Федеральное государственное казенное образовательное учреждение высшего образования
«Сибирский юридический институт Министерства внутренних дел Российской Федерации»
Кафедра уголовного процесса (кафедра № 7)

Направление подготовки (специальность) Правоохранительная деятельность

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

по теме:

Процессуальные особенности изъятия и использования в доказывании компьютерной информации по уголовным делам о преступлениях в сфере незаконного оборота наркотиков

Выполнил:
Слушатель
группы П1201, младший
лейтенант полиции
Бережнов Никита Петрович

Руководитель:
старший преподаватель кафедры
уголовного процесса
майор полиции
Карлов Андрей Леонидович

Решение о допуске к защите:
допущен к защите

Начальник кафедры уголовного
процесса
полковник полиции
_____ Н.Г. Логинова
«15» 05 2017 г.

Консультант
старший преподаватель
кафедры информационно-правовых
дисциплин и специальной техники
Сибюрид
к.т.н, капитан полиции
_____ Голушин П.В.

Дата защиты:
«21» 06 2017 г.

Оценка: отлично

Председатель ГЭК
полковник полиции _____ С.В. Шульгин
(специальное звание) (подпись) (инициалы, фамилия)

Красноярск 2017

Федеральное государственное казенное образовательное учреждение высшего образования
«Сибирский юридический институт Министерства внутренних дел Российской Федерации»
Кафедра уголовного процесса (кафедра № 7)

Направление подготовки (специальность) Правоохранительная деятельность

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

по теме:

Процессуальные особенности изъятия и использования в доказывании компьютерной информации по уголовным делам о преступлениях в сфере незаконного оборота наркотиков

Выполнил:
Слушатель
группы П1201, младший
лейтенант полиции
Бережнов Никита Петрович

Решение о допуске к защите:
_____

Начальник кафедры уголовного процесса
полковник полиции
_____ Н.Г. Логинова
«___» _____ 20__ г.

Руководитель:
старший преподаватель кафедры уголовного процесса
майор полиции
Карлов Андрей Леонидович

Дата защиты:

«___» _____ 20__ г.

Оценка: _____

Председатель ГЭК

_____ _____ _____

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

Красноярск 2017

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В мире высоких технологий смартфоны, планшеты, персональные компьютеры, ноутбуки и другие гаджеты стали неотъемлемой частью жизни современного человека благодаря их многофункциональности, надежности, высокой производительности и относительной доступности для потенциального покупателя. С помощью данных средств связи человек способен осуществлять банковские операции, не выходя из дома, обмениваться информацией по шифрованным каналам связи, обеспечивая тем самым конфиденциальность и целостность передаваемой информации.

Гаджеты сделали нашу жизнь значительно комфортнее и облегчили её, поэтому информатизация стала явлением массовым, повсеместным. Так, по данным Российского филиала исследовательского концерна GfK (Gesellschaft fur Konsumforschung) Group, 26.01.2017 г., в их опубликованном отчете "Тенденции развития Интернет-аудитории в России", аудитория Интернет пользователей в России в возрасте от 16 лет и старше составляет порядка 84 млн. человек. Проникновение интернета среди молодых россиян (16-29 лет) достигло предельных значений еще в предыдущие годы и составляет 97%.[1]

Однако, массовость данного явления имеет и негативную сторону. С ростом уровня компьютеризации и развитием информационных технологий увеличилось количество преступлений, совершенных при помощи компьютерной техники, в частности, преступления в сфере незаконного оборота наркотиков. Данная проблема стала актуальной в последнее десятилетие в связи с массовыми случаями контрабандных поставок из соседних для России государств, в частности, Китая, синтетических аналогов наркотических средств. Наблюдается повышение преступного профессионализма и организованности наркодилеров, что

[1] Исследование GfK: Тенденции развития Интернет-аудитории в России [Электронный ресурс]. URL: http://www.gfk.com/ru/insaity/press-release/issledovanie-gfk-tendencii-razvitija-internet-auditorii-v-rossii.

выражается в использовании при сбыте наркотических средств современных технологий и программного обеспечения с целью гарантирования анонимности и приватности при использовании сети Интернет. Уже длительное время наблюдается тенденция осуществления сбыта наркотических средств бесконтактным способом при помощи так называемых «закладок» посредством использования тайников, с расчётом за приобретение наркотиков при помощи системы электронных кошельков: «QIWI», «Webmoney», «Paypal» и т.д. Как правило, связь между сбытчиком и покупателем осуществляется при помощи интернет-приложений и мессенджеров, таких как «WhatsApp», «Viber», «Skype», «Telegram» и других, обеспечивающих шифрование сети и невозможность перехвата третьими лицами конфиденциальной информации. Информация, хранящаяся на ноутбуках, компьютерах лиц и других электронных носителях информации, с которых велась переписка покупателя со сбытчиком, а также на различных серверах, имеет большое доказательственное значение. Однако, в связи с невозможностью перехвата данной информации традиционными средствами из-за различных видов шифрования, применяющихся в современных мессенджерах, возникает вопрос о её правомерном изъятии и использовании в доказывании по уголовным делам о преступлениях в сфере незаконного оборота наркотиков. Необходимо подчеркнуть тот факт, что согласно ст. 74 УПК РФ[1] (Уголовно-процессуальный кодекс (далее УПК РФ), законодатель не относит к отдельному виду доказательств электронные носители информации, считая их вещественными доказательствами. Но если с электронными носителями информации законодатель определился, то как быть с таким понятием как компьютерная информация? Является ли компьютерная информация доказательством по уголовному делу? А если является, то к какому виду

[1] "Уголовно-процессуальный кодекс Российской Федерации" от 18.12.2001 N 174-ФЗ (ред. от 17.04.2017, с изм. от 11.05.2017) // СПС КонсультантПлюс.

доказательств ее можно отнести? Или стоит выделить отдельный вид доказательства «компьютерная информация»?

В связи с этим возникает необходимость системного и комплексного теоретического исследования способов изъятия и использования в доказывании компьютерной информации по уголовным делам в сфере незаконного оборота наркотиков. Нужно определить, с помощью каких следственных действий возможно правомерно получить доступ к компьютерной информации, показать их отличия от сходных оперативно-розыскных мероприятий, определить, каков судебный порядок назначения и производства указанных следственных действий, конкретизировать процессуальный порядок изъятия и использования в доказывании компьютерной информации, а на основе проделанной работы попытаться вынести предложения по совершенствованию законодательства в данной области. Перечисленные выше обстоятельства послужили поводом выбора данной темы моего исследования, определили его объект, предмет, цель и задачи.

Объектом исследования являются правоотношения между участниками уголовного процесса, возникающие в процессе производства следственных и иных процессуальных действий, направленных на получение компьютерной информации с различных электронных носителей, смартфонов и т.п.

Предмет исследования – уголовно-процессуальные нормы, а также положения иных законов, регулирующих производство следственных действий, связанных с получением компьютерной информации.

Целью данного исследования является выявление и рассмотрение проблемных вопросов, связанных с процессуальными особенностями изъятия и использования в доказывании компьютерной информации по уголовным делам в сфере незаконного оборота наркотиков.

Для достижения указанной цели необходимо поставить и решить следующие задачи:

- проанализировать юридическую природу компьютерной информации, её доказательственное значение;

- определить виды и особенности проведения следственных действий, направленных на изъятие компьютерной информации, определить процессуальный порядок их производства, а также закрепления их результатов в качестве доказательств по уголовному делу;

- выявить проблемы в нормативной регламентации данных следственных действий, а также сложности при проведении указанных следственных действий;

- сформулировать научно обоснованные предложения по совершенствованию правового регулирования анализируемых следственных действий и оптимизации практики их производства.

Сказанное подчеркивает необходимость разработки единого процессуального порядка обнаружения, закрепления, изъятия, сохранения и исследования компьютерной информации, с целью дальнейшего её использования в качестве доказательства по уголовному делу.

Глава 1. ОБЩАЯ ХАРАКТЕРИСТИКА И ВИДЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ, ИСПОЛЬЗУЕМОЙ В ДОКАЗЫВАНИИ ПО УГОЛОВНЫМ ДЕЛАМ

§ 1. Основные подходы к понятию компьютерной информации в контексте уголовно-процессуального доказывания

Огромное значение имеет определение понятия компьютерной информации, поскольку оно используется как в теории, так и в практической деятельности. В УПК РФ уже закреплены сопутствующие понятия, такие как: получение информации о соединениях между абонентами и (или) абонентскими устройствами; электронные носители информации; фото, видео-кинопленка. Данные понятия имеют огромное значение в расследовании уголовных дел, что подтверждает необходимость определения такого понятия, как компьютерная информация тоже.

Для начала рассмотрим различные подходы к понятию компьютерной информации в контексте уголовно-процессуального доказывания.

В общем смысле, «компьютерная информация - сведения, представленные в электронно-цифровой форме на материальном носителе, создаваемые аппаратными и программными средствами фиксации, обработки и передачи информации, а также набор команд (программ), предназначенные для использования в электронно-вычислительной машине (ЭВМ), системе ЭВМ или управления ими».[1]

Наверное, первым понятие компьютерной (машинной) информации определил в 1990 году И.З. Карась, который понимал ее как информацию, которая циркулирует в вычислительной среде, зафиксированную на

[1] Зигура Н.А. Компьютерная информация как вид доказательств в уголовном процессе России: Автореф. дисс…канд.юр.наук. Челябинск. 2010. С. 21.

физическом носителе в форме, доступной для понимания ЭВМ, или передается телекоммуникационными каналами.[1] В.Б. Вехов в 1995 году усовершенствовал это определение, предложив его в такой редакции: «Под машинной информацией понимается информация, циркулирующая в вычислительной среде, зафиксированная на физическом носителе в форме, доступной для восприятия ЭВМ, передается по телекоммуникационным каналам: сформированная в вычислительной среде информация, пересылаемая благодаря электромагнитным сигналам с одной ЭВМ в другую, из ЭВМ на периферийное устройство или управляющий датчик оборудования.[2]

В середине 90-х годов прошлого века в странах СНГ компьютерная информация (на машинном носителе, в компьютере) была выделена как объект уголовно-правовой охраны, что послужило началом научной дискуссии по этому поводу. В частности, П.Н. Панченко отождествлял компьютерную информацию с общим понятием информации.[3]

С.В. Бородин, Ю.И. Ляпунов и С.В. Максимов предлагали под компьютерной информацией понимать информацию на машинном носителе, в ЭВМ, их системе или сети.[4]

С криминалистической точки зрения — это понятие исследовал В.В. Крылов и пришел к выводу, что как предмет преступного посягательства компьютерная информация – это сведения, знания или

---

[1]Карась И.З. Экономический и правовой режим информационных ресурсов // Право и информатика / под ред. Е.А. Суханова. – М.: Изд-во МГУ, 1990. – С. 40.

[2]Вехов В.Б. Криминалистическая характеристика и совершенствование практики расследования и предупреждения преступлений, совершаемых с использованием средств компьютерной техники: дис. … канд. юрид. наук. Волгоград: ВСШ МВД России, 1995. С. 32.

[3] Хахановский В. В международном научно-практическом правовом журнале: «Закон и жизнь».. Компьютерная информация как особенные фактические данные в уголовном процессе. №13. 2013. С. 50.

[4]Ляпунов Ю.И., Максимов С. В. Ответственность за компьютерные преступления // Законность. 1997. № 1. С. 9.

набор команд (программ), предназначенных для использования в ЭВМ или управления ею.[1]

В.А. Мещеряков понимает компьютерную информацию как информацию, представленную в специальном (машинном) виде, предназначенном для ее автоматизированной обработки, хранения и передачи, которая находится на материальном носителе и имеет собственника, установившего порядок ее создания (генерации), обработки, передачи и уничтожения.[2]

Е.Р. Россинская считает, что: «компьютерная информация в процессе доказывания – это фактические данные, обработанные компьютерной системой и (или) те, которые передаются по телекоммуникационным каналам, доступные для восприятия, и на основе которых в определенном законом порядке устанавливаются обстоятельства, имеющие значение для правильного разрешения уголовного дела».[3]

По мнению Н.А. Зигуры, «компьютерная информация – это сведения, представленные в электронно-цифровой форме на материальном носителе, создаваемые аппаратными и программными средствами фиксации, обработки и передачи информации, а также набор команд (программ), предназначенные для использования в электронно-вычислительной машине (ЭВМ), системе ЭВМ или управления ими. Причем автор подчеркивает, что компьютерная информация как вид доказательств является комплексным образованием, поэтому она будет иметь значение доказательства при наличии нескольких элементов, а именно: носителя компьютерной информации; процессуального акта – протокола осмотра компьютерной информации, в котором описано происхождение носителя такой информации, условия и обстоятельства его

---

[1] Крылов В.В. Информационные компьютерные преступления. М.: ИНФРА-М НОРМА, 1997. С. 17.

[2] Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации : автореф. дис.…д-ра. юрид. наук. Воронеж, 2001. С. 15.

[3] Россинская Е.Р., Усов А.И. Судебная компьютерно-техническая экспертиза. М.: Право и закон, 2001. С. 14-15.

обнаружения, изъятия, упаковки, а также краткое описание содержания находящейся на нем информации (может быть представлена распечатка) с указанием реквизитов такой информации.[1]

Д.В. Вершок считал, что компьютерная информация является разновидностью радиоэлектронной информации. [2]

В.Б. Вехов, проанализировав приведенные и другие позиции ученых-юристов, сделал, на наш взгляд, весьма важные и правильные выводы относительно рассматриваемого понятия, а именно:

- «компьютерная информация – это сведения (сообщения, данные), находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе или передаваемые каналами связи при помощи электромагнитных сигналов;

- компьютерная информация является одной из объективных форм существования информации – электронно-цифровой формой, она всегда будет опосредована через материальный носитель, без которого физически не может существовать;

- как и некоторые другие материальные вещи, компьютерная информация может быть предметом коллективного пользования, поскольку доступ к ней могут одновременно иметь несколько человек (например, при работе в сети Интернет);

- компьютерная информация достаточно просто и быстро превращается из одной объективной формы в другую, копируется на определенные виды материальных носителей и пересылается на любые расстояния, ограниченные только радиусом действия современных средств связи;

- осуществление процессов сбора, исследования и использования криминалистически значимой компьютерной информации возможно

[1]Зигура Н. А. Указ. соч. С. 21.

