6. КРИМИНАЛИСТИКА, СУДЕБНО-ЭКСПЕРТНАЯ ДЕЯТЕЛЬНОСТЬ; ОПЕРАТИВНО-РОЗЫСКНАЯ ДЕЯТЕЛЬНОСТЬ

6.1. ОСОБЕННОСТИ ИЗЪЯТИЯ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ ПО УГОЛОВНЫМ ДЕЛАМ

Сергеев М. С., аспирант кафедры уголовного процесса и криминалистики юридического факультета

Место учебы: Казанский (Приволжский) Федеральный Университет

sergeev.s.maksim@gmail.com

Муратов К. Д. Должность: канд. юрид. наук, ассистент кафедры уголовного процесса и криминалистики юридического факультета

Место работы: Казанский (Приволжский) Федеральный Университет

Аннотация: В научной статье рассматриваются актуальные вопросы и проблемы уголовно-процессуального права в сфере изъятия электронных доказательств. Раскрыт правовой статус электронных доказательств, особенности процедуры выемки электронных доказательств, юридическая природа и необходимость участия специалиста в следственных действиях. Проанализированы также такие процессуальные действия как «Получение информации о соединениях между абонентами и (или) абонентскими устройствами», «Наложение ареста на почтово-телеграфные отправления, их осмотр и выемка», «Контроль и запись переговоров». По результатам исследования выработаны предложения по внесению изменений в уголовно-процессуальное законодательство.

Ключевые слова: электронные доказательства, выемка, изъятие, контроль и запись переговоров, участие специалиста

FEATURES OF SEIZURE OF DIGITAL EVIDENCES IN CRIMINAL CASES

Sergeev M. S., postgraduate student at the Criminal procedure and criminalistics department

Study place: Kazan Federal University

sergeev.s.maksim@gmail.com

Muratov K. D., Candidate of Law Sciences, Associate Professor at the Criminal procedure and criminalistics department

Work place: Kazan Federal University

Annotation: In research examined topical issues and criminal procedure law problems of seizure of digital evidences. Disclosed a digital evidences legal status, legal nature, features of the procedure of seizure and mandatory participation of specialists in investigation actions. Also was analyzed procedural actions such as "Obtaining connection details information between subscribers and (or) subscriber devices", "Seizure and examination of postal and telegraph dispatches", "Control and record of the talks". By results of research authors proposed the amendments to the criminal procedure law

Keywords: digital evidences, seizure, record of voice call, participation of specialists in the criminal investigations

В Докладе Уполномоченного по правам человека в Российской Федерации от 21 февраля 2014 г. Лукин В.П. отметил необходимость разработки эффективного механизма судебной защиты права на достоинство личности, имущества, персональных данных и других прав, которые могут быть нарушены в ходе дознания и следствия[1]. Это касается и следственных действий, сопровождающихся изъятием имущества, предметов, документов (в том числе и на электронных носителях), персональных данных и др. К наиболее распространенным следственным действиям такого рода относится выемка (ст.183 УПК РФ), правовыми последствиями которой являются: изъятие и признание предметов и документов вещественными доказательствами, соблюдение процедуры их хранения, уничтожения, реализации или возвращения законным владельцам; передача предметов и документов в порядке международного сотрудничества в сфере уголовного судопроизводства[2].

В настоящее время возникают проблемы правоприменения уголовно-процессуального законодательства в сфере изъятия электронных источников доказательств.

Важность проблемы обусловлена повсеместным использованием электронных средств связи, хранения информации в быту и как следствие важность таких предметов в качестве доказательств уголовном судопроизводстве.

Внесенными Федеральным законом от 28 июля 2012 года «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» поправками в УПК РФ вводится понятие «электронные носители информации» в качестве отдельного вида вещественного доказательства.

Электронный носитель информации - это материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники[3]. В связи с тем, что использование технологий растет в геометрической прогрессии, преступления против конфиденциальности, целостности и доступности целевых компьютерных систем становятся все более распространенными. Количество правонарушений, совершенных с помощью компьютерных систем, таких как мошенничество, детская порнография и преступления против интеллектуальной собственности, стремительно растет. Кроме того, работа сотрудников правоохранительных органов включает в себя подтверждение и сбор доказательств в электронной форме в отношении любого преступления[4]. В связи с глобальной информатизацией общества и как следствие появление новых видов преступлений, способов их со-

[1] [Электронный ресурс] URL: http://ombudsmanrf.org/ - дата посещения 01.01.2015.

[2] Муратов К.Д. Сущность, значение и правовые последствия выемки по уголовным делам: монография//Муратова К.Д. – Москва: Изд-во «Юрлитинформ», 2013.

