Оконенко Роман Иванович. "Электронные доказательства" и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации: диссертация ... кандидата Юридических наук: 12.00.09 / Оконенко Роман Иванович;[Место защиты: Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)], 2016

**Содержание к диссертации**

Введение

**1 .«Электронные доказательства»: общие положения 15**

1.1. «Электронные доказательства» как новый объект исследования российской уголовно-процессуальной науки 15

1.2. Электронные носители информации в УПК РФ 35

1.3.«Электронные доказательства» в законодательстве и судебной практике США 42

1.4. Правовая характеристика «электронных доказательств» в рамках юридической доктрины США 57

**2. Проблемы обеспечения права граждан на тайну личной жизни при производстве обыска и осмотра компьютера 65**

2.1.Доктрины «разумных ожиданий» и «видного места» как критерии невмешательства в личную жизнь граждан США 65

2.2. Проблемы, возникающие в практике судов США при обыске и изъятии «электронных доказательств» 71

2.3.Осмотр компьютера как следственное действие, ограничивающее права граждан РФ наличную и семейную тайну 84

**3. «Электронные доказательства» и проблемы обеспечения права граждан на тайну личной жизни при личном обыске задержанного 100**

3.1. Изъятие портативных электронных устройств в ходе обыска, вытекающего из правомерного ареста, в праве США 100

3.2. Совершенствование предусмотренной УПК РФ процедуры личного обыска 117

Заключение 138

Список условный обозначений 148

Список литературы

**Введение к работе**

**Актуальность** **темы** **диссертационного** **исследования.**

Законодательное определение понятия «электронного доказательства»  
отсутствует в УПК РФ, и данный термин пока используется только в научной  
литературе. Однако необходимость исследования «электронного

доказательства» и правового регулирования этого нового явления  
обусловлена реальными потребностями практики, которая все чаще  
использует в доказывании информацию, полученную из электронных  
источников. Интерес представляет зарубежный опыт, в частности  
законодательный и правоприменительный опыт США, где данное  
юридическое явление возникло раньше и к настоящему времени уже  
представляет собой активно развивающийся отдельный институт

доказательственного права.

Роль и значение информационных технологий для существующих  
общественных отношений, в том числе и уголовно-процессуальных  
правоотношений, достаточно велика и постоянно возрастает. Граждане и  
организации в своей повседневной деятельности активно пользуются  
различными электронными носителями информации. Такое использование  
связано с хранением, передачей, переработкой и иными видами  
использования сведений, составляющих ту или иную тайну, охраняемую  
законом, в том числе частной жизни человека. Особую значимость проблема  
обеспечения права на защиту тайны личной жизни приобретает в сфере  
уголовно-процессуального права, где органы государственной власти  
наделены наиболее широкими полномочиями. Главная опасность при  
исследовании электронных носителей информации в уголовном

судопроизводстве состоит в том, что субъекты, ведущие процесс, получают неограниченный доступ к информации, имеющейся на электронных

носителях, что может существенно нарушать право на защиту тайны личной жизни.

При этом наиболее значительно право на защиту тайны личной жизни владельцев электронных носителей информации ограничивается при проведении следственного осмотра и обыска, в рамках которых любой электронный носитель, используемый гражданином, становится средством точной и подробной фиксации его жизнедеятельности, может содержать, помимо информации о преступлении, значительное число сведений, не имеющих значения для уголовного дела, которые лицо считает целесообразным или уместным сохранить в тайне от широкого круга лиц.

В то же время уголовно-процессуальное законодательство Российской Федерации регулирует деятельность по исследованию электронных носителей информации на основании правил, разработанных до появления современных информационных технологий, которые не учитывают специфики «электронных доказательств», в том числе в контексте обеспечения прав граждан на защиту тайны личной жизни.

Актуальность настоящего исследования определяется широким внедрением информационных технологий в жизнь граждан при отсутствии в уголовном процессуальном законодательстве специальных процессуальных гарантий прав владельцев электронных носителей информации на защиту тайны личной жизни, в то время как необходимость выработки указанных гарантий предопределена реальными потребностями общества и юридически значимыми особенностями электронных носителей информации.

**Степень** **разработанности** **темы** **исследования.** Изучение

«электронных доказательств» в контексте проблем обеспечения прав граждан на защиту тайны личной жизни не было предметом самостоятельного монографического исследования отечественных правоведов. Существуют работы, посвященные общим вопросам использования в доказательственной деятельности сведений, выраженных в электронной форме. Первоначально данные исследования проводились специалистами в области гражданско-

процессуального и арбитражно-процессуального права: М.В. Гореловым, М.А. Митрофановой в форме кандидатских диссертационных исследований. Проблемам использования компьютерной информации в гражданском и уголовном процессе посвящено диссертационное исследование С.П. Ворожбит. Вопрос отнесения компьютерной информации к отдельному виду доказательств в уголовном процессе изучался в кандидатских диссертациях А.В. Кудрявцевой, Н.А. Зигуры и нашел отражение в вышедшей позднее монографии указанных авторов.

Отдельным аспектам использования компьютерной информации и работы с электронными носителями информации в уголовном процессе посвящены работы В.Б. Вехова, С.В. Зуева, С.П. Кушниренко, Е.И. Панфиловой, Ю.Н. Соколова.