[2] Вершок, Д.В. Правовой режим радиоэлектронной информации: автореф. дис. … канд. юрид. наук. Минск, 2003. С.24 [Электронный ресурс]. 2012. Режим доступа: http://www.law. edu.ru/book/ book.asp?bookID=124340.

только с помощью специальных орудий – компьютерных программ, баз данных, машинных и других материальных носителей, электронно-цифровых устройств, компьютерных систем и сетей».[1]

Анализируя все вышеуказанные понятия, можно сделать вывод о том, что с истечением времени термин компьютерная информация видоизменяется, в него добавляются новые признаки, которые позволяют все больше рассматривать данное понятие в рассматриваемом аспекте, как доказательство. В УПК РФ и иных нормативно-правовых актах пока нет конкретного закрепления компьютерной информации, как доказательства и указаний по ее использованию в доказывании. Наиболее часто на практике компьютерную информацию фактически отождествляют с её носителем (носитель, на котором содержится информация приобщается к делу в качестве вещественного доказательства) либо к иным документам (например, скриншот переписки приобщается в виде фотографии к материалам уголовного дела).

Необходимо отметить, что нормативно-правовое определение информации можно найти в федеральном законе «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 г. где указывается, что информация - сведения (сообщения, данные) независимо от формы их представления.[2]

Обобщая все вышесказанное, мы попробовали сконструировать свое понятие компьютерной информации. Итак, компьютерная информация-это сведения (сообщения; данные; конкретный файл, а не его носитель), представленные в специальном (машинном) виде, создаваемые аппаратными и программными средствами фиксации, обработки и передачи информации, которые передаются по телекоммуникационным

---

[1] Вехов В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки : монография / В. Б. Вехов. - Волгоград : ВА МВД России, 2008. С. 21.

[2] ФЗ РФ «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 г.// СПС КонсультантПлюс.

каналам, доступные для восприятия, и на основе которых в определенном законом порядке устанавливаются обстоятельства, имеющие значение для правильного разрешения уголовного дела.

§ 2. Классификация компьютерной информации, используемой в доказывании по делам о наркопреступлениях, и её доказательственное значение

Для начала хотелось бы рассмотреть компьютерную информацию как объект исследования в уголовном процессе. Мы считаем, что ее можно условно разделить на два вида: процессуальную и не процессуальную. Процессуальная информация, по нашему мнению, является доказательственной, то есть имеющая формальное доказательственное значение, и получаемая в соответствии с нормами УПК РФ, а не процессуальной, скорее, выступает оперативно-розыскная, поскольку она может быть получена не предусмотренным УПК РФ порядке, например посредством проведения оперативно-розыскных мероприятий. Такое разделение компьютерной информации, используемой в уголовном процессе, достаточно условно, однако отличительной особенностью оперативно-розыскной информации является то, что она может быть использована в доказывании по уголовным делам только при ее представлении в объеме и форме, позволяющих оценить содержащиеся в них фактические данные с точки зрения их относимости к расследуемому уголовному делу, допустимости и достоверности в соответствии с требованиями, установленными нормами УПК РФ.

Существует множество мнений по поводу классификаций компьютерной информации, используемой в доказывании. Наиболее интересные из них предлагает Н.А. Зигура:

1) по связи с событием преступления:

- компьютерная информация, которая служила орудием совершения преступления;

- компьютерная информация, которая сохранила на себе следы преступления;

- компьютерная информация, на которую были направлены преступные действия;

- иная компьютерная информация, которая устанавливает наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для уголовного дела.

2) по происхождению:

компьютерная информация, созданная пользователем;

компьютерная информация, созданная аппаратными и программными средствами. Эту информацию можно подразделить на регистрируемые данные (лог-файлы) и научные данные.

3) по типу данных:

- текстовая информация;
- базы данных;
- графическая информация;
- анимация;
- мультимедийная;
- программы для ЭВМ.

4) по типу носителя:

компьютерная информация на энергозависимом носителе;

компьютерная информация на энергонезависимом носителе.

5) по степени свободы использования на основании закона:

общедоступная(открытая);

ограниченного доступа (охраняемая законом - государственная тайна, коммерческая тайна, служебная тайна, иная тайна).

6) по степени защищенности программными средствами:

–открытая (незащищенная);

–скрытая (защищенная).[1]

В большинстве своем приведенные выше классификации имеют лишь криминалистическое значение, и для целей нашей работы нет необходимости подробно их все рассматривать. Остановимся лишь на тех классификациях, которые могут быть использованы для разрешения уголовно-процессуальных вопросов.

Как уже говорилось ранее, компьютерную информацию, чаще всего вместе с её носителем относят к вещественным доказательствам либо иным документам, поэтому хотелось бы провести разграничение между данными видами доказательств. Предлагаем последовательно проанализировать к какому из указанных выше видов доказательств необходимо относить полученную в рамках уголовного судопроизводства компьютерную информацию.

В ч.2 ст. 84 УПК РФ законодатель указал, что входит в понятие «иной документ»: «материалы фото- и киносъемки, аудио- и видеозаписи и иные носители информации». Действительно, компьютерная информация может быть представлена в качестве фотоизображения (например скриншот страницы сети Интернет), или аудиозаписи (с обязательным приложением к ней стенограммы). Однако, как быть с компьютерной информацией, которая представлена в виде фрагмента программного кода вирусной программы, используемой злоумышленниками в корыстных целях? Или каким образом отнести к иным документам веб-сайт по продаже наркотических средств, если он был обнаружен в компьютере у администратора данного сайта? А как зафиксировать компьютерную информацию, которая находится на оперативном запоминающем устройстве (ОЗУ), если принять во внимание тот факт, что при отключении устройства от питания, все данные, находящиеся на момент выключения, стираются? Поскольку к иным документам данные формы

[1] Зигура Н. А. Указ. соч. С. 23

компьютерной информации отнести затруднительно, стоит обратиться к ст. 81 УПК РФ – вещественные доказательства.

В ч.1 ст. 81 УПК РФ указан примерный перечень того, что можно признать в качестве вещественного доказательства по уголовному делу. Анализируя данную статью и пытаясь сравнивать компьютерную информацию и вещественные доказательства, мы находим некоторое сходство между ними. Так, «согласно ст. 81 УПК РФ, вещественными доказательствами признаются любые предметы, обладающие признаками, в ней указанными. Как мы видим, основным признаком вещественных доказательств является их объективная связь с исследуемым событием, в силу которой они и могут служить средствами установления фактических обстоятельств дел. Этот признак в полной мере можно отнести и к компьютерной информации, которая может служить и орудием преступления, например, программа, содержащая вирус, и сохранять на себе следы преступления, например, попытки несанкционированного доступа, зафиксированные в журналах регистрации различных программ, и являться объектом, на который были направлены преступные действия, например, перевод денежных средств с одного счета на другой».[1]

Попытаемся все-таки разграничить сравниваемые нами понятия. В большинстве случаев в практической деятельности компьютерную информацию вместе с носителем, на котором она находится, относят к вещественным доказательствам. Мы считаем это ошибочным мнением поскольку доказательственное значение компьютерной информации, хранящейся на носителе, состоит в самой информации, а не в физических свойствах, составе или внешнем виде ее носителя – что является важным для вещественных доказательств. Надо понимать, что «вещественное доказательство – это предмет, а компьютерная информация – это

[1]Зигура Н.А. Разграничение компьютерной информации и вещественных доказательств // Вестник Калининградского юридического института МВД России №1. С. 283.

содержание сведений».[1] Носитель, на котором находится компьютерная информация, не имеет никакого доказательственного значения, поскольку он не обладает такими качествами как «незаменимость и уникальность»[2] из-за того, что данный физический носитель может быть заменен на идентичный ему носитель.

«Ю.К. Орлов указывает на следующие признаки разграничения документов и вещественных доказательств: 1) в документе информация выражена в какой-то условной, знаковой системе, закодирована. В вещественном доказательстве информация содержится в своем естественном, некодированном виде; 2) доказательственное значение документа определяется его содержанием, доказательственное значение вещественного доказательства - его физическими признаками (или местонахождением).»[3] По нашему мнению, данные признаки вполне подходят и к компьютерной информации.

В связи с приведенными выше аргументами и отсутствием в законе более подходящего вида доказательств, полагаем необходимым внести изменения в ч.2 ст. 74 УПК РФ и предусмотреть специальный вид доказательств – компьютерная информация. Данной точки зрения придерживается в своей научной статье «Природа компьютерной информации как доказательства» Зигура Н.А., предлагая выделить компьютерную информацию в самостоятельный источник доказательств: «компьютерная информация – это сведения, представленные в электронно-цифровой форме на материальном носителе, создаваемые посредством использования аппаратных и программных средств фиксации, обработки и передачи информации, а также набор команд (программ), предназначенных для использования в ЭВМ или управления ею, на основе

---

[1] Зигура Н.А. Указ. соч. С. 284.

[2] Строгович М. С. Материальная истина и судебные доказательства в советском уголовном процессе. М., 1955. С. 334; он же Курс советского уголовного процесса. М., 1966. Т. 1. С. 109-118. Чельцов М.А. Советский уголовный процесс. М., 1962. С. 207.

[3] Орлов Ю.К. Основы теории доказывания в уголовном процессе. М., 2000. С. 112,122.

которых суд, следователь, дознаватель в порядке, определенном уголовно-процессуальным законодательством, устанавливает наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для уголовного дела, полученные с соблюдением процессуального порядка их собирания и приобщения к уголовному делу специальным постановлением».[1]

Также есть пример решения данного вопроса на законодательном уровне зарубежных стран. Так, в УПК Социалистической Республики Вьетнам в редакции 2015 г., принятой Парламентом СРВ, были внесены изменения, которыми «электронные данные» признаны источником доказательств. «С вещественными доказательствами электронные средства доказывания объединяет то, что электронные документы сами по себе недоступны человеческому восприятию, а служат лишь средством установления обстоятельств, имеющих значение для дела. Вместе с тем информация, содержащаяся в памяти ЭВМ, тиражируема, т.е. обладает свойством письменного доказательства».[2]

Следующие критерии разграничения компьютерной информации от вещественных доказательств и иных документов предложила Н.А. Зигура:

«Компьютерная информация в отличие от иных документов:

1) по механизму формирования:

- источником выступает автор документа (иной документ);
- создается с помощью алгоритма, заданного программой (компьютерная информация);

2) по среде существования:

- предназначен для обработки мыслящими субъектами, людьми (иной документ);

[1] Зигура Н.А. Природа компьютерной информации как доказательства. // Вестник Южно-Уральского государственного университета. 2009. С. 52.

[2] Ж.В. Хацук. Электронные доказательства в судебном процессе. // Вестник Гродненского государственного университета им. Янки Купалы. 2014. С. 38.

- обрабатывается техническими объектами, аппаратными и программными средствами (компьютерная информация);

3) по привязке к носителю:

- привязка к материальному носителю (иной документ);
- материальный носитель может использоваться многократно для записи различной информации (компьютерная информация).

4) по признаку воспроизведения:

- непосредственно воспринимается органами чувств человека (иной документ);
- непосредственно воспринимается только объектом электронной цифровой среды, человек воспринимает опосредованно с помощью технических и программных средств (компьютерная информация).

Компьютерная информация в отличии от вещественного доказательства.

1) по механизму образования:

- механическое отражение фактов (вещественное доказательство);
- определяется алгоритмом, который задан разработчиком и реализуется в конкретной программе, которая является средством отражения фактов (компьютерная информация).

2) по признаку восприятия:

- информация содержится в своем естественном, не кодированном виде, и преобразование ее для восприятия, не нужно (вещественное доказательство);
- опосредована через машинный носитель информации, вне которого она не может существовать, и восприятие её возможно только посредством технического средства (компьютерная информация).

3) по признаку среды существования:

- является частью аналоговой среды (вещественное доказательство);

– среда программных и технических средств, то есть электронная среда (компьютерная информация)».[1]

Как нам уже известно, компьютерная информация, используемая в доказывании по делам о наркопреступлениях содержит очень мало традиционных следов и под рассмотренные классификации подходит не всегда. И поскольку преступления данной категории совершаются чаще всего путем использования сети Интернет, именно компьютерная информация имеет основное доказательственное значение. Мы составили перечень возможных доказательств, в которых содержится компьютерная информация при расследовании наркопреступлений.

Во-первых, это переписка «приобретателя» наркотического средства и его «сбытчика», чаще всего, с указанием конкретного времени и даты переписки.

Во-вторых, IP-адреса предполагаемых преступников, с помощью которых возможно определить местоположение и пользователя компьютера, с которого совершалось преступление.

В-третьих, MAC-адреса, которые позволяют идентифицировать устройство, при помощи которого осуществлялся выход в сеть.

В-четвертых, фото и видео элементы, которые зачастую прилагаются к переписке в такого рода преступлениях, с указанием места закладки наркотического средства и существуют только в электронном варианте на конкретном сайте и в конкретной переписке.

В-пятых, история браузера (просмотров) на конкретном электронном устройстве, принадлежащая владельцу, благодаря которой возможно определить намерения человека при подготовке к определенному преступлению. Например, при приготовлении к преступлению, предусмотренному ст. 228.1 УК РФ (незаконное производство наркотических средств, психотропных веществ или их аналогов), лицо закупает специальное оборудование для приготовления наркотического

[1] Н.А. Зигура. Указ. соч. С. 24.

средства, осваивает способ приготовления путем поиска информации в сети Интернет.

В-шестых, информацию и переписку в социальных сетях в сети Интернет также можно использовать в качестве характеризующего материала на подозреваемого (обвиняемого), поскольку в современном мире информации в социальных сетях порой бывает больше, чем правоохранительным органам могут предоставить с мест учебы, работы.

