащие.

Также, как отмечает С.А. Шейфер, «проверка источника компьютерной информации должна заключаться в выяснении, исправно ли было оборудование, с которого или при помощи которого была снята компьютерная информация, а также корректно ли работало программное обеспечение»[67].

При проверке допустимости компьютерной информации как доказательства по уголовному делу, необходимо предусмотреть возможность ее идентификации и аутентификации. При этом под аутентификацией следует понимать способность проверять целостность и неизменность содержания

---

[66]Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 18.02.2020)[Электронный ресурс]. СПС КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_34481

[67]Шейфер С.А. Понятие доказательства: спорные вопросы теории. М.: Государство и право, 2008. С. 19.

электронного документа, а под идентификацией – способность идентифицировать лицо, от которого получен такой документ.

Одним из способов проверки допустимости, как уже отмечалась, может быть проведение компьютерной экспертизы, в данном случае экспертные заключениямогут подтверждать отсутствие изменений в электронных документах.

Учитывая данные особенности, Н.А. Зигура и А.В. Кудрявцева [68] выработали специальные правила, которые предлагают применять к компьютерной информации на этапе проверки:

- необходимо четко определить с какого электронного носителя компьютерной информации была получена компьютерная информация

- необходимо произвести проверку на соответствие все параметров электронного носителя информации с теми параметрами, которые указаны в протоколе следственного действия.

- необходимо четко установить программное оборудование, при помощи которого была получена или скопированная компьютерная информация

- необходимо установить все исходные реквизиты компьютерного объекта, содержащего необходимую компьютерную информацию (дата создания, последнего изменения и т.д)

- необходимо принять все меры для сохранения неизменности первоначального компьютерного объекта и содержащейся на ней информации.

При этом отмечается, что одним из эффективных средств проверки компьютерной информацииможе тявляетсяспециальная компьютерно-техническая экспертиза.

Следующим элементом доказывания является оценка собранных доказательств, которая заключается в выяснении их способности объективно удостоверять юридически значимые обстоятельства. В соответствии со ст. 88 УПК РФ «каждое доказательство подлежит оценке с точки зрения относимости,

[68]Зигура Н.А., Кудрявцева А.В. Компьютерная информация как вид доказательств в уголовном процессе России: монография. М.: Юрлитинформ, 2011. С. 80-82.

допустимости, достоверности, а все собранные доказательства в совокупности — достаточности для разрешения уголовного дела»[69].

Важно отметить, что вопреки распространенному мнению оценка доказательств не является только заключительным этапом процесса доказывания. Каждый этап процесса доказывания должен завершаться оценкой доказательств и изложением вытекающих из нее выводов в соответствующих процессуальных документах.

В связи с чем можно выделить оценку как отдельно взятого доказательства (например, оценка конкретного доказательства в ходе его собирания), так и оценку всей совокупности отобранных доказательств (окончательную оценку, позволяющую установить фактические обстоятельстваперед принятием соответствующего уголовно-процессуального решения, в частности перед разрешением уголовного дела по существу).

Уголовный процесс имеет публичные начала, из-за чего согласно ч. 2 и ч. 3 ст. 88 УПК РФ оценку доказательств осуществляет суд, прокурор, следователь и дознаватель. Однако стоит отметить, что в оценке доказательств могут принимать участие и иные субъекты уголовного процесса путем заявления ходатайств о недопустимости доказательств, обжалования действий и решений властных субъектов, связанных с оценкой доказательств.

Прежде чем рассматривать особенности оценки электронных доказательств, следует уяснить, что вообще понимается под оценкой доказательств.

По мнению Ю. К. Якимовича в общем виде оценка доказательств представляет собой «мыслительную логическую деятельность дознавателя, следователя, прокурора и суда (судьи), осуществляемую в соответствии с законом и правосознанием, по внутреннему убеждению, которая направлена наопределение относимости, допустимости доказательств, ихдостоверности,

[69]Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. От 18.02.2020)[Электронный ресурс]. СПС КонсультантПлюс.URL: http://www.consultant.ru/document/cons_doc_LAW_34481

достаточности в целях установления истиныпо делу и принятия определенного процессуального решения»[70].

Таким образом, исходя из определения, оценка компьютерной информации осуществляется с точки зрения относимости, допустимости, достоверности и достаточности.

Относимость — это требование, обращенное к содержанию доказательства, это способность доказательства своим содержанием служить средством установления обстоятельств, имеющих отношение к конкретному делу. Таким образом, относимыми являются такие доказательства, содержание которых воспроизводит (предположительно или достоверно) фактическое обстоятельство, необходимое для правильного разрешения дела.

