УДК 343
DOI: 10.17223/22253513/23/10

И.В. Чаднова, Н.С. Соколовская, А.Ю. Кирсанов

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ «ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ ДАННЫХ»[1] В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

В статье рассматривается процессуальная регламентация и информационный потенциал электронных носителей данных в их различных вариантах, в том числе через процессуальные и технические возможности верификации полученной в ходе следственных действий электронной информации. Приводится возможный алгоритм получения доказательственной информации с электронных носителей в зависимости от типа носителя, выдвигаются предложения по дифференциации механизма получения такой информации в ходе следственных действий.
Ключевые слова: *процесс доказывания, следственное действие, электронные носители информации, доказательство, обыск, выемка.*

В условиях динамичного развития и все расширяющегося использования электронных носителей и хранилищ информации перед предварительным расследованием и уголовным процессом в целом все более актуальными и востребованными становятся задачи как по получению и сохранению информации с электронных носителей данных, так и по разработке процессуальных правил трансформации полученных данных в доказательства.

Законодатель время от времени дополняет Уголовно-процессуальный кодекс Российской Федерации (далее – УПК РФ) различными нормами, внедряющими в той или иной форме в уголовное судопроизводство возможности использования как в процессе доказывания, так и в процедуре судопроизводства электронной системы документов и носителей информации. Однако такие дополнения вносились в разное время и по разному поводу, потому разнообразны и не систематизированы. В ряде случаев подобные уголовно-процессуальные правила в силу непоследовательного нормативного регулирования имеют неоднозначное понимание и создают проблемы в правоприменении.

Так, в УПК РФ используются понятия:

– «электронные средства контроля». Статья 107 УПК РФ, предусматривающая использование в целях осуществления контроля за лицом, в отношении которого избрана мера пресечения в виде домашнего ареста, аудиовизуальных, электронных и иных технических средств контроля. Перечень и порядок применения таких средств определен постановлением Правительства РФ и не требует дополнительной регламентации в уголовно-процессуальном законодательстве;

[1] Носитель данных – материальный объект, предназначенный для записи и хранения данных (ГОСТ 15971–90).

– «электронная почта». Статьи 42, 313 УПК РФ предусматривают возможность использования электронной почты для уведомления лица о принятом процессуальном решении. Имеющееся нормативное регулирование, как и довольно однозначное понимание понятия электронной почты, не требует его дополнительного уточнения в УПК РФ. В то же время возможность использования электронной почты для получения уведомлений сейчас носит в УПК РФ скорее частный характер (только в двух случаях);

– «электронные сообщения». Статья 185 УПК РФ устанавливает необходимость осмотра и выемки сведений, имеющих значение для уголовного дела, содержащихся в электронных сообщениях или иных передаваемых по сетям электросвязи сообщениях. Указанная формулировка не отличается корректностью, так как оставляет неясность в том, что подлежит осмотру и выемке, – «сведения, имеющие значение для уголовного дела» или «электронные сообщения или иные передаваемые по сетям электросвязи сообщения». Кроме того, может быть подвергнута сомнению достоверность полученного в результате данного следственного действия доказательства, проверяемость источника, так как при направлении электронных писем возможен подлог, письмо будет выслано с одного (указанного официально) сервера, тогда как на самом деле это может быть промежуточный «прокси» сервер, симулирующий настоящий. Протокол smtp, по которому передается электронная почта, не является верифицируемым и позволяет послать сообщение от имени любого пользователя сети любому. Причиной этому является наличие так называемых «открытых релеев». Без дополнительной процессуальной регламентации вышеуказанного мероприятия возможны произвольные (не всегда «процессуально корректные») действия по выемке сведений или сообщений;

– «электронная подпись», «усиленная квалифицированная электронная подпись». В отдельных вопросах судопроизводства законодатель предусмотрел возможность использования разновидностей электронной подписи. В соответствии с ч. 1 ст. 474.1 УПК РФ ходатайство, заявление, жалоба, представление могут быть поданы в суд в форме электронного документа, подписанного лицом, направившим такой документ, электронной подписью. В полномочиях суда предусмотрена возможность изготовления в форме электронного документа с заверением усиленной квалифицированной электронной подписью как судебного решения (ч. 2 ст. 474 УПК РФ), так и исполнительного листа (ч. 2 ст. 393 УПК РФ). Порядок использования электронной цифровой подписи (ЭЦП) при подписании документов регламентирован ФЗ от 06.04.2011 № 63-ФЗ (ред. от 23.06.2016) «Об электронной подписи» [1]. Закон называет три вида электронной подписи: 1) простая – служит для подтверждения того, что документ исходит от определенного лица; 2) усиленная неквалифицированная – не только указывает на лицо, ее поставившее, но и подтверждает, что после ее проставления каких-либо изменений в документ не вносилось; 3) усиленная квалифицированная – обладает характеристиками неквалифицированной ЭЦП, но выдается только в специализированных центрах, имеющих аккредитацию от Минкомсвязи. Именно квалифицированная подпись согласно ФЗ «Об электронной подписи» придает документу полную юридическую силу (в полной мере заменяет рукописную подпись, а также