В США проблемой обеспечения прав граждан на защиту тайны личной жизни при исследовании и изъятии электронных носителей информации занимается целый ряд правоведов, среди которых Patrick Brown, Ray Ming Chang, Adam Gershowitz, Orin Kerr, Stephen Mason, Andrew Pincus, Kate Ward.

**Объектом диссертационного исследования** выступает совокупность правоотношений, возникающих между владельцем цифрового устройства и властными субъектами уголовного процесса при исследовании «электронных доказательств», когда существует угроза соблюдению права граждан на защиту тайны личной жизни.

**Предметом** **исследования** являются положения российской

уголовно-процессуальной науки об общих вопросах доказательственного  
права, правовой природе электронных носителей информации, их  
содержанию; американская правовая доктрина, изучающая проблемы  
обеспечения права на защиту тайны личной жизни владельцев электронных  
носителей информации; действующие уголовно-процессуальные

законодательства Российской Федерации и США, регулирующие

отношения по использованию электронных носителей информации, «электронных доказательств» в рамках уголовного судопроизводства;

прецедентное право США, судебная практика Российской Федерации, касающаяся случаев обнаружения, изъятия и исследования электронных носителей информации в контексте конкретных ситуаций.

**Цель работы** заключается в выработке научных положений по  
вопросам использования электронных носителей информации в

доказательственной деятельности по уголовному делу, а также в разработке предложений по совершенствованию процедур осмотра и обыска электронных носителей информации для обеспечения прав граждан на защиту тайны личной жизни.

Для достижения означенной цели в ходе исследования были поставлены и решены следующие **задачи**:

1) проведен анализ действующего уголовно-процессуального  
законодательства Российской Федерации, регулирующего вопросы  
использования в доказывании электронных носителей информации;

2) изучены существующие в отечественной юридической науке точки  
зрения на правовую природу электронных носителей информации, их  
значение в рамках доказательственной деятельности по уголовному делу;

3) исследована правовая доктрина США на предмет определения  
термина «электронного доказательства», признаков и свойств «электронных  
доказательств»;

4) проведено сопоставление понятия электронного носителя  
информации в праве Российской Федерации и понятия «электронного  
доказательства» в праве США;

5) проведен сравнительный анализ законодательства, доктрины,  
правоприменительной практики Российской Федерации и США для  
выявления юридически значимых признаков электронных носителей  
информации;

6) выявлены основные угрозы для права владельцев электронных  
носителей информации на защиту тайны личной жизни, встречающиеся в  
отечественной и американской правоприменительных практиках;

7) определены основные инструменты обеспечения права граждан на защиту тайны личной жизни при исследовании электронных носителей информации, существующие в правовых системах Российской Федерации и США; сформулированы предложения по их совершенствованию.

**Методологической основой исследования** является концепция  
системного анализа, в рамках которой применялись такие общенаучные  
методы познания, как теоретическое моделирование, анализ и синтез,  
индукция, дедукция, функциональный подход. Также применены

частнонаучные и специальные методы: логический, историко-юридический, сравнительно-правовой, формально-юридический.

**Теоретическую основу исследования** составили труды отечественных процессуалистов по общим вопросам доказательственного права, а именно: Б.Т. Безлепкина, Ш.Р. Валиева, А.Я. Вышинского, Е.А. Доли, В.Я. Дорохова, К.Б. Калиновского, Н.М. Кипниса, В.П. Колмакова, В.М. Корнукова, П.А. Лупинской, А.В. Смирнова, М.С. Строговича, М.А. Чельцова, С.А. Шейфера; работы В.Б. Вехова, С.В. Зуева, С.П. Кушниренко, Е.И. Панфиловой, Ю.Н. Соколова, касающиеся отдельных аспектов использования электронных носителей информации в уголовном процессе; исследования С.П. Ворожбит, Н.А. Зигуры, А.В. Кудрявцевой о проблемах использования компьютерной информации в уголовно-процессуальном доказывании, а также труды американских правоведов Patrick Brown, Ray Ming Chang, Adam Gershowitz, Orin Kerr, Stephen Mason, Andrew Pincus, Kate Ward об обеспечении прав граждан на защиту тайны личной жизни при исследовании «электронных доказательств».

**Нормативно-правовую базу исследования** составляют Конституция Российской Федерации, Уголовно-процессуальный кодекс Российской Федерации, Уголовно-процессуальный кодекс Российской Советской Федеративной Социалистической Республики 1960 года, Уголовный кодекс Российской Федерации, Конституции США, Билль о правах 1791 года,

Федеральные правила о доказательствах США, Федеральные правила уголовного процесса США.

**Эмпирическую базу судебной практики** составляют определения Конституционного Суда Российской Федерации от 02 октября 2003 года № 345-О, от 8 ноября 2005 года № 439-О, определения судов субъектов Российской Федерации, в частности 77 апелляционных определений и постановлений Судебной коллегии по уголовным делам Московского городского суда по теме диссертации за период с октября 2003 года по апрель 2015 года, решения Верховного Суда США по делам “Chimel versus California” (1969), “United States versus Robinson” (1973), “Katz versus United States” (1976), “Payton versus New York” (1980), “New York versus Belton” (1981), “United States versus Ross” (1982), “Arizona versus Hicks” (1987), “California versus Greenwood” (1988), “Horton versus California” (1990); “Riley versus California” (2014), 20 решений окружных судов США по теме диссертации за период с марта 1969 года по июнь 2014 года.