[3] Единая система конструкторской документации. Электронные документы. Общие положения. ГОСТ 2.051-2006 - [Электронный ресурс] URL: http://vsegost.com/Catalog/42/4288.shtml- дата посещения 15.01.2015.

[4] «Стратегия обучения сотрудников правоохранительных органов. Выдержки из докладов страна Восточного партнерства»// Совет 2014 – 8 июля [Электронный ресурс] URL: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_project_eap/Chisinau_International_Conference_Nov2014/EAP_Chisinau_WS.asp

...ении все чаще возникает необходимость изъятия в ... процессуальных следственных действий таких ...метов, как электронные носители информации, ко... зачастую содержат важную для расследования ...мацию. Изъятие данного типа доказательство в ... обыска и выемки регламентировано ч. 9.1. ст. 182 ... РФ и ч.3.1. ст. 183 УПК РФ, с учетом положений ч.4 ..., ч.5 ст.82 УПК РФ.

...емка – следственное действие, предусмотренное ст. ... УПК РФ, целью которого является изъятие опреде...ных предметов, документов имеющих значение для ... В отличие от другого следственного действия – ...ыска, при производстве выемки заранее известен ха...ктер изымаемых предметов и место их хранения. Изъ...тие предметов возможно как путем добровольной вы...чи, так и принудительно (ч.5 ст.183 УПК РФ).

...лучить в полной мере и провести осмотр электронных ...точников доказательств на месте, чаще всего, не пред...тавляется возможным, в связи с этим возникает необ...ходимость изъятия данного вида источника доказа...тельств (изымают и компьютер, и флеш-карты, и диски, и ...бильные устройства, и файлы из памяти компьютера, ...информацию о вхождении в телекоммуникационную ...стему Интернет, и информацию с определенных Сай...тов из социальных сетей Интернет). Необходимым усло...вием при изъятии электронных носителей информации ...ляется участие специалиста. Согласно ч. 1 ст. 58 УПК ... специалист – это лицо, обладающее специальными ...ниями, привлекаемое к участию в процессуальных ...йствиях в порядке, установленном УПК РФ, для содей...ствия в обнаружении, закреплении и изъятии предметов ... документов, применении технических средств в иссле...довании материалов уголовного дела. Данное требова...ние, установленное законодателем, обеспечивает со...блюдение законных прав и интересов владельцев и об...ладателей информации, а также, учитывая техническую ...ложность процессуального действия по изъятию элек...тронной информации, позволяет в полной мере собрать ...ажные для расследования доказательства, обеспечить ...х правильное хранение.

Законодатель закрепил в ст.ст.182 и 183 УПК РФ необ...ходимость обязательного участия специалиста в след...ственных действиях – обыск и выемка, в ходе которых ...пециалист производит копирование информации на ...лектронном носителе информации. В связи с этим мож...но предположить, что обязательность участия специали...ста связана с рядом процедурных моментов:

1) необходимость произвести копирование информа...ции;

2) обнаружение необходимых файлов и их демонстра...ция в различных форматах (Word, Excel) в случае ходатайства об этом;

3) осмотр и выемка информации с телекоммуникаци...онных сайтов сети Интернет, их копирование;

4) осмотр и выемка электронной почты с конкретного компьютера.

Судебная практика касающаяся жалоб на отсутствие специалиста при выемке электронных носителей информации еще не сложилась, и мнения могут быть противоположные. Так, суд указал, что в ситуации, когда в ходе производства выемки был изъят весь системный блок, а ходатайство о копировании информации с этих носителей от представителя заявителя не поступало, отсутствие при производстве выемки специалиста не может быть основанием для признания незаконными действий должностного лица, производившего выемку[5]. Однако в другом случае, суд признает действия следователя по непривлечению специалиста при производстве обыска, в ходе которого были изъяты электронные носители информации, незаконными, но отмечает, что 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[6].

В связи с этим необходимо конкретно обозначить роль специалиста и порядок действий при обнаружении электронных источников доказательств. Процессуалист М.В. Старичков предлагает дополнить ч.9.1. ст. 182 и ч. 3.1. ст. 183 УПК РФ фразой: «Допускается изъятие электронных носителей информации без участия специалиста, если электронные носители изымаются целиком и изъятие производится без копирования содержащейся на них информации»[7].