печать организации). Учитывая вышеизложенное, полагаем, что электронные документы в уголовном судопроизводстве могут быть подписаны только ЭЦП второго или третьего вида (никак не первого), что требует уточнения формулировки в ч. 1 ст. 474.1 УПК РФ;

– «электронный документ», «документ, выполненный электронным способом». Согласно ст. 474 УПК РФ любой процессуальный документ в уголовном судопроизводстве может быть выполнен электронным способом. Логическое толкование положений ст. 474 УПК РФ позволяет предположить, что речь идет о составлении документа с использованием компьютерной техники с последующей его распечаткой на бумажном носителе.

Электронный документ – это документированная информация, представленная в электронной форме, т.е. в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах (п. 11.1 ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ (ред. от 19.12.2016) «Об информации, информационных технологиях и о защите информации» [2]). Согласно определению, представленному в п. 3.1 ГОСТ Р 7.0.8–2013. «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения» (утв. Приказом Росстандарта от 17.10.2013 № 1185-ст) [3], электронный документ – это документ, информация которого представлена в электронной форме. Исходя из этого, можно сделать вывод, что электронный документ – это любой документ, который представлен в электронном виде, в том числе это может быть скан-образ документа, файл, набранный в текстовом редакторе, и т.п. Электронные документы могут быть формализованными, т.е. составленными в таком виде, который позволяет с помощью программных средств распознавать их содержимое, и неформализованными (например, скан-копия). Понятие электронного документа использовано в ст. 393, 474.1 УПК РФ, однако не конкретизировано в части формализации. Следовательно, в рамках обмена электронными документами участники уголовного судопроизводства могут использовать как формализованные, так и неформализованные документы;

– «электронные носители информации» – термин, наиболее часто используемый применительно к процессуальной регламентации изъятия, хранения и копирования содержащейся на этих носителях информации, вещественных доказательств (ст. 81, 81.1, 82, 166, 182, 183 УПК РФ). Исчерпывающее определение электронного носителя содержит ГОСТ 2.051–2013. «Межгосударственный стандарт. Единая система конструкторской документации. Электронные документы. Общие положения», устанавливающий, что под электронным носителем понимается «материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники» [4].

Все вышеперечисленные положения УПК РФ касаются электронных носителей информации как локальных носителей данных, в то время как технологии хранения данных активно совершенствуются, что ведет к увеличению объема, повышению надежности, усложнению носителей данных. На уровне решений для предприятий (организаций) эта гонка приводит к усложнению

решений по хранению данных. Стремление вендора[1] к производительности линейно увеличивает количество физических дисков, участвующих в формировании одного логического носителя данных.

В наше время с развитием SSD-накопителей потребность к объему данных продолжает расти, что приводит к более высоким требованиям к скорости записи и чтения. Вендор для увеличения скорости доступа, в силу ограничения скорости доступа на один физический диск, строит системы хранения, соединяя несколько физических дисков как один логический, распределяя доступ информации сразу на все диски. С одной стороны, мы имеем более быстрые показатели записи и чтения на логический диск, но с другой – процесс восстановления или изъятия данных с физических дисков значительно усложняется (хотя возможность восстановления увеличивается, так, все системы логического объединения дисков (raid) преследуют цель максимального сохранения информации, а значит, они, как минимум, дублируют блок информации, чтобы в случае выхода из строя физического носителя информация не потерялась). Фактически файл, расположенный на логическом диске одним сплошным куском, может состоять из 20 кусочков и каждый кусок файла может лежать на отдельном физическом диске. В таких случаях неприменим заложенный в статьях УПК РФ алгоритм поиска и изъятия электронных носителей информации, например, в ходе обыска или выемки. Так, дата-центр[2] в организации может состоять из нескольких серверных стоек с расположенными на них 30–100 серверами, на которых распределен огромный объем информации. Извлечение физических дисков всего дата-центра в ходе обыска не принесет желаемого результата, так как логическое распределение информации на этих дисках позволяет ее извлечь только в самом дата-

