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

Кафедра уголовного процесса
Направление подготовки (специальность)
40.05.02 Правоохранительная деятельность

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
по теме:

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННО-ЦИФРОВОЙ ИНФОРМАЦИИ В ДОКАЗЫВАНИИ ПО УГОЛОВНЫМ ДЕЛАМ

Выполнил:
слушатель взвода П1303
младший лейтенант полиции
Албогачиев Багаудин
Магометович

Решение о допуске к защите:
допущен
Начальник кафедры
подполковник полиции
_____ А. Б. Судницын
«14» 05 2018 г.

Руководитель:
профессор кафедры
уголовного процесса
кандидат юридических наук, доцент
полковник юстиции
Шинкевич Дмитрий Валерьевич

Дата защиты:
«20» июня 2018 г.

Оценка: удовлетворительно

Председатель ГЭК
полковник полиции _____ _____
(специальное звание) (подпись) (инициалы, фамилия)

Красноярск 2018

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

Кафедра уголовного процесса
Направление подготовки (специальность)
40.05.02 Правоохранительная деятельность

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
по теме:

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННО-ЦИФРОВОЙ ИНФОРМАЦИИ В ДОКАЗЫВАНИИ ПО УГОЛОВНЫМ ДЕЛАМ

Выполнил:
слушатель взвода П1303
младший лейтенант полиции
Албогачиев Багаудин
Магометович

Решение о допуске к защите:
_____
Начальник кафедры
подполковник полиции
_____ А. Б. Судницын
«___»_____ 2018 г.

Руководитель:
профессор кафедры
уголовного процесса
кандидат юридических наук, доцент
полковник юстиции
Шинкевич Дмитрий Валерьевич

Дата защиты:
«___»_____ 2018 г.

Оценка: _____

Председатель ГЭК

_____	_____	_____
(специальное звание)	(подпись)	(инициалы, фамилия)

Красноярск 2018

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Бурное развитие информационных технологий обусловило появление новых возможностей для использования информации в жизни общества. Появление новейших технических разработок диктует необходимость переосмысления положений науки уголовно-процессуального права относительно их использования в процессе доказывания по уголовным делам. Созданное учение об уголовно-правовых доказательствах нуждается в адаптации к новым правовым, научно-техническим условиям. Наметившиеся тенденции в применении цифровых дистанционных технологий в жизни общества открывает широкие возможности для оптимизации деятельности следователя. Однако, в условиях отсутствия системы регулирования в уголовно-процессуальном законодательстве деятельности следователя при работе с электронно-цифровой информацией и дальнейшее ее использование в доказывании по уголовным делам, обуславливает потребность в разработке рекомендаций по нормативному регулированию правоприменительной деятельности, связанной с использованием в доказывании сведений, имеющих форму электронно-цифрового документа.

Объектом настоящего исследования является комплекс правоотношений, складывающихся в процессе доказывания по уголовным делам, а также судебно-следственная практика по применению уголовно-процессуальных норм при использовании в доказывании электронно-цифровой информации.

Предметом указанного исследования выступает электронно-цифровая информация как источник доказательства, а также закономерности ее получения, исследования и оценки при расследовании преступлений.

Целью исследования является разработка и обоснование рекомендаций по использованию в процессе доказывания электронно-цифровой информации, совершенствование нормативного регулирования и правоприменительной деятельности, связанной с использованием в доказывании по уголовным делам электронно-цифровой информации.

Для достижения указанной цели необходимо решить следующие задачи:

- исследовать понятие электронно-цифровой информации и сформулировать ее определение, а также установить характерные для нее признаки;

- определить виды, формы и источники получения электронно-цифровой информации;

- выявить особенности изъятия и хранения электронно-цифровой информации;

- определить особенности проверки и оценки электронно-цифровой информации при доказывании по уголовным делам;

- сформулировать нормы уголовно-процессуального законодательства, направленные на эффективное использование электронно-цифровой информации в доказывании по уголовным делам.

Нормативную базу исследования составляли нормативно-правовые акты РФ их числе Уголовный Кодекс РФ и Уголовно-процессуальный Кодекс РФ.

Теоретическую базу исследования составили труды отечественных ученых в области уголовного процесса: Андреев Б.В. Булыжкин А.В. Вехов, В.Б., Зигура, Н.А. Карлов А.Л. Кириллова Н.П., Козловский, П.В., Краснова Л.Б., Кудрявцева, А.В., Кукарникова, Т.Э., Осипенко, А.Л., Першин А.Н., Старичков, М.В., Строгович М.С., Сутягин К.И., Ткачев, А.В., Тузов А.Г., Шигуров А.В.

Эмпирическую базу исследования составили решения районных судов, судов субъекта, а также решения Верховного суда Российской Федерации.

В данной дипломной работе были использованы такие общенаучные и частнонаучные методы как анализ нормативно-правовых актов, отнесенных к теме исследования, изучения и обобщения отечественной и зарубежной практики, сравнения, синтеза, индукции, дедукции, аналогии, а также сравнительно-правовой метод.

Глава 1. ЭЛЕКТРОННО-ЦИФРОВАЯ ИНФОРМАЦИЯ КАК ИСТОЧНИК ДОКАЗАТЕЛЬСТВ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ, ЕЕ ВИДЫ ФОРМЫ И ОСОБЕННОСТИ

§1. Понятие электронно-цифровой информации как источник доказательств в уголовном судопроизводстве, ее виды, формы и особенности.

С течением времени компьютеризация общества приобретает все больший охват, иначе говоря, набирает все новые обороты. Быстрыми темпами повышается степень популяризации компьютеров, сотовых (мобильных) телефонов, планшетов, а также иных электронных устройств, доступности сети Интернет.

Информационные телекоммуникационные технологии в настоящее время используются во всех областях жизнедеятельности человека.

Появление данных технологий в жизни человека – особенно важное условие для перехода к информационному обществу.

Впрочем, указанные технологии служат источником не только развития общества. Также они являются в своем роде стимулятором для применения данных технологий в противоправных действиях.

В связи с нарастающим уровнем количества преступлений, которые совершаются с использованием технических средств и преступлений в сфере компьютерной информации, на первом плане, среди иных, выступает вопрос о применении электронно-цифровой информации в качестве доказательств при рассмотрении и разрешении по уголовным делам.

В настоящее время определение электронной информации законом не установлено, однако исследуя точки зрения правоведов, занимающихся изучением этих вопросов, электронную информацию можно определить как - образ существующей реальности, созданный и представленный в

символьной (двоичной) форме с помощью специально созданного искусственного языка в виде последовательной записи на ЭВМ.

В отличие от аналоговой информации, для выражения которой в тексте используется естественный язык традиционного алфавита, в электронной форме информации используется специально созданный искусственный язык (программирования) и цифровая (двоичная) форма представления.

Основное ее назначение состоит в удовлетворении потребностей граждан и других субъектов в общении и взаимодействии между собой. Так же следует отметить, что развитие систем мобильной и спутниковой связи, информационно-телекоммуникационной сети «Интернет», зарождение новых информационных технологий и иных форм телекоммуникаций значительно увеличили роль электронно-цифровой информации в формировании глобального информационного пространства.

Федеральным законом № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации» закреплено определение «информации» как правовой категории. Информация – «это сведения, сообщения, данные, не зависимо от формы их представления[1]».

Понятие «цифровая информация» прочно влилось в нашу повседневную жизнь. Кроме того, понятие «цифровая информация» оказывает значительное воздействие на правоотношения, которые складываются в сфере электронной коммерции. Современные возможности обращения электронно-цифровой информации порождают все новые виды преступлений, направленных на завладение и манипулирование ей.

[1] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ // Собрание Законодательства РФ. – 2006. (с изм. и доп., от 23.04.2018). — СПС «Консультант»

Впрочем, действующим законодательством не предусмотрена электронная информация как отдельный вид доказательства и как следствие не урегулирован порядок изъятия и приобщения к материалам уголовного дела такой информации. Отсюда возникает проблема допустимости и относимости такой информации в качестве доказательств.

До вступления в силу изменений в УК РФ в редакции Федерального закона «от 7 декабря 2011 г. № 420-ФЗ» в российском законодательстве отсутствовало легальное определение компьютерной информации. Так, раньше в ст. 272 УК РФ не давалось определения понятия компьютерной информации, а только говорилось о носителях, в которых эта информация содержится. Данный вопрос не учтен также и в основном нормативном акте, регулирующем отношения в сфере обращения информации. Так, Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» не дает определения понятия компьютерной информации.

Электронная уголовно-процессуальная информация - это образ события преступления как явления социальной действительности, отраженный в сознании участников уголовного судопроизводства, созданный, закрепленный и представленный в электронной форме, которая допустима уголовно-процессуальным законом, с целью получения истинного представления (понимания) его ретроспективной картины.

Названная нами информация обладает всеми признаками, которые характерны для уголовно-процессуальной информации, и является одним из ее видов, основным отличием выступает электронная форма ее представления.

Разновидностью электронно-цифровой информации является компьютерная информация, под которой понимаются сведения (сообщения, данные), которые представлены в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Указанный термин впервые на уровне действующего уголовного закона

определил понятие компьютерной информации как предмета преступления.

Если ранее специфика преступлений в сфере электронно-цифровой информации была обусловлена использованием новых технологий и необходимостью обладания определенным уровнем специальных познаний, то сегодня в информационно-телекоммуникационной сети «Интернет» присутствуют как программы, предназначенные для совершения несанкционированных действий с названной информацией, так и инструкции по их применению.

Для обособления электронно-цифровой информации необходим соответствующий носитель. В настоящее время законодатель не закрепил содержание термина - "электронный носитель информации" в уголовно-процессуальном законе, что способствует неоднозначному пониманию его смысла.

Данная проблема обусловлена различными целями и задачами, которые с юридической и технической точек зрения имеют полярное толкование.

Так, современные электронные носители представляют собой сложные устройства, и их толкование должно приводиться в национальных стандартах Российской Федерации, однако данные правовые акты могут стать правовыми нормативными актами только в определенных законом случаях. Кроме того, «национальный стандарт» - это документ, разработанный участниками работ по стандартизации, утвержденный федеральным органом исполнительной власти в данной сфере, в котором для всеобщего применения устанавливаются общие характеристики объекта стандартизации.

Сегодня только на уровне названных документов содержится общее и юридически неопределенное понятие «электронного носителя информации», под которым понимается-материальный носитель,

используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники.

Даже самый поверхностный анализ вышеприведенного определения не позволяет выделить основные, отличительные признаки рассматриваемого нами объекта.

Например, являются ли «электронными носителями информации» сервер федерального оператора связи, предназначенный для регулирования потоков электронной информации, ее хранения, а также воспроизведения голосовой информации в реальном режиме времени с помощью программно-аппаратных средств, или материальный носитель, содержащий случайную комбинацию цифр, предназначенный для получения доступа к чему-либо? С учетом вышеприведенного понятия однозначно и не ответишь.