**Научная новизна работы** обусловлена тем, что в ней определяются  
юридически значимые признаки электронных носителей информации в  
специфическом контексте проблем защиты тайны личной жизни через  
сопоставление и сравнительный анализ юридической науки,

законодательства и правоприменительной деятельности Российской

Федерации и Соединенных Штатов Америки.

В работе приводится ряд оригинальных предложений по

совершенствованию уголовно-процессуального законодательства Российской Федерации в области защиты тайны личной жизни с учетом изученных свойств электронных носителей информации; дается определение новым для процессуальной науки понятиям: «электронному доказательству» и «исследованию электронного доказательства»; устанавливается в каких процессуальных формах должно происходить изучение содержания электронного носителя информации в рамках существующих средств доказывания.

**Основные положения, выносимые на защиту:**

1. Под «электронным доказательством» понимается электронный носитель информации, содержащий сведения о значимых обстоятельствах по конкретному уголовному делу и обладающий следующими юридически значимыми признаками: а) значительным объемом памяти; б) простотой передачи и копирования сведений с одного электронного носителя информации на другой; в) возможностью удаленного доступа к содержанию электронного носителя и информационно-телекоммуникационным системам (в частности к сети Интернет); г) относительностью и неочевидностью содержания.
2. Исследование «электронного доказательства» – это изучение информационного содержания электронного носителя информации, связанное с совершением действий в виртуальной среде (открытием папок с файлами, самих файлов, изучением свойств файлов посредством использования иных программ и т.п.). Не может приравниваться к исследованию «электронного доказательства» внешний осмотр либо иное изучение характеристик электронного носителя информации как реального материального объекта (в частности определение его веса, размера, формы, производителя, модели, других внешних индивидуализирующих признаков).

**3.** Следует выделять два вида исследования «электронного  
доказательства». Первый вид исследования представляет собой изучение  
основного содержания файла – сведений, для хранения и воспроизводства  
которых файл создан (звук и видеозапись при открытии видеофайла, текст  
при открытии текстового файла, звук при открытии аудиофайла и т.п.).  
Второй вид исследования связан с изучением сведений, касающихся свойств  
и характеристик самого файла (о времени создания и изменения, о месте  
нахождения, о доступе к файлу и т.п.). Если значение для дела имеет только  
основное содержание файла, то обнаруженные и относящиеся к уголовному  
делу сведения необходимо процессуально оформлять в качестве такого вида  
доказательств как иной документ. Если же значение для дела имеет, наряду с

основным содержанием файла, еще и информация о его свойствах и характеристиках, то полученные относимые сведения и сам источник необходимо оформлять и приобщать к делу в качестве вещественного доказательства.

**4.** «Электронное доказательство» обладает характеристиками, которые  
могут создавать угрозу нарушения права человека на защиту тайны личной  
жизни при использовании электронных носителей информации в уголовном  
судопроизводстве. Значительный объем памяти электронного носителя  
информации предопределяет существование на нем большого числа не  
относящихся к делу сведений личного характера. Неочевидность и  
относительность содержания электронного носителя информации не  
позволяет гражданину предвидеть, какой объем данных имеется на  
изымаемом носителе. Удаленный доступ предоставляет сотрудникам  
правоохранительных органов возможность не только исследовать  
информацию, которая имеется непосредственно на электронном носителе, но  
и получать данные из информационно-телекоммуникационной сети  
Интернет или иной схожей системы, что значительно расширяет объект  
исследования и распространяет его на еще больший объем сведений о  
частной жизни. В то же время простота передачи и копирования  
информации позволяет изымать значительные объемы информации о  
частной жизни без каких-либо затруднений. Указанные признаки  
электронных носителей информации имеют существенное значение в  
контексте обеспечения законных интересов граждан по защите тайны  
частной жизни.

**5.** Изучение судебной практики свидетельствует о том, что  
исследование информационного содержания электронных носителей  
информации производится правоохранительными органами путем осмотра.  
Между тем в силу присущей «электронному доказательству» неочевидности  
содержания файлы, исследование которых необходимо произвести,  
находятся за пределами свободного доступа. Для их открытия и изучения

необходимо осуществить определенные целенаправленные поисковые действия в виртуальной среде, что может иметь место только при проведении обыска. Сравнительно-правовой анализ законодательства и практики использования «электронных доказательств» в российском уголовном судопроизводстве и судопроизводстве США показал, что неочевидность содержания электронного носителя информации делает возможным его исследование только посредством проведения активного целенаправленного поиска. Прецедентными правовыми нормами, сформулированными судами США, такой носитель информации приравнен к закрытому контейнеру, содержание которого скрыто от непосредственной видимости сотрудника полиции. В уголовном судопроизводстве для исследования электронных носителей информации и путем изучения основного содержания файлов, и путем изучения свойств и характеристик файлов должен проводиться не осмотр, а обыск.