[1] Вендор – это (от англ. vendor– торговец, продавец) физическое или юридическое лицо, которое поставляет объединенные в одну торговую марку товары и услуги. Различают независимый вендор аппаратных средств и вендор программного обеспечения – компании, которые специализируются на создании или продаже аппаратных средств либо программного обеспечения, разработанного для распространения его на массовом или нишевых (специализированных) рынках. Источник: https://biznes-prost.ru/vendor.html

[2] Дата-центр (от англ. data center), или центр (хранения и) обработки данных (ЦОД/ЦХОД) – это специализированное здание для размещения (хостинга) серверного и сетевого оборудования и подключения абонентов к каналам сети Интернет. Дата-центр исполняет функции обработки, хранения и распространения информации, как правило, в интересах корпоративных клиентов – он ориентирован на решение бизнес-задач путём предоставления информационных услуг. Консолидация вычислительных ресурсов и средств хранения данных в ЦОД позволяет сократить совокупную стоимость владения IT-инфраструктурой за счёт возможности эффективного использования технических средств, например, перераспределения нагрузок, а также за счёт сокращения расходов на администрирование. Источник: http://dic.academic.ru/dic.nsf/ruwiki/633220

Типичный дата-центр состоит из информационной инфраструктуры, включающей в себя серверное оборудование и обеспечивающей основные функции дата-центра – обработку и хранение информации; телекоммуникационной инфраструктуры, обеспечивающей взаимосвязь элементов дата-центра, а также передачу данных между дата-центром и пользователями; инженерной инфраструктуры, обеспечивающей нормальное функционирование основных систем дата-центра. Инженерная инфраструктура включает в себя прецизионное кондиционирование для поддержания температуры и уровня влажности в заданных параметрах; бесперебойное и гарантированное электроснабжение обеспечивает автономную работу дата-центра в случаях отключения центральных источников электроэнергии, а также повышает качество электропитания; охранно-пожарная сигнализация и система газового пожаротушения; системы управления и контроля доступом. Источник: http:// dic. academic.ru/dic.nsf/ruwiki/107308

центре. Перемещение же всех серверов дата-центра невозможно в силу сложности его инфраструктуры и большого объема оборудования.

Носители данных можно классифицировать по типу доступа, представленного в табл. 1.

Таблица 1

	Облачные	Сетевые	Локальные
Носители данных	Paas[1] IaaS[2] Облачные хранилища CMS[3]	usb-over-ip IaaS Сетевые хранилища CMS	Локальные диски USB-флеш-накопитель Телефоны Смартфоны Карты памяти CD, DVD

[1] PaaS (Platform as a Service) – платформа как услуга.
[2] IaaS (Infrastructure-as-a-Service) – инфраструктура как услуга.
[3] CMS (Content management system) – система управления содержимым (контентом).

При этом различные типы систем хранения (частные случаи носителей данных) могут относиться к нескольким типам доступа:

– локальные носители данных – с этим типом носителей все достаточно прозрачно, из-за форм-фактора последних, их изъятие не представляет сложности, что и регламентируют ст. 81, 81.1, 82, 166, 182, 183 УПК РФ;

– сетевые носители данных – могут представлять как простые элементы для изъятия, так и более сложно организованные элементы, изъятие которых требует глубоких познаний в технологиях организации хранилищ данных;

– облачные носители данных – это сложно организованные элементы, изъятие которых практически невозможно либо по причине сложной организации, либо территориальной распределенности (физическое хранилище может находиться на территории другого государства).

Для уяснения возможностей изъятия и доказательственного оформления электронной информации попробуем классифицировать носители данных по сложности извлечения данных с физических дисков. Для начала определим, что можно извлечь из носителя данных:

- сам носитель данных (внутренний накопитель на жестком магнитном диске, оптические диски различных видов, магнитно-оптические диски, карты памяти различных форматов, USB-флэш-накопители, гибкие магнитные диски, интегральная микросхема памяти, оперативное запоминающее устройство ЭВМ и др.);
- мета-данные (о носителе). Мета-данные – информация о носителе данных, уникально идентифицирующая носитель, его характеристики, также может содержать описание сложной структуры, частью которой является. На данный момент широко применяются следующие три класса мета-данных:

1. Внутренние мета-данные. Это информация, которая описывает составные части вещей, их структуру и что она собой представляет. В качестве примера можно привести размер и формат файла.