В дополнении же, более эффективным в долгосрочной перспективе, на наш взгляд, решением проблемы представляется обязательное прохождение обучения, подготовки всех следователей основам процессуальных действий, связанных с электронными источниками информации. Это позволит привлекать к участию специалистов лишь в крайнем случае, что приведет к повышению оперативности следственных мероприятий. Подобная концепция реализована в совместном проекте Европейского Союза и Совета Европы CyberCrime@EAP только лишь в рамках борьбы с компьютерными преступлениями. Эта программа предоставляет возможность разработки национальных стратегий по подготовке правоохранительных органов, которые имеют решающее значение для успешной реализации потенциала по созданию реальных и долгосрочных изменений в возможностях стран по борьбе со всеми типами киберпреступности, в том числе, теми традиционными преступлениями, неотъемлемой частью которых в настоящее время являются технологии. В соответствии с целями которой, для достижения положительных результатов необходимо проведение занятий по подготовке и повышению квалификации во всех правоохранительных органах. Принятие и реализация устойчивой и основанной на стандартах стратегии подготовки сотрудников правоохранительных органов будет означать, что все сотрудники правоохранительных органов проходят подготовку на должном уровне, чтобы быть в состоянии идентифицировать и работать с электронными доказательствами, расследовать преступления, связанные с использованием технологий, а некоторые из них - расследовать киберпреступления и проводить судебно-криминалистическую экспертизу электронных доказательств[8]. Данная программа реализована в

[5] Постановление Ставропольского краевого суда (Ставропольский край) № 22-1260/14 22К-1260/2014 от 20 марта 2014 г.// [Электронный ресурс] URL: http://sudact.ru/regular/doc/uvMXksSQ0ZJQ/ - дата посещения12.12.2014.

[6] Постановление Центрального районного суда г. Омска № 22-3496/2013 от 23.09.2013 г. // [Электронный ресурс] URL:https://rospravosudie.com/court-omskij-oblastnoj-sud-omskaya-oblast-s/act-441660122// – дата посещения12.12.2014.

[7] Старичков М.В. Вопросы использования носителей компьютерной информации в качестве доказательств//Журнал «Известия Тульского государственного университета», №2-2, 2014. – С.12

[8] «Стратегия обучения сотрудников правоохранительных органов. Выдержки из докладов страна Восточного партнерства»// Совет 2014 – 8 июля [Электронный ресурс] URL: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_pr

Азербайджане, Армении Беларуси, Грузии, Молдове и Украине.

Реализованы также и отечественные курсы повышения квалификации: на базе Волгоградской Академии МВД России изучается Программа повышения квалификации «Расследование преступлений в сфере компьютерной информации и высоких технологий»[9], при МГТУ им. Н.Э. Баумана ведет свою деятельность Центр компьютерного обучения «Специалист»[10].

По утверждению специалистов компании Group IB, из-за несовершенства правовых норм Российской Федерации, отсутствия устойчивой правоприменительной практики и систематического повышения квалификации по вопросам противодействия компьютерным преступлениям, отсутствия жестких санкций, злоумышленники несут ответственность, несоразмерную совершенным деяниям[11].

Другим важным моментом является то, что по ходатайству законного владельца изымаемого электронного носителя информации или обладателя содержащейся на нем информации специалистом осуществляется копирование информации. Однако в ходатайстве может быть отказано в случае, если это может воспрепятствовать расследованию преступления, или же по заявлению специалиста повлечь за собой утрату или изменение информации.

Законодатель не допускает выборочного изъятия информации, значимой для расследования, но в большинстве случаев не вся изъятая информация представляет ценность для расследования. В связи с этим ФЗ от 28.07.2012 №143-ФЗ в Уголовно-процессуальный кодекс РФ были внесены дополнения, которые обеспечивают соблюдение прав и законных интересов владельцев предметов. Статья 81 УПК РФ была дополнена частью 4, в соответствии с которой изъятые в ходе досудебного производства, но не признанные вещественными доказательствами предметы, включая электронные носители информации и документы, подлежат возврату лицам, у которых они были изъяты[12].

Одно из решений данного вопроса было предложено процессуалистом С.В. Задерако. В своем диссертационном исследовании он предлагает следующее: «Если находящиеся на электронных носителях информации электронные документы выданы их обладателями добровольно, и у следователя и специалиста нет оснований опасаться их сокрытия, уничтожения или изменения, то следователь вправе не изымать компьютерное средство или иной носитель информации полностью»[13]. Данное предложение актуально лишь в том случае, когда отс[illegible]ствует конфликт интересов между лицом, владеющ[illegible] информацией, и следователем.