В УПК РФ рассматриваемый термин был введен Федеральным законом[1] с целью учесть особенности порядка проведения следственных действий[2], сопровождающихся изъятием электронных носителей информации. Идея разработчиков законопроекта выражалась в том, что на современном этапе развития информационных технологий необходимо упорядочить процедуру изъятия в ходе расследования уголовных дел электронных носителей информации и порядка возвращения изъятых электронных носителей информации и (или) копирования содержащейся на них информации[3].

---

[1] Федеральный закон от 28 июля 2012 г. N 143-ФЗ "О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации" // Собрание законодательства Российской Федерации. 2012. N 31. Ст. 4332.

[2] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 29.07.2017) (с изм. и доп., вступ. в силу с 01.09.2017) // Собрание законодательства РФ, 24.12.2001, N 52 (ч. I), ст. 4921.

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

Данный термин был включен в общие правила производства обыска и выемки, в связи с чем изменения уголовно-процессуального законодательства затронули процессуальную деятельность органов предварительного расследования, осуществляемую не только по экономическим преступлениям, но и по всем тем уголовным делам, в предмет доказывания которых входят обстоятельства, свидетельствующие об использовании электронных носителей информации подозреваемым (обвиняемым) в ходе подготовки, совершения, сокрытия преступления[1].

В текстах стандартов «материальный носитель документированной информации» определяется как материальный объект, используемый для закрепления, хранения и воспроизведения речевой, звуковой или изобразительной информации[2].

Электронный носитель информации является не просто материальным носителем, а сложным по своему внутреннему строению, конфигурации и технологичности электронным устройством, обладающим следующей спецификой:

- материал, из которого изготовлен носитель, способен многократно сохранять, изменять и воспроизводить записанную на нем электронную информацию в зависимости от потребностей пользователя или назначения устройства;

- наличием программного обеспечения, изначально хранящегося во внутренней памяти устройства, для визуализации, имеющейся (записываемой) на нем бинарной информации, на экране компьютера или возможности ее передачи в соответствии с транспортными протоколами

---

[1] Бархатова Е.Н. Особенности квалификации мошенничества в сфере компьютерной информации и его разграничение с иными составами преступлений / Е.Н. Бархатова // Современное право. 2016. N 9. С. 110

[2] ГОСТ Р. 7.0.8-2013. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения: утв. Приказом Росстандарта от 17.10.2013 N 1185-ст // Доступ из справ.-правовой системы "КонсультантПлюс" (дата обращения: 15.07.2017).

передачи данных по единой сети электросвязи РФ и согласующихся с ней международных сетей электросвязи;

- обеспечением возможности долговременного хранения записанной электронной информации во внутренней памяти устройства (особенностью самого материала носителя, осуществляющего данную функцию, или же наличием дополнительных (внешних или внутренних) источников энергии, способных поддерживать такую способность носителя);

- исключением возможности модификации, записанной (имеющейся) на носителе электронной информации, т.е. ее безопасностью. Безопасность в данном случае должна пониматься не только в аспекте (угрозы) изменения и уничтожения электронной информации, но и несанкционированного копирования, т.е. незаконного доступа к содержанию электронного носителя информации;

- возможностью обособления имеющейся электронной информации от ее возможных аналогов, хранящихся на подобных носителях или источниках информации, при подключении электронного носителя информации к компьютерным устройствам или информационно-телекоммуникационным каналам передачи данных.

С учетом вышеприведенной специфики рассматриваемого носителя для единообразного понимания и применения в сфере уголовного судопроизводства выделим юридически значимые признаки понятия электронного носителя информации:

- сложность внутреннего строения, конфигурации и технологичность носителя;

- способность многократно сохранять, изменять и воспроизводить записанную на нем электронную информацию;

- наличие энергонезависимого (энергозависимого) программного обеспечения, изначально хранящегося во внутренней памяти устройства;

- долговременное хранение записанной электронной информации во внутренней памяти устройства;

- обеспечение защиты записанной (имеющейся) на носителе информации и возможности разграничения доступа к ее уровням;

- возможность обособления электронной информации.

Таким образом, под электронным носителем информации следует понимать технически и технологически адаптированное к многократному использованию электронное устройство, предназначенное для записи, хранения, передачи и воспроизведения электронной информации с помощью доступных технических средств, а также защиту, обособление и разграничение доступа к имеющейся информации.

Для единообразного толкования закона предлагаемое понятие может быть закреплено в ст. 5 УПК РФ. Это позволит ввести в научный и практический оборот важный термин для уголовного процесса, обеспечить его однозначное понимание, возможность уточнения и конструирования отдельных норм уголовно-процессуального закона.

В предлагаемом понятии логично употреблять такие термины, как "электронная информация" и "электронное устройство", а не "компьютерная информация", "машинная информация", "компьютер", "средства вычислительной техники", "цифровое устройство", т.к. первичные понятия являются большими по объему и включают в свое содержание существующие виды электронной информации и иных электронных устройств.

Разнообразие электронных носителей информации обусловлено отдельными видами электронной информации, информационных технологий и используемых при этом технических средств.

Можно утверждать, что для уголовного судопроизводства неважна классификация данных носителей в зависимости от способов их создания и применения в конкретной сфере человеческой деятельности, а актуально их разграничение в зависимости от их роли и назначения в уголовном процессе.

Целесообразно выделять электронные носители информации, если они:

- могут выступать в качестве самостоятельных средств доказывания (вещественные доказательства или иные документы);

- получены в ходе проведения следственных или иных процессуальных действий при использовании альтернативных средств фиксации информации (видеозапись, фотосъемка и др.);

- использованы в ходе уголовного судопроизводства для записи, хранения, передачи или воспроизведения уголовно-процессуальной информации (протоколы следственных и иных процессуальных действий, заключения эксперта (специалиста), электронный протокол судебного заседания, постановления следователя, приговор суда и др.);

- представлены или истребованы в ходе уголовного судопроизводства (результаты оперативно-розыскной деятельности, материалы, полученные с камер наружного наблюдения, размещенных с целью обеспечения личной или общественной безопасности и др.).

Место носителей и информации, содержащейся на таких носителях, - вопрос дискуссионный. Причиной тому является то, что законодательно такие категории как «носитель электронной информации» и «электронная информация» не закреплены ни за одним источником доказательств, установленных статьей 74 УПК РФ. В большинстве своем, ученые-процессуалисты относительно данного вопроса сводятся к двум группам:

- Первые утверждают, что электронная информация и носители электронной информации относятся к иным документам;

- Вторая убеждена в том, что такие носители и информация являются вещественными доказательствами.

Ученые, мнение которых заключается в том, что электронная информация и ее носители относятся к иным документам, обосновывают свои доводы в первую очередь толкованием статьи 84 УПК РФ.

Суть данной статьи заключается в том, что документы, которые содержат информацию об обстоятельствах, подлежащих доказыванию, фиксируют такую информацию в письменном и ином виде.

Частью второй указанной статьи установлено также и то, что иными документами являются и иные носители информации, получаемые, истребованные или представляемые в порядке, согласно статьи 86 УПК РФ.

Так, по мнению данных ученых, закрепленные частью 2 статьи 84 УПК РФ иные носители информации, подразумевались законодателем именно как носители электронной информации.

При этом необходимо разграничить понятия документа и документированной информации. Цель разграничения – установление признаков иного документа. Выявив признаки мы получим возможность отнесения электронной информации и носителей электронной информации к данному виду доказательств.

Понятие документа обширное и устанавливается в различных Федеральных законах, которые не применяются в уголовном судопроизводстве. Понятие же документированной информации закреплено в Федеральном законе «Об информации, информационных технологиях и о защите информации». Сфера применения данного федерального закона – отношения, возникшие в результате осуществления права на поиск, на получение, на передачу, на производство и распространение информации. Также в эту сферу входят отношения по применению информационных технологий и возникающие при обеспечении защиты информации[1].

Расследование абсолютно всех преступлений неразрывно связано с поиском, получением и защитой информации. Так, представляется, что

[1] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ // Собрание Законодательства РФ. – 2006. (с изм. и доп., от 23.04.2018). — СПС «Консультант»

нормы указанного закона вполне применимы к понятию «иной документ» в уголовном процессе.

Документированная информация, в силу данного закона, - зафиксированная на материальном носителе путем документирования информация с реквизитами, которые позволяют определить такую информацию или ее материальный носитель.

По мнению Ткачева А.В., реквизиты именно то, что дает возможность отграничивать документы от недокументированной информации; определять электронные документы как иные документы[1].

Однако, не стоит забывать, что в силу части 4 статьи 84 УПК, документы, которые имеют признаки вещественных доказательств, признаются и приобщаются к материалам дела именно как вещественные доказательства.

В связи с этим следует отметить, что электронные носители информации в ходе уголовно-процессуального доказывания могут выступать и в роли вещественных доказательств, по мнению другой части ученых, т.к. в данном случае правоприменитель должен руководствоваться строгой процессуальной формой их закрепления, а не "аморфностью", присущей иным документам[2].

Основу же убеждения такой группы составляет часть 4 статьи 81 УПК РФ, которая устанавливает, что в совокупность предметов, не признанных вещественными доказательствами и подлежащих возврату, входят носители электронной информации. Также в основу положена

---

[1] Ткачев А.В. Использование электронных (компьютерных) документов в качестве документов-доказательств и письменных доказательств в процессуальных отношениях // Библиотека криминалиста. Научный журнал.. – 2013. – № 5. – С. 128–135; 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. – № 3. – С.436–442.

[2] Давлетов А.А. Уголовное судопроизводство Российской Федерации. Курс лекций / А.А. Давлетов. Изд. 2-е. Екатеринбург, 2013. С. 124

статья 82 УПК РФ, регулирующая хранение вещественных доказательств, которой закреплен порядок хранения вещественных доказательств, являющихся электронными носителями информации.

Еще одним фактом, согласно мнению данной группы ученых, служит часть 1 статьи 81.1 УПК РФ, которой установлено, что носители электронной информации должны быть признаны вещественными доказательствами и приобщены к материалам дела с вынесением соответствующего постановления при расследовании экономических преступлений.

Вещественные доказательства являются обширной категорией. В научной литературе выделяются различные основания для их классификации. Например, по специфике материального носителя, по количественным характеристикам, по отношению к доказываемым обстоятельствам преступления и версии обвинения, наличию носителей - посредников между доказываемым фактом и источником уголовно-процессуальной информации[1].

Основным отличием электронного носителя информации, признанного вещественным доказательством в соответствии с требованиями уголовно-процессуального закона, от иных видов вещественных доказательств, является то, что субъектов доказывания, как правило, интересует информация, содержащаяся на названном носителе, а не его внешний вид[2].