2. Административные мета-данные. Требуются для процессов обработки информации, а также для назначения вещи. Например, кто автор, редактор, когда был создан файл.

3. Описательные мета-данные. Используются, чтобы охарактеризовать природу файла и его признаки (к какой категории относится, с чем ещё связан)[1];

- данные. Для дальнейшего понимания правил работы с электронными носителями информации стоит определить часть извлекаемых сведений с физических носителей данных как «сырую» информацию, которую нужно обрабатывать, чтобы получить искомую информацию. Для удобства воспользуемся термином «данные» для описания сырой информации;
- информация (искомая).

Шифрование носителя данных никак не связано с его структурой организации, так как обычно шифрование применяют на самом верхнем уровне организации хранилища. Поэтому введем просто подкласс для шифрованных носителей данных. Итак, разделим носители данных на три класса (с учетом выделения подклассов для шифрованных носителей данных, представленных в табл. 2)

Таблица 2

№ п/п	Класс	Возможно извлечение				Носители данных
		Носитель	Мета-данные	Данные	Инф-ция	
1	1	Да	Да	Да	Да	Локальные диски USB-флеш-накопитель Телефоны Смартфоны Карты памяти CD, DVD
2	1ш	Да	Да	Да	Да	
3	2	Нет	Да	Да	Да	IaaS Сетевые хранилища usb-over-ip
4	2ш	Нет	Да	Да	Да	
5	3	Нет	Нет	Нет	Да	Paas IaaS Облачные хранилища CMS
6	3ш	Нет	Нет	Нет	Да	

Процедура извлечения информации для Классов 1 и 1ш:

1) обнаруживаем носитель данных (не требует специальных знаний);

2) обесточиваем/отключаем/вынимаем носитель (не требует специальных знаний);

3) фиксируем его мета-данные (требует специальных знаний);

4) изымаем носитель данных/данные/информацию (кроме 1ш) (возможно, требует специальных знаний);

5) (1ш) обнаруживаем или вычисляем ключ дешифрации (требует специальных знаний);

6) (1ш) дешифруем данные в информацию (требует специальных знаний).

Процедура извлечения для Классов 2 и 2ш:

1) обнаруживаем носитель данных (требует специальных знаний);

[1] Подробнее: http://fb.ru/article/234327/metadannyie-eto-chto.

2) физически ограничиваем доступ к носителю данных (не требует специальных знаний);

3) фиксируем его мета-данные (требует специальных знаний);

4) изымаем данные/информацию (кроме 2ш) (возможно, требует специальных знаний);

5) (2ш) обнаруживаем или вычисляем ключ дешифрации (требует специальных знаний);

6) (2ш) дешифруем данные в информацию (требует специальных знаний).

Процедура извлечения для Классов 3 и 3ш (требует специальных знаний):

1) определение типа носителя данных (фактически ip адреса (dns-имени) сервиса, предоставляемого вендором);

2) определение владельца и учетных данных;

3) подключение к сервису с учетными данными владельца и смена пароля, чтобы избежать вмешательства;

4) обнаруживаем носитель данных;

5) фиксируем его мета-данные;

6) изымаем информацию (кроме 2ш);

7) (2ш) обнаруживаем или вычисляем ключ дешифрации;

8) (2ш) дешифруем данные в информацию.

В некоторых случаях для Классов 2 и 3 определение носителя данных может быть сопряжено с некоторыми сложностями. Например, IaaS разрабатывался так, чтобы вливаться в текущую физическую инфраструктуру прозрачно. Поэтому могут быть проблемы с обнаружением носителей данных через этот сервис.

Как видно из данных процедур, уже Классы 1 и 1ш требуют специальных знаний, которые далеко не всегда могут быть обеспечены простым участием специалиста в ходе следственного действия.

В профессиональной экспертной деятельности в настоящее время уже имеются специальные разработки по получению информации с различных носителей данных. Так, для получения информации из облачных хранилищ существует программа «Мобильный Криминалист» – технико-криминалистическая экспертная программа, сделавшая возможным извлечение данных из облачного хранилища с помощью модуля Oxygen Forensic Extractor for Clouds [5]. Oxygen Forensic Extractor for Clouds может подключаться к облачному хранилищу, используя только данные учетной записи: адрес электронной почты и пароль. Как только соединение установлено, Oxygen Forensic Extractor for Clouds начинает извлечение данных. Сильной стороной данного модуля является не только извлечение данных, но и представление данных в удобном для анализа виде и наличие различных инструментов для анализа, что позволяет специалисту экономить очень много времени [6]. Другой пример: при использовании пользователями мобильных устройств на платформе Android приложения Play Market, Gmail и других приложений от компании Google при регистрации в них пользователь автоматически даёт согласие на отправку геоданных – это информация о географическом местоположении, хранящаяся в формате, который может быть использован в географических информационных системах. Это необходимо для