Д.А. Медведев[14] считает, что особое внимание необ[illegible]димо обратить на соблюдение правил выемки элект[illegible]ных носителей информации, содержащих сведения, к[illegible]торые необходимы для деятельности хозяйствующ[illegible] субъектов, или содержащих информацию о персонал[illegible]ных данных. Последствия производства выемки предм[illegible]тов и документов в виде изъятия электронных носител[illegible] информации либо финансово-хозяйственной докумен[illegible]ции, наложения ареста на имущество, а также необход[illegible]мость корректировки формулировок федеральных зак[illegible]нов неоднократно были предметом дискуссий ученых, [illegible] практических работников на конференциях и научных [illegible] форумах[15]. В процессе сбора эмпирического матери[illegible] по данным вопросам получено мнение Следственно[illegible] управления Следственного комитета РФ по Республик[illegible] Татарстан и Прокурора Республики Татарстан. Та[illegible] Следственное управление обратило внимание, что чащ[illegible] всего проблемным является вопрос о судьбе предмето[illegible] изъятых в ходе доследственной проверки, проводимо[illegible] соответствии со ст. 144 УПК, в ходе которой могут бы[illegible] изъяты и исследованы электронные носители информ[illegible]ции. По мнению прокурора РТ К.Ф. Амирова, существ[illegible] необходимость осуществления контроля со стороны ор[illegible]ганов прокуратуры существующих официальных проц[illegible]дур выемки[16]. Поэтому необходимо приглашать специ[illegible]листа в сфере компьютерных технологий. В литературе [illegible] ранее отмечалось, что после принятия необходимых мер [illegible] безопасности можно приступить к выемке компьютеров [illegible] иных электронных носителей, придерживаясь при этом [illegible] следующих рекомендаций:

- перед выключением питания по возможности корректно з[illegible]крыть все используемые на компьютерах программы, а в сомн[illegible]тельных случаях просто выключить компьютер;
- при наличии на компьютерах программ, защищенных па[illegible]лем, принять меры к установлению паролей доступа; выключи[illegible] питание всех компьютеров, находящихся в месте их выемки, н[illegible] пытаться на месте просматривать информацию, содержащу[illegible] в компьютерах и на магнитных носителях;
- изымать только системные блоки персональных компьютеров [illegible] и дополнительные периферийные устройства (стримеры, моде[illegible]мы, сканеры, фотосчитыватели, перфораторы, принтеры и т.п.);
- изымать полностью все имеющиеся на месте выемки комп[illegible]ютеры и магнитные носители.[17]

oject_eap/Chisinau_International_Conference_Nov2014/EAP_Chisinau_WS.asp - дата посещения01.12.2014.

[9] Официальный сайт Волгоградской Академии МВД// [Электронный ресурс] URL:http://va-mvd.ru/ - дата посещения15.12.2014.

[10] «Киберпреступления: следствие ведут профессионалы»// [Электронный ресурс] URL: http://www.group-ib.ru/index.php/o-kompanii/176-news?view=article&id=1204 - дата посещения15.12.2014.

[11] «Проблемы квалификации преступлений, связанных с хищением денежных средств в системах интернет-банкинга»// [Электронный ресурс] URL: http://www.group-ib.ru/?view=article&id=1001 - дата посещения15.12.2014.

[12] Федеральный закон Российской Федерации от 28 июля 2012 г. N 143-ФЗ "О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации"// [Электронный ресурс] URL: http://www.rg.ru/2012/08/01/veshdok-dok.html - дата посещения15.12.2014.

[13] Задерако С.В. «Особенности расследования корыстных преступлений в сфере строительства, связанных с фальсификацией проектно-сметной и отчетной документации.» – Автореф...к.ю.н. Ростов-на-Дону, 2013. - С.11

[14] ««Кошмарить» бизнес станет чуть сложнее.», Газета Business FM, 16.02.2012// [Электронный ресурс] URL: http://www.bfm.ru/news/171093 - дата посещения 15.10.2014

[15] Материалы парламентского «Круглого стола» о перспективе введения в РФ института «Сделки с правосудием», 8 февраля 2007 г. // Из-е фракции «Родина-Патриоты» в Гос.Думе Федерального собрания РФ; Научно-практическая конференция «Перспективы развития и проблемы процессуальной деятельности государственных органов, обеспечивающих в пределах своих полномочий исполнение законодательства РФ об уголовном судопроизводстве» (23 июня 2011г.) – г. Нижний Новгород. «Круглый стол» (видео-конференцсвязь) по вопросам повышения уровня защиты интересов хозяйствующих субъектов в ходе оперативно-розыскной и процессуальной деятельности // Аппарат полномочного представителя Президента Российской Федерации в Приволжском федеральном округе, 17 августа 2011г. Казань-Н.Новгород-Саратов.

[16] Муратов К.Д. Приложение 12 в монографии - Сущность, значение и правовые последствия выемки по уголовным делам: монография//Муратова К.Д. – Москва: Изд-во «Юрлитинформ», 2013. – С.238-242.