Таким образом, предлагаем разделить указанные доказательства на группы:

Первая группа: непосредственные доказательства преступления – это те доказательства, которые на прямую указывают на факт преступления или на его отдельные этапы. К данной группе можно отнести переписку «приобретателя» наркотического средства и его «продавца», фото и видео элементы, которые зачастую прилагаются к переписке.

Вторая группа: опосредованные – это те доказательства, которые на прямую не указывают на совершение лицом наркопреступления, но дают повод оперативным сотрудникам провести оперативную проверку в отношении лица по подозрению в совершении преступления традиционными способами. К этой группе можно отнести, IP-адреса предполагаемых преступников, история браузера (просмотров и поисковых запросов) на конкретном электронном устройстве, информацию и переписки в социальных сетях в сети Интернет.

Также можно использовать разработанную в теории доказывания классификацию данных доказательств по источнику формирования, или иначе говоря, по характеру связи между устанавливаемым обстоятельством и источником сведений. Соответственно по данному критерию доказательства, содержащие компьютерную информацию, делятся на:

- первоначальные (отображают устанавливаемый факт без промежуточных носителей сведений о нем, например, веб-страница в Интернете, зафиксированная в ходе осмотра или обыска);
- производные доказательства (обязательно наличие промежуточного носителя, например, файл, находящийся на изъятом по делу электронном носителе).

Преимущество первоначальных доказательств в том, что им в меньшей мере присущи искажения, утрата сведений, которые возможны при формировании производных доказательств, к тому же они более объективны. Однако производные доказательства незаменимы, когда первоначальные невозможно получить по различным объективным причинам, например в случаях, когда информация поступает непосредственно в ходе следственного действия. Также они используются для проверки первоначальных.

Кроме того, мы решили соотнести компьютерную информацию с одной из наиболее популярных классификаций доказательств в целом. А именно, личные и вещественные. К личным предлагаем отнести страницы в социальных сетях (как с предоставлением пароля, так и без него), электронную почту, искусственную память (облако) электронного носителя и т.д. А к вещественным, файлы, которые уже ранее скачивались с компьютера, гаджета на флеш-карту или иной электронный носитель информации.

Таким образом, необходимо подчеркнуть важность использования различных классификаций компьютерной информации, поскольку всесторонний подход к пониманию данного понятия необходим для правильного использования в качестве доказательства по уголовному делу компьютерной информации.

2. ИСПОЛЬЗОВАНИЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В ДОКАЗЫВАНИИ ПО УГОЛОВНЫМ ДЕЛАМ О ПРЕСТУПЛЕНИЯХ В СФЕРЕ НЕЗАКОННОГО ОБОРОТА НАРКОТИКОВ

§ 1. Правовой режим доступа к отдельным видам компьютерной информации

Законодатель в Федеральном законе "Об информации, информационных технологиях и о защите информации" в статье 3 указал следующие принципы правового регулирования отношений в сфере информации: «свобода поиска, получения, передачи, производства и распространения информации любым законным способом», и «открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами»[1]. Пользователь (им может быть любой гражданин, орган государственной власти, орган местного самоуправления) вправе «осуществлять поиск и получение любой информации в любых формах и из любых источников»[2], при этом не обосновывая необходимость запрашиваемой информации у ее владельца. Разумеется, это касается общедоступной информации. Однако, нас интересует другая информация, для которой законом предусмотрен более сложный порядок получения и обработки, так как она связана с правами отдельных категорий граждан или интересами государства. Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и

[1] Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 19.12.2016) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.01.2017) //СПС КонсультантПлюс.

[2] Там же.

безопасности государства. Ограничение доступа к такой информации осуществляется посредством введения специального режима доступа к ней – правового режима доступа. «Правовой режим информации - объектный режим, вводимый законодательным актом и позволяющий обеспечить комплексность воздействия в информационной сфере посредством совокупности регулятивных, охранительных, процессуально-процедурных средств, характеризующих особое сочетание дозволений, запретов и обязательств, а также гарантий по его соблюдению».[1]

К наиболее часто встречающимся видам тайн, связанным с использованием компьютерной информации по уголовным делам относят:

1) личную тайну;
2) государственную тайну;
3) служебную тайну;
4) коммерческую тайну;
5) банковскую тайну.

«Основной целью специальных правовых режимов информации является обеспечение информационной безопасности различных субъектов: государственная тайна – интересы безопасности государства; коммерческая тайна – интересы безопасности субъектов экономической деятельности; информация ограниченного доступа личного характера – права, свободы и интересы обеспечения безопасности физических лиц. Предметом охраны в правовом режиме тайны выступают общественно значимые интересы вышеуказанных субъектов. Объект режима – сведения ограниченного доступа».[2]

Соответственно для определенных видов информации в силу их особого значения устанавливаются специфические правовые режимы. Это

[1]Интернет-ресурс: // URL: http://jurkom74.ru/materialy-dlia-ucheby/poniatie-pravovogo-rezhima-informatcii / (дата обращения 13.05.2017)

[2]Г. Г. Камалова. Правовой режим информации ограниченного доступа: вопросы формирования понятийного аппарата // Вестник Удмуртского университета. Серия «Экономика и право». 2016. №4 С. 123.

относится к информации, не предназначенной для широкого распространения, в связи с этим эта информация подлежит охране от несанкционированного доступа. Использование особых правовых режимов является одной из мер правовой защиты информации.

Например, компьютерная информация в виде переписки, личных фотографий и видеозаписей посягает на личную тайну, поскольку фактически нарушает тайны неприкосновенности частной жизни, которые предусмотрены Конституцией РФ. Компьютерная информация в виде документов, изъятых со служебных компьютеров работников государственной службы может содержать государственную либо иную служебную тайну, а документы, изъятые со служебных компьютеров юридических лиц и работников банковской сферы, вероятнее всего, будет посягать на коммерческую либо банковскую тайну.

Для характеристики информации с особым правовым режимом доступа используется термин конфиденциальная информация.[1]

Конфиденциальная информация – документированная информация, доступ к которой ограничивается законодательством. Под конфиденциальностью в ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации» понимается обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя. Предлагаем более подробно рассмотреть режимы тайн, выделенные ранее.

Режим личной тайны.

Каждый гражданин в процессе своей жизни вступает во взаимоотношения с различными предприятиями и гражданами, при этом у последних происходят накопления данных о лице, причем иногда

[1] Право: учеб. пособие / под общ. ред. С.Ю. Наумова, Т.В. Касаевой, А.А. Шаповалова. Саратов: ССЭИ РЭУ им. Г.В. Плеханова, 2016. С. 22.

специфических (о заболеваниях, судимостях, доходах). По различным причинам эти сведения лицо разглашать не желает.

В целях защиты этих сведений вводится режим персональных данных, необходимость защиты которых признается мировым сообществом.

Международное право обязывает государство принимать надлежащие меры для охраны персональных данных, накопленных в автоматизированных баз данных от случайного или несанкционированного доступа, изменения или распространения. При этом сведения о национальности, политических взглядах или религиозных убеждениях, здоровья, сексуальной жизни, судимости могут подвергаться автоматической обработке только в тех случаях, когда национальное право предусматривает надлежащие гарантии.

Закон «Об информации, информатизации и защите информации» устанавливает, что персональные данные относятся к категории конфиденциальной информации.

Согласно ч.1 ст.23 Конституции РФ, «сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются»[1], но о судебном решении законодатель здесь не указывает, следовательно, можно сделать вывод, что оно вообще обязательно далеко не во всех случаях, а только напрямую указанных в законе. Например, в ч.3 ст.55 Конституции РФ законодатель напрямую говорит нам о возможности ограничения личной тайны, тайны частной жизни, семейной тайны и т.д. в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

[1]"Конституция Российской Федерации"(принята всенародным голосованием 12.12.1993) //СПС КонсультантПлюс.

Далее более подробно хотелось бы остановиться на тайне связи, поскольку это тоже очень немаловажный аспект жизни современного человека, и поэтому правоохранительные органы при расследовании уголовных дел зачастую сталкиваются с ней.

Статья 63 Федерального закона «О связи» конкретизирует, что же входит в понятие тайна связи: «тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи».[1]

Первая проблема, с которой сталкивается правоприменитель при ограничении тайны связи – это вопрос отнесения получаемых сведений к тайне связи. Можно выделить несколько обязательных признаков, наличие которых позволяет говорить об отнесении той или иной информации к тайне связи.

Одним из признаков является нахождение переписки (либо сведений о переписке) в ведении оператора связи. Обязательность данного признака подтверждается в том числе положениями ст. 63 Федерального закона «О связи» №126-ФЗ от 07.07.2003 г., согласно которому, соблюдение тайны связи обязаны обеспечивать именно операторы связи;

Сведения, содержащиеся в переписке должны носить личный характер, т. е. отражать отдельные стороны частной жизни конкретного человека (так как переписка служебного или рекламного характера не подпадает под тайну связи). Необходимо помнить, что в соответствии с решением Конституционного Суда РФ от 2 октября 2003 г. №435-О, к тайне связи необходимо относить не только непосредственно текст переданного или полученного сообщения, но и информация о самом факте отправки или получения сообщения, адресате, времени и т.д. между тем

[1] Федеральный закон от 07.07.2003 N 126-ФЗ (ред. от 06.07.2016) "О связи" Статья 63. Тайна связи // СПС КонсультантПлюс.

сам по себе адрес электронной почты, IP-адрес и другие идентификаторы к тайне связи относить нельзя. [1]

Переписка, или иная информация должна находиться в ограниченном доступе, то есть доступ к ней должен иметь не любой пользователь сети Интернет, а только тот, кого определил отправитель (переписка в открытых чатах, комментариях к чему-либо к тайне связи относиться не может).[2]

При наличии указанных признаков получение и (или) просмотр интернет-переписки должен расцениваться как ограничение тайны связи и требует обязательного получения судебного решения. Соответственно информация, хранящаяся в памяти электронного устройства (в том числе телефона) не может относиться к тайне связи и получение судебного решения для её просмотра не требуется. Необходимо отметить, что встречаются противоположные мнения. Например, А.А. Хайдаров в своей статье "Незаконная практика фиксации личной переписки граждан на мобильных устройствах" считает, что в ходе осмотра телефона сотрудники правоохранительных органов осматривают содержимое памяти сотового телефона без судебного решения, незаконно ограничивая их право на тайну переписки. Но доводов не приведено, а во-вторых, не соответствуют положениям закона, поэтому считаем это мнение ошибочным. Еще одним примером, подтверждающим приведенные доводы является практика получения детализаций телефонных переговоров, так если такая детализация получается у оператора связи, то в соответствии со ст. 186.1

---

[1] Такой вывод частично подтверждается в решении Девятого арбитражного апелляционного суда от 19.09.2013 г. по делу № А40-56844/2013 // СПС КонсультантПлюс.

[2] 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 уровни : материалы XVII международной научно-практической конференции (17-18 апреля 2014 года). Красноярск: СибЮИ ФСКН России, 2014.Ч 2. С. 39.

УПК РФ на это требуется судебное решение, если же такую детализацию мы обнаружили в ходе обыска или осмотра жилища, а также в ходе выемки у одного из участников процесса – судебное решение не получается. В таких случаях, как и в случае с перепиской, хранящейся в памяти телефона эти сведения составляют личную тайну с соответствующим ей правовым режимом доступа.

Иллюстративным является следующий пример из следственной практики. Потерпевшей было подано заявление о краже ее сотового телефона. После возбуждения уголовного дела, следователем было принято решение, вызвать потерпевшую на допрос, при этом следователь предложил потерпевшей принести с собой детализацию телефонных переговоров с ее абонентского номера в период кражи телефона. После чего следователем была проведена выемка. Потерпевшая добровольно выдала детализацию. Таким образом, судебного решения для этого не потребовалось. [1]

Рассмотрим служебную тайну.

Необходимость рассмотрения вызвана тем, что обыск и выемка в каких-либо организациях зачастую связаны с изъятием служебной компьютерной техники, соответственно она может содержать сведения, составляющие служебную тайну.

Перечень сведений, составляющих служебную тайну устанавливается государственными и муниципальными органами. Документы, содержащие эту информацию имеют гриф для служебного пользования. Охрана служебной тайны возлагается на руководителей организации и должностных лиц, владеющих этой тайной. Судебное решение для получения вышеуказанной тайны для расследования уголовного дела не требуется. Изъять информацию возможно следственными и иными процессуальными действиями.

[1] Из архива отела полиции №2 МУ МВД РФ г.Красноярска "Красноярское" уголовное дело №1040038009753.

Служебная тайна имеется в различных отраслях.

Режим коммерческой тайны регулируется Федеральным законом «О коммерческой тайне».[1]

Информация представляет коммерческую тайну, только если отвечает трем признакам:

- имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам;
- отсутствует свободный доступ к информации;
- владелец информации принимает меры по охране ее конфиденциальности.

При использовании правоохранительными органами при расследовании преступления доказательств, которые представляют собой компьютерную информацию и составляют коммерческую тайну, могут быть:

- деловая переписка;
- бизнес-план;
- содержание договоров.

Данные сведения не являются общедоступными, они могут быть представлены в обязательном порядке только специально уполномоченным на то органам государственной власти. Например: документы об уплате налогов только налоговым органам. А в ходе расследования уголовного дела такую тайну возможно получить путем проведения следственных действий: выемка, обыск либо по судебному решению. А при использовании ч.3 ст.55 Конституции РФ, судебное решение не требуется, следовательно, получаем на основании УПК РФ. Аналогично, при проведении каких-либо следственных, процессуальных действий или оперативных мероприятий в банках, возможно изъятие

[1] Федеральный закон от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне»// Система ГАРАНТ: (дата обращения: 15.04.2017).

компьютерной информации, которая содержит в себе банковскую тайну. Согласно ФЗ "О банках и банковской деятельности" к банковской тайне относится: информация, которая находится в ведении банка; информация, которая по содержанию связана с движением денежных средств.