**6.** Процессуальное законодательство следует дополнить правилом о  
возможности проведения обыска электронного носителя информации как  
отдельного следственного действия после осмотра местности, осмотра или  
обыска помещения, а также после проведения личного обыска, в рамках  
которых такой носитель был изъят.

**7.** При обнаружении электронного носителя информации в ходе  
личного обыска задержанного необходимо соблюдать определенную  
последовательность процессуальных действий. Во-первых, такое устройство  
сначала в установленном законом порядке должно быть изъято в ходе  
личного обыска как материальный объект. Во-вторых, должно быть получено  
судебное решение на обыск электронного носителя информации. В-третьих,  
должно быть произведено виртуальное исследование содержания  
соответствующего электронного носителя информации.

**8.** Из общего правила о необходимости получения судебного решения  
на исследование электронного носителя информации, обнаруженного в ходе  
личного обыска задержанного, допустимы некоторые исключения.

Проведение такого обыска без судебного решения может считаться допустимым, во-первых, в случае, когда лицо застигнуто в момент совершения очевидной противоправной операции на компьютере либо совершения действий, связанных с явно незаконными манипуляциями электронными носителями информации, а, во-вторых, когда из обстановки задержания с очевидностью следует, что ход преступления записывается на электронный носитель информации, который и предполагается изъять.

**9.** Установление в прецедентном решении Верховного Суда США  
запрета на обыск сотового телефона без судебной санкции не учитывает то,  
что при современных темпах развития информационных технологий  
постоянно появляются новые виды электронных носителей информации  
(ноутбуки, смартфоны, планшеты и т.д.), которые нельзя однозначно отнести  
к понятию «сотовый телефон». В уголовно-процессуальном праве России  
необходимо установить запрет на обыск без судебного решения не  
определенной технологии, например, сотового телефона, но любого  
электронного носителя информации, обладающего значительным объемом  
памяти и (или) способностью получать сведения посредством удаленного  
доступа (в том числе через информационно-телекоммуникационную сеть  
Интернет). Запрет на исследование «электронных доказательств» без  
судебного решения должен относиться не к определенному виду  
электронного носителя информации, на смену которому в скором времени  
может прийти другой вид, а к наличию или отсутствию у того или иного  
вида электронного носителя информации заранее определенных в законе  
признаков.

**10.** Для того чтобы «электронное доказательство» получило правовое  
закрепление и регулирование в УПК РФ как самостоятельный новый вид  
доказательства, дальнейшие исследования данной темы, учитывая  
зарубежный опыт, должны пройти ряд этапов: а) завершение научного  
изучения всех признаков и особенностей электронных носителей  
информации; б) выявление из этих признаков тех, которые имеют правовое

значение; в) формирование новых процессуальных правил обнаружения и  
изъятия электронных носителей информации и их исследования с учетом  
юридически значимых признаков. Это позволит обеспечить возможность  
использования в уголовном судопроизводстве «электронного

доказательства» не только как научной идеи, но и как самостоятельного  
института доказательственного права. Правовое закрепление и

регулирование обеспечит гарантии защиты права человека на тайну частной жизни при использовании в доказывании электронных источников информации.

**Теоретическая значимость исследования** заключается в том, что в  
нем формулируется понятие «электронного доказательства», определяются  
признаки электронных носителей информации, выявляются значимые для  
юриспруденции закономерности. Данные научные идеи могут

использоваться в качестве теоретического основания для последующих изысканий в сфере доказательственного права, использования в уголовно-процессуальной деятельности информационных технологий.

**Практическая значимость исследования** определяется тем, что его результаты могут быть использованы в следующих направлениях:

в нормотворческой деятельности для совершенствования уголовно-процессуального законодательства, обеспечения его соответствия новым тенденциям развития общества, вызванным появлением информационных технологий;

в учебно-преподавательской деятельности при подготовке лекций, проведении практических и семинарских занятий в рамках курса «Уголовный процесс»;

в правоприменительной деятельности при разработке конкретных предложений и рекомендаций относительно производства отдельных следственных действий (прежде всего, осмотра и обыска).

**Степень** **достоверности** **и** **обоснованности** **результатов**

**исследования** определяется тем, что выводы работы были получены путем

использования общепризнанных научных методов исследования, на основании системного изучения теоретических положений, нормативно-правовых актов, судебной практики Российской Федерации и США, их сопоставления по функционально схожим, корреспондирующим правовым институтам и нормам.

**Апробация результатов исследования.** Положения диссертационного исследования были обсуждены и одобрены на кафедре уголовно-процессуального права Университета имени О.Е. Кутафина (МГЮА).

Результаты исследования представлялись на международных научно-  
практических конференциях «Кутафинские чтения», прошедших в  
Университете имени О.Е. Кутафина (МГЮА), юридическом факультете  
Московского государственного университета имени М.В. Ломоносова в 2013  
и 2014 годах, на II Всероссийской научно-практической конференции  
молодых ученых и специалистов «Современная российская наука глазами  
молодых исследователей», проведенной Научно-инновационным центром г.  
Красноярска в 2012 году, и V Международной научно-практической

конференции «Современная наука: тенденции развития», организованной Научно-издательским центром «Априори» в 2013 году.