[17] Руководство для следователей / Под общ. ред. В.В. Мозякова. – Изд-во «Экзамен». – Москва, 2005. – С.684

При производстве выемки электронных доказательств важна оперативность в действиях сотрудников, так как в сравнении с другими видами доказательств, данный тип подвержен полной утрате в краткие сроки ввиду установленных сроков хранения информации, либо намеренному удаленному воздействию на информацию злоумышленниками. Так, например, в соответствии с п. 12 Постановления Правительства РФ № 538 от 27.08.2005 оператор связи обязан своевременно обновлять информацию, содержащуюся в базах данных об абонентах оператора связи и оказанных им услугах связи, данная информация должна храниться оператором связи в течение 3 лет.[18] Однако, по словам главы Бюро специальных технических мероприятий /БСТМ/ МВД России Алексея Мошкова, в процессе взаимодействия с операторами сотовой связи возникают проблемы получения информации, необходимой для возбуждения уголовных дел и сбора доказательственной базы.[19]

Федеральным законом от 1 июля 2010 г. №143 – ФЗ была введена ст.186.1 УПК РФ «Получение информации о соединениях между абонентами и (или) абонентскими устройствами» и введен новый пункт 12 ч.2 ст.5 УПК РФ – необходимо судебное решение о получении информации о соединениях между абонентами и (или) абонентскими устройствами. Законодателем приняты во внимание потребности следственных органов в правовой регламентации процедуры получения криминалистически значимой и доказательственной информации об использовании мобильных телефонов при подготовке, совершении и сокрытии преступления.

Согласно позиции Конституционного Суда РФ: «право каждого на тайну телефонных переговоров по своему конституционно-правовому смыслу предполагает комплекс действий по защите информации, получаемой по каналам телефонной связи, независимо от времени поступления, степени полноты и содержания сведений, фиксируемых на отдельных этапах ее осуществления. В силу этого, информацией, составляющей охраняемую Конституцией РФ и действующими на территории РФ 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. Иное означало бы несоблюдение требования ст. 23 (ч. 2) Конституции РФ о возможности ограничения права на тайну телефонных переговоров только на основании судебного решения».

Под информацией о соединениях между абонентами понимается не только детализация входящих и исходящих звонков и данных об абонентах и их телефонных аппаратах, но и сведения о номерах и месте расположения приемо-передающих базовых станций. Следователи имеют право запрашивать у операторов данные не только о совершенных телефонных соединениях, но и предстоящих. Период получения информации о предстоящих соединениях ограничен шестью месяцами, однако может продлеваться неограниченное число раз[20]. УПК РФ обязывает следователя хранить документы, содержащие информацию о соединениях между абонентами и абонентскими устройствами, в опечатанном виде в условиях, исключающих возможность ознакомления с ними посторонних лиц и обеспечивающих их сохранность. Это следственное действие, как видно из ч.1 ст.189.1 УПК РФ является неотложным, так как законодателем регламентировано, что получение этой информации допускается на основании судебного решения, принимаемого в порядке, установленного ст.165 УПК РФ, то есть – последующий судебный контроль. Хотя ч.2 ст.13 УПК РФ прямого указания не предусмотрено. Является ли это противоречием? До вступления в силу данного изменения в уголовно-процессуальном законодательстве на протяжении долгого времени действовала правовая позиция Конституционного Суда РФ о том, что получение информации о соединениях абонентов возможно только по судебному решению. Определением Конституционного Суда от 2 октября 2003 г. №345-0 «Об отказе в принятии к рассмотрению запроса Советского районного суда города Липецка о проверке конституционности ч.4 ст.32 Федерального закона от 16 февраля 1995 г. «О связи», было сформулирована следующая правовая позиция. Запросом суда было запрошено осуществление судебного контроля соответствия ч.4 ст.32 ФЗ «О связи» Конституции РФ, предусматривающей судебное решение на прослушивание телефонных переговоров. В запросе был отмечено, что при расширительном истолковании конституционных пределов ограничения прав граждан на тайну телефонных переговоров необходимо наличие судебного решения и на получение иных сведений о них. В частности, речь шла о возможности вынесения судебного решения, позволяющего истребовать в ОАО «Ростелеком» сведения о входящих и исходящих телефонных звонках гражданки, в отношении которой имелись данные о совершении ею мошеннических действий. Конституционный суд РФ в Определении однозначно объявил, что судья также обязан не допускать сужения сферы судебного контроля. Норма, содержащаяся в ч.4 ст.32 ФЗ «О связи» является специальной, конкретизирующей и обеспечивающей действие ст.23 (ч. 20) и ст.24 (ч.1) Конституции РФ применительно к вопросам сохранения тайны связи. Право каждого на тайну телефонных переговоров по своему конституционно-правовому смыслу предполагает комплекс действий по защите информации, получаемой по каналам телефонной связи, поэтому охраняемой информацией 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 необходимо получение судебного решения[21].