Режим доступа к информации, содержащей банковскую тайну, зависит от ее вида. Например, справки по операциям и счетам юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, выдаются кредитной организацией им самим, судам и арбитражным судам (судьям), Счетной палате Российской Федерации, налоговым органам, Пенсионному фонду Российской Федерации, Фонду социального страхования Российской Федерации и органам принудительного исполнения судебных актов, актов других органов и должностных лиц в случаях, предусмотренных законодательными актами об их деятельности, а при наличии согласия руководителя следственного органа - органам предварительного следствия по делам, находящимся в их производстве.

Справки по операциям и счетам юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, выдаются кредитной организацией им самим, судам и арбитражным судам (судьям), Счетной палате Российской Федерации, налоговым органам, Пенсионному фонду Российской Федерации, Фонду социального страхования Российской Федерации и органам принудительного исполнения судебных актов, актов других органов и должностных лиц в случаях, предусмотренных законодательными актами об их деятельности, а при наличии согласия руководителя следственного органа - органам предварительного следствия по делам, находящимся в их производстве.

Справки по счетам и вкладам физических лиц выдаются кредитной организацией им самим, судам, органам принудительного исполнения судебных актов, актов других органов и должностных лиц, организации,

осуществляющей функции по обязательному страхованию вкладов, при наступлении страховых случаев, предусмотренных федеральным законом о страховании вкладов физических лиц в банках Российской Федерации, а при наличии согласия руководителя следственного органа - органам предварительного следствия по делам, находящимся в их производстве.

Справки по операциям и счетам юридических лиц и индивидуальных предпринимателей, по операциям, счетам и вкладам физических лиц выдаются на основании судебного решения кредитной организацией должностным лицам органов, уполномоченных осуществлять оперативно-розыскную деятельность, при выполнении ими функций по выявлению, предупреждению и пресечению преступлений по их запросам, направляемым в суд в порядке, предусмотренном статьей 9 Федерального закона от 12 августа 1995 года N 144-ФЗ "Об оперативно-розыскной деятельности", при наличии сведений о признаках подготавливаемых, совершаемых или совершенных преступлений, а также о лицах, их подготавливающих, совершающих или совершивших, если нет достаточных данных для решения вопроса о возбуждении уголовного дела. Перечни указанных должностных лиц устанавливаются нормативными правовыми актами соответствующих федеральных органов исполнительной власти.[1]

Безусловно, также, при использовании компьютерной информации, содержащей государственную тайну возникает немало проблем, поскольку государственная тайна имеет огромное количество ограничений, поэтому для доступа к ней необходимо иметь допуск определенной степени, соответствующий степени секретности документа. Следовательно, для изъятия компьютерной информации может допускаться сотрудник только

[1] Федеральный закон от 02.12.1990 N 395-1 (ред. от 03.07.2016) "О банках и банковской деятельности" (с изм. и доп., вступ. в силу с 01.01.2017) ст.26 Банковская тайна.

имеющий вышеуказанный допуск. Для использования такой информации в рамках уголовного дела необходимо произвести процедуру рассекречивания документа и только после этого, документ может быть приобщен в качестве доказательств. А согласно ч.2 ст. 183 УПК РФ выемка таких сведений только на основании судебного решения.

За нарушение особых правовых режимов предусматривается юридическая ответственность

1. Уголовная (ст.137, ст.138, ст.183, ст.283 УК РФ);
2. Административная (ст.13.12, ст.13.13, ст.13.14 КоАП РФ);
3. Гражданско-правовая;
4. Дисциплинарная.

Подводя краткий итог данного параграфа, констатируем важность вышеуказанных вопросов. Мы пришли к выводу, что следователь должен в первую очередь правильно оценить изымаемую компьютерную информацию, после чего он определяет правовой режим её изъятия. Знания о режиме доступа обеспечивают в последующем допустимость полученных доказательств и препятствуют злоупотреблениям и противодействию стороны защиты.

§ 2. Уголовно-процессуальные аспекты получения компьютерной информации при расследовании наркопреступлений

Расширение сферы применения современных информационных технологий, появление новых видов преступлений приводят к тому, что при расследовании уголовных дел в ходе проведения осмотров, выемок, обысков все чаще возникает необходимость изъятия электронных носителей информации, содержащих данные, которые впоследствии могут быть использованы в доказывании. На таких носителях могут быть обнаружены:

– специальное программное обеспечение, использовавшееся при совершении противоправных действий (например, позволяющее получать доступ к запрещенным в РФ сайтам по продаже наркотических средств), а также вредоносные программы;

– электронная корреспонденция участников преступления, касающаяся его организации и исполнения, сведения о связях преступников и используемых средствах коммуникации, о распределении ролей в преступных группах и планируемых преступлениях;

– иная информация, представляющая интерес для следствия.[1]

Так, закрепление в законе понятия электронного носителя информации без его разъяснения вынуждает правоприменителя обращаться к иным нормативным актам и документам для уяснения его сущности.[2] Отметим, что в справке Государственно-правового управления, комментирующей принятие указанного Федерального закона, в качестве электронных носителей информации названы компьютерные блоки, серверы, ноутбуки и карты памяти[3]. Полагаем, такой перечень не может быть применим в следственной практике, так как не учитывает другие виды схожих устройств[4], например MP3-плееры Apple iPod, флеш-карты, установленные в цифровые фотоаппараты, нелицензионные CD-диски с аудиозаписями, на которые возможно записать любую другую информацию, в отличие от лицензионных CD-дисков. Ввиду использования в законе технического термина для его толкования будет

---

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

[2] Ларин Е.Г. Копирование информации с электронных носителей при производстве по уголовному делу // Законодательство и практика. Омская академия МВД России, 2012. № 2 (29). С. 55.

[3] Уточнён порядок изъятия и возвращения электронных носителей в ходе расследования уголовных дел. Интернет ресурс. URL: http://www.kremlin.ru/news/16111./04/12/17/.

[4] Осипенко А.Л., Гайдин А.И. Указ.соч. С. 5.

оправданным обращение к понятию, которое дает ГОСТ 2.051-2006: «Электронный носитель — это материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники».[1] Однако такое определение, на наш взгляд, не вносит достаточной ясности в отношении круга объектов, при изъятии которых должны применяться указанные нормы УПК РФ поскольку любые устройства, оборудования, которые способны хранить информацию в электронном виде, а не только те, которые для этого напрямую предназначены.

Предлагаем далее определить следственные действия, при производстве которых возможно изъятие электронных носителей. К ним можно отнести: обыск, выемку, осмотр, следственный эксперимент, проверку показаний на месте. Конечно, список не является закрытым, поскольку в ходе некоторых других следственных действий также получаются электронные носители, например получение информации о соединениях между абонентами, контроль и запись телефонных переговоров и др., однако законом предусмотрены специальные правила именно для изъятия электронных носителей, в связи с чем более подробно необходимо рассмотреть первую группу следственных действий.

В УПК РФ внесен ряд изменений, касающийся электронных носителей. Рассмотрим некоторые из них.

Ст. 82 УПК РФ, определяющая порядок хранения вещественных доказательств, дополнена положениями о том, что электронные носители информации хранятся в опечатанном виде в условиях, исключающих возможность ознакомления посторонних лиц с содержащейся в них информацией и обеспечивающих их сохранность и сохранность информации. Носители возвращаются их законному владельцу после

[1] Единая система конструкторской документации. Электронные документы. Общие положения. ГОСТ 2.051-2006 (введен Приказом Ростехрегулирования от 22.06.2006 N 119-ст). Консультант плюс. (дата обращения: 21.04.2017).

осмотра и производства других необходимых следственных действий, если это возможно без ущерба для доказывания. После производства неотложных следственных действий в случае невозможности возврата электронных носителей информации их законному владельцу содержащаяся на этих носителях информация может быть скопирована по ходатайству их законного владельца.[1]

Копирование информации должно осуществляться с участием законного владельца изъятых электронных носителей информации и (или) его представителя и специалиста в присутствии понятых в подразделении органа предварительного расследования или в суде.

Сразу необходимо оговориться, что УПК РФ предусмотрено копирование информации с электронных носителей информации, однако в рамках какого процессуального действия его производить, законодатель не уточнил. Мы считаем, что за неимением такого следственного действия как осмотр электронного устройства и компьютерной информации, наиболее подходящим следственным действием для производства копирования является осмотр предмета (ч. 2 ст. 176 УПК РФ). В данном случае, следователь, обнаружив предмет, имеющий отношение к уголовному делу (например, мобильный телефон, ноутбук и др.), на котором хранится компьютерная информация, имеющая доказательственное значение, при поступлении ходатайства законного владельца или обладателя о её копировании, принимает решение о производстве осмотра предмета, то есть электронного носителя информации, с помощью специалиста. Специалист в ходе данного следственного действия, если электронный носитель информации уже упакован, должен распаковать его, снять копию, а затем снова запаковать.

Данную точку зрения не разделяет Ларин Е.Г. в своей научной статье «Копирование информации с электронных носителей при производстве по уголовному делу», предлагая действию, с помощью которого

[1] Осипенко А.Л., Гайдин А.И. Указ.соч. С. 3.

осуществляется копирование, а также протокол, в котором фиксируется ход действий специалиста, дать следующее наименование: «Протокол копирования информации и передачи электронных носителей, содержащих скопированную информацию». Мы считаем это мнение ошибочным, поскольку УПК РФ не предусматривает такого процессуального действия и наименования протокола.

Следует отметить, что осмотр, в ходе которого производится копирование будет являться четвертым СД, производимым с обязательным участием понятых, несмотря на то, что в ст. 170 УПК РФ это не предусмотрено.

Копирование производится на другие электронные носители, предоставленные законным владельцем изъятых носителей. При копировании информации должны обеспечиваться условия, исключающие возможность ее утраты или изменения.[1] Закон определяет, что копирование информации не допускается, если это может воспрепятствовать расследованию преступления либо, по заявлению специалиста, повлечь за собой утрату или изменение информации. Однако, к сожалению, четкие критерии, подтверждающие возможность наступления при копировании указанных последствий, отсутствуют. Это обстоятельство в отдельных случаях способно приводить к безосновательному отказу в копировании. Например, апелляционным определением Московского областного суда от 20 июня 2013 года по делу №22-4172/2013 было признано незаконным постановление старшего следователя, которым отказано в удовлетворении ходатайства адвоката о разрешении переписать данные с жестких дисков изъятых компьютеров ООО "...", а также о получении ксерокопий всех изъятых документов в

[1] Ларин Е.Г. Указ. соч. С. 53.

связи с тем, что следователем не приведено убедительных мотивов отказа в удовлетворении ходатайства.[1]

Электронные носители, содержащие скопированную информацию, передаются законному владельцу изъятых носителей. Об осуществлении копирования и о передаче электронных носителей информации, содержащих скопированную информацию, законному владельцу изъятых носителей составляется протокол.[2]

Федеральным законом внесены также дополнения в статьи 182 и 183 УПК РФ, согласно которым при производстве обыска или выемки электронные носители информации изымаются с участием специалиста. По ходатайству законного владельца изымаемых носителей специалистом, участвующим в обыске (выемке), в присутствии понятых с изымаемых электронных носителей информации осуществляется копирование.[3]

В УПК РФ внесены поправки, регулирующие вопросы изъятия и копирования информации с компьютеров. Эти изменения призваны обеспечить дополнительную защиту прав граждан и решить задачу продолжения деятельности хозяйствующих субъектов в случае изъятия электронных носителей в ходе расследования преступлений. Согласно принятому закону электронные носители информации могут признаваться вещественными доказательствами по уголовным делам (п. 5 ч. 2 ст. 82 УПК). В противном случае они должны возвращаться их владельцам или законным пользователям (ст. 81 УПК).

Также более подробно хочется сказать о копировании информации с электронных носителей. Информация может быть скопирована по ходатайству ее законного владельца или обладателя. Данное ходатайство должно быть выполнено в письменной форме и в последующем

---

[1] Апелляционное определение № 22-4172/2013 от 20 июня 2013 г. по делу № 22-4172/2013// [Электронный ресурс]. URL: http://www.gcourts.ru/case/14090650.

[2] Ларин Е.Г. Указ. соч. С. 54.

[3] Осипенко А.Л., Гайдин А.И. Указ.соч. С. 4.

приобщается к материалам уголовного дела, копия вручается заявителю, а оригинал же остается при уголовном деле. В ч.2.1 ст.82 УПК РФ указано, что не допускается копирование информации, если это может воспрепятствовать следствию. Далее решение о копировании информации либо об отказе в копировании принимает должностное лицо и выносит постановление, которое также приобщается к материалам уголовного дела.

Копирование указанной информации осуществляется с участием законного владельца изъятых электронных носителей информации и (или) его представителя и специалиста в присутствии понятых в подразделении органа предварительного расследования или в суде на другие электронные носители информации, предоставленные законным владельцем изъятых электронных носителей информации. При копировании информации должны обеспечиваться условия, исключающие возможность ее утраты или изменения. Электронные носители информации, содержащие скопированную информацию, передаются законному владельцу изъятых электронных носителей информации. Об осуществлении копирования информации и о передаче электронных носителей информации, содержащих скопированную информацию, законному владельцу изъятых электронных носителей информации составляется протокол в соответствии с требованиями ст. 166 УПК.

При производстве обыска, выемки либо осмотра аналогично возможно копирование информации с электронных носителей, которое осуществляется по ходатайству законного владельца или обладателя электронного носителя, но законодательно не закреплено конкретно, кто является законным владельцем, а кто обладателем. Зачастую на практике законным владельцем вещи признают лицо, которое имеет документы, подтверждающие собственность, но в случае с электронными носителями практически во всех случаях таких документов не предоставляется, поскольку вообще их не существует, ведь при приобретении флеш карты, диска и т.п. кроме чека, подтверждающего стоимость, более ничего не

предоставляется. Поэтому единственно верным решением мы считаем признавать законным владельцем или обладателем электронного носителя лицо, либо у которого данный носитель находится, либо того, чья информация хранится там. Далее в присутствии понятых, на другие электронные носители, предоставленные законным владельцем электронного носителя, если это не может воспрепятствовать расследованию уголовного дела. Об этом делается отметка в протоколе проводимого следственного действия.