работы сервисов Google, чтобы ускорить поиск на Google-картах или рекламных объявлений, которые пользователь видит на сервисах Google и сторонних сайтах. Отправка геоданных позволяет сохранять новые сведения о местоположении мобильного устройства, в том числе если пользователь передвигается по улице или совершает поездку на автомобиле [5]. Для того чтобы получить историю местоположений мобильного устройства, достаточно зайти на официальный сайт Google по ссылке: https:// maps. google.com/ locationhistory/, выполнить аутентификацию и выбрать интересующий нас временной интервал местоположений [7].

Уголовный процесс в силу различных причин не настолько «мобилен», ограничен, в том числе рамками «понимания» законодателем механизмов получения информации с электронных носителей. В результате в существующие правила традиционных следственных действий (обыск и выемка) «встроены» положения об изъятии электронных носителей информации, без анализа различий между такими носителями. Однако изъятие жесткого диска с персонального компьютера конкретного пользователя и изучение базы данных ЦОД из 100 серверов – задачи разного уровня сложности, требующие дифференцированного подхода.

Такие носители данных, как сетевые хранилища, Paas, IaaS, облачные хранилища, CMS, позволяют получить только информацию, без возможности извлечения носителя (и получения мета-данных), что делает невозможным проведение необходимых процессуальных «манипуляций» для придания такому носителю статуса вещественного доказательства. Полагаем, что изучение вышеперечисленных носителей данных с целью получения доказательственной информации по делу не укладывается в рамки «классического» обыска или выемки и предусмотренное ч. 91.1 ст. 182, п. 3.1 ст. 183 УПК РФ участие специалиста не спасает ситуацию. В распоряжение должностного лица, осуществляющего производство по уголовному делу, поступает только информация, без ее материального носителя, что требует некоего иного процессуального оформления с целью сохранения доказательственного значения такой информации. Для их изучения в ходе уголовного судопроизводства необходимы специализированный механизм и процессуальная форма, детальная регламентация (возможно, в виде «специального вида» выемки электронной информации (без получения носителя) – для облачных хранилищ либо в виде производства экспертизы в месте нахождения базы данных ЦОД).

Таким образом, говорить о возможном правовом регулировании процедуры использования электронных носителей информации в качестве доказательств по уголовным делам можно только в случае, если имеет место быть ситуация, предполагающая возможность обнаружения, изъятия и фиксации электронного носителя в материальном виде (в простом варианте – персональный компьютер в жилище или офисе). Если же доступ к материальному носителю электронной информации затруднен или невозможен, то следует констатировать тот факт, что действующий УПК РФ сегодня оставляет эти ситуации не урегулированными.

Литература

1. *Федеральный* закон от 06.04.2011 № 63-ФЗ (ред. от 23.06.2016) «Об электронной подписи» // Собрание законодательства РФ. 2011. № 15. Ст. 2036.

2. *Федеральный* закон от 27.07.2006 № 149-ФЗ (ред. от 19.12.2016) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3448.

3. *ГОСТ* Р 7.0.8–2013. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения (утв. Приказом Росстандарта от 17.10.2013 № 1185-ст). В соответствии с Приказом Росстандарта от 17.10.2013 № 1185-ст данный документ введен в действие с 1 марта 2014 года. Документ опубликован не был.

4. *ГОСТ* 2.051–2013. Межгосударственный стандарт. Единая система конструкторской документации. Электронные документы. Общие положения. Приказом Федерального агентства по техническому регулированию и метрологии от 22 ноября 2013 г. № 1628-ст межгосударственный стандарт ГОСТ 2.051-2013 введен в действие в качестве национального стандарта Российской Федерации с 1 июня 2014 г. (Докипедия: ГОСТ 2.051–2013 ЕСКД. Электронные документы. Общие положения).

5. *Нестеров А.Д.* Получение информации из облачных хранилищ при расследовании инцидентов в сфере информационной безопасности. URL: http://sci-article.ru/stat.php?i=1433879423

6. *Тушканова О.В.* Терминологический справочник судебной компьютерной экспертизы: справ. пособие. М.: ЭКЦ МВД России, 2005. 56 с.