Статистическая картина по обращениям в суд с ходатайством о нарушении тайны сообщений в порядке проведения оперативно-розыскных мероприятий в соответ-

[18] Постановление Правительства Российской Федерации от 27 августа 2005 г. N 538 «Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность»// [Электронный ресурс] URL: http://www.rg.ru/2005/09/02/pravila-dok.html - дата посещения 15.12.2014

[19] «МВД испытывает трудности в получении информации от операторов сотовой связи», Информационное агентство России ТАСС//[Электронный ресурс] URL:http://itar-tass.com/obschestvo/597943 - дата посещения 14.12.2014

[20] Куприянов А. Сведения о телефонных звонках будут выдаваться по решению суда.//Уголовный процесс, 2010, №7 – С.6.

[21] Определение КС ФР от 2 октября 2003 года №345-О // Российская газета, 2003, 10 декабря.

ствии ФЗ «Об оперативно-розыскной деятельности» только лишь по одному районному суду выглядит следующим образом: 2005 г. – 2372 (удовлетворено – 2372), в 2006 г. – 2369 (удовлетворено – 2369), 2007 г. – 2748 (удовлетворено – 2748), в 2008 г. – 2772 (удовлетворено – 2772), в 2009 г. – 2847 (удовлетворено – 2847), в 2010 г. – 2828 (удовлетворено – 2828)[22]. В связи с этим, видится необходимым внести в часть 4 ст.186.1 УПК РФ изменения следующего содержания: после слов «но не реже одного раза в неделю» включить предложение: «Следователь производит выемку документов, содержащих информацию о соединениях между абонентами и (или) абонентскими устройствами, в том объеме, который имеет значение для уголовного дела в порядке ст.183 УПК РФ». Также следует учесть, что информация о соединении между абонентами может быть получена не только лишь в рамках ст.186.1 УПК РФ. Свидетель, потерпевший, либо иное заинтересованное лицо, может добровольно предоставить сведения о детализации входящих и исходящих соединений, полученных от оператора связи, без необходимости получения разрешения суда.

Об актуальности доказательственного значения получения информации о телефонных соединениях свидетельствует широкий аспект мнений:

- о том, что это – ключевое условие эффективного расследования хищений сотовых телефонов[23];

- об отсутствии должной дифференциации контроля и записи телефонных и иных переговоров и получении сведений о соединениях[24];

- о процессуальной форме получения этих сведений – выемка или истребование документов[25].

Нередко приходится сталкиваться с выемкой электронной корреспонденции, пейджинговых сообщений, либо иных передаваемых по сетям электросвязи сообщений. В соответствии с ч. 2 статьи 23 Конституции РФ у каждого есть право на тайну переписки, телефонных переговоров, телеграфных, почтовых и иных сообщений. Согласно с ч.3 ст.63 Федерального закона от 07.07.2003 № 126-ФЗ «О связи», ознакомление с информацией и документальной корреспонденцией, передаваемыми по сетям электросвязи и сетям почтовой связи, осуществляется только на основании решения суда. Это относится и к электронной почте, пейджинговым сообщениям, либо иным передаваемым по сетям электросвязи сообщениям обвиняемого или подозреваемого в преступлении лица. Выемка данного вида источника доказательства регламентирована статьей 185 УПК РФ «Наложение ареста на почтово-телеграфные отправления, их осмотр и выемка». В соответствии с данной нормой все процессуальные действия, связанные с «сообщениями электросвязи», осуществляются на основании постановления суда. Целями данного следственного действия являются: получение доказательственных данных, имеющих значение для расследуемого дела; ограничение доступа к информации в целях сохранения и недопущения ее распространения; обеспечение тайны следствия. Законодателем прямо не предусмотрено, в течение какого срока производится контроль отправлений. Однако, принимая во внимание тесную связь между данным следственным действием и контролем и записью переговоров, по аналогии можно считать срок ареста в пределах 6 месяцев (ч. 5 ст. 186 УПК РФ). Изучение судебной практики, а также официальной судебной статистки показало, что данный вид выемки не является самым распространенным. Так, процент судебных решений о разрешении выемки данных об электронных почтовых сообщениях в 2008г. составил 1.7% – 10 решений, а в 2009 г. уже больше 2,4% - 18, и все данные ходатайства были удовлетворены. За 2009 г. выявлено одно судебное решение о выемке почтово-телеграфных оправлений в отделениях связи, в то время как за 2008 г. не было ни одного судебного решения[26].