По мнению Красновой Л.Б. у носителей электронной информации статус вещественных доказательств, согласно следующим признакам[3]:

---

[1] Егоров Н.Н. Вещественные доказательства: уголовно-процессуальные и криминалистические аспекты / Н.Н. Егоров. М.: Юрлитинформ, 2007. С. 304

[2] Андреев Б.В. Расследование преступлений в сфере компьютерной информации / Б.В. Андреев, П.Н. Пак, В.П. Хорст. М.: Юрлитинформ, 2011. С. 152

[3] Краснова Л. Б. Электронные носители информации как вещественные доказательства // Известия Тульского государственного университета. Экономические и юридические науки. 2013. – № 4. – С.254–260.

- носители электронной информации являются средством установления обстоятельств дела;

- данные носители могут иметь, помимо информации о преступлении, следы преступления;

- данные на носителях хранятся во внешних признаках (а не в вербальной форме);

- способ получения, хранения, передачи невербальной информации – материальный.

Помимо приведенных двух условных групп, существует и еще ряд авторов, придерживающихся альтернативной точки зрения. По их мнению электронную информацию и ее носители вообще необходимо признать как отдельный вид доказательств.

Сторонником данного «течения» является Батурин Ю.М., который утверждает, что запись в памяти электронной вычислительной машины преобразуется в код, а следовательно оцениваться должно, помимо записи в памяти, программа съема информации[1].

Еще одним сторонником является Зигура Н.А. Он обособляет электронную (компьютерную) информацию как вид доказательств. Причиной тому является то, что фиксация такой информации используя электронные вычислительные машины, протекает без переработки информации сознанием людей, то есть именно в объективно существующей форме без влияния субъективного восприятия человека, который ее закрепляет. Именно в этом Зигура Н.А. видит огромную ценность такой информации[2].

И в заключение хотелось бы отметить, что информационные технологии будут совершенствоваться и далее, разнообразные технические

---

[1] Батурин Ю. М. Проблемы компьютерного права. — М.: Юридическая литература, 1991. — 272 с.

[2] Зигура, Н.А., Кудрявцева, А. В. Компьютерная информация как вид доказательств в уголовном процессе России: монография / Н. А. Зигура, А. В. Кудрявцева. — М.: Юрлитинформ, 2011. — 176 с.

(информационные) термины - проникать в материю права, какими бы консервативными ни были существующие отрасли права. Полагаем, что законодатель должен своевременно реагировать на подобные изменения, наполнять, толковать и закреплять в действующем законодательстве "новые" понятия с учетом современных аспектов. Уголовно-процессуальный закон не является исключением, а с учетом его назначения его содержание предполагает к себе особое внимание.

§ 2. Источники получения электронно-цифровой информации, особенности ее изъятия и хранения

Согласно статьи 85 Уголовно-процессуального кодекса, цель доказывания как процесса заключается в установлении обстоятельств, которые соответственно подлежат доказыванию. Элементами процесса доказывания выступают:

1) Собирание;
2) Проверка;
3) Оценка доказательств.

Собирание доказательств. В силу части 1 статьи 86 Уголовно-процессуального кодекса в ходе уголовного процесса дознавателем, следователем, прокурором, судом при производстве предусмотренных законом процессуальных действий осуществляется собирание доказательств.

Данная часть работы посвящена проблемам сопутствующим процессу собирания доказательств. Основной способ такого сбора, как уже

упоминалось, - осуществление следственных действий (и иных процессуальных действий)[1].

Относительно электронной информации выделяются следующие приемы собирания:

1) Копирование, имеющей значение для дела, информации.

2) Изъятие носителей электронной информации и исследование названной информации.

Оба приема имеют положительные и отрицательные стороны, что дает возможность выбора одного из приемов, для реализации на практике[2].

Положительной стороной при изъятии является наличие возможности, в дальнейшем, более тщательно, с привлечением специалистов, исследовать полученную информацию, что во многом устраняет возможность сокрытия информации.

Отрицательной стороной, в свою очередь, при таком подходе, будет являться наличие препятствий технического характера, которые мешают изъятию всех средств. Такое изъятие является нецелесообразным.

Также, при изъятии носителей электронной информации, возникает проблема защиты прав хозяйствующих субъектов, изъятие у которых производится. Дело в том, что зачастую на названных носителях, помимо прочих, существуют сведения, при отсутствии которых нормальное функционирование субъектов затрудняется, и в таком случае данным субъектам причиняется ущерб.

Такая проблема учтена законодательством. В Уголовно-процессуальном кодексе содержатся нормы, регулирующие порядок изъятия носителей электронной информации и соответственно порядок их

---

[1] Уголовный процесс : учебник для бакалавриата юридических вузов / О. И. Андреева [и др.] ; под ред. О. И. Андреевой, А. Д. Назарова, Н. Г. Стойко и А. Г. Тузова. Ростов н/Д, 2015. С. 143.

[2] Сутягин К. И., Зуев С. В., Извеков Ю. А. Электронное копирование информации как самостоятельное следственное действие // Следователь. 2003. No 4. С. 14.

возвращения или же копирования информации, заключенной в таких носителях.

Упомянутые нормы дают возможность дополнительной защиты прав и разрешают проблему продолжения осуществления деятельности хозяйствующим субъектом при изъятии носителей электронной информации.

Так, существует возможность копирования информации по ходатайству владельца изымаемого носителя информации или же по ходатайству обладателя информации, содержащейся на носителе.

Впрочем, этим решены не все проблемы.

Копирование информации по ходатайству, конечно, приносит облегчение продолжению нормальной деятельности организации, однако не всегда обеспечиваются все гарантии прав. К примеру, на изымаемых носителях информации, возможно наличие, помимо этой самой информации, используемого программного обеспечения, имеющееся в одном единственном экземпляре.

Также согласно уголовно-процессуальному законодательству запрещено копирование информации, при наличии возможности воспрепятствования расследованию или же утраты или изменения информации.

Впрочем, согласно мнению отдельных авторов, каких-либо критериев, устанавливающих возможность наступления указанных последствий, нет, что приводит в определенных случаях к отказам без оснований[1].

Учитывая практику, можно отметить, что в определенных случаях вместо изъятия носителей информации – оригиналов, вполне является достаточным изготовление защищенных от всяческих изменений их копий.

[1] Шигуров А. В. Проблемы регулирования порядка проведения следственных действий, сопровождающихся изъятием электронных носителей информации // Библиотека криминалиста : научный журнал. No 5 (10). М., 2013. С. 140.

Однако часть авторов утверждают, что более целесообразным будет распоряжение следствием или же судом носителями информации, изъятыми в ходе процессуальных действий, нежели носителями со скопированной информацией, по причине того, что лицо, у которого произошло изъятие, в дальнейшем получает возможность отрицать принадлежность указанных носителей.

В тоже время, согласно сложившейся судебной практики, копирование информации на носители, как способ получения информации признан правомерным.

Отсюда возникает вопрос – необходим ли при проведении такого действия специалист? Суды приходят к выводу, что участие специалиста в данных случаях необязательно. Основу их мнения составляет то, что для таких случаев, в сравнении с изъятием носителей электронной информации, уголовно-процессуальным законодательством участие специалиста не установлено. Тем не менее, выполнение копирования информации подразумевает использование специальных знаний и навыков, для устранения возможности утраты, изменения информации или же потери ей доказательственной природы вследствие неосторожного доступа к такой информации следователем, не имеющим познаний в данной сфере.

В тоже время, участие специалиста является обязательным тогда, когда копирование осуществляется с изымаемых носителей на носители, которые предоставляет владелец изымаемых носителей или же обладатель информации, которая содержится на изымаемых носителях, по ходатайству таких владельца или обладателя.

Учеными-процессуалистами выдвигается предложение о введении такого следственного действия как копирование электронной информации. Основание введения такого следственного действия согласно их мнению –

осмотр, обыск, выемка в сравнении с копированием электронной информацией обладают различной природой[1].

Так, Зуев С.В., Сутягин К.И., Извеков Ю.А. применительно к данному действию, устанавливают обязательность в процессе его осуществления участие специалиста в сфере компьютерных технологий и информатики. Кроме того, по их мнению, в такой деятельности обязательно также участие понятых, которые имеют познания в сфере компьютерной техники, для удостоверения фактов, содержания и результатов производимых при их участии действий.

Приемы получения определенных объектов электронной информации нужно рассматривать в плане необходимости обеспечения их сохранности в том виде, в котором они были обнаружены. Основная проблема при этом заключается в том, что изъятие электронных объектов невозможно. Изъять можно только носитель электронной информации, с имеющимися на нем объектами такой информации, но вместо этого возможно произвести копирование. Впрочем, на практике нередко встречаются такие определения, как изъятие видеозаписи и подобные…

Интересным представляется вопрос изъятия переписки находящейся на электронных носителях расположенных в сети Интернет. Так, Карлов А.Л.[2] предлагает свой алгоритм фиксации переписки (см. приложение №1).

Целесообразным по нашему мнению будет разобрать данную схему фиксации подробнее. Для решения вопроса о процессуальном закреплении интернет-переписки следователь должен поэтапно проанализировать следующие элементы исходной следственной ситуации по делу:

---

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

[2] Карлов А.Л. Пахорукова Ю.Е. Процессуальная фиксация интернет-переписки в качестве доказательств по уголовным делам о преступлениях в сфере незаконного оборота наркотиков // Вестник Сибирского юридического института МВД России №4(25). 2016. С. 111 – 117.

1) местонахождение переписки (сервер оператора связи либо электронный носитель пользователя);

2) наличие свободного доступа неограниченного круга лиц;

3) характер переписки (личная, служебная);

4) готовность пользователя дать согласие на ознакомление с его интернет-перепиской;

Перечисленные обстоятельства имеют значение для разрешения вопроса об отнесении интернет-переписки к тайне связи[1] (соответственно, о необходимости получения судебного решения для ознакомления с ней), а также для определения процессуальных средств её получения и фиксации.

Проанализируем каждый элемент с моделированием конкретной ситуации, в которой может оказаться следователь.

1. При использовании преступниками сети Интернет для обмена данными содержание переписки, а также другие сведения о ней сохраняются как на электронных носителях пользователей, так и на серверах оператора связи (в распоряжении компании, обеспечивающей передачу данных). Соответственно, следователь имеет возможность получить данную переписку, изъяв электронные устройства, с которых велась переписка, либо обратившись за содействием к оператору связи.