Конечно, сразу нельзя сделать однозначный вывод о наличии объективной связи между доказательством и устанавливаемым фактом, наличие такой связи изначально лишь предполагается, далее, по мере расследования уголовного дела, выявляется обоснованность такого предположения, а окончательный вывод делается лишь на заключительном этапе доказывания.

Как отмечает Н.А. Зигура и А.В. Кудрявцева, «одной из особенностей определения относимости компьютерной информации является то, что оценке подлежит не только содержание компьютерной информации, но и свойтсва компьютерного объекта в котором она содержится, а именно его реквизиты, дата создания и т.д. Оценка относимости заключается не только в установлении того, что компьютерная информация по тем или иным признакам соотносится с предметом доказывания, а так же и в установлении того, как именно она связана, какие обстоятельства устанавливает, какой версии соответствует, а какой противоречит.

[70] Андреева О.И. Уголовный процесс: учебник для бакалавриата юридических вузов. Ростов: Феникс, 2015. С. 148.

Допустимость представляет собой требование, касающееся формы доказательства. Данное свойство указывает на необходимость соблюдения формальных законных требований к их получению.

Как уже отмечалось в предыдущих разделах, общее требование допустимости можно сформулировать из следующих положений: надлежащий (законный) источник получения доказательств, надлежащий (законный), способ получения доказательств, получение доказательств надлежащим субъектом, так же в дополнение можно выделить надлежащее процессуальное оформление доказательства.

В данной работе не рассматривается свойство допустимости — это самостоятельный обширный вопрос, подлежащий отдельному исследованию.

Однако представляется важным обратить внимание на то, что для признания компьютерной информации допустимым доказательством по делу с учётом специфики такой информации важно соблюдение следующих условий:

- обязательное наличие электронного носителя информации либо наличие процессуального документа, вовлекающего компьютерную информацию в уголовный процесс, в случае если изъятие электронного носителя не осуществляется;

- необходимо соблюдения целостности, полноты и неизменностикомпьютерной информации при ее хранении;

- обязательно наличие постановления о признании компьютерной информации в качестве доказательства и приобщении электронных носителей информации к уголовному делу.

Если допустимость отражает формальную сторону доказательства, то достоверность — его содержательную сторону: «доказательство должно соответствовать фактам, т.е. тому, что произошло в реальной действительности»[71].

Однако в отношении компьютерной информации, требование достоверности имеет свою специфику, так оценка электронных доказательств с

[71] Головко Л.В. Курс уголовного процесса. М.: Статут, 2017. С. 454.

позиции достоверности требует внимания как к правильности данных, так и к правильности функционирования программы обработки.

Так, Н.А. Зигура и А.В. Кудрявцева[72] в качестве критериев достоверности электронных доказательств выделяют следующие:

- достоверное доказательство может быть получено только в результате корректной работы технически исправных компьютерных устройств и программ.

- необходимо использовать научные методы получения компьютерной информации и соответствующее программное обеспечение.

- необходимо принять все меры по обеспечению неизменности и сохранности полученной компьютерной информации.

Свойство достоверности компьютерной информации должно подтверждаться путем анализа её свойств и содержания и в сравнении и сопоставлении с другими доказательствами по данному уголовному делу.

Существенным проблемным моментом в достоверности компьютерной информации является то, что в такую информации очень просто внести изменения, которые без специальных знаний и программного обеспечения практически невозможно обнаружить.

Достаточность характеризует качественную характеристику имеющейся системы доказательств с позиций ее убедительности для обоснования того или иного вывода или процессуального решения.

В отношении компьютерной информации сложно выделить какие-либо специальные требования достаточности. Разве что можно заметить, что для установления достаточности компьютерной информации собирать всю информацию, содержащуюся на электронном носителе не нужно. Однако на практике зачастую именно так и происходит, что, по сути, только усложняет и затягивает процесс доказывания.

---

[72]Зигура Н.А., Кудрявцева А.В. Компьютерная информация как вид доказательств в уголовном процессе России: монография. М.: Юрлитинформ, 2011. С. 131

Подводя итого, можно сказать, что проверка и оценка компьютерной информации как доказательства по уголовному делу подчиняется общим правилам проверки и оценки доказательств. Однако, в связи со своей спецификой и особенностями, проверка и оценка компьютерной информации требует применения специальных правил, а так же специальных знаний и применения специального технического и программного обеспечения.