Также проведено сравнение с результатами изучения статистических данных по одному из районов г. Казани с 2005 г. по 2010 г.: в 2005г. было одно ходатайство о наложении ареста на корреспонденцию, разрешении на её осмотр и выемку в учреждениях связи и оно удовлетворено судом; в 2006г. – было заявлено 36 ходатайств об этом следственном действии органами следствия; в 2007 г. – 5 ходатайств; в 2009 г.- 2 ходатайства; в 2010г. – 6 ходатайств и все удовлетворены судом[27].

Если частью 2 ст. 13 УПК РФ закреплено, что наложение ареста на почтовые и телеграфные отправления и их выемка в учреждениях связи, контроль и запись телефонных и иных переговоров, получение информации о соединениях между абонентами и (или) абонентскими устройствами могут производиться только на основании судебного решения, то касательно ознакомления с перепиской подозреваемого в ходе осмотра, обыска, выемки такое указание отсутствует. В результате анкетирования руководителей следственных управлений (отделов), а также руководителей управлений (отделов) криминалистики по данному вопросу выяснилось, что основными критериями, лежащими в основе правовой возможности ограничения прав граждан на тайну переписки, по их мнению, являются:

1. Наличие (или отсутствие) согласия лица на извлечение информации из мобильного устройства связи или компьютера. В частности, ряд руководителей считают беспрепятственную возможность извлечения данных переписки из мобильных устройств и компьютеров с помощью криминалистической техники только в случае получения согласия собственника мобильного устройства. В противном случае необходимо получать решение суда по аналогии с ч. 5 ст. 177 УПК РФ и ч. 2 ст. 186 УПК РФ.

2. Процессуальный статус участника уголовного судопроизводства, которому принадлежит мобильное устройство или компьютер (если подозреваемый или обвиняемый – согласие и решение суда не требуется, если свидетель или потерпевший и ознакомление не связано с оценкой достоверности их показаний – необходимо согласие, в противном случае – решение суда).

---

[22] Сущность, значение и правовые последствия выемки по уголовным делам: монография//Муратова К.Д. – Москва: Изд-во «Юрлитинформ», 2013 – с. 133

[23] Шебалин А.В. Расследование хищений средств сотовой связи. – Автореф…к.ю.н. ,Томск, 2010. - С.20.

[24] Ширёв Д.А. Контроль и запись телефонных и иных переговоров и их доказательственное значение в уголовном судопроизводстве России. – Автореф. …к.ю.н., 2009. – С.14-15.

[25] Волынская О.В., Шишкин В.С. К вопросу о доказательственном значении сведений
о телефонных соединениях// Российский следователь, 2011, №2. –С.12-15. Саницкий Р. Процессуальный порядок получения информации о телефонных контактах// Законность, 2007. №3 – С.32.

[26] Муратов К.Д. Приложение №1 в монографии - Сущность, значение и правовые последствия выемки по уголовным делам: монография//Муратова К.Д. – Москва: Изд-во «Юрлитинформ», 2013. – С.200-201.

[27] Сущность, значение и правовые последствия выемки по уголовным делам: монография//Муратова К.Д. – Москва: Изд-во «Юрлитинформ», 2013 – с. 134

установлено ли лицо, которому принадлежит электронное устройство, а также известно ли, что в мобильном устройстве имеются данные, имеющие значение для дела. В случаях, когда телефон обнаружен на месте происшествия и его принадлежность не установлена, либо на трупе, судебное решение не нужно. Если следователь не располагает достоверной информацией о том, имеются ли в содержании переписки данные, относящиеся к делу, также необходимости нет в получении решения суда и наоборот[28].