При изъятии электронных носителей подозреваемых и ознакомлении с хранящейся на них перепиской процессуальных проблем не возникает, поскольку УПК РФ предусматривает такое следственное действие, как осмотр предметов (предметом будет выступать компьютер или иной электронный носитель информации), при необходимости в отношении такого носителя может быть проведена компьютерно-техническая экспертиза. Также в данном случае не возникает проблем с режимом доступа к данной переписке (нет необходимости получать судебное

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

решение), так как одним из обязательных критериев отнесения информации к тайне связи является её нахождение в ведении оператора связи[1], тогда как переписка, сохранившаяся на жестком диске, уже выбыла из ведения оператора связи, соответственно, получение судебного решения для осмотра или судебной экспертизы не требуется. Следует отметить, что сами по себе сведения на электронных носителях подозреваемого, в зависимости от их содержания, могут быть отнесены к личной тайне или к тайне частной жизни (ч. 1 ст. 23 Конституции РФ), однако в соответствии с ч. 3 ст. 55 Конституции РФ данное право может быть ограничено федеральным законом, к которым относится УПК РФ.

При необходимости в ходе расследования уголовного дела использовать в доказывании переписку, расположенную на сервере оператора связи, возникает целый ряд вопросов, разрешение которых зависит от следующего элемента исходной ситуации, которым выступает наличие или отсутствие доступа к интернет-переписке.

2. Большая часть информации в сети Интернет имеет открытый характер, то есть доступ к ней имеет неограниченный круг лиц, таким свойством может обладать и интернет-переписка, которая содержится на форумах, в открытых чатах и др. Данная информация зачастую имеет большое доказательственное значение и требует правильного процессуального закрепления[2].

---

[1] Карлов А.Л. Правовой режим использования в доказывании по уголовным делам электронной переписки, содержащейся в памяти технических средств коммуникации // Актуальные проблемы профилактики наркомании и противодействия правонарушениям в сфере легального и незаконного оборота наркотиков: национальный и международный уровней материалы XVII международной научно-практической конференции (17-18 апреля 2014 года). Красноярск: СибЮИ ФСКН России, 2014. Ч 2. С.194.

[2] Так, согласно материалам уголовного дела, находящегося в производстве ГСУ ГУ МВД России по г. Москве, с целью установления факта и периода знакомства, а также совместного времяпрепровождения был произведен осмотр электронных документов – интернет-страниц с содержанием профилей пользователей социальной сети «ВКонтакте», которые содержали соответствующие записи и фотографии.

В силу общедоступности вопрос об отнесении данных сведений к какому-либо виду тайны не стоит, соответственно, получена она может быть посредством следственных действий. По нашему мнению, наиболее подходящим и рациональным будет проведение такого следственного действия, как осмотр документа. В данном случае любая страница сайта представляет собой электронный документ, под которым, согласно п. 11.1 ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», следует понимать документированную информацию, представленную в электронной форме, в виде, пригодном для восприятия человеком с использованием электронных и вычислительных машин, а также для передачи по информационного-телекоммуникационным сетям или обработки в информационных системах. Кроме того, п. 11 ст. 2 указанного Федерального закона предусматривает один из обязательных признаков документированной информации – наличие реквизитов, позволяющих определить информацию или её носитель. Для страницы в сети Интернет таким реквизитом выступает её уникальный адрес. При изучении следственной практики МВД России было установлены случаи фиксации содержания интернет-страниц в ходе такого следственного действия, как осмотр предмета (компьютера, ноутбука и др.), при том что осмотру подвергались сведения, расположенные в сети Интернет, однако, на наш взгляд, такая практика является ошибочной, поскольку сам по себе компьютер в данном случае осматриваемой информации не содержит и выступает лишь техническим средством, обеспечивающим её визуализацию.

Далее следует рассмотреть ситуации, при которых переписка, расположенная в сети Интернет, доступна ограниченному кругу лиц (например, личная переписка между пользователями социальных сетей, личные сообщения электронной почты и др.). Для определения порядка

процессуальной фиксации такой переписки, необходимо определить её характер, то есть выяснить, является она личной либо служебной.

3. В связи с тем, что без ознакомления с перепиской мы не можем определить ее характер, следователю в данном случае следует исходить из того, в чьем распоряжении она находится. Переписка, которая производится с использованием служебных аккаунтов (представленных работодателем), может располагаться на серверах разных операторов (работодатель самостоятельно решает, какой из сервисов для этого использовать, но наиболее распространенными являются такие почтовые сервисы, как Mail.ru, Gmail, Yahoo messenger, Яндекс.Почта и др.), при этом работодатель имеет право на получение и использование данной переписки в полном объеме, поскольку эти данные не относятся к тайне связи[1]. Соответственно, в случае необходимости получения интернет-переписки, которая осуществлялась со служебных аккаунтов, следователь может произвести выемку носителей с данной перепиской у представителя работодателя либо произвести её осмотр (осмотр электронного документа или осмотр предмета (носителя) в зависимости от её местонахождения) в присутствии представителя работодателя.

4. В ситуации, когда расположенная на сервере оператора переписка признана личной, для принятия решения о способе её фиксации необходимо выяснить, готов ли подозреваемый дать согласие на ознакомление с его интернет-перепиской. Этот вопрос является принципиально важным, поскольку, как было указано выше, ограничение права на тайну связи допускается только на основании судебного решения. В то же время ч. 2 ст. 17 Конституции РФ предусматривает, что основные права и свободы (в том числе право на тайну связи) не отчуждаемы и принадлежат человеку от рождения, однако это право является

[1] Постановление ЕСПЧ от 12.01.2016 по делу «Барбулеску (Bărbulescu) против Румынии» (жалоба № 61496/08) URL:: http://hudoc.echr.coe.int/rus?i=001-159906 (дата обращения: 03.05.2018).

субъективным, что означает возможность человека самостоятельно выбирать вид и меру своего поведения [1], а также свободу поведения и поступков в границах, установленных нормой права[2]. Исходя из такой трактовки, любой человек может самостоятельно распоряжаться своим правом; соответственно, в ситуации, когда ознакомление с интернет-перепиской осуществляется с согласия пользователя, ограничение его права на тайну связи не происходит, а значит, судебного санкционирования такие действия не требуют.

При наличии такого согласия, исходя из удостоверительного характера доказывания, оно должно быть оформлено письменно и с участием защитника (для подозреваемого, обвиняемого). При решении вопроса о выборе следственного действия, которое следует произвести, в первую очередь нужно определиться с его целями. В случае, если целью является осмотр и фиксация данных, о котором пользователь дал подробные показания, целесообразно произвести такое следственное действие, как осмотр документа (электронного) с участием пользователя[3]. В ситуации, когда показания пользователя носят фрагментарный характер и целью ознакомления с перепиской является получение новых сведений или уточнение его показаний, следователь может произвести проверку показаний на месте. В случае же, если целью следователя является проверка навыков пользователя работы в сети Интернет (в том числе способность отправлять и получать различного рода сообщения), следует производить следственный эксперимент.

Однако зачастую следователи сталкиваются с тем, что злоумышленники не дают согласия на осмотр их переписки, так как

---

[1] Невирко Д.Д. Права и свободы человека и гражданина: проблемы соотношения, взаимодействия и иерархии : монография. Красноярск, 2006 С. 22.

[2] Строгович М.С. Проблемы советского социалистического государства в современный период. Некоторые теоретические вопросы. М., 1967. С. 170.

[3] На наш взгляд, при наличии письменного согласия участие пользователя не является обязательным.

получаемые в этом случае сведения могут стать доказательствами их причастности к совершенному преступлению. Используя приведенные выше доводы, можно заключить, что в такой ситуации получение судебного решения на ограничение права на тайну связи является обязательным.

Далее перед следователем встает вопрос о том, на проведение какого следственного действия необходимо получить санкцию суда? Найти ответ на этот вопрос в научной литературе не удалось. В результате выяснилось, что следователи в подобных сучаях применяют выемку, однако немногие считают ее проведение приемлемым, что, на наш взгляд, связано с существенными временными и ресурсными затратами (выемка производится по месту нахождения сервера оператора связи, который может находиться на значительном удалении, преимущественно в г. Москве и г. Санкт-Петербурге). Более того, выемка становится фактически невозможной в случае необходимости получения сведений с таких интернет-сервисов, как «Facebook» или «Gmail», так как их серверы расположены за переделами Российской Федерации. В данном случае проведение выемки связано с непосредственным получением переписки у сотрудников оператора связи, однако, на наш взгляд, ознакомиться и процессуально зафиксировать интернет-переписку можно также посредством дистанционного осмотра электронного документа. Но в статье 29 УПК РФ не указано полномочие суда давать согласие на производство осмотра, пункт 7 ч. 2 ст. 29 УПК РФ говорит лишь о даче судом разрешения на производство выемки предметов и документов, содержащих иную охраняемую федеральным законом тайну. На наш взгляд, при разрешении данного вопроса можно использовать допустимую в уголовном процессе аналогию закона. При проведении дистанционного осмотра интернет-переписки, находящейся на сервере оператора связи, без получения согласия пользователя может также возникнуть вопрос о доступе к конкретному аккаунту (профилю), однако пароль может быть

получен в ходе исследования изъятых технических устройств, оперативно-розыскной деятельности, а также при обращении с запросом к оператору связи.

Таким образом, несмотря на существующие проблемы, следователи располагают процессуальными средствами получения и сведений, в том числе переписки, расположенных в сети Интернет и на электронных носителях. Предложения и алгоритмы, сформулированные в данной работе, будут способствовать существенной экономии сил и средств, затрачиваемых на расследование, одновременно обеспечивая соблюдение прав и законных интересов всех участников уголовного судопроизводства.

Глава 2. ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННО-ЦИФРОВОЙ ИНФОРМАЦИИ В ДОКАЗЫВАНИИ ПО УГОЛОВНЫМ ДЕЛАМ

§ 1. Собирание электронно-цифровой информации в доказывании по уголовным делам

Анализ ч. 2 ст. 74 УПК России и смежных с ней статей показывает, что названные виды документированной информации допускаются в качестве доказательств лишь как вещественные доказательства (ст. 81 УПК России)[1].

Статья 81 Уголовно-процессуального кодекса, определяющая вещественные доказательства была расширена частью 4, в силу которой предметы и документы (в том числе и носители электронной информации), изымаемые в процессе предварительного следствия, которые не были утверждены в качестве вещественных доказательств, в том числе носители электронной информации, должны быть возвращены участникам, у которых данные предметы и документы соответственно были изъяты, с учётом предписаний о соблюдении разумного срока. Часть 2 статьи 82 УПК РФ, была дополнена п. 5, согласно которому носители электронной информации должны храниться в опечатанном виде в условиях, которые исключают вероятность изучения хранящейся на таких носителях информации третьими лицами и гарантирующих их сбережение и сохранность информации. При этом такие носители впоследствии должны быть возвращены их законному владельцу.