ЗАКЛЮЧЕНИЕ

В рамках данного исследования были проанализированы особенности использование компьютерной информации в качестве доказательств в уголовном процессе, рассмотрены соответствующие проблемы, возникающие в правоприменительной практике, а также изучены основные законодательные и доктринальные положения, касающиеся данного вопроса. Результатом проделанной работы стало решение задач, представленных во введении.

Во-первых, было детально рассмотрено понятие компьютерной информации и основные подходы к его пониманию. Так, на сегодняшний день законодатель понимает под компьютерной информацией сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Однако данное определение нельзя признать корректным, оно слишком широко трактует содержание компьютерной информации, поскольку не содержит одного из основных ее признаков — пригодность для обработки компьютерными устройствами и использования ее в них. В связи с чем в данной работе было предложено внести изменения в понятие компьютерной информации, закрепленное в примечании к ст. 272 УК, включив в него указанный выше признак.

Во-вторых, были исследованы носители компьютерной информации как источники доказательств. Поскольку законодательного определения «электронного носителя информации» в УПК РФ нет, опираясь на научные работы исследователей в данной области, был сделан вывод, что наиболее теоретически обоснованным будет рассмотрение электронного носителя информации в узком и широком понимании. Материальным носителем компьютерной информации в узком смысле является устройство, конструктивно предназначенное для постоянного или временного хранения информации в форме, пригодной для использования в компьютерном устройстве, а также для ее передачи и обработке в информационных сетях, а в

широком смысле это физическое (электромагнитное) поле, на котором зафиксировано определенное содержание компьютерной информации. Однако теоретических положений недостаточно для решения практических процессуальных проблем, имеется явная потребность в законодательном урегулировании, либо комментировании со стороны Пленума Верховного Суда РФ положений, касающихся понятия и особенностей электронных носителей информации.

В-третьих, было определено место компьютерной информации в системе доказательств по уголовному делу. Так, законодателем компьютерная информация не выделяется в качестве отдельного вида доказательств. Однако это не препятствует использованию компьютерной информации в качестве доказательства при рассмотрении и расследовании уголовных дел. Компьютерная информация может быть:

1) в форме электронного документа и являться иным документом как видом доказательств

2) в форме электронного документа, и являться вещественным доказательством

3) в форме, не обладающей признаками электронного документа, однако отвечать при этом всем признакам вещественного доказательства.

В связи с чем было высказано предложение о внесении изменений в ст. 81 УПК РФ путем закрепления в ней положений о том, что компьютерная информация может выступать в качестве доказательства по уголовному делу как вещественное доказательство.

В-четвертых, был проведен анализ особенностей и проблем собирания компьютерной информации. Собирание компьютерной информации может осуществляться как в рамках получения доказательств, так и в рамках получения непроцессуальных данных, относимых к делу. Законодателем выделено два основных способа собирания компьютерной информации как доказательства: копирование представляющей интерес компьютерной информации на электронные носители предоставленные органами следствия

или дознания и изъятие электронных носителей информации у их владельцев с последующим исследованием представленной на них информации.

Изменениями, внесенными в УПК РФ 27.12.2018 г., была прямо закреплена возможность следователя производить копирование компьютерной информации с электронных носителей. Более того, была предусмотрена и процедура, в соответствии с которой это копирование должно осуществляться. Таким образом, законодатель устранил пробел, допущенный им ранее, официально закрепив устоявшуюся до нововведений практику копирования компьютерной информации без изъятия ее непосредственного носителя.

Изъятие, в свою очередь, имеет более обширное процессуальное регулирования, имеется ряд серьезных ограничений при производстве следственных действий, одним из которых является запрет на необоснованное применение мер, которые могут привести к приостановлению законной деятельности юридических лиц или индивидуальных предпринимателей, также не допускается необоснованное изъятие электронных носителей информации. Помимо ограничений, УПК РФ предусматривает и особый процессуальный порядок изъятия электронных носителей информации. Однако законодательные положения достаточно спорны и вызывают ряд дискуссий, в частности касающихся обязательного участия специалиста при изъятии электронных носителей информации. В данной работе разделяется позиция законодателя относительно обязательного участия специалиста, поскольку отсутствие специалиста при изъятии электронных носителей лишает их законного владельца или обладателя содержащейся на них информации потенциальной возможности реализовать право на ее копирование.