Стоит отметить отсутствие достаточного законодательного регулирования ареста, обыска и выемки сообщений электросвязи. В частности, отсутствует определение сообщений электросвязи. В связи с этим возникают проблемы правоприменения. Так, в апреле 2013 года Федеральной службой по финансовым рынкам в соответствии с ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации», а также в соответствии с ФЗ «О защите прав и законных интересов инвесторов на рынке ценных бумаг» на интернет-компанию «Рамблер» был наложен административный штраф в размере 500000 рублей за отказ в предоставлении без судебного постановления регистрационных данных владельца электронной почты и сведений об адресах, с которыми велась переписка, а на компанию «МТС» наложен административный штраф за отказ в выдаче без судебного постановления детализации счетов и IMEI телефонов. Арбитражным судом г. Москвы постановление, вынесенное в отношении «МТС», было оставлено в силе на основании того, что ФСФР в соответствии с ФЗ №224 «О противодействии неправомерному использовании инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты РФ» не предусмотрено право на обращение в суд за разрешением об истребовании информации о детализации счетов абонента и информации об IMEI. В свою очередь, постановление, вынесенное в отношении компании «Рамблер», было отменено Арбитражным судом г. Москвы, на основании того, что запрашиваемая ФСФР информация может быть предоставлена исключительно через доступ к информации, содержащейся непосредственно в сообщениях Пользователя, которые относятся к тайне переписки. Однако 9 Арбитражным апелляционным судом решение, вынесенное ранее в отношении компании «МТС» было отменено, поскольку затребованные детализация счета и IMEI, составляют тайну телефонных переговоров и могли быть переданы не иначе как на основании решения суда, которое ФСФР России не предоставлено, и требования о предоставлении данных сведений были признаны незаконными.

В то же время решение Арбитражного суда г. Москвы №А40-56844/2013, вынесенное по делу компании «Рамблер» было отменено со ссылкой на то, что сведения об адресах электронной почты, с которыми осуществлялась переписка пользователем, не относятся к информации, указанной в п.3 ст.63 Закона о связи[29].

В результате проведенного исследования можно сделать вывод, что нет необходимости в разработке строго регламентированных правил в условиях стремительно изменяющихся технологий, однако следует выработать четкий понятий аппарат, установить разумные и понятные пределы компетенции, а также ежедневно повышать профессионализм сотрудников. В целях создания комфортных условий для хозяйственных предприятий, а также добросовестных граждан устранить выявленные проблемы, соблюдая конституционные права и интересы всех участников правоотношений.

На основе проведенного исследования, были выработаны следующие выводы и предложения:

1) электронные носители информации – относительно новые источники доказательств, которые могут быть выявлены в разных формах: материальных и виртуальных. Отсутствует единая, общепризнанная классификация электронных доказательств, а именно - обоснованная классификация, которая поможет правильно использовать документы в качестве доказательств в уголовном судопроизводстве. Материальными источниками электронной информации могут быть персональные компьютеры, мобильные устройства связи, мультимедиа устройства (фотоаппараты, видеокамеры, аудио-, видеоплееры), разного рода и вида носители информации (флеш-накопители, оптические диски, магнитные диски и т.д.); виртуальными - сайты телекоммуникационной сети Интернет, лог-файлы соединения абонента с адресом интернет-провайдера, IP-адреса пользователей телекоммуникационной сети Интернет и т.д.

2) доследственная проверка должна содержать необходимые процессуальные формы изъятия и приобщения в качестве вещественных доказательств электронные носители информации – логичным представляется дополнить ст. 144 «Порядок рассмотрения сообщения о преступлении» пунктом 1.3. «В рамках проведения проверки сообщения о преступлении изъятие предметов и документов (в том числе электронных доказательств) проводится в соответствии с требованиями, установленными гл. 25 УПК РФ».

3) оценка электронных источников доказательств должна производиться с участием специалиста. В связи с этим необходимо внести изменения в ст. 88 УПК РФ «Правила оценки доказательств», пунктом 3.1. установить: «Оценка относимости, допустимости и достоверности доказательств, изъятых при участии специалиста (в том числе электронных доказательств), производится с привлечением специалиста.

Список литературы:

1. Волынская О.В., Шишкин В.С. К вопросу о доказательственном значении сведений о телефонных соединениях// Российский следователь, 2011, №2. –С.12-15. Саницкий Р. Процессуальный порядок получения информации о телефонных контактах// Законность, 2007. №3
2. Газета Business FM, «Кошмарить» бизнес станет чуть сложнее.», 16.02.2012// [Электронный ресурс] URL: http://www.bfm.ru/news/171093 - дата посещения 15.10.2014
3. Единая система конструкторской документации. Электронные документы. Общие положения. ГОСТ 2.051-2006 - [Электронный ресурс] URL:

[28] С.Ю. Скобелин Пределы ограничения конституционных прав граждан на тайну переписки при расследовании преступлений// Материалы Международной научно-практической конференции «Конституция российской федерации как гарант прав и свобод человека и гражданина при расследовании преступлений». ч.2 – 2010. – [Электронный ресурс] URL: http://www.academy-mvd.ru/science/forums/14.11.13-%D1%87.2.pdf – дата посещения 10.01.2015

[29] «9ААС лишил владельцев электронной почты "Рамблер" тайны переписки», Право.ру//[Электронный ресурс] URL: http://pravo.ru/story/view/100136/88463/