Статья 82 УПК РФ была дополнена также ч. 2.1, в силу которой после производства неотложных следственных действий, в случаях, когда

[1] Вехов В.Б. Электронные документы как доказательства по уголовным делам // Компьютерная преступность и кибертерроризм: Сборник научных статей / Под ред. В.А. Голубева, Н.Н. Ахтырской. Запорожье: Центр исследования компьютерной преступности, 2012. Вып. 2. С. 122

невозможно вернуть носители электронной информации их законному владельцу, хранящиеся на таких носителях сведения копируются по ходатайству их законного владельца или обладателя содержащейся на этих носителях информации.

Были внесены также положения, регламентирующие порядок производства копирования:

Указанное действие может быть осуществлено при участии законного владельца изъятых носителей электронной информации и (или) его представителя и специалиста в присутствии понятых в подразделении органа предварительного расследования или в суде;

Копирование осуществляется на другие носители, предоставляемые законным владельцем изъятых носителей. Кроме того, при производстве копирования информации должны соблюдаться условия, устраняющие возможность ее утраты или изменения;

Копирование информации не допускается, в случае если это воспрепятствует расследованию преступления или же по заявлению специалиста, может повлечь за собой утрату или изменение информации.

Необходимо отметить, что законодательством не уточняются критерии, которые подтверждали бы возможность наступления при производстве копирования таких последствий, что влечет безосновательные отказы в осуществлении копирования.

Кроме того, в ч. 2.1 анализируемой нормы права установлено, что носители, хранящие скопированные сведения, вручаются законному владельцу изъятых носителей или обладателю содержащейся на ней информации. При этом об осуществлении копирования и о вручении таких носителей, хранящих скопированную информацию, законному владельцу изъятых носителей составляется протокол в соответствии с правилами статьи 166 УПК РФ (ч. 2.1. ст. 82 УПК РФ).

Федеральным законом от 28 июля 2012 г. № 143-ФЗ были внесены дополнения и в ч. 8 ст. 166 УПК РФ, согласно которой, в числе прочего, к

протоколу должны прилагаться носители электронной информации, приобретенной или скопированной с других носителей электронной информации в процессе осуществления следственного действия.

Изменения были внесены и в ст. 182 и 183 УПК РФ, которые регламентируют основания и порядок производства обыска и выемки. Эти изменения по своему содержанию идентичны, а соответственно они будут рассмотрены в единстве. Согласно данным изменениям, изъятие носителей электронной информации при производстве обыска (ч. 9.1 ст. 182 УПК РФ) и выемки (ч. 3.1 ст. 183 УПК РФ) должно происходить при непосредственном участии соответствующих специалистов. По ходатайству законного владельца изымаемых носителей электронной информации или обладателя содержащейся на них информации специалистом, участвующим в обыске (выемке), в присутствии понятых с изымаемых носителей осуществляется копирование информации на другие носители, предоставленные законным владельцем изымаемых носителей электронной информации или обладателем содержащейся на них информации. Копирование производится в порядке, описание которому было дано ранее.

Кроме того, нужно рассмотреть проблемы, возникающие в связи с толкованием и применением указанных норм.

Одной из проблем, является недостаточное обеспечение гарантий прав законных владельцев носителей при изъятии последних, в связи с тем, что копирование информации по ходатайству её законного владельца не всегда удовлетворяет потребностям продолжения нормальной деятельности организации, у которой изымаются такие носители.

Во-первых, ФЗ от 28 июля 2012 г. № 143-ФЗ не указывает на то, какая информация должна быть скопирована на носители, предоставленные законным владельцем изымаемых носителей электронной информации.

Во-вторых, указанный ФЗ определил, что копирование информации не допускается, если это может воспрепятствовать расследованию

преступления либо, по заявлению специалиста, повлечь за собой утрату или изменение информации. Считаю уместным мнение некоторых авторов о том, что отсутствуют чёткие критерии, подтверждающие возможность наступления указанных последствий при осуществлении копирования. Это обстоятельство в отдельных случаях способно приводить к безосновательному отказу в копировании. Как указывает Шигуров А.В., термин «воспрепятствование расследованию преступления» допускает произвольное толкование, что может привести к нарушениям прав законных владельцев носителей электронной информации[1]. Согласно сложившейся судебной практики, следователи отказывают в удовлетворении ходатайства о копировании цифровой информации в большинстве случаев.

Другой проблемой является то, что ФЗ № 143 было введено обязательное участие специалиста в изъятии носителей электронной информации в ходе обыска и выемки. Соответственно логичным является то, что если данное изъятие будет осуществлено без участия специалиста, то это будет являться нарушением требований УПК РФ, и сторона защиты сможет на основании п. 3 ч. 2 ст. 75 УПК РФ требовать признания доказательств, которые будут получены в результате такого изъятия, недопустимыми. Указанная норма законодательства о необходимом привлечении специалиста во всех случаях изъятия носителей электронной информации осуждается в различных статьях и работах.

Противники данной нормы оперируют несколькими основными аргументами.

1. На практике и впрямь затруднительно отыскать нужное количество специалистов для участия в анализируемых следственных действиях, принимая во внимание тот факт то, что в данный период

[1] Шигуров А. В. Проблемы регулирования порядка проведения следственных действий, сопровождающихся изъятием электронных носителей информации // Библиотека криминалиста : научный журнал. No 5 (10). М., 2013. С. 140.

электронно-технические средства нашли довольно обширное применение во всех отраслях деятельности человека и, соответственно, вопрос о необходимости изъятия носителей электронной информации встаёт довольно часто.

2. Сомнению подвергается в общем потребность в привлечении специалистов во всех случаях предполагаемого изъятия носителей электронной информации. Старичков М.В. в своей работе указывает, что: «не порождает сомнений, что изъятие носителей электронной информации, которые являются составными частями иных устройств или подключаемых к другому оборудованию, а равно копирование информации с носителей подлежащих изъятию в интересах третьих лиц должно производиться только специалистом. Однако едва ли существует техническая необходимость привлекать специалиста для изъятия, к примеру, различных телефонов, фотоаппаратов, плееров, в то время как в силу требований УПК РФ в ходе обыска или выемки это обязательно».

3. Обязательное привлечение специалиста для изъятия носителей электронной информации противоречит требованию процессуальной самостоятельности органов расследования[1].

Проблема обязательного привлечения специалиста в процессе изъятия указанных носителей в ходе рассматриваемых следственных действий затрагивают Кириллова Н. П. и Кушниренко С. П., которые указывают, что необходимость привлечения специалиста для изъятия носителей электронной информации возникает не во всех случаях. Авторы рассуждают о том, что помощь специалиста (а соответственно, и его необходимость участия в изъятии в процессе осуществления следственных действий) предопределяется тем, что существует вероятность внесения изменений в информацию на некоторых носителях электронной

[1] Козловский П. В., Седельников П. В. Участие специалиста в изъятии электронных носителей // Научный вестник Омской академии МВД России. 2014. No 1 (52). С. 18.

информации. Кириллова Н. П. и Кушниренко С. П. призывают различать носители электронной информации, в которые могут быть внесены изменения, и те, которые могут быть осмотрены и изъяты следователем самостоятельно и предлагают уточнить редакцию ст. 182- 183 УПК РФ, конкретизировав случаи обязательного участия специалиста[1].

Соответственно с анализируемой проблемой считаю необходимым произвести толкование комментируемой нормы, то есть установить её целевую направленность и определить роль, которую законодатель отводит специалисту при изъятии носителей электронной информации.

По этой тематике можно установить наличие представляющих интерес мнений в работах различных учёных. К примеру, Осипенко А. Л. и Гайдин А. И. в своей статье определяют, что положения, устанавливающие необходимость участия специалиста в ходе обыска и выемки, были закреплены в соответствующих статьях одновременно с положениями, которые предъявляют требование к специалисту по ходатайству законного владельца или обладателя содержащейся на носителях электронной информации осуществить копирование информации, содержащейся на таких носителях, на другие носители, предоставленные данными лицами[2]. Так авторы предполагают, что обязательное участие специалиста необходимо рассматривать в связке с обязанностью осуществить по ходатайству указанных лиц копирование информации с изымаемых носителей. И если толковать указанные нормы таким образом, то в случае, если в ходе изъятия носителей электронной информации при производстве соответствующих следственных действий ходатайство на копирование информации не заявлено, то и присутствие специалиста не требуется.

[1] Кириллова Н. П., Кушниренко С. П. Проблемы осуществления уголовного преследования по делам о преступлениях, совершаемых в сфере высоких информационных технологий // Правоведение. 2013. No 3. С. 83 – 84.

[2] Осипенко А. Л., Гайдин А. И. Правовое регулирование и тактические особенности изъятия электронных носителей информации // Вестник Воронежского института МВД России. 2014. No 1. С.158 – 159.

Однако, существует и иная точка зрения, согласно которой участие специалиста обеспечивает правильное проведение изъятия носителей, а также обеспечение их правильного хранения в дальнейшем, а копирование информации – это лишь сопутствующая задача.

Более подробная регламентация участия специалиста в ходе изъятия носителей электронной информации в процессе производства следственных действий позволила бы решить указанную проблему.

Согласно мнению некоторых исследователей изъятие носителей электронной информации без участия специалиста может быть осуществлено в случае, если такие носители изымаются целиком и в ходе их изъятия не осуществляется копирование содержащейся на них цифровой информации[1].

Сложившаяся судебная практика также стоит на позиции дифференциации случаев привлечения специалиста для участия в изъятии носителей электронной информации в ходе осуществления следственных действий.

В большинстве проанализированных судебных решений вопрос о необходимости привлечения специалиста для участия в изъятии носителей электронной информации решается исходя из того, осуществлялось ли копирование информации, содержащейся на изъятых предметах, на другие носители. Если копирование не производилось, то участие специалиста не требуется.

В тоже время существует и другая позиция, которая основывается на буквальном толковании положений УПК РФ, касающихся изъятия носителей электронной информации, исходя из которого суды выводят необходимость участия специалиста в любом случае изъятия носителей в ходе осуществления обыска или выемки безотносительно того,

[1] Старичков М. В. Вопросы использования носителей компьютерной информации в качестве доказательств // Известия ТулГУ: Экономические и юридические науки. 2014 г. Выпуск 2. С. 121. и др.

заявлялось ли законным владельцем изымаемых носителей ходатайство о копировании информации.

Следующей проблемой явилось то, что нормы, регулирующие порядок изъятия носителей электронной информации, были включены в статьи, посвящённые определенным следственным действиям (а именно: обыск, выемка) тем самым оставив без внимания другие следственные действия, в процессе осуществления которых также может потребоваться изъять носители (например, осмотр места происшествия).

Результаты анализа судебной практики показали, что суды не идут по пути аналогии уголовно-процессуального закона и решают вопрос о необходимости участия специалиста в таких следственных действиях отрицательно. В силу того, что прямого указания на необходимость привлечения специалиста к участию в иных следственных действиях нет, привлекать для участия данного следственного действия специалиста право, а не обязанность следователя.