При производстве выемки проблем не возникает, поскольку правоохранительные органы изымают то, что изначально было запланировано, не считая предметов, запрещенных в гражданском обороте и при ходатайстве законного владельца электронного носителя о копировании информации, у него есть возможность предоставить иной электронный носитель. А вот при обыске изымаются все электронные носители, находящиеся в обыскиваемом помещении и при желании обыскиваемого скопировать информацию с электронного носителя, он не имеет возможности предоставить иной электронный носитель, поскольку при производстве обыска обыскиваемый не имеет права покидать помещение, в котором проводится обыск. Следовательно, такая возможность может у него появится только после проведения обыска, если нужный ему электронный носитель не опечатают во время приобщения его в качестве доказательства.

Также, признавая электронные носители в качестве вещественных доказательств, можно при проведении иных следственных действий неоднократно копировать информацию, которая находится на данном носителе, только меняя при этом носитель. Копирование одной и той же информации, меняя при этом только лишь носитель не может считаться расширением доказательственной базы.

В настоящее время перечисленные электронные носители информации являются наиболее распространенными. Их повсеместное

применение предопределили небольшие габариты, простота использования, надежность и невысокая стоимость. В то же время при проведении следственных действий в отдельных случаях еще могут быть обнаружены и такие практически вышедшие из употребления носители информации, как дискеты (накопители на гибких магнитных дисках), накопители на магнитной ленте (кассеты стримеров), магнитооптические диски и диски для устройств Zip-drive.

Кроме того, электронными носителями информации являются установленные в средствах вычислительной техники внутренние накопители на жестких магнитных дисках (НЖМД, «винчестеры»). Именно на таких устройствах, входящих в состав серверов компаний и персональных компьютеров сотрудников, наиболее часто находится информация, представляющая особый интерес для следствия.

Законодатель, закрепляя требование об обязательном участии специалиста в производстве обыска и выемки, прежде всего, на наш взгляд, преследовал цель обеспечить законные интересы владельцев носителей информации или обладателей содержащейся на них информации. Использование термина «электронный носитель информации» в соответствующих нормах не является ключевым. Очевидно, основное значение придается правильному вводу в уголовный процесс хранимой на таких носителях криминалистически значимой информации. Соответственно, применение указанных норм направлено не на все обнаруженные носители, а лишь на содержащие или могущие содержать такую информацию.

Вообще, позиция законодателя относительно роли специалиста при производстве выемки и обыска, связанных с изъятием электронных носителей информации, заслуживает отдельного обсуждения. Норма об обязательном участии специалиста в указанных следственных действиях была закреплена в ст. ст. 182 и 183 УПК РФ одновременно с нормой, устанавливающей требование к специалисту осуществить копирование

информации на другие носители, предоставленные законным владельцем изымаемых носителей или обладателем содержащейся на них информации, по их ходатайству. Это позволяет предположить, что необходимость участия специалиста связывается с его обязанностью произвести копирование информации с изымаемых носителей при наличии ходатайства определенных в законе лиц.[1] В таком случае изъятие электронных носителей информации при производстве обыска и выемки, если ходатайство на копирование информации не заявлено, не требовало бы присутствия специалиста.[2]

Очень важно обеспечить целостность данных так, чтобы носитель информации не изменился в процессе копирования. Для этого используют специальное оборудование, реализующее функцию запрета записи на носитель, с которого ведется копирование (блокираторы записи, криминалистические дубликаторы). При необходимости изъятия носителей и отсутствии препятствий копированию содержащейся на них информации следователь должен обеспечить его осуществление на предоставленные их законным владельцем носители. К сожалению, УПК РФ не устанавливает срок для производства копирования.[3]

Следующим после изъятия этапом является осмотр электронного носителя информации, в качестве которого часто выступает компьютер. Рассмотрим алгоритм осмотра компьютера при расследовании преступлений, связанных с незаконным оборотом наркотиков. Компьютер выступает одним из средств совершения преступлений, связанных с незаконным оборотом наркотических средств, психотропных и

---

[1] Иванов А.Н. Новый порядок изъятия электронных носителей информации при производстве обыска и выемки // Проблемы уголовного процесса, криминалистики и судебной экспертизы. Саратов: Сарат. гос. юр. акад., 2012. №1. С. 24.

[2] Родивилин И.П., Шаевич А.А. Об участии специалиста при изъятии электронных носителей информации в ходе производства обыска и выемки // Криминалистика: вчера, сегодня, завтра: сборник научных трудов. Иркутск: ВСИ МВД России, 2013. № 3. С. 153.

[3] Осипенко А.Л., Гайдин А.И. Указ. соч. С. 10.

сильнодействующих веществ, совершаемых с использованием информационно-телекоммуникационных сетей. Значимость информации, которая может быть при этом получена сложно переоценить. Так, в процессе его производства могут быть обнаружены как материальные следы (следы пальцев рук, микрообъекты и т.д.), так и виртуальные (посещения сайтов с рекламой наркотиков, архив переписки пользователя, управления счетами электронных платежных систем и т.д.), способствующие формированию полноценной доказательственной базы и изобличающие не только его пользователя, но и иных лиц причастных к совершению преступления: курьеров, менеджеров по региону, кассиров, организаторов преступных групп.[1]

В подтверждение сказанного приведем пример судебно-следственной практики. При производстве обследования жилища гр. Ш. по адресу: ул. Кирова д. «..» кв. «..» г. Норильска, выполнявшей функции в организованной преступной группе – «Склада-хранителя», был изъят системный блок, монитор «PHILIPS», ноутбук «ASUS». В ходе следственного осмотра, произведенного с участием специалиста, на диске «С» была обнаружена папка «Ozon77777» с файлами, содержащими текстовые записи представляющими переписку абонентов «Ozon77777», «Ellektra911» за период с 19.10.2013 года по 14.12.2013 года. В ходе расследования было установлено, что под логином «Ellektra911» выступала сама Ш. Логин «Ozon77777» принадлежал лицу, осуществлявшему в организованной преступной группе функции оператора. В результате изучения переписки было установлено, что оператор передавал Ш. партии наркотиков для дальнейшего сбыта, давал указания о производстве закладок с наркотиками, инструктировал Ш. о

[1] Земцова С.И., Суров О.А., Галушин П.В. Алгоритм осмотра компьютера при расследовании преступлений, связанных с незаконным оборотом «дизайнерских» наркотиков, совершаемых с использованием интернет-магазинов // Вестник Сибирского юридического института ФСКН России. - 2016. - №3 (24). С. 2.

правилах безопасного осуществления преступной деятельности, а также требованиях к отчетности о количестве приготовленных «закладок» и массе реализуемых наркотиков. Ш. в свою очередь, сообщала оператору адреса и места нахождения приготовленных ею закладок с наркотиками, номера своих QIWI-кошельков для получения денежного вознаграждения – зарплаты от оператора за произведенную Ш. работу по сбыту наркотиков.

В памяти ноутбука «ASUS» также была обнаружена переписка с использованием программы «Brosix» между «Ellektra911» и «Иван Иванов», а впоследствии «Ozon77777», состоящая в получении заданий по реализации наркотиков.[1]

Надлежащим следственным действием для осмотра несомненно является осмотр предмета, однако зачастую следователи подменяют понятия и фактически осматривая сведения, расположенные в сети Интернет, ошибочно указывают в качестве объекта осмотра – компьютер, однако нужно понимать, что компьютер, в данном случае, выступает лишь используемым техническим средством, и сам осмотр не направлен на установление его свойств.[2] За неимением ничего более подходящего, мы предлагаем использовать в подобных случаях «протокол осмотра электронного документа», поскольку применение в данном случае указанного следственного действия более оправдано, так как фиксируемые данные находятся не в памяти компьютера. Данная позиция косвенно подтверждается положениями Федерального закона «Об информации, информационных технологиях и защите информации» №149-ФЗ от 27.07.2006 г., а именно электронным документом признается документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием

[1][Электронный ресурс]. URL://https://rospravosudie.com/court-norilskij-gorodskoj-sud-krasnoyarskij-kraj-s/act-480133707.

[2] Карлов А.Л. Указ. соч. С. 51.

электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.[1] А страница сети Интернет - это часть сайта в сети Интернет, доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта в сети Интернет. Безусловно страница сети Интернет попадает под некоторые признаки электронного документа, а именно средствами идентификации: электронный адрес и т.д.

Для преступлений в сфере незаконного оборота наркотиков рассмотренный вопрос является очень актуальным, так как для установления связей и доказывания факта длительного знакомства и тесных связей возникает необходимость фиксации открытых сведений из социальных сетей, и других ресурсов сети Интернет. Указанные обстоятельства подтверждают необходимость решения данной проблемы на законодательном уровне.

Следует учитывать тот факт, что в последнее время практика пошла по такому пути, при котором интернет-переписка, содержащая тайну, охраняемую федеральным законом, производится во ходе выемки предметов и документов непосредственно у представителя оператора связи на основании судебного решения. С учетом положений ст. 13 и п.7 ч.2 ст. 29 УПК РФ данный подход можно признать в полной мере законным и обоснованным, однако с учетом расположения организаций, владеющих серверами крупных социальных сетей и других коммуникационных сервисов (г. Москва, г. Санкт-Петербург), производство таких выемок становится достаточно затратным как по времени, так и по средствам реализации, а в случае нахождения сервера за пределами Российской Федерации (электронные почтовые ящики @gmail.com, @google.com,

[1] Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 19.12.2016) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.01.2017) / СПС «КонсультантПлюс».

@hotmail.com, социальная сеть facebook) – практически невозможным.[1] Что, в очередной раз, ставит в тупик следствие и приводит к необходимости продления процессуальных сроков по делу.

Встречаются случаи производства следственного эксперимента, в ходе которого лицо, чья переписка представляет интерес, самостоятельно заходит на соответствующий ресурс сети Интернет и, открывая входящие и исходящие сообщения, позволяет следователю зафиксировать в протоколе их содержание. Стоит отметить, что данный подход не лишен логики, поскольку результат совершаемых действий заранее не известен (страница сети Интернет может быть удалена, изменена и т.д.). А цели в общем соответствуют заявленным в ст. 181 УПК РФ (проверяется возможность восприятия каких-либо фактов, совершения определенных действий, наступления какого-либо события, а также выявляются последовательность происшедшего события и механизм образования следов).

Важно, что на электронных носителях может оставаться информация из предварительно удаленных пользователем файлов, которые при использовании специального программного обеспечения могут быть восстановлены. Но данный вопрос решается с помощью экспертизы. В большинстве случаев, информацию удается восстановить, поэтому распространенными в практике являются случаи проведения судебной компьютерно-технической экспертизы.

Также компьютерно-сетевая экспертиза, в ходе которой могут быть получены сведения о переписке. Но само по себе вышеуказанное следственное действие используется достаточно редко, поскольку чаще подозреваемый/обвиняемый отказывается демонстрировать определенные действия, подтверждающие его вину, в особенности в наркопреступлениях.

---

[1] Карлов А.Л. Указ. соч. С. 42.

Однако процессуальная форма фиксации зачастую не решает вопроса о доступе к информации в ходе указанных следственных действий . Такой доступ может быть получен по-разному:

- посредством подбора пароля, либо с использованием логина и пароля, имеющихся в материалах уголовного дела;
- с участием лица, при этом он сам предоставляет пароль;
- установление пароля при проведении судебной КТ экспертизы либо осмотра компьютера.

Например, в настройках браузера «Yandex», если перейти по ссылке «browser://settings/passwords» возможно ознакомиться с логинами и паролями, которые были сохранены пользователем данного компьютера. такую функцию поддерживают многие браузеры, такие как «Google Chrome», «Opera», «Mozilla Firefox» и некоторых других.

Также остается не решенным вопрос о преодолении визуального кода на телефонах фирмы Apple: iPhone 5s, 6, 7 и некоторых иных смартфонов для обеспечения доступа к содержимому телефона, однако следователь если планирует ознакомиться с содержимым, то он может дать поручение оперативным сотрудникам, которые могут установить пароль.

Также одним из приемлемых вариантов является фиксация интернет-переписки в ходе такого оперативно-розыскного мероприятия как снятие информации с технических каналов связи, с дальнейшим предоставлением материалов следователю в качестве результатов оперативно-розыскной деятельности, при этом все рассмотренные требования об обеспечении права на тайну связи также должны быть учтены.[1] Единственным препятствием реализации такого подхода в рамках возбужденного уголовного дела может выступить запрет на подмену оперативно-розыскными мероприятиями процессуальных действий, для осуществления которых уголовно-процессуальным законом установлена

[1] Карлов А.Л. Указ. соч. С. 58.

специальная процедура,[1] однако, таковой УПК РФ как раз не предусматривает. Но предусматривает ФЗ "Об оперативно-розыскной деятельности", поскольку недавно было введено новое оперативно-розыскное мероприятие - получение компьютерной информации. Но несмотря на это сотрудники правоохранительных органов находят способы расследования преступлений, путем проведения следственных действий, как, например, в производстве следственной службы РУ ФСКН России по Красноярскому краю находилось уголовное дело в отношении жителя Павлова И., совершившего несколько преступлений в сфере незаконного оборота наркотических средств с использованием сети Интернет.[2] По делу было установлено, что Павлов, находясь по месту своего жительства, используя ноутбук, подключенный к сети Интернет, на одном из сайтов приискал неустановленное следствием лицо, находящееся на территории Королевства Нидерландов, которое за вознаграждение путем направления международного почтового отправления на указанный Репиным адрес обязалось незаконно переслать ему наркотические средства – d-Лизергид (ЛСД, ЛСД-25) и кокаин в значительном размере. После этого Павлов посредством электронных платежных систем оплатил наркотические средства, представив отправителю свои персональные данные о личности и адрес проживания.

В процессе доказывания органами предварительного расследования помимо традиционного комплекса следственных действий (допросов, обысков, осмотров, судебно-химических экспертиз) проведена компьютерно-техническая экспертиза, согласно выводам которой на исследуемом ноутбуке имеется программное обеспечение, предназначенное для работы в сети Интернет: программа Tor Browser.

---

[1] Исаенко В.Н. О некоторых вопросах использования материалов оперативно-розыскной деятельности в уголовно-процессуальном доказывании// Отрасли права. – 2017. №3. С. 41.