Основные положения, выводы, предложения и рекомендации, содержащиеся в диссертации, нашли свое отражение в шести научных публикациях автора в журналах и сборниках, общий объем которых составил 3 п.л.

**Структура** **диссертационного** **исследования.** Диссертационная

работа состоит из введения, трех глав, разделенных на девять параграфов, заключения, библиографического списка, включающего в себя книги, монографии, статьи российских и американских авторов, нормативно-правовые акты, судебную практику США и Российской Федерации.

## Электронные носители информации в УПК РФ

В уголовно-процессуальном праве «электронные доказательства» чаще всего относят либо к вещественным доказательствам, либо к иным документам. Некоторые исследователи указывают, что разграничение электронных носителей информации на вещественные доказательства и иные документы должно происходить по классическому для доказательственного права критерию - если значимая для дела информация определяется исходя из физических свойств и качеств объекта материального мира, то соответствующий предмет или документ необходимо приобщить к делу в качестве вещественного доказательства; если же правовое значение имеет смысловое содержание объекта, то его необходимо рассматривать в качестве иного документа20.

Согласно второй точке зрения, «электронные доказательства» представляют собой особые группы в рамках уже существующих видов доказательств, а потому должны наделяться специальным правовым статусом, учитывающим их особенности. К примеру, Ю.Н. Соколов пишет, что информация в электронной форме, выраженная в виде вещественного доказательства, обладает определенной спецификой - доказательственное значение здесь имеет не сам материальный носитель, но та информация, которая на нем содержится. В связи с этим он предлагает отдельно включить в ст. 81 УПК РФ указание на то, что вещественным доказательством может признаваться также информация в электронном виде, которая служила орудием преступления или сохранила на себе следы преступления, либо на которую были направлены преступные действия21.

Третья точка зрения предполагает, что электронные данные - это совершенно новый вид доказательств наряду с другими, обозначенными в ч. 4 ст. 74 УПК РФ. В обоснование своей позиции авторы приводят ряд признаков, отграничивающих компьютерную информацию от иных видов доказательств. Так, при сопоставлении компьютерной информации и иных документов указывается на следующее.

Прежде всего, отмечают исследователи, компьютерная информация создается программой, а документ - непосредственно человеком. Во-вторых, документ выполняется на определенном материальном носителе, компьютерная информация же выполнена посредством совокупности команд, записанных в память того или иного устройства, в связи с чем она может быть скопирована на другой материальный носитель без потери своей информативности. Наконец, в отличие от документа, компьютерная информация может быть воспроизведена только при помощи соответствующего электронного устройства, в то время как документ доступен непосредственному восприятию человеком.

Отграничивая компьютерную информацию от вещественных доказательств, исследователи указывают на то, что доказательственную ценность имеет содержание информации, записанной на материальный носитель, а не свойства этого материального носителя. Верно и обратное - внешний вид материального носителя, его форма, размеры, специфические признаки и свойства никак не влияют на содержание тех сведений, которые на нем записаны. Второе существенное отличие авторы видят в механизме образования данного вида доказательства. Если вещественное доказательство представляет собой предмет, свойства которого предопределены простым физическим взаимодействием между предметами материального мира, то компьютерная информация формируется не путем отражения одного объекта через другой, а через алгоритм программы, заданный разработчиком. Кроме того, вещественное доказательство, как и документ, доступно непосредственному восприятию органами чувств человека, в то время как компьютерная информация может быть воспроизведена лишь опосредованно через специально предназначенное для этого устройство.

С учетом этих различий указанные исследователи делают вывод о необходимости введения в процесс особого вида доказательств - компьютерной информации23.

Несмотря на то, что Н.А. Зигура и А.В. Кудрявцева обстоятельно мотивировали свою позицию, она представляется спорной.

Прежде всего, это касается утверждения о том, что свойства материального носителя электронной информации не представляют для участников процесса какой-либо ценности, а его размеры и форма не имеют какого-либо значения для дела. Действительно, компьютерные диски, дискеты после записи на них той или иной информации не меняют свою форму, размеры и иные видимые свойства, однако это вовсе не означает, что после записи с ними не произошло никаких физических изменений. Теория отражения, составляющая и сегодня прочную основу учения о доказательствах, базируется на утверждении о том, что «без материальной формы информация не может существовать, перерабатываться и передаваться»24. Очевидно, что и на электронном носителе сведения не могут существовать сами по себе, но воспроизводятся путем считывания микроскопических механических либо магнитных изменений на поверхности диска25. Таким образом, если учитывать микроскопические механические или магнитные изменения, то диск при записи на него информации меняет свои свойства, хотя и не столь значительно, чтобы это было заметно человеку без специальных устройств.

## Правовая характеристика «электронных доказательств» в рамках юридической доктрины США

Несмотря на изложенное, практика идет по другому пути, о чем свидетельствуют многочисленные криминалистические рекомендации, в том числе разработанные научными институтами при правоохранительных органах, согласно одной из которых, «приступая к осмотру компьютера, следователь и специалист, который должен непосредственно производить все действия, должны придерживаться следующих рекомендаций: перед выключением питания по возможности закрыть все используемые на компьютере программы; ...принять меры к установлению пароля доступа в защищенных программах; при активном вмешательстве сотрудников предприятия, пытающихся оказать противодействие следственной группе, отключить питание всех компьютеров на объекте, опечатать их и изъять вместе с магнитными носителями для изучения информации в спокойной обстановке; ...изымать следует все компьютеры (системные блоки) и магнитные носители; при осмотре документов следует обратить особое внимание на рабочие записи операторов ЭВМ, т.к. часто именно в этих записях неопытных пользователей можно обнаружить коды, пароли и другую очень ценную для следствия информацию»127.