Однако всё же встаёт вопрос о необходимости участия специалиста в таких следственных действиях, и в части обеспечения прав владельцев носителей электронной информации (например, в возможности осуществления копирования информации с изымаемых носителей).

Исходя из буквального толкования норм УПК РФ при изъятии носителей электронной информации в ходе следственных действий, за исключением обыска и выемки, участие специалиста не требуется. Однако, в таком случае будут не обеспечены права законных владельцев носителей.

О необходимости урегулирования порядка изъятия носителей электронной информации в ходе осмотра места происшествия и других следственных действий, где может потребоваться изъятие таких носителей по аналогии с регулированием, предусмотренным для обыска и выемки (в части возможности осуществления копирования информации на носители законного владельца изымаемых носителей, а также необходимости

участия в таких случаях специалиста) пишут Кириллова Н. П. и Кушниренко С. П., Шигуров А. В. и другие авторы.

Представляется, что необходимо внести положения о порядке изъятия носителей электронной информации также в другие статьи УПК РФ, посвящённые порядку проведения следственных действий, в ходе которых может потребоваться изъятие таких носителей.

§ 2. Особенности проверки и оценки электронно-цифровой информации как доказательство в уголовном судопроизводстве

Особенности проверки электронных документов.

Переходим к следующему элементу процесса доказывания, в качестве которого выделяют проверку доказательств. Рассматриваемому элементу процесса доказывания посвящена статья 87 УПК РФ.

Проверка доказательств может осуществляться путём:

1. сопоставления,
2. анализа,
3. определения первоисточника доказательства,
4. посредством производства следственных и иных процессуальных действий. В процессе таких действий собираются новые доказательства впоследствии соотносимые с проверяемыми доказательствами.

В ходе проверки анализируются свойства доказательств и первоисточник их возникновения, определяется достоверны ли сведения содержащиеся в доказательствах.

Проверка доказательств содержится во всех стадиях процесса и осуществляется в первую очередь следующими субъектами:

1. дознавателем,
2. следователем,

3. прокурором,

4. судом.

В проверке доказательств в порядке, определенном УПК РФ, имеют право участвовать также иные лица, не обладающие властными полномочиями, но относящиеся к стороне обвинения или защиты. В частности, они вправе принимать участие в проверке доказательств, полученных в ходе следственных действий, в которых указанные лица участвовали.

Трудности в проверке электронных доказательств п р е д определяются своеобразностью цифровой информации, которая рассматривалась ранее. На носителях электронной информации зачастую содержится большой объем файлов, а необходимая для использования в процессе доказывания информация может быть сокрыта или удалена, ввиду чего для обнаружения или восстановления такой информации требуется определенное программное обеспечение.

Очередной особенной чертой проверки электронных доказательств выступает необходимость обращения специалисту в ходе работы с указанными доказательствами. Верная постановка вопросов перед специалистом является важной частью процесса проверки электронных доказательств.

Проверка источника электронного доказательства подразумевает, что должны сохраняться подлинники носителей, которые помогут установить отсутствие внесения изменений при помощи технических средств.

Особенности оценки электронных документов.

Анализируя понятие и признаки доказательств в общем и в отношении отдельных их видов – документов – речь шла о таких свойствах доказательств как:

1. относимость,

2. допустимость,

3. достоверность,

4. достаточность как характеристика совокупности доказательств.

Рассмотрим соответственно особенности оценки данных свойств применительно к объектам цифровой информации, применяемым в качестве доказательств в уголовном процессе. Сущность свойств доказательств в некоторой степени раскрывалась ранее при исследовании понятия и признаков доказательств. Перейдем к данным признакам и проанализируем особенности оценки электронных доказательств в уголовном процессе.

Одно из свойств доказательств - их относимость. Подразумевает под собой данное свойство требование, направленное на содержание доказательства, это возможность доказательства своей сущностью служить средством установления обстоятельств, которые содержат в себе значение для соответствующего дела[1].

Как отмечают Зигура Н. А. и Кудрявцева А. В., характерная черта относимости электронной информации состоит в том, что определение возможно при воспроизведении такой информации при помощи технических средств и исследовании не только содержания компьютерной информации, но и её свойств (реквизитов). Применительно к относимости оценивается как содержание компьютерной информации, так и её свойства, такие как дата создания, изменения, открытия. При этом определение связи электронного доказательства с обстоятельствами, которые имеют значение для уголовного дела, зачастую вызывает необходимость привлечения специалиста или произведения экспертизы.

Допустимость воплощает требование, обращенное к форме доказательства. Анализируемое свойство указывает на необходимость следованию требованиям, предусмотренным законодательством.

[1] Орлов Ю. К. Указ. соч. С. 40; Уголовный процесс: учебник для бакалавриата юридических вузов / под ред. О.И. Андреевой, А.Д. Назарова, Н.Г. Стойко, А.Г. Тузова., 2014. С. 73.

В общем виде, требование допустимости формулируется из таких элементов как:

Законность источника;

Законность обстоятельств образования доказательства, приема его приобретения;

Соответствующее процессуальное оформление доказательства;

Надлежащий субъект, уполномоченный производить действия направленные на получение доказательства.

Свойства относимости и допустимости доказательств некоторые ученые-процессуалисты называют гарантией их достоверности.

В качестве критериев достоверности электронных доказательств Зигура Н. А. и Кудрявцева А. В. выделяют такие как:

1. Соответствующее доказательство должно быть образовано в результате корректной работы аппаратных и программных средств.

2. Следует разрешить вопрос о научности методов получения цифровой информации, что преимущественно актуально в случае получения такой информации с помощью специального программного обеспечения.

3. Следует решить вопрос о гарантии неизменности цифровой информации.

4. Достоверность цифровой информации должна удостоверяться посредством анализа её содержания и свойств и сопоставления с иными доказательствами.

При этом авторы обращают внимание на то, что оценивание электронных доказательств с точки зрения достоверности требует обращения «как к верности сведений, так и к правильности работы программы обработки».

Подозрения в достоверности электронных документов определяются, в частности, тем, что в такие документы не представляет особого труда внесение изменений, которые без помощи эксперта выявить сложно.

Александров А. С. и Кувычков С. И. в своей статье указывают на то, что одна из актуальных стратегий защиты заключается в расшатывании доверия к электронной информации, предоставляемой в качестве доказательств. Однако, тот или иной факт работы с файлом, в том числе различные изменения (модификации) цифровой информации возможно установить и проверить с помощью экспертизы.

Обратимся к крайнему из свойств доказательств, которое определяет их комплекс с точки зрения «убедительности для аргументирования того или иного вывода или процессуального решения».

Как отмечают Зигура Н. А. и Кудрявцева В. А., при установлении достаточности как свойства доказательств применительно к цифровой информации, нет необходимости в сборе всей хранящейся на исследуемом носителе информации.

Подводя итог, следует отметить, что проверка и оценка электронных доказательств, с одной стороны, подчиняется как общим закономерностям, присущим проверке и оценке доказательств по уголовным делам. А с другой – вследствие специфики объектов цифровой информации проверка и оценка электронных доказательств требует применения определенных знаний о сущности такого рода информации, а также в необходимых случаях использования соответствующего программного-аппаратного обеспечения.

§ 3.Совершенствование правового регулирования использования электронно-цифровой информации в процессе доказывания

Приемы получения определенных объектов электронной информации нужно рассматривать в плане необходимости обеспечения их сохранности в том виде, в котором они были обнаружены. Основная проблема при этом заключается в том, что изъятие электронных объектов

невозможно. Изъять можно только носитель электронной информации, с имеющимися на нем объектами такой информации, но вместо этого возможно произвести копирование. Впрочем, на практике нередко встречаются такие определения, как изъятие видеозаписи и подобные.

Отрицательная сторона копирования состоит в том, что такое действие не разрешает вопросов, связанных с обеспечением сохранности объектов в том виде, в котором они обнаружены. Так результатом производства данного действия будет изменение даты, времени последней операции с названным объектом.

Данную отрицательную сторону подчеркивает и Кукарникова Т.Э[1]. Согласно ее мнению такой негативный результат производства копирования, влечет утрату особенно важной в доказывании информации, о фактической дате и времени создания файла, который был подвергнут копированию. Это усложняет процесс признания копированной информации доказательствами.

В указанных случаях, когда копирование преграждает путь по установлению истины, то есть когда при копировании изменяются дата и время последней операции, вместо копирования прибегают к изъятию носителей электронной информации.

Итак, переходим к рассмотрению второго приема получения электронной информации, а именно изъятие носителей электронной информации и ее исследование.

Такой способ применяется в большем количестве случаев, в сравнении с копированием электронной информации.

Изъятие носителей электронной информации используется по обширному кругу дел. Причина тому состоит в том, что разные устройства

[1] Кукарникова, Т. Э. Электронный документ в уголовном процессе и криминалистике: дис. … канд. юрид. наук : 12.00.09 / Т. Э. Кукарникова. – Воронеж, 2003. – 204 с.

и гаджеты используются абсолютно во всех сферах жизнедеятельности людей.

Согласно анализу, приведенному ранее, в уголовно-процессуальном законодательстве содержатся нормы касающиеся порядка изъятия носителей электронной информации, возвращения, копирования имеющейся на них информации в процессе расследования.

При утверждении данных норм, первоочередной проблемой стало отсутствие определения понятию носитель электронной информации. В тоже время, согласно справке государственно-правового управления, данными носителями являются:

1) Компьютерные блоки;
2) Серверы;
3) Ноутбуки;
4) Карты памяти.

Но, представляется, что данный перечень не полон или же является более ориентирующим.

Обращаясь к иным актам, можно установить и иные определения.

К примеру, согласно ГОСТ 2. 051-2013 «ЕСКД. Электронные документы. Общие положения», исследуемый носитель понимается как: «материальный носитель, который используется для записывания, хранения, воспроизводства информации, которая обрабатывается при помощи средств вычислительной техники». Такое определение является довольно обширным, что ведет к образованию проблем в практике.

Так, за отсутствием четко установленного определения понятие носитель электронной информации, следует вопрос – необходимо ли соблюдать требования, содержащиеся в части 9.1 статьи 182 и в части 3.1 статьи 183 Уголовно-процессуального кодекса РФ. Наибольшую значимость данный вопрос приобретает при столкновении с ситуацией, связанной с привлечением специалиста для изъятия носителей.

Отсутствие четкого определения, а также проблема отнесения различных устройств к типу носителей электронной информации отразилось на судебной практике.

Проблему отнесения различных устройств к носителям, суды разрешают по разному. К примеру, вопрос об отнесении мобильных телефонов к носителям электронной информации, разрешается неоднозначно.

Одни суды устанавливают, что мобильные телефоны не являются носителями, а соответственно при их изъятии участие специалиста не обязательно. В тоже время, другие суды, исходят из того, что мобильные телефоны – носители электронной информации.