На сегодняшний день очевидно, что выделенных законодателем способов недостаточно для собирания всех видов имеющей значения для дела компьютерной информации. В связи с чем на практике приходится адаптировать уже имеющиеся положения о проведении следственных действий применительно к компьютерной информации. Однако научным сообществом

предлагается иной подход — введение в УПК РФ самостоятельного вида осмотра — дистанционного осмотра информационных ресурсов.

В-пятых, были рассмотрены процедуры проверки и оценки компьютерной информации. Проанализировав законодательные и доктринальные положения, был сделан вывод, что проверка и оценка компьютерной информации как доказательства по уголовному делу подчиняется общим правилам проверки и оценки доказательств. Однако, в связи со своей спецификой и особенностями, проверка и оценка компьютерной информации требует применения специальных правил, а так же специальных знаний и применения специального технического и программного обеспечения.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

А. Нормативно - правовые акты.

1. Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации [Электронный ресурс]. Исполнительный комитет СНГ официальный сайт. URL: http://www.cis.minsk.by/page.php?id=866

2. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 23.04.2019) [Электронный ресурс]. СПС КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_10699

3. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. От 13.06.1996) [Электронный ресурс]. Система Гарант. URL: http://base.garant.ru/3975363

4. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 18.02.2020) [Электронный ресурс]. СПС КонсультантПлюс.URL:http://www.consultant.ru/document/cons_doc_LAW_34481

5. Федеральный закон от 07.12.2011 N 420-ФЗ "О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации"[Электронный ресурс]. СПС КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_122864

6. Федеральный закон от 21.07.1993 г. N 5485-1 (ред. от 29.07.2018) "О государственной тайне"[Электронный ресурс]. СПС КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_2481

7. Межгосударственный стандарт ГОСТ 2.051-2013 "Единая система конструкторской документации. Электронные документы. Общие положения" (введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 22 ноября 2013 г. N 1628-ст) [Электронный ресурс]. Система Гарант. URL:http://base.garant.ru/70665820

Б. Материалы судебной практики. Акты судов общей юрисдикции.

8. Апелляционное постановление Верховного суда Удмуртской Республики от 04 декабря 2014 г.по делу N 22К-3299/2014.

9. Апелляционное постановление Кемеровского областного суда от 13 марта 2014 г. по делу N 22К-1137/2014.

10. Апелляционное постановление Приморского краевого суда от 24 сентября 2015 г. N 22-5674/15.

11. Апелляционное постановление Самарского областного суда от 28.10.2015 г. по делу N 22-5640/2015.

12. Апелляционное постановление Соликамского городского суда Пермского края от 17 октября 2017 г. N 10-83/2017.

13. Определение Верховного Суда от 7 августа 2012 г. по делу N 2–7/12.

14. Определение Конституционного Суда РФ от 26 января 2017 г. N 204-О «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».

15. Постановление Пленума Верховного Суда Российской Федерации от 19.12.2017 № 51 «О практике применения законодательства при рассмотрении уголовных дел в суде первой инстанции (общий порядок судопроизводства»

16. Приговор Кетовского районного суда Курганской области от 25 августа 2015 г. по делу N 1-89/2015.

17. Приговор Кинельского районного суда Самарской области от 12 августа 2014 по делу N 1-129/2014.

18. Приговор Лысьвенского городского суда Пермского края от 16 декабря 2013 г. по делу N 1-4/2014.

19. Приговор Ленинского районного суда г. Ульяновска от 23 марта 2018 г. по делу № 1-25/18.

В. Специальная литература.

20. Александров А.С., Кувычков С.И. О надёжности «электронных доказательств» в уголовном процессе. М.: Библиотека криминалиста: научный журнал, 2013. С. 76-84.

21. Андреева О.И. Уголовный процесс: учебник для бакалавриата юридических вузов. Ростов: Феникс, 2015. 445 с.

22. Белкин А.Р. Теория доказывания в уголовном судопроизводстве. Ч. 2. М.: Юрайт, 2017. 231 с.

23. Васюков В.Ф., Булыжкин А.В. Изъятие электронных носителей информации при расследовании преступлений: нерешенные проблемы правового регулирования и правоприменения. М.: Российский следователь, 2016. N 6. С. 3-8.

24. Воробей С.Н. Проблемы правовой регламентации процессуального порядка изъятия электронных носителей и копирования содержащейся на них информации. М.: Закон и право, 2020. С. 111-114.

25. Гаврилин Ю.В. Электронные носители информации в уголовном судопроизводстве. М.: Труды Академии управления МВД России, 2017. N4. С. 45-50.