[2] [Электронный ресурс]. URL: https://24.мвд.рф/04/21/17/.

Кроме того, проведен следственный эксперимент с участием специалиста, в ходе которого установлено, что с указанного компьютера с помощью программы Tor Browser осуществлялся выход в сеть Интернет. Согласно информации, представленной оперативным отделом службы УФСКН России по Красноярскому краю, указанный сайт имеет тип электронной торговой площадки в виде «черного рынка» (в настоящее время закрыт по инициативе ФБР), оплата заказов производилась через криптовалюту «Bit coin». К уголовному делу также приобщены результаты оперативно-розыскных мероприятий «оперативный эксперимент», «прослушивание телефонных переговоров» и информации ФГУП «Почта России», Шереметьевской таможни ФТС России.

Первоначально Павлов не признавал вину в совершении инкриминируемых деяний, однако после предъявления ему совокупности добытых доказательств был вынужден сознаться в содеянном. Приговором Красноярского районного суда от 2 апреля 2014 г. Павлов признан виновным в совершении пяти преступлений в сфере незаконного оборота наркотиков, совершенных с использованием сети Интернет.

Рассмотренные в данном параграфе вопросы, дают основание полагать, что в настоящее время уже существует множество как правовых, так и технических средств , применяемых при расследовании уголовных дел, по которым доказательствами служит компьютерная информация. Экспертные службы в целом уже приспособились к работе с электронными носителями, компьютерной информации и т.п., но есть еще огромное количество пробелов, которые законодателю предстоит разрешить.

§ 3. Вопросы оценки компьютерной информации в качестве доказательства по уголовным делам в сфере незаконного оборота наркотиков

В данной работе нами уже рассматривались вопросы об отнесении компьютерной информации к конкретным видам доказательств, в связи с чем необходимо остановиться на особенностях оценки свойств доказательств. Вопрос установления относимости, допустимости, достоверности и достаточности имеет огромное значение применительно к компьютерной информации, так как любой вид доказательства должен отвечать данным требованиям, и компьютерная информация, претендующая на самостоятельный вид доказательства, не исключение. «Поскольку нет заранее установленной силы доказательств, следовательно, нет приоритета среди доказательств. При оценке каждого доказательства проверяется его относимость, допустимость и достоверность. Лишь то доказательство, которое соответствует всем этим трем требованиям, может быть положено в основу судебного решения».[1]

Рассмотрим компьютерную информацию с точки зрения относимости, то есть ее пригодности устанавливать факт, входящий в предмет доказывания. в УПК Республики Казахстан относимость определена следующим образом: «доказательство признается относящимся к делу, если оно представляет собой фактические данные, которые подтверждают, опровергают или ставят под сомнение выводы о существовании обстоятельств, имеющих значение для дела»[2]. Иначе говоря, должна прослеживаться логическая связь полученной информации с тем, что необходимо установить по конкретному уголовному делу. В наркопреступлениях, совершенных бесконтактным путем посредством сети Интернет, чаще всего, сомнений в относимости компьютерной информации к уголовному делу не возникает, поскольку это является основным доказательством, на котором основывается обвинение.

[1] Интернет-ресурс //URL:// https://www.zonazakona.ru/law/comments/art/14289/ (дата обращения: 14.05.2017).

[2] Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года № 231-V (с изменениями и дополнениями по состоянию на 18.04.2017 г.).// [Электронный ресурс]. URL: http://online.zakon.kz/Document/?doc_id=31575852.

Применительно к компьютерной информации относимость позволяет установить или опровергнуть, что данное доказательство может служить способом установлением обстоятельств, имеющих значение для уголовного дела. Как отмечает Н. А. Зигура и А. В. Кудрявцева, «особенность определения относимости компьютерной информации заключается в том, что это возможно при воспроизведении данной информации с использованием технических средств и анализе не только содержания компьютерной информации, но и её свойств (реквизитов). С точки зрения относимости оценивается как содержание компьютерной информации, так и её свойства: дата создания, изменения, открытия». При этом установление связи электронного доказательства с обстоятельствами, имеющими значение для уголовного дела, часто требует участия специалиста или же проведения экспертизы. Можно рассмотреть более подробно на примере. При установлении сбытчика наркотического средства бесконтактным путем посредством сети Интернет - владельца интернет-магазина, занимающегося распространением наркотиков, необходимо установить, действительно ли определенный сайт относится к конкретному лицу: это можно сделать путем установлением его IP-адреса, MAC-адреса устройства, с которого подозреваемый (обвиняемый) посещал сайт, наличие прав администратора сайта, созданного для незаконного сбыта наркотиков, наличие переписки с «покупателями».[1]

Обратимся к другому примеру. Так, «сведения, используемые хозяйствующими субъектами и гражданами при осуществлении предпринимательской и иной деятельности (в том числе и сведения, хранящиеся, обрабатываемые, передающиеся с помощью компьютерной техники), в зависимости от обстоятельств уголовного дела могут иметь значение для установления факта совершения преступления и виновности конкретных лиц, т. е. они отвечают требованиям относимости. Особенно важны эти сведения при расследовании экономических преступлений.

[1] Зигура Н. А. Указ.соч. С. 20.

Такие сведения являются фактическими данными (см. ст.65 УПК Украины). Это не только факты, но и сведения о фактах. Например, сведения о сумме начисленной заработной платы работникам предприятия, о дате и сумме перечисления денежных средств на расчетный счет контрагента и прочая информация.»[1]

Говоря о критериях допустимости компьютерной информации в качестве доказательства, нужно подчеркнуть, что на нее распространяются как общие правила признания доказательства допустимым (доказательства должны быть получены надлежащими субъектами, правомочными по данному делу проводить то процессуальное действие, в ходе которого получено доказательство; фактические данные должны быть получены только из источников, установленных законодательством; доказательства должны быть получены с соблюдением правил производства следственного действия, в ходе которого получено доказательство, т.е. при помощи законных приемов и способов; при получении доказательств должны быть соблюдены все требования, предъявляемые к форме их закрепления[2]), так и специальные, связанные с процессом обработки и фиксации доказательственной информации. В целях получения допустимых доказательств, необходимо соблюсти не только требования, прямо предъявляемые законом, но и удостовериться, что: устройство, при помощи которого производится осмотр, на протяжении всего осмотра имеет связь с сетью Интернет, а передаваемая и получаемая информация не искажается или подменяется кем - либо; информация получается непосредственно из сети Интернет, а не из временного буферного хранилища; пользователям, которые обращаются к осматриваемому веб - сайту с разных адресов, передается одинаковая информация;

[1] Голубев, В.А. Компьютерная информация как доказательство по уголовному делу [Электронный ресурс]. URL: http://www.crime-reseach.org/library/Golu_UPK.html.

[2] Интернет ресурс: //URL:// http://knigi.link/page/otcenka-dokazatelstv/ist/ist-15--idz-ax259--nf-5.html/ (дата обращения 14.05.2017).

осматриваемая веб - страница одинаково отображается в различных браузерах.[1]

Проанализируем правила признания доказательства допустимым.

Субъектом получения компьютерной информации является следователь, причем, согласно ч. 9^1 ст. 182 и ч. 3^1 ст. 183 УПК РФ, электронные носители информации, на которых записана компьютерная информация, подлежат изъятию с обязательным присутствием специалиста вне зависимости от произведенных при изъятии манипуляций с электронными устройствами, а также их «сложности». Представляет практический интерес постановление Омского областного суда от 21.11.2013 г. №22-3496/2013, которым действия следователя по не привлечению специалиста при производстве обыска, в ходе которого были изъяты электронные носители информации, признаются незаконными. При этом суд не находит оснований для признания самого обыска незаконным, поскольку «изъятие электронных носителей было произведено в рамках Уголовно-процессуального кодекса РФ, конституционные права участников уголовного судопроизводства нарушены не были». Разъясняя свою позицию, суд приводит в качестве довода следующий тезис: «Само по себе изъятие системного блока и ноутбука не представляло какой-либо сложности, требующей участия лица, обладающего специальными познаниями, и не повлияло на законность самого обыска».

Еще одним требованием к допустимости доказательств является получение фактических данных из надлежащего источника. «Источниками получения фактических данных являются: показания свидетеля, показания потерпевшего, показания подозреваемого, показания обвиняемого, выводы эксперта, вещественные доказательства, протоколы следственных и судебных действий, протоколы с соответствующими дополнениями,

[1] Пастухов П. С. Модернизация уголовно - процессуального доказывания в условиях информационного общества: автореф. дис. … докт. юрид. наук. М., 2015. С. 23.

составленными уполномоченными органами по результатам оперативно-розыскных мероприятий, и другими документами.»[1] Рассмотрим подробнее источники получения компьютерной информации.

Как правило, осмотр электронных носителей информации на месте затруднен в связи со сложностью выявления фактов, имеющих значение для уголовного дела, а также на это требуется продолжительное время. По этим причинам возникает основание для изъятия носителя информации специалистом в ходе производства следователем обыска или выемки электронных носителей информации. Данный процессуальный акт должен включать в себя: описание происхождения носителя компьютерной информации; условия и обстоятельства его обнаружения, изъятия, упаковки, а также краткое описание содержания находящейся на нем информации (может быть представлена распечатка компьютерной информации), с указанием реквизитов данной информации. В протоколе необходимо указать программу, с помощью которой возможно воспроизведение компьютерной
информации. Чтобы приобщить компьютерную информацию к уголовному делу, необходимо вынести постановление о признании компьютерной информации доказательством и приобщении ее к уголовному делу, в котором индивидуальные признаки носителя компьютерной информации и ее реквизиты должны обязательно совпадать с указанными в протоколе.

Поскольку в настоящее время не разработан единый алгоритм действий по собиранию компьютерной информации, мы считаем, что за неимением специального следственного действия, направленного на изъятие компьютерной информации, будет правильным получать ее в ходе проведения обыска, выемки электронных носителей информации, поскольку законодатель определил, что при производстве данных следственных действий необходимо участие специалиста, который

[1] Муравин А.Б. Уголовный процесс. Учебное пособие Х.: 000 «Одиссей», 2000. С. 65.

обеспечит правильность изъятия компьютерной информации, тем самым сводя к минимуму шансы на то, что данное доказательство в ходе судебного заседания будет признано недопустимым.

Следующим требованием является соблюдение правил производства следственного действия, в ходе которого получено доказательство. Мы не будем касаться общих правил производства вышеуказанных следственных действий, поскольку они указаны в УПК РФ. Остановимся на специальных правилах производства обыска и выемки компьютерной информации. Так, в ч. 9^1 ст. 182 и ч. 3^1 ст. 183 УПК РФ указано, что при производстве данных следственных действий электронные носители информации изымаются с участием специалиста. Примером к данному правилу может послужить решение Индустриального районного суда г. Барнаула о признании недопустимым протокола выемки, в ходе которой была изъята распечатка текстовых сообщений с интернет-сайта, в связи с тем, что для изъятия информации с электронных носителей информации не был привлечён специалист. Соответственно, судом были признаны недопустимыми доказательствами протокол выемки, протокол осмотра изъятой распечатки, а также распечатка сообщений.

Также специальным правилом является то, что в ходе производства данных следственных действий по ходатайству законного владельца изымаемых электронных носителей информации или обладателя содержащейся на них информации специалистом в присутствии понятых с изымаемых электронных носителей производится копирование информации на другие электронные носители информации, предоставленные законным владельцем изымаемых электронных носителей информации или обладателем содержащейся на них информации. Данные специальные правила при копировании были рассмотрены в нашей работе ранее.

Последним требованием является надлежащая форма закрепления компьютерной информации для признания ее доказательством. Здесь

законодатель также не определился с конкретной формой закрепления, предоставляя выбор следователям. Поэтому, форма напрямую зависит от следственного действия, в ходе которого изымается компьютерная информация: протокол обыска, выемки, личного обыска, результаты судебной экспертизы и т.д. Например, «Гагаринский районный суд г. Москвы в приговоре от 10 июня 2013 г., признал гражданина Т. виновным в совершении преступлений, предусмотренных ч 1 ст. 183, ч 2 ст. 183 УК РФ. Суд обосновал виновность указанного лица, в частности, следующими доказательствами: протоколом выемки, согласно которому в ООО "Мэйл.ру" была изъята распечатка сообщений электронной почты, принадлежащей Т. и CD-диск с электронным содержанием сообщений электронной почты; протоколом осмотра, согласно которому были осмотрены предметы и документы, изъятые в ходе проведения выемки в ООО «Мэйл.ру».[1]

Н.А. Зигура предлагает внести в действующую редакцию УПК РФ статьи, которые бы регламентировали использование в доказывании компьютерной информации в качестве доказательства по уголовному делу:

«Статья 84.1 «Компьютерная информация.

1. Компьютерная информация допускается в качестве доказательств, если изложенные в ней сведения имеют значение для установления обстоятельств, подлежащих доказыванию, а также иных обстоятельств, имеющих значение для уголовного дела.

2. Компьютерная информация - сведения, представленные в электронно-цифровой форме на материальном носителе, создаваемые аппаратными и программными средствами фиксации, обработки и передачи информации, а также набор команд (программ), предназначенных для использования в электронно-вычислительной машине (ЭВМ), системе ЭВМ или управления ими.

[1] [Электронный ресурс]URL: http://gagarinsky.msk.sudrf.ru.

3. Материальные носители компьютерной информации - материальные объекты, в том числе физические поля, в которых сведения находят свое отображение в виде символов, сигналов, предназначенных для перенесения информации во времени и в пространстве, обладающих реквизитами, позволяющими идентифицировать данную информацию, подтвердить её подлинность и целостность в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети.

4. Компьютерная информация осматривается, при этом составляется протокол, признается доказательством и приобщается к материалам уголовного дела на материальном носителе. Хранятся носители компьютерной информации в течение всего срока хранения уголовного дела. Порядок приобщения компьютерной информации устанавливается ст. 84.2 настоящего кодекса. Компьютерная информация может быть представлена в порядке установленном ст. 84.3 настоящего кодекса.