Столь наступательный характер приведенных тактических предложений вполне объясним, ведь, производя осмотр компьютера, должностные лица стремятся решить сразу две задачи, во-первых, избавляют себя от необходимости выполнять дополнительные процессуальные правила, а, во-вторых, получают огромный массив информации о совершенном преступлении. Соответствие способов получения таких сведений целям минимально возможного вторжения в частную жизнь граждан или деятельность организации, как видно из текста рекомендации, не является здесь приоритетом.

При этом, если в одних случаях производство осмотра вместо обыска позволяет обойти не столь значительные процессуальные гарантии, то, к примеру, при исследовании компьютера в ходе осмотра жилища следователь уже пренебрегает процедурой получения судебной санкции на обыск, что существенным образом снижает уровень защищенности личности перед органами публичного преследования.

Не будем забывать и о том, что ч. 91 ст. 182 УПК РФ предполагает при обыске электронных носителей информации, во-первых, обязательное участие специалиста, а во-вторых, возможность копирования изымаемой информации для ее владельца. Производя осмотр, правила проведения которого не устанавливают таких гарантий, следователь лишает граждан права на получение копии изымаемой информации и сужает круг обязательных участников следственного действия.

Таким образом, пользуясь отсутствием четких, обозначенных в законе границ между осмотром и обыском, правоохранительные органы, по сути, сами оценивая свои действия как осмотр, фактически производят обыск.

Действительно, различая осмотр и обыск лишь по характеру и цели поиска, мы попадаем в ситуацию, когда разграничение процессуальных действий происходит не по юридическим, а по криминалистическим и иным критериям. Наиболее показателен здесь пример с разграничением следов преступления от предметов и документов.

Как уже было отмечено, даже в физической реальности те или иные объекты трудно классифицировать только как предмет или только как след. В информационной среде данное разграничение становится еще более оценочным, нечетким и зависящим от субъективных предпочтений. Так, в криминалистической литературе появилось представление о виртуальной среде как следообразущей поверхности или как об особом месте преступления128.

Данная точка зрения довольно интересна, потому что многие преступления, например, хищение денежных средств со счетов кредитных организаций по сети Интернет, по сути, «совершаются в компьютере», и искать их следы в физическом мире неэффективно. В указанном криминалистическом контексте специалистам удобно проводить аналогию между физическим местом и информационной системой. Однако, придавая таким рассуждениям юридическое значение, мы можем получить неожиданные и весьма сомнительные результаты: ведь если правоприменители начнут ассоциировать компьютер не с предметом, не с хранилищем предметов (как и в американском праве), но с местом со следами преступления и, исходя из этого, принимать юридически значимые решения, то уровень правовой защищенности граждан в области сохранности персональных данных нельзя будет назвать высоким, так как, во-первых, это будет означать возможность производства осмотра компьютера, а во-вторых, позволит правомерно проникнуть на другой компьютер или сервер и исследовать всю информацию уже на нем, ведь ничто не ограничивает следователя при осмотре места происшествия в изучении прилегающих территорий. В результате мы можем получить ситуацию, когда для вскрытия запертого ящика стола сотрудник правоохранительного органа должен будет провести обыск, а для взлома и исследования целой компьютерной сети - осмотр, то есть следственное действие, которое может быть произведено без вынесения отдельного постановления и других значимых процессуальных гарантий, характерных для обыска.

Указанные рассуждения наглядно демонстрируют, к чему может привести попытка разграничения юридических явлений (в данном случае следственных действий) по криминалистическим основаниям, особенно в случае, когда речь идет о сложных технологических устройствах, принцип работы которых основан на множестве физических, кибернетических, информационных закономерностей. К таким ситуациям неприменимы условные и неточные внеправовые формулировки, напротив, здесь необходимо полагаться только на выверенные юридические концепции, к которым можно отнести право граждан на защиту тайны личной жизни, имеющее свою историю, появившееся и значительно развившееся именно в юридической системе США129.

Исходя из изложенного, приходим к выводу о том, что исследование компьютера необходимо осуществлять в форме обыска, а в случае его нахождения в жилище - только на основании судебного решения. Иное противоречит Конституции Российской Федерации, не основано на нормах УПК РФ, не согласуется с историей эволюции правовых гарантий в области неприкосновенности частной жизни, выраженной в американском стандарте «видного места».