Кроме того, исходя из судебной практики, невозможно дать четкий ответ и на такой вопрос, как: является ли оптический диск носителем или нет.

Относительно установленной проблемы некоторыми учеными-процессуалистами высказывается мнение о необходимости комментирования данной темы Пленумом Верховного Суда РФ[1].

В тоже время, другая часть авторов утверждают, что необходим широкий подход к пониманию носителей электронной информации. Так, под данными носителями должны пониматься все материальные носители:

1) Внешние;

2) Являющиеся составной частью устройства.

Согласно статье Старичкова М.В., сотрудникам правоохранительных органов более часто приходится сталкиваться с персональными компьютерами[2]. Самыми встречающимися на практике, в этом плане, являются такие носители как:

---

[1] Першин А. Н. Электронный носитель информации как новый источник доказательств по уголовным делам // Уголовный процесс. 2015. No 5. С. 51 – 52.

[2] Старичков М. В. Вопросы использования носителей компьютерной информации в качестве доказательств // Известия Тул ГУ: Экономически е и юридические науки. 2014. Выпуск 2. С. 121.

1) Жесткие магнитные диски;

2) USB накопители;

3) Сменные карты памяти;

4) Оптические диски.

Встречаются и иные носители, которые в силу небольшого объема и низкой надежности почти не используются, но в практике еще упоминаются. К примеру, гибкие магнитные диски.

Учитывая судебную практику по делам, связанным с изъятием носителей, с мнением Старичкова М.В. можно согласиться.

Вернемся к приемам приобретения электронной информации, положительные и отрицательные стороны которых были рассмотрены ранее.

Важность изъятия носителей электронной информации обуславливается рядом причин. Во-первых, на таких носителях могут храниться сведения из удаленных или же скрытых файлов. При использовании специального программного обеспечения такие файлы можно восстановить. Во-вторых, учитывая мнение определенных авторов, осмотр названных носителей не всегда возможно осуществить на месте, это является следствием того, что для обнаружения следов преступления, которые существуют на таких носителях, необходимо продолжительный период времени[1].

Как уже было отмечено ранее, кроме информации, имеющей значение для расследования уголовного дела, на носителях электронной информации могут содержаться также и сведения, которые не относятся к данному делу, но необходимы для владельцев таких носителей.

Очень часто, сведения, которые заключены в изымаемых носителях, важны для нормальной деятельности субъектов, которые помимо всего

[1] Осипенко А. Л., Гайдин А. И. Правовое регулирование и тактические особенности изъятия электронных носителей информации // Вестник Воронежского института МВД России. 2014. No 1. С. 156

прочего могут быть никак не связаны с расследуемым преступлением. Так, необходимо учитывать интересы владельцев носителей.

Следует отметить, что законодательство не всегда поспевает за научно-техническим прогрессом и потребность в изменениях, которые вводятся в процессуальное законодательство, возникает намного раньше внесения таких изменений.

До внесения изменений в уголовно-процессуальное законодательство регламентация порядка изъятия носителей электронной информации не обладала какими-то особенностями. Так, применению подлежали общие нормы указанные в главе 2.1.

ЗАКЛЮЧЕНИЕ

Результатом проведенного анализа могут служить следующие выводы:

1. Продиктованное достижениями научно-технического прогресса внедрение в большинство областей деятельности человека информационных технологий неизбежно ведет к замене бумажного документооборота электронным. Соответственно возникает необходимость приспособления законодательства под современные условия информационного общества.

2. Существующее определение термина «документ», принимающее в расчет достижения научно-технического прогресса, допускает возможность относить к документам различные их виды, включая электронные документы, что определяет закономерности их использования в любой из сфер жизнедеятельности, в том числе и в правовой. Кроме того, правовое понятие «документа» конкретизируется в рамках понятийного аппарата определенной отрасли.

3. Функциональное назначение традиционных и электронных документов является общим. Однако электронные документы обладают некоторыми технологическими особенностями, которые должны учитываться при их использовании в правоотношениях.

Указанные особенности выражаются в следующем:

А) Электронный документ не имеет сильной привязки к материальному носителю (такой документ можно отделить от носителя);

Б) Несоблюдение определенных условий влечет возникновение сложностей при непосредственном восприятии человеком (к примеру, отсутствие необходимых технических и программных средств);

В) Усложненный процесс идентификации автора соответствующего электронного документа (такие документы не представляется возможным

собственноручно подписать или же идентифицировать без использования определенного программного обеспечения);

Г) Электронный документ в большей степени доступен для внесения разного рода изменений.

4. Особенности разных объектов цифровой информации определяют особенности использования в разных правоотношениях, что устанавливает большое значение определения места электронных документов в системе разнообразных объектов цифровой информации. Такие понятия как «электронный документ» и «цифровая информация» соотносятся как часть и целое. Мнение ряда авторов о том, что данные термины являются синонимами представляется неверным.

5. Для определения природы электронного документа как доказательства в уголовном процессе, считаю необходимым ориентироваться на требования, устанавливаемые уголовно-процессуальным законодательством.

Находящиеся в электронном документе сведения должны быть значимыми для соответствующего уголовного дела, а сам такой документ должен быть получен при соблюдении норм Уголовно-процессуального кодекса РФ, регламентирующих процесс собирания доказательств.

Так, в силу статьи 88 Уголовно-процессуального кодекса РФ электронные документы как доказательства в уголовном процессе должны соответствовать требованиям допустимости, относимости и достоверности, а в совокупности с иными доказательствами – достаточности для разрешения уголовного дела.

6. Согласно проанализированной судебной практики по уголовным делам, в процессе которых появлялась необходимость в сборе цифровой информации в ходе осуществления следственных действий, основным способом получения такой информации являлось изъятие носителей электронной информации.

7. Изменения, регулирующие порядок изъятия в ходе расследования уголовных дел носителей электронной информации, вносимые в Уголовно-процессуальный кодекс РФ не разрешают всех проблем, связанных с порядком изъятия и возвращения носителей электроннойсителей информации в ходе расследования уголовных дел.

Так, остается не конкретизированным определение понятие «носитель электронной информации», что влечет различные толкования в правоприменении. Необходимым является уточнение данного понятия.

Также установив нормы регламентирующие порядок изъятия носителей электронной информации в ходе обыска и выемки, законодателем было установлено обязательное участие специалиста во всех случаях изъятия указанных носителей, что вытекает из буквального толкования норм УПК РФ. Однако представляется, что участие специалиста во всех случаях изъятия носителей электронной информации является необоснованным. Это подтверждается сложившейся судебной практикой. Представляется необходимым дифференциация случаев участия специалиста в процессе таких следственных действий.

Кроме того, нормы, регламентирующие порядок изъятия носителей электронной информации включены в статьи, посвященные обыску и выемке, при этом остались без внимания иные следственные действия, в ходе осуществления которых может также потребоваться изъятие указанных носителей.

8. Проверка и оценка электронных доказательств требует применения специальных познаний о природе такого рода информации, вследствие специфики объектов цифровой информации.

Таким образом, проделанную работу, считаю выполненной успешно.

Цель работы - исследование проблем применения электронных документов в уголовно процессуальном доказывании, была достигнута. Проблемы были проанализированы, выделены соответствующие выводы и предложения.

Задачами согласно цели являлись:

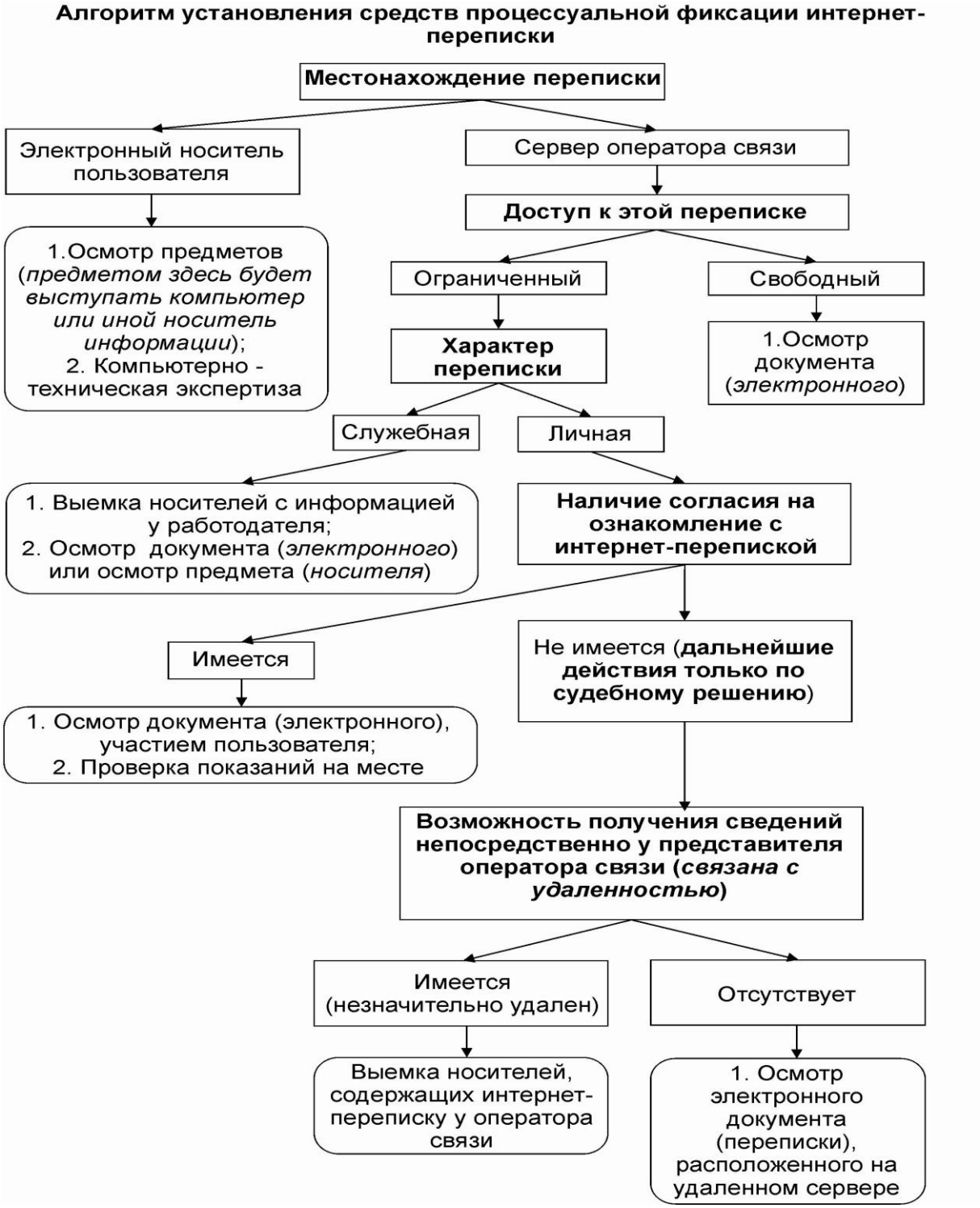
1. Рассмотреть понятие и значение электронной информации как источник доказательств в уголовном судопроизводстве, ее виды, формы и особенности.