5. По ходатайству законного владельца изъятые и приобщенные к уголовному делу носители компьютерной информации или их копии могут быть переданы ему».

Статья. 84.2: «Процессуальный порядок приобщения к делу компьютерной информации в качестве доказательств.

1. При обнаружении компьютерной информации, предположительно относимой к уголовному делу, в процессе осмотра, обыска (включая личный обыск), выемки в протоколе осмотра указываются конкретное место, обстоятельства и условия обнаружения компьютерной информации, порядок и основания изъятия носителя компьютерной информации, индивидуальные признаки носителя компьютерной информации. Носитель компьютерной информации упаковывается и опечатывается. Действия, производимые с носителем компьютерной информации, описываются в протоколе, а также фиксируются в форме видеозаписи и приобщаются к делу. На действия, обстоятельства и условия обнаружения носителя компьютерной информации обращается внимание компетентных понятых.

Участие специалиста в следственном действии, связанном с собиранием, проверкой и оценкой компьютерной информации, обязательно.

2. Если изъятие носителя компьютерной информации в процессе производства следственного действия невозможно (компьютерная информация находится на удаленном носителе, например, осмотр удаленного информационного ресурса, изъятие носителя приведет к неустранимым последствиям), то компьютерная информация копируется специалистом с помощью сертифицированного программного обеспечения на новый носитель, о чем делается пометка в протоколе. В протоколе необходимо указать технические средства и программы, с помощью которых было произведено копирование. Сведения о скопированной на носитель компьютерной информации и ее реквизиты (список файлов, расположение файлов на носителе, тип, объем, дата и время создания, изменения, открытия файлов) вносятся в протокол. В протоколе описывается краткое содержание скопированной компьютерной информации или к протоколу прилагается распечатка (машинограмма) данной информации. Носитель компьютерной информации упаковывается и опечатывается. Действия, производимые с компьютерной информацией, фиксируются в форме видеозаписи. На действия, обстоятельства и условия копирования носителя компьютерной информации обращается внимание компетентных понятых. Участие специалиста в следственном действии, связанном с собиранием, проверкой и оценкой компьютерной информации, обязательно.

3. Компьютерная информация признается доказательством и приобщается к уголовному делу, о чем выносится соответствующее постановление. В постановлении о признании компьютерной информации в качестве доказательства и приобщении к уголовному делу должны быть указаны предполагаемые обстоятельства, которые могут быть установлены с помощью этого доказательства, индивидуальные признаки носителя компьютерной информации, список и реквизиты компьютерной

информации, содержащейся на данном носителе. Сведения о программах, с помощью которых возможно воспроизведение данной информации».

Статья 84.3. «Представление компьютерной информации участниками процесса или иными лицами.

1. При представлении носителя компьютерной информации в порядке ч. 2 и 3 ст. 86 настоящего кодекса следователь, дознаватель составляют протокол представления и получения носителя компьютерной информации, в котором указываются следующие сведения: кто, когда, где представил носитель компьютерной информации и описываются его индивидуальные признаки.

2. Лицо, представившее носитель компьютерной информации, допрашивается об обстоятельствах и условиях его обнаружения, цели его представления, предположительно для установления какого из обстоятельств уголовного дела он представлен. По результатам допроса должен быть составлен протокол, в котором находят отражение обстоятельства и условия обнаружения и получение носителя компьютерной информации представившим лицом.

3. После допроса лица, представившего носитель компьютерной информации, должен быть произведен осмотр компьютерной информации с участием специалиста и компетентных понятых. В процессе осмотра компьютерная информация должна быть воспроизведена. Сведения о компьютерной информации и ее реквизиты на представленном носителе (список файлов, размещение файлов на носителе, тип, объем, дата и время создания, изменения, открытия файлов) вносятся в протокол. В протоколе описывается краткое содержание компьютерной информации или к протоколу прилагается распечатка (машинограмма) компьютерной информации.

4. Компьютерная информация признается доказательством и приобщается к уголовному делу, о чем выносится соответствующее постановление. В постановлении о признании компьютерной информации

в качестве доказательства и приобщении к уголовному делу должны быть указаны предполагаемые обстоятельства, которые могут быть установлены с ее помощью, индивидуальные признаки носителя компьютерной информации, список и реквизиты компьютерной информации, содержащейся на данном носителе. Сведения о программах, с помощью которых возможно воспроизведение данной информации».[1]

С предложенной выше редакцией норм статей мы полностью согласны, поскольку законодатель не относит компьютерную информацию к отдельному виду доказательств, что в нынешнее время необходимо сделать, учитывая развитие компьютерных технологий и проникновение их во все сферы жизни человека. Поскольку на данный момент в УПК РФ отсутствует понятие компьютерной информации, четкая регламентация изъятия и использования компьютерной информации в доказывании, мы считаем нужным внести в УПК РФ предложенные Зигурой Н.А. изменения.

Следующим свойством является достоверность. Именно достоверность компьютерной информации, обычно, ставят под сомнение.. По крайней мере, пока наше уголовное судопроизводство не готово принимать компьютерную информацию, как полноценное самостоятельное доказательство. Необходимо отметить, что компьютерная информация как вид доказательства является сложным, комплексным образованием, поэтому она будет иметь доказательственное значение при наличии некоторых элементов: носителя данной информации, процессуального акта (с указанием происхождения носителя информации, реквизитов изъятой информации и т.д.), постановления о признании компьютерной информации доказательством и приобщении ее к уголовному делу (реквизиты изъятой информации должны совпадать с реквизитами, указанными в протоколе осмотра). Важна идентичность реквизитов компьютерной информации (дата создания, имя, расширение,

[1] Н.А. Зигура. Указ.соч. С.15-17

размер файла) вышеуказанных документах, поскольку зачастую следователи неумело производят следственные действия, направленные на изъятие компьютерной информации, что в будущем может привести к вынесению стороной защиты ходатайства о фальсификации или признании недопустимым доказательства.[1]

Рассматривая вопрос достоверности компьютерной информации как доказательства, нужно обратиться к ее природе. Компьютерная информация не обладает возможностью непосредственного восприятия человеком, поскольку среда, в которой существует компьютерная информация является электронной, то есть она может существовать лишь в средствах вычислительной техники (компьютер, телефон и т.д.). В.Я. Дорохов писал по этому поводу, что сведения, не обладающие свойством непосредственного восприятия, теряют основные качества сигнала (быть переносчиком информации), а содержащаяся в них информация не включается в поле зрения органов расследования и суда.[2]

В связи с этим, восприятие компьютерной информации возможно лишь с помощью аппаратных и программных средств, которые могут исказить информацию. Исход из этого, специалист при изъятии компьютерной информации в протоколе должен указать необходимые реквизиты: какая операционная система установлена на устройстве, на котором хранилась компьютерная информация; расширение файла; дата его создания, изменения; с помощью какой программы осуществляется доступ к просмотру содержимого файла и т.д.

«Весьма существенным недостатком электронного обмена документами через каналы Интернет, равно как и недостатком электронного документа вообще, является легкость внесения в него изменений и, как следствие, отсутствие уверенности в достоверности

[1] Зигура Н.А. Указ.соч. С. 20

[2] Дорохов В.Я. Природа вещественных доказательств //Советское государство и право.1971. №10. С.109.

полученного электронного документа.»[1] Действительно, компьютерная информация легко поддается изменениям и модификациям, выявить которые возможно лишь в ходе проведения экспертиз. Однако, разработан механизм, позволяющий допускать электронный документ обладающим юридической силой – электронная подпись. Она позволяет установить подлинность и отсутствие модификаций в электронном документе. Данную функцию используют при проведении компьютерно-технической экспертизы с целью полного и всестороннего изучения документа для получения доказательственной информации по уголовному делу. Но далеко не вся компьютерная информация имеет электронную подпись, поэтому для определения подлинности компьютерной информации проводятся компьютерно-технические экспертизы.

Также нельзя оставить без внимания местонахождение компьютерной информации и ее подлинность. Изымаемая у подозреваемого (обвиняемого) компьютерная информация может быть искажена, модифицирована, заражена вирусными программами, удалена в силу того, что данное лицо не заинтересовано в том, чтобы данная информация послужила доказательством его вины по уголовному делу. Поэтому, для того, что получить достоверную информацию, необходимо обратиться к серверу оператора связи и запросить данную информацию. Однако, сразу же встает вопрос о правомерности доступа к данной информации, поскольку информация, хранящаяся на серверах, может быть предоставлена следователю лишь по решению суда. [2]

Последним свойством доказательства является достаточность. В отличие от достоверности, данное свойство действует только при оценке всех доказательств по уголовному делу. Достаточность доказательств

---

[1] Боннер, А. Т. Доказательственное значение информации, полученной из Интернета //Интернет-ресурс. URL:// http://www.center-bereg.ru/h1579.html/ (дата обращения 14.05.2017).

[2] А.Л. Карлов. Процессуальная фиксация интернет-переписки в качестве доказательств по уголовным делам о преступлениях в сфере незаконного оборота наркотиков / Вестник Сибирского юридического института. 2016. С. 114.

означает их количественное и качественное накопление в материалах уголовного дела, которое позволяет принять по делу то или иное процессуальное решение. Данное свойство никаким образом не отличается от достаточности обычных доказательств, поэтому останавливаться на нем мы не будем.

Подводя итог, можно заключить, что к компьютерной информации, выступающей в качестве доказательств, предъявляются требования, указанные в ст. 88 УПК РФ. Однако, помимо общих правил оценки доказательств, существуют и специальные, без соблюдения которых при собирании, проверке и оценке компьютерной информации, признать ее доказательством не представится возможным.

ЗАКЛЮЧЕНИЕ

УПК РФ предусматривает пять следственных действий, с помощью которых возможно обнаружить и изъять компьютерную информацию: осмотр (ст. 176 УПК РФ), следственный эксперимент (ст. 181 УПК РФ), обыск (ст. 182 УПК РФ), выемка (183 УПК РФ), проверка показаний на месте (ст. 194 УПК РФ). Действующий УПК РФ не выделяет в качестве отдельного вида доказательства компьютерную информацию, относя её к вещественным доказательствам или к иным документам, что, по нашему мнению, не совсем правильно. Н.А. Зигура в своей научной статье «Природа компьютерной информации как доказательства» отмечает, что «механизм образования и специфическая форма существования компьютерной информации являются основой для выделения компьютерной информации в самостоятельный вид доказательств».[1] Нельзя не согласиться с мнением Н.А. Зигуры, поскольку нам представляется, что наиболее рациональным было бы введение законодателем в ч. 2. ст. 74 УПК РФ нового вида доказательства – компьютерная информация. Это нововведение способствовало бы более лучшей процессуальной регламентации процесса изъятия компьютерной информации в ходе производства следственных действий, и использования в качестве доказательства по уголовным делам, поскольку компьютерная информация в процессе присваивания ей статуса иного документа может подвергнуться изменениям как случайным (незнание следователем порядка обращения с электронными носителями информации и содержащейся на ней компьютерной информации), так и специальным (подозреваемый, имея удаленный доступ к информации, которая впоследствии может стать доказательством в совершении преступления, намеренно исказил или уничтожил её без возможности восстановления).

[1] Зигура Н.А. Указ.соч. С. 50-52.

Также необходимо увеличить уровень познаний следователей в области современных компьютерных технологий для повышения эффективности расследования уголовных дел в сфере незаконного оборота наркотиков, поскольку в настоящее время способы конспирации, позволяющие исключать личный контакт продавца с покупателями во избежание распространения какой-либо информации о незаконных сделках, развиваются, преступления все больше переходят в сеть Интернет, что значительно затрудняет ход следствия. По-нашему мнению, все возможные способы изъятия и использования компьютерной информации при расследовании уголовного дела в работе мы обозначили. На сегодняшний день, других вариантов, как подмена компьютерной информации под друге виды доказательств нет.

Библиографический список

Нормативные правовые акты и иные официальные документы:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ). // СПС КонсультантПлюс.
2. Гражданский кодекс Российской Федерации (ГК РФ) от 07.02.2017 N 12-ФЗ, от 28.03.2017 N 39-ФЗ. // СПС КонсультантПлюс.
3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 17.04.2017). // СПС КонсультантПлюс.
4. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 17.04.2017). // СПС КонсультантПлюс.
5. Федеральный закон "О банках и банковской деятельности" от 02.12.1990 N 395-1 (ред. от 03.07.2016) (с изм. и доп., вступ. в силу с 01.01.2017). // СПС КонсультантПлюс.
6. Федеральный закон «О коммерческой тайне» от 29 июля 2004 г. N 98-ФЗ (с изменениями и дополнениями от:2 февраля, 18 декабря 2006 г., 24 июля 2007 г., 11 июля 2011 г., 12 марта 2014 г.) // СПС КонсультантПлюс.
7. Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ (ред. от 22.02.2017). // СПС КонсультантПлюс.
8. Федеральный закон «О связи» от 07.07.2003 N 126-ФЗ (последняя редакция). // СПС КонсультантПлюс.
9. Федеральный закон «О Федеральной службе безопасности» от 03.04.1995 N 40-ФЗ (последняя редакция). // СПС КонсультантПлюс.
10. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ (ред. от 19.12.2016) // СПС КонсультантПлюс.

11. Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.1995 N 144-ФЗ (последняя редакция). // СПС КонсультантПлюс.
12. Федеральный закон «Об электронной подписи» от 06.04.2011 N 63-ФЗ (последняя редакция). // СПС КонсультантПлюс.
13. Федеральный закон РФ «О государственной тайне» от 21.07.1993 N 5485-1 (ред. от 08.03.2015) // СПС КонсультантПлюс.
14. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года № 231-V (с изменениями и дополнениями по состоянию на 18.04.2017г.)//[Электронный ресурс]. URL: http://online.zakon.kz/Document/?doc_id=31575852.
15. Проект Федерального закона N 107599-3 «Об электронном документе» (ред., внесенная в ГД ФС РФ, текст по состоянию на 27.06.2001). // СПС КонсультантПлюс.
16. Единая система конструкторской документации. Электронные документы. Общие положения. ГОСТ 2.051-2006 (введен Приказом Ростехрегулирования от 22.06.2006 N 119-ст). // СПС КонсультантПлюс.