26. Головко Л.В. Курс уголовного процесса. М.: Статут, 2017. 1280с.

27. Григорьев О.Г. Роль и уголовно-процессуальное значение компьютерной информации на досудебных стадиях уголовного судопроизводства: Дисс. … канд. юрид. наук. Тюмень, 2003. 221с.

28. Ефремова М.А. К вопросу о понятии компьютерной информации. М.: Российская юстиция, 2012. N 7. С. 50-52.

29. Зазулин А.И. Компьютерная информация в уголовном процессе: сущность и способы закрепления в качестве доказательства по уголовному делу. М.: Бизнес в законе. Экономико-юридический журнал, 2015. N 6. С. 130-133.

30. Зуев С.В., Черкасов В.С. Новые правила изъятия электронных носителей и копирования информации: преимущества и недостатки новеллы. Сибирское юридическое обозрение, 2019. N 2. С. 196-199.

31. Зигура Н.А., Кудрявцева А.В. Компьютерная информация как вид доказательств в уголовном процессе России: монография. М.: Юрлитинформ, 2011. 176 с.

32. Калиновский К.Б., Маркелова Т.Ю. Доказательственное значение «электронной» информации в российском уголовном процессе. М.: Российский следователь, 2014. N 6. С. 137 – 139.

33. Кириллова Н.П., Кушниренко С.П. Проблемы осуществления уголовного преследования по делам о преступлениях, совершаемых в сфере высоких информационных технологий. Правоведение. 2013. N 3. С. 83–84.

34. Кучина Я.О. Понятие компьютерной информации и его влияние на квалификацию преступлений, предусмотренных ст. 272 УК РФ. Иркутск: Академический юридический журнал, 2019. N 2. С. 25-34.

35. 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.

36. Осипенко А.Л., Гайдин А.И. Правовое регулирование и тактические особенности изъятия электронных носителей информации. Вестник Воронежского института МВД России. 2014. N 1. С.158–159.

37. Пастухов П.С. О развитии уголовно-процессуального доказывания с использованием электронных доказательств. СПС «КонсультантПлюс».

38. Пастухов П.С. Электронное вещественное доказательство в уголовном судопроизводстве. Вестник Томского государственного университета. 2015, № 396. С 149–153.

39. Перякина М.П., Унжакова С.В., Шишкина Н. Э. Процессуальные и криминалистические аспекты изъятия электронных носителей информации в свете защиты прав участников уголовного судопроизводства. Сибирский Юридический Вестник, 2019. N 3. С. 77–84.

40. Рыжаков А.П. Обыск и выемка: основания и порядок производства. М.: Издательство Дело и Сервис, 2015. 224 с.

41. Старичков М.В. Понятие «Компьютерная информация» в российском уголовном праве. Вестник Восточно-Сибирского института МВД России. Иркутск: ФГОУ ВПО ВСИ МВД России, 2014. N 1. С. 16-20.

42. Ткачев А.В. Вопросы использования электронных носителей компьютерной информации в уголовном процессе в качестве доказательств иных документов. Известия Тульского государственного университета. Экономические и юридические науки, 2016. N 3. С.436-442.

43. Цуканов Н.Н., Карлов А.Л. К вопросу об изъятии электроны носителей информации при производстве следственных действий. Алтайский юридический вестник, 2019. N 4. С. 135–140.

44. Чернышов В.Н., Лоскутова Е.С. Проблемы собирания и использования цифровых доказательств. Тамбов: Социально-экономические явления и процессы, 2017. С. 199-203.

45. Шейфер С.А. Понятие доказательства: спорные вопросы теории. М.: Государство и право, 2008. С. 17-21.

46. Шигуров А.В. Проблемы регулирования порядка проведения следственных действий, сопровождающихся изъятием электронных носителей информации. Библиотека криминалиста, 2013. С. 140.

Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Юридический институт
институт

Кафедра уголовного процесса и криминалистики
кафедра

УТВЕРЖДАЮ
Заведующий кафедрой
_____ А.Д. Назаров
подпись инициалы, фамилия
«07» 07 2020 г.

БАКАЛАВРСКАЯ РАБОТА

40.03.01 – «Юриспруденция»
код – наименование направления

Использование компьютерной информации в качестве доказательств в уголовном процессе
Тема

Руководитель _____ доцент, к.ю.н. А.С. Шагинян
подпись, дата должность, ученая степень инициалы, фамилия

Выпускник _____ П.А. Недбайлов
подпись, дата инициалы, фамилия

Красноярск 2020