## Проблемы, возникающие в практике судов США при обыске и изъятии «электронных доказательств»

С учетом отграничения производства осмотра от обыска, сделанного в предыдущей главе настоящей работы, представляется, что осмотр предмета может сопровождаться только обозрением внешних его габаритов и свойств, в том числе посредством применения средств криминалистической техники. В то же время изучение содержания таких объектов возможно в случае, если они были открыты или вскрыты при проведении обыска, а в ходе проведения осмотра уже выявленное содержание контейнера подлежит лишь более внимательному и тщательному описанию. При этом не может быть признан правомерным осмотр предмета, если он сопровождается его открытием, нарушением конструктивной целостности в случае, когда в рамках следственного действия, при проведении которого он был обнаружен, такие виды обследования не имели места. Иными словами, если при проведении обыска следователь изымает из жилища подозреваемого сейф, который не вскрывается, а потом производит его вскрытие в ходе осмотра предмета, то тем самым он фактически превращает осмотр предмета в его обыск. Также обстоит дело и с чемоданом, который нельзя открывать при осмотре, если только он не был открыт при проведении личного обыска. Верно и другое - любой контейнер или хранилище, изъятые в рамках осмотра, вообще не могут быть открыты или вскрыты, так как первоначальный осмотр такого вскрытия не предполагает, а возможность проведения обыска отдельных предметов УПК РФ не предусмотрена.

Данные утверждения представляются логичными, ведь не может же следователь, осмотрев контейнер без права его открытия, получить такое право путем составления отдельного протокола осмотра. Также и лицо, производящее обыск и не открывшее соответствующий предмет, будь то сумка или портфель, не может сделать этого в рамках последующего осмотра, который представляет собой следственное действие по обследованию внешних свойств того или иного объекта.

Сказанное имеет важное значение для отграничения сферы личного обыска электронного носителя информации. Следуя указанной логике, такое доказательство может быть исследовано в ходе осмотра предмета только в том объеме, в каком оно было исследовано при проведении личного обыска. Это позволяет говорить о том, что правила производства обыска, установленные в УПК РФ, необходимо доработать путем включения, помимо осмотра, еще и процедуры обыска отдельного предмета или электронного устройства. Такое нововведение позволит правоохранительным органам производить обследование соответствующих объектов, используя для этого процессуальный режим, соответствующий степени их вторжения в личную жизнь гражданина, в отличие от сегодняшней практики исследования цифровых устройств посредством осмотра.

Помимо включения в УПК РФ процедуры обыска предмета (в том числе сотового телефона) немаловажным остается вопрос о том, необходимо ли получение судебной санкции для исследования содержания портативного цифрового устройства. Как было изложено в предыдущем параграфе, американское право после череды судебных дел, где сотовый телефон был отождествлен с обычным контейнером, наконец признало, что для его обыска требуется получение судебного ордера.

В отечественном законодательстве и правоприменительной практике не все настолько однозначно.

Так, ч. 2 ст. 29 УПК РФ содержит перечень случаев, когда следователю или дознавателю необходимо получение судебного решения для проведения следственного либо иного процессуального действия. Применительно к осмотру и обыску санкция органа правосудия должна быть получена, когда производится личный обыск (за исключением личного обыска задержанного в порядке ст.ст. 91-92 УПК РФ), обыск в жилище, осмотр жилища при отсутствии согласия проживающих в нем лиц либо осмотр корреспонденции в учреждениях связи. При этом в указанном перечне отсутствует указание на такое следственное действие, как осмотр телефона, что породило случаи осмотра цифрового устройства без получения судебного решения.

Следует признать, что в основе обозначенной практики лежат понятные суждения. Как уже было сказано, ч. 2 ст. 29 УПК РФ не содержит требования о предварительном санкционировании осмотра телефона, в то время как исследование портативного цифрового устройства также нельзя назвать ни контролем и записью телефонных переговоров, ни выемкой предметов и документов, содержащих государственную или иную охраняемую федеральным законом тайну, ни даже получением информации о соединениях между абонентами и (или) абонентскими устройствами (поскольку последнее представляет собой специфическое процессуальное действие, регламентированное ст. 1861 УПК РФ и предполагающее участие организации связи). В итоге, осмотр телефона, который по уровню вторжения органов уголовного преследования в личную жизнь граждан сравним с процедурами, изложенными в ч. 2 ст. 29 УПК РФ, оставлен без какого-либо упоминания в положении процессуального закона, очерчивающем круг следственных действий, которые должны быть санкционированы судом.

В то же время ,согласно ст. 13 УПК РФ, ограничение права гражданина на тайну переписки, телефонных и иных переговоров, почтовых, телеграфных и иных сообщений допускается только на основании судебного решения.

Анализируя содержание данной нормы, нетрудно заметить, что она, во-первых, является более общей по отношению к иным нормам УПК РФ, в том числе ч. 2 ст. 29, во-вторых, говорит о безусловности получения судебного решения применительно к любым переговорам и сообщениям, безотносительно к технологии передачи данных либо виду следственного действия, и наконец, в Кассационное определение Судебной коллегии по уголовным делам третьих, основана на ст. 23 Конституции Российской Федерации, что предопределяет ее особую значимость.

Учитывая изложенное, можно утверждать, что осмотр сотового телефона в рамках отечественного уголовно-процессуального права все-таки подлежит предварительному судебному контролю, несмотря на игнорирование данного следственного действия частью 2 статьи 29 УПК РФ.