Монографии, учебники, учебные пособия:

17. Александров А.С. Использование производных доказательств в уголовном процессе: монография/ Александров А.С., Бостанов Р.А. М.: Юрлитинформ, 2013. - 216 с.
18. Варданян А.В. Расследование преступлений в сфере высоких технологий и компьютерной информации: учеб.пособ./А.В. Варданян, Е.В. Никитина. М.: Проспект, 2007. 118 с.
19. Вехов В. Б. Криминалистическая характеристика и совершенствование практики расследования и предупреждения преступлений, совершаемых с использованием компьютерной техники : дис. ... канд. юрид. наук / В. Б. Вехов. Волгоград, 1995. 276 с.
20. Вехов В. Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки

:Монография /В. Б. Вехов ; МВД России. Волгоградская академия. - Волгоград :Волгоградская академия МВД России,2008. 401 с.

21. Вехов В.Б. Расследование компьютерных преступлений в странах СНГ: монография / Вехов В.Б., Голубев В.А. под ред. Б.П. Смагоринского. — Волгоград, 2004. 203 с.
22. Гаврилов М.В. Осмотр при расследовании преступлений в сфере компьютерной информации: науч.-практ. пособие / Гаврилов М.В., Иванов А.Н. М., 2007. 45 с.
23. Галяшина Е.И. Теоретические и прикладные основы судебной фоноскопической экспертизы: автореф. дис. … докт. юрид. наук. Воронеж, 2002. – 214 с.
24. Григорьев О.Г. Особенности расследования преступлений, связанных с незаконным сбытом наркотических средств, психотропных веществ и их аналогов: учебно-практическое пособие/ Григорьев О.Г., Кривощеков Н.В. Тюмень: Тюменский юридический институт МВД России, 2010. –104 с.
25. Костин П.В. Исследование машинных носителей информации при расследовании преступлений в сфере экономики: учеб. пособие. - Н.Новгород: Нижегородская академия МВД России, 2009. 201 с.
26. Крылов В.В. Информационные компьютерные преступления: Учебное и практическое пособие. – М.: Инфра-М – Норма, 1997. – 285 с.
27. Муравин А.Б. Уголовный процесс : учебное пособие / 3-е изд., испр. и доп. Харків : Бурун Книга, 2008 . – 234 с.
28. Орлов Ю.К. Основы теории доказательств в уголовном процессе. Научно-практическое пособие / - М.: Проспект, 2001. - 144 с.
29. Пастухов П. С. Модернизация уголовно-процессуального доказывания в условиях информационного общества : автореферат дис. ... доктора юридических наук : 12.00.09 / Пастухов Павел Сысоевич; [Место защиты: Моск. акад. экономики и права]. - Москва, 2015. - 64 с.
30. Пивовар А.Г. Большой англо-русский полный юридический словарь. - М.: Экзамен, 2013. - 918 с.

31. Право: учеб. пособие / под общ. ред. С.Ю. Наумова, Т.В. Касаевой, А.А. Шаповалова. – Саратов: ССЭИ РЭУ им. Г.В. Плеханова, 2016ч. 168 с.
32. Ремизов М.В. Оперативно - розыскная деятельность: правовое регулирование и использование результатов в уголовном судопроизводстве : Учебное пособие / Ремизов М.В., Ласточкина Р.Н; Яросл. гос. ун-т. Ярославль, 2007. – 315 с.
33. Россинская Е. Р. Криминалистика: учебник /. М.:Проспект, 2016.- 464 с.
34. Строгович М. С. Материальная истина и судебные доказательства в советском уголовном процессе. Монография. — Москва, Ленинград : Издательство Академии наук СССР, 1955. 384 с.
35. Уголовное право России. Общая часть: Учебник / Под ред. В.П. Ревина. - М.: Юстицинформ. 2016. – 460 с.

Научные публикации и статьи в иных периодических изданиях:

36. Акимова С.А. Виды ответственности за нарушение законодательства//Административное право. – 2015. - № 16. – С.20-28.
37. Белых Ю.Л. Судебное исследование аудиодокументов (процессуально-криминалистический аспект) // Эксперт-криминалист. - 2010. - № 4. - С. 21–24.
38. Боннер А. Т. Доказательственное значение информации,полученной из Интернета / А. Т. Боннер // Закон. - 1968. - №12. - С.85-98.
39. Вершок Д. В. Правовой режим радиоэлектронной информации: Автореферат диссертации на соискание ученой степени кандидата юридических наук. Специальность 12.00.14 Административное право; Финансовое право ; Информационное право /Д. В. Вершок ; Науч. рук. Л. М. Рябцев ; Белорусский государственный университет. -Минск,2003. 24 с.
40. Вехов В. Б. Документы на машинном носителе // Законность. - 2009. - № 2. - С. 18-21.

41. Галяшина Е.И. Возможности видео-фоноскопической экспертизы в раскрытии и расследовании преступлений // Вестник МВД РФ. - 2014. - № 1. С.10-16.
42. Галяшина Е.И. Возможности использования цифровой фонограммы как доказательства // Эксперт-криминалист. - 2008. - № 4. - С. 26–29.
43. Галяшина Е.И. Оценка достоверности цифровых фонограмм в уголовном процессе // Доказывание и принятие решений в современном уголовном судопроизводстве. Материалы международной науч.-практич. конференции, посвященной памяти докт. юрид. наук, профес. Полины Абрамовны Лупинской: сб. науч. трудов. М.: Изд-во «Элит», 2011. С. 131–135.
44. Галяшина Е.И., Галяшин В.Н. Цифровые фонограммы как судебное доказательство // Воронежские криминалистические чтения. № 8. Воронеж: Изд-во Воронежского государственного университета, 2007. С. 69–77.
45. Дорохов В.Я. Природа вещественных доказательств //Советское государство и право.1971. №10. С.109-114.
46. Земцова С.И., Суров О.А., Галушин П.В. Алгоритм осмотра компьютера при расследовании преступлений, связанных с незаконным оборотом «дизайнерских» наркотиков, совершаемых с использованием интернет-магазинов. //Вестник Сибирского юридического института ФСКН России. - 2016. - №3 (24). –С. 1 -22.
47. Зигура Н. А. Компьютерная информация как вид доказательств в уголовном процессе России :автореферат диссертации на соискание ученой степени кандидата юридических наук. Специальность 12.00.09 Уголовный процесс, криминалистика; Оперативно-розыскная деятельность /Н. А. Зигура ; Науч. рук. А. В. Кудрявцева. Челябинск, 2010. 21 с.
48. Зигура Н.А. Разграничение компьютерной информации и вещественных доказательств // Вестник Калининградского юридического института МВД

России. Научно-теоретический журнал. - Калиниград: Изд-во Калинингр. ЮИ МВД России, 2008, № 1 (15). - С. 283-288.

49. Иванов А.Н. Новый порядок изъятия электронных носителей информации при производстве обыска и выемки // Проблемы уголовного процесса, криминалистики и судебной экспертизы. — Саратов: Сарат. гос. юр. акад., 2012. —№1. — С. 25—26.
50. Исаенко В.Н. О некоторых вопросах использования материалов оперативно-розыскной деятельности в уголовно-процессуальном доказывании// Отрасли права. – 2017. - №3. – С.37-55.
51. Камалова Г.Г. Правовой режим информации ограниченного доступа: вопросы формирования понятийного аппарата // Вестник Удмуртского университета. Серия «Экономика и право». 2016. №4 С.118-125.
52. Карась И.З. Экономический и правовой режим информационных ресурсов //В кн.: Право и информатика / под ред. Е.А. Суханова. М.: Изд-во МГУ, 1990. С. 40-59.
53. 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 уровни: материалы XVII международной научно-практической конференции (17-18 апреля 2014 года). Красноярск: СибЮИ ФСКН России, 2014.Ч 2. - 194 с.
54. Карлов А.Л. Процессуальная фиксация интернет-переписки в качестве доказательств по уголовным делам о преступлениях в сфере незаконного оборота наркотиков/ Вестник Сибирского юридического института.2016.С.111-117.
55. Ларин Е.Г. Копирование информации с электронных носителей при производстве по уголовному делу // Законодательство и практика. Омск: Омская академия МВД России, 2012. № 2 (29). С. 52—55.

56. Ляпунов Ю.И., Максимов С. В. Ответственность за компьютерные преступления // Законность. 1997. № 1. С.8-15
57. Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации : автореф. дис.…д-ра. юрид. наук. Воронеж, 2001.С.14-15.
58. Осипенко А.Л., Гайдин А.И. Правовое регулирование и тактические особенности изъятия электронных носителей информации// Вестник Воронежского института МВД России. - 2014 - № 1. – С.1-15.
59. Ошлыкова Е.А. Особенности расследования незаконного сбыта наркотических средств совершаемого бесконтактным способом с использованием сети и интернет // Гражданское общество и правовое государство. – 2015. - №2. – С.121-123.
60. Родивилин И.П., Шаевич А.А. Об участии специалиста при изъятии электронных носителей информации в ходе производства обыска и выемки // Криминалистика: вчера, сегодня, завтра: сборник научных трудов. — Иркутск: ВСИ МВД России, 2013. — № 3. — С. 153—157.
61. Россинская Е.Р., Усов А.И. Судебная компьютерно-техническая экспертиза. – М.: Право и закон, 2001. С.14-15
62. Старичков М.В. Тактика проведения обыска, связанного с изъятием носителей компьютерной информации // Криминалистика: актуальные вопросы теории и практики: сборник седьмой Всероссийской научно-практической конференции. — Ростов-на-Дону: РЮИ МВД России, 2010. — С. 167—169.
63. Сухаренко А. Анонимов выведут из тени // эж-Юрист. – 2014. – №23. С.21-29.
64. Хахановский В. В международном научно-практическом правовом журнале: «Закон и жизнь».. Компьютерная информация как особенные фактические данные в уголовном процессе. №13. 2013. С. 50-52.

65. Хацук Ж.В. Электронные доказательства в судебном процессе. // Вестник Гродненского государственного университета им. Янки Купалы. 2014. С.37-46.

Интернет ресурсы:

66. Главное управление МВД России по Красноярскому краю, Управление по контролю за оборотом наркотиков. [Электронный ресурс]. https://24.мвд.рф/04/21/17/.
67. Понятие правового режима информации. [Электронный ресурс]. // URL: http://jurkom74.ru/materialy-dlia-ucheby/poniatie-pravovogo-rezhima-informatcii / (дата обращения 13.05.2017)
68. Прослушки в России: опытная бригада монтажников посадит в тюрьму // Новая газета. - 2013. 2 июля. [Электронный ресурс]. URL: http: //www. novayagazeta. ru/ inquests/ 2863.html /04/13/17/.
69. Правовой режим персональных данных [Электронный ресурс]. http // jurkom 74. ru /04/27/17/.
70. Уточнён порядок изъятия и возвращения электронных носителей в ходе расследования уголовных дел. [Электронный ресурс]. URL: http://www.kremlin.ru/news/16111./04/12/17/.
71. Исследование GfK: Тенденции развития Интернет-аудитории в России [Электронный ресурс]. URL: http://www.gfk.com/ru/insaity/press-release/issledovanie-gfk-tendencii-razvitija-internet-auditorii-v-rossii.
72. Решение Девятого арбитражного апелляционного суда от 19.09.2013 г. по делу № А40-56844/2013 // [Электронный ресурс] URL: http://sudact.ru/arbitral/doc/s4ftfYdcxa5O/.
73. Решение по делу 1-271/2014 [Электронный ресурс]. URL: //http://rospravosudie.com/court-norilskij-gorodskoj-sud-krasnoyarskij-kraj-s/act-480133707/.

74. Относимость, допустимость, и достоверность доказательства в уголовном процессе [Электронный ресурс]. //URL:// http://knigi.link/page/otcenka-dokazatelstv/ist/ist-15--idz-ax259--nf-5.html
75. Оценка доказательств [Электронный ресурс]. URL:// http://www.zonazakona.ru/law/comments/art/14289/.
76. Голубев В.А. Компьютерная информация как доказательство по уголовному делу [Электронный ресурс]. URL: http://www.crime-reseach.org/library/Golu_UPK.html.

Эмпирические материалы:

77. Уголовное дело №23224271 по обвинению Ш. в совершении преступлений, предусмотренных: ч.3 ст.30, п. «а», «г» ч.4 ст.228.1 УК РФ, ч.1 ст.30, п. «а», «г» ч.4 ст.228.1 УК РФ, ч.3 ст.30, п. «а», «г» ч.4 ст.228.1 УК РФ,ч.3 ст.30, ч.5 ст.228.1 УК РФ, ч.1 ст.30, ч.5 ст.228.1 УК РФ, ч.1 ст.174.1 УК РФ направлено заместителю прокурора г. Норильска 25 июня 2014 года.
78. Уголовное дело № 20132800125 по обвинению Ш. в совершении преступления, предусмотренного ч.1 ст. 226.1 УК РФ, направленное прокурору г. Пскова 22 мая 2013 г.
79. Уголовное дело № 25718 по обвинению гр. А. в совершении преступлений, предусмотренных ч. 2 ст. 228, п. «г» ч. 3 ст. 228.1, п. «г» ст. 228.1, ст. 30, п. «г» ч. 3 ст. 228.1 УК РФ; гр. Г. в совершении преступлений, предусмотренных ч. 2 ст. 228, ч. 5 ст. 33, ч. 2 ст. 228, п. «г» ч. 3 ст. 228.1, ч. 1 ст. 30, п. «г» ч. 3 ст. 228.1 , ч. 2 ст. 228 УК РФ, направленное 11 марта 2013 г. заместителю прокурора г. Обь Новосибирской области.
80. Уголовное дело №1040038009753 из архива отдела полиции №2 МУ МВД РФ г. Красноярска "Красноярское".
81. Апелляционное определение № 22-4172/2013 от 20 июня 2013 г. по делу № 22-4172/2013// [Электронный ресурс]. URL: http://www.gcourts.ru/case/14090650.