7. *Типовые* экспертные методики исследования вещественных доказательств: Ч. I / под ред. канд. техн. наук Ю.М. Дильдина; общ. ред. канд. техн. наук В.В. Мартынова. М.: ИНТЕР-КРИМ-ПРЕСС, 2010. 568 с.

Chadnova Irina V., Sokolovskaya Natalia S., Kirsanov Artem Yu. Tomsk state University of control systems and Radioelectronics (Tomsk, Russian Federation)

TO THE QUESTION OF USE OF ELECTRONIC DATA STORAGE DEVICES IN CRIMINAL PROCEDURE

Key words: process of proof, investigative action, electronic data storage device, evidence, search, seizure.

The article deals with procedural possibilities for the use of different types of electronic data, including electronic data storage devices. Under the conditions of dynamic development and the extending use of electronic data storage devices, criminal trial faces more and more urgent and demanded tasks of receiving and saving information from electronic data storage devices, and of developing the procedural rules of transformation of the obtained data into proofs.

The Criminal Procedure Code of the Russian Federation operates with such concepts as "electronic control devices", "e-mail", "electronic messages", "digital signature", "the strengthened qualified digital signature", " electronic document", "the document drawn up in the electronic way" "electronic data storage devices" without establishing an accurate regulation for their use in appropriate cases. The research of electronic data storage devices in the course of investigative operations and transformation of the received data in proofs cause the greatest number of questions.

Having analyzed the types of electronic data storage devices and the algorithm for obtaining data from different types of devices, the authors conclude that traditional legal rules for search and seizure cannot be applied to such systems of storage as network and cloudy media due to their specificity. Nowadays, regulations on the withdrawal of electronic media of information, without analysis of distinctions between them "are built in" the existing rules of traditional investigative actions (search and seizure). Whereas network storages, Paas, IaaS, cloudy storages, SMS allow to obtain only information, without the possibility of extracting electronic media, it is impossible to carry out any necessary procedural "manipulations" for giving such electronic media the status of physical evidence. The officer involved in criminal proceedings will have only the information without its material storage device and this requires some other procedural registration for preserving the evidentiary value of such information. Their research during criminal legal proceedings requires a specialized mechanism, procedural form, and a detailed regulation with fixing in separate procedural (investigative) action (in the form of

"a special type" of seizure of electronic information (without receiving the storage device) – for cloudy storages, or in the form of expert examination in the location of database of DPC).

References

1. Russian Federation. (2011) Federal'nyy zakon ot 06.04.2011 № 63-FZ (red. ot 23.06.2016) "Ob elektronnoy podpisi" [Federal Law No. 63-FZ of April 6, 2011 (as amended on June 23, 2016) "On electronic signature"]. *Sobranie zakonodatel'stva RF – Legislation Bulletin of the Russian Federation*. 15. Art. 2036.

2. Russian Federation. (2006) Federal'nyy zakon ot 27.07.2006 № 149-FZ (red. ot 19.12.2016) "Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii" [Federal Law No. 149-FZ of July 27, 2006 (as amended on December 19, 2016) "On Information, Information Technologies and Information Protection"]. *Sobranie zakonodatel'stva RF – Legislation Bulletin of the Russian Federation*. 31(1). Art. 3448.

3. Russian Federation. (2013a) *GOST R 7.0.8-2013. National standard of the Russian Federation. The system of standards on information, librarianship and publishing. Office work and archival business. Terms and definitions (approved by Order № 1185-cm of Rosstandart of October 17, 2013).* (In Russian). [The document was not published].

4. Russian Federation. (2013b) *GOST 2.051-2013. Interstate Standard. The unified system of design documentation. Electronic documents. General provisions*. (In Russian).

5. Nesterov, A.D. (2015) *Poluchenie informatsii iz oblachnykh khranilishch pri rassledovanii intsidentov v sfere informatsionnoy bezopasnosti* [Obtaining information from cloud storages while investigating incidents relating to information security]. [Online] Available from: http://sci-article.ru/stat.php?i=1433879423.

6. Tushkanova, O.V. (2005) *Terminologicheskiy spravochnik sudebnoy komp'yuternoy ekspertizy* [Terminological Reference Book of Forensic Computer Expertise]. Moscow: ETC of the Ministry of Internal Affairs of Russia.

7. Dildin, Yu.M. & Martynov, V.V. (eds) (2010) *Tipovye ekspertnye metodiki issledovaniya veshchestvennykh dokazatel'stv* [Typical expert techniques for the study of physical evidence]. Moscow: INTERKRIM-PRESS.