2. Выделить особенности электронных документов в уголовно-процессуальном доказывании.

Задачи были выполнены. Сформировано личное убеждение относительно понятия и значения электронной информации в уголовном процессе, в тоже время были рассмотрены также мнения ученых на этот счет. Не остались без внимания подходы к определению места электронной информации в системе доказательств. А также основываясь на сложившейся практике и теоретических работах различных авторов были выделены особенности электронных документов.

ПРИЛОЖЕНИЕ №1

Рисунок 1. Алгоритм установления средств процессуальной фиксации интернет-переписки



БИБЛИОГРАФИЧЕСКИЙ СПИСОК

I. Нормативно правовые акты РФ и иные официальные документы.

1. Уголовно-процессуальный кодекс РФ [Электронный ресурс]: от 18.12.2001 № 174-ФЗ (ред. от 23.04.2018) – СПС «КонсультантПлюс».
2. Федеральный закон «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]: от 27.07.2006 № 149-ФЗ (ред. 23.04.2018) – СПС «КонсультантПлюс».
3. Федеральный закон от 06.04.2011 N 63-ФЗ (ред. от 23.06.2016) "Об электронной подписи" (с изм. и доп., вступ. в силу с 31.12.2017) // Собрание законодательства РФ, 11.04.2011, N 15, ст. 2036.
4. Федеральный закон от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи" (с изм. от 23 июня 2016 г.) // Собрание законодательства Российской Федерации. 2011. N 15. Ст. 2036.
5. Федеральный закон от 29 июня 2015 г. N 162-ФЗ "О стандартизации в Российской Федерации" (с изм. от 3 июля 2016 г.) // Собрание законодательства Российской Федерации. 2015. N 27. Ст. 3953.
6. Государственный стандарт РФ ГОСТ 2.051-2013. Единая система конструкторской документации (ЕСКД). Электронные документы. Общие положения. М.: Стандартинформ, 2014. 9 с
7. Федеральный закон от 28 июля 2012 г. N 143-ФЗ "О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации" // Собрание законодательства Российской Федерации. 2012. N 31. Ст. 4332.
8. ЕСКД. Электронные документы. Общие положения. [Электронный ресурс] ГОСТ 2.051-2013. Введен приказом Росстандарта от 22 ноября 2013 г. № 1628-ст. – М.: Стандартинформ. – СПС «КонсультантПлюс».

9. ГОСТ Р. 7.0.8-2013. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения: утв. Приказом Росстандарта от 17.10.2013 N 1185-ст // Доступ из справ.-правовой системы "КонсультантПлюс" (дата обращения: 15.07.2017).

10. Постановление ЕСПЧ от 12.01.2016 по делу «Барбулеску (Bărbulescu) против Румынии» (жалоба № 61496/08) URL:: http://hudoc.echr.coe.int/rus?i=001-159906 (дата обращения: 03.05.2018).

II. Монографии, учебники, учебные пособия

11. Андреев Б.В. Расследование преступлений в сфере компьютерной информации / Б.В. Андреев, П.Н. Пак, В.П. Хорст. М.: Юрлитинформ, 2011. С. 152

12. Батурин Ю. М. Проблемы компьютерного права. — М.: Юридическая литература, 1991. — 272 с.

13. Вехов В.Б. Электронные документы как доказательства по уголовным делам // Компьютерная преступность и кибертерроризм: Сборник научных статей / Под ред. В.А. Голубева, Н.Н. Ахтырской. Запорожье: Центр исследования компьютерной преступности, 2012. Вып. 2. С. 122

14. Давлетов А.А. Уголовное судопроизводство Российской Федерации. Курс лекций / А.А. Давлетов. Изд. 2-е. Екатеринбург, 2013. С. 124.

15. Егоров Н.Н. Вещественные доказательства: уголовно-процессуальные и криминалистические аспекты / Н.Н. Егоров. М.: Юрлитинформ, 2007. С. 304.

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

17. Краснова Л. Б. Электронные носители информации как вещественные доказательства // Известия Тульского государственного университета. Экономические и юридические науки. — 2013. — № 4. — С.254–260.

18. Невирко Д.Д. Права и свободы человека и гражданина: проблемы соотношения, взаимодействия и иерархии: монография. Красноярск, 2006 С. 22.

19. Орлов Ю. К. Указ. соч. С. 40; Уголовный процесс: учебник для бакалавриата юридических вузов / под ред. О.И. Андреевой, А.Д. Назарова, Н.Г. Стойко, А.Г. Тузова., 2014. С. 73.

20. Строгович М.С. Проблемы советского социалистического государства в современный период. Некоторые теоретические вопросы. М., 1967. С. 170.

21. Уголовный процесс : учебник для бакалавриата юридических вузов / О. И. Андреева [и др.] ; под ред. О. И. Андреевой, А. Д. Назарова, Н. Г. Стойко и А. Г. Тузова. – Ростов н/Д : Феникс, 2015. – 445, [1] с. – (Высшее образование).

III. Научные публикации и статьи в иных периодических изданиях

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

23. Карлов А.Л. Правовой режим использования в доказывании по уголовным делам электронной переписки, содержащейся в памяти

технических средств коммуникации // Актуальные проблемы профилактики наркомании и противодействия правонарушениям в сфере легального и незаконного оборота наркотиков: национальный и международный уровней материалы XVII международной научно-практической конференции (17-18 апреля 2014 года). Красноярск: СибЮИ ФСКН России, 2014. Ч 2. С.194.

24. Карлов А.Л. Пахорукова Ю.Е. Процессуальная фиксация интернет-переписки в качестве доказательств по уголовным делам о преступлениях в сфере незаконного оборота наркотиков // Вестник Сибирского юридического института МВД России. – 2016. – №4(25). С. 111 – 117.

25. Кириллова Н. П., Кушниренко С. П. Проблемы осуществления уголовного преследования по делам о преступлениях, совершаемых в сфере высоких информационных технологий // Правоведение. 2013. No 3. С. 83 – 84.

26. Козловский, П. В., Седельников, П. В. Участие специалиста в изъятии электронных носителей / П. В. Козловский, П. В. Седельников. // Научный вестник Омской академии МВД России. – 2014. – № 1 (52). – С. 19.

27. Осипенко А. Л., Гайдин А. И. Правовое регулирование и тактические особенности изъятия электронных носителей информации // Вестник Воронежского института МВД России. 2014. No 1. С. 156

28. Осипенко, А. Л., Гайдин, А. И. Правовое регулирование и тактические особенности изъятия электронных носителей информации / А. Л. Осипенко, А. И. Гайдин // Вестник Воронежского института МВД России. – 2014 г. – № 1. – С. 163.

29. Першин А. Н. Электронный носитель информации как новый источник доказательств по уголовным делам // Уголовный процесс. 2015. No 5. С. 51 – 52.

30. Першин, А.Н. Электронный носитель информации как новый источник доказательств по уголовным делам / А. Н. Першин. // Уголовный процесс. – 2015. – № 5. – С. 54.

31. Старичков М. В. Вопросы использования носителей компьютерной информации в качестве доказательств // Известия ТулГУ: Экономические и юридические науки. 2014 г. Выпуск 2. С. 121. и др.

32. Старичков, М. В. Вопросы использования носителей компьютерной информации в качестве доказательств / М. В. Старичков. // Известия ТулГУ: Экономические и юридические науки. – 2014 г. – Вып. 2. – С. – 125.

33. Сутягин К. И., Зуев С. В., Извеков Ю. А. Электронное копирование информации как самостоятельное следственное действие // Следователь. 2003. No 4. С. 14.

34. Ткачев, А. В. Использование электронных (компьютерных) документов в качестве документов-доказательств и письменных доказательств в процессуальных отношениях / А. В. Ткачев // Библиотека криминалиста: научный журнал. – 2013. – № 5 (10). – С. 134.

35. Шигуров А. В. Проблемы регулирования порядка проведения следственных действий, сопровождающихся изъятием электронных носителей информации // Библиотека криминалиста : научный журнал. No 5 (10). М., 2013. С. 140.

IV. Авторефераты и диссертации

36. Вехов, В. Б. Криминалистическая характеристика и совершенствование практики расследования и предупреждения преступлений, совершаемых с использованием средств компьютерной техники: дис. … канд. юрид. наук : 12.00.09 / В. Б. Вехов. – Волгоград, 1995. – 276 с.

37. Кукарникова, Т. Э. Электронный документ в уголовном процессе и криминалистике: дис. … канд. юрид. наук : 12.00.09 / Т. Э. Кукарникова. – Воронеж, 2003. – 204 с

V. Эмпирические материалы

38. Апелляционное постановление суда города Севастополя от 29.10.2015 г. по делу № 22К-713/2015 [Электронный ресурс]. URL: http://sudact.ru/

39. Апелляционное постановление Сургутского городского суда Ханты- Мансийского автономного округа от 15.05.2014 г. по делу №10-5/2014. [Электронный ресурс]. URL: https://rospravosudie.com/

40. Апелляционное постановление Ставропольского краевого суда от 20.03.2014 г. по делу 22К-1260/2014 [Электронный ресурс]. URL: https://rospravosudie.com/

41. Апелляционное постановление Краснодарского краевого суда от 18.02.2015 г. по делу №22К-805/2015 [Электронный ресурс]. URL: https://rospravosudie.com/

42. Апелляционное постановление Верховного суда Удмуртской Республики от 04.12.2014 г. по делу №22К-3299/2014 [Электронный ресурс]. URL: https://rospravosudie.com/

43. Апелляционное определение Судебной коллегии по уголовным делам Орловского областного суда от 22.05.2013 г. по делу №22К-953/2013 [Электронный ресурс]. URL: https://rospravosudie.com/

44. Апелляционное определение Судебной коллегии по уголовным делам Пермского краевого суда от 13.02.2014 г. по делу №22-896/2014 [Электронный ресурс]. URL: https://rospravosudie.com/

45. Апелляционное постановление Воронежского областного суда от 15.10.2013 г. по делу №22К-1686/2013 [Электронный ресурс]. URL: https://rospravosudie.com/

46. Апелляционное постановление Приморского краевого суда от 17.12.2013 г. по делу №22К-7097/2013 [Электронный ресурс].

47. URL: https://rospravosudie.com/

48. Апелляционное постановление Приморского краевого суда от 21.01.2014 г. по делу №22-130/2014 [Электронный ресурс]. URL: https://rospravosudie.com/