В обоснование данного утверждения можно сослаться на Определение Конституционного Суда Российской Федерации от 02 октября 2003 года № 345-0, согласно которому: «...информацией, составляющей охраняемую Конституцией Российской Федерации и действующими на территории Российской Федерации законами тайну телефонных переговоров, считаются любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью телефонной аппаратуры, включая данные о входящих и исходящих сигналах соединения телефонных аппаратов конкретных пользователей связи; для доступа к указанным сведениям органам, осуществляющим оперативно-розыскную деятельность, необходимо получение судебного решения»1

## Совершенствование предусмотренной УПК РФ процедуры личного обыска

Отличие же третьей группы преступлений от второй состоит только в том, что использование цифровых устройств при реализации объективной стороны их состава становится не просто возможным, но обязательным, обусловленным конструкцией соответствующей нормы уголовного закона.

Таким образом, собирание «электронных доказательств» в ходе личного обыска может быть полезным при расследовании любого деяния, запрещенного уголовным законом, разница заключается лишь в характере получаемой информации и большей или меньшей вероятности обнаружить следы преступления при обследовании цифровых устройств.

В этой связи стоит заметить, что установление правила судебного санкционирования обыска портативного компьютерного устройства, обнаруженного при задержанном, применительно к первым двум группам преступлений выглядит оправданным, поскольку они могут быть совершены без использования информационных технологий.

Относительно же третьей группы - преступлений в сфере компьютерной информации подобная мера представляется не вполне разумной. Так как конструкция состава указанных противоправных деяний с необходимостью предполагает использование всевозможных информационных технологий, то вероятность нахождения доказательств в цифровых устройствах обыскиваемого существенно возрастает.

Обратим внимание и на тот факт, что ч. 1 ст. 91 УПК РФ предполагает обнаружение явных следов преступления (п. 1) либо очевидной пространственной связи преступления и лица его совершившего (п. 2). Несомненно и то, что такие следы, связи, по смыслу указанного положения закона, должны проявляться в физической реальности, быть доступны для непосредственного наблюдения сотрудника правоохранительного органа.

Понятие «след» в данном контексте требует отдельного пояснения. Так, если для обычных преступлений под его «следами» могут пониматься результаты различных физических, химических процессов, а также предметы, указывающие на противоправную активность, то для компьютерных преступлений «следами» могут быть только строго определенные явления. Если любое компьютерное преступление представляет собой не что иное, как совокупность электронно-вычислительных операций, то и наиболее явным его внешним проявлением может быть только выведение процесса и результатов таких операций через специальные элементы компьютера в форме доступной для непосредственного восприятия человека информации (например, отображение процедуры уничтожения файлов на мониторе). Представляется, что только производство на глазах у полицейского или очевидцев электронно-вычислительной операции, носящей явно преступный характер, может быть самым бесспорным основанием к задержанию того или иного лица. Вместе с тем представляется возможным задержать лицо не только тогда, когда оно инициирует ту или иную операцию, но и когда его виртуальная активность остается вне поля зрения, в то время как физические действия прямо указывают на совершение противоправной компьютерной операции. К примеру, за противозаконный доступ к компьютерной информации лицо может быть задержано как в случае, если кто-либо увидит его противозаконные действия по копированию определенных данных на мониторе устройства, так и когда будут заметны лишь действия по подключению к охраняемому компьютеру внешнего электронного носителя информации.

Говоря об основаниях задержания относительно преступлений, совершаемых в виртуальной среде, необходимо отметить, что сам по себе факт наблюдения компьютерной операции не может быть достаточен для этого, так как, по смыслу ст. 91 УПК РФ, никто не может получить основания для задержания преступника, наблюдая исключительно за работой того или иного компьютера, без очевидной связи виртуальной активности с конкретным человеком. Иными словами, для задержания необходимо либо увидеть операцию по использованию цифрового устройства конкретным человеком, либо наблюдать лицо в непосредственной близости от устройства, в информационной сфере которого происходит противозаконная активность (например, работа вредоносной программы). Часть 1 ст. 91 УПК РФ в качестве одного из оснований указывает также сообщения очевидцев и (или) потерпевших, однако представляется, что они также могут наблюдать лишь операции конкретного человека с определенным цифровым устройством.

Учитывая, что конструкция ч. 1 ст. 91 УПК РФ применительно к компьютерным преступлениям, как было показано, уполномочивает провести задержание только при наблюдении выполнения лицом операций с использованием конкретных цифровых устройств, ограничение полиции в полномочии на немедленное исследование таких устройств выглядит излишним. Например, если пользователь того или иного электронного устройства (в частности, планшета, смартфона) был задержан при подключении к локальной сети для активации вредоносного программного обеспечения, у представителей правоохранительных органов может возникнуть реальная потребность в срочном обыске данного цифрового устройства, и лишать их такого права было бы неразумным.

Кроме того, необходимо учитывать, что информация о компьютерном преступлении может храниться только в электронном виде, а раз так, то абсолютный запрет на обыск портативного цифрового устройства, по сути, полностью лишает полицию возможности оперативно получить сведения о совершенном преступлении.

Таким образом, в то время как при расследовании противозаконных действий, которые совершаются либо могут быть совершены в физической реальности, обследование персональных цифровых устройств неоправданно расширяет полномочия органов публичного преследования, применительно к задержанию подозреваемого в совершении компьютерного преступления данная мера, напротив, представляется разумной, учитывающей их специфику.