ПАВЕЛ ГЕННАДЬЕВИЧ СМАГИН,
преподаватель кафедры уголовного процесса ФГКОУ ВПО «Воронежский институт МВД России»

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ ПРИ РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Раскрываются понятие и сущность электронного документа в контексте возможности его использования в ходе предварительного расследования преступлений.

Ключевые слова: электронный документ, документооборот, электронная цифровая подпись, уголовное судопроизводство, расследование, следователь, доказательство.

P.G. Smagin, Lecturer, Subdepartment of Criminal Procedure Russia MI Institute (Voronezh City); **e-mail: pasha_smagin@mail.ru, tel.: 8 (473) 247-67-07.**

Specificities of using electronic documents in detecting and clearing-up crimes.

The concept and main points of an electronic document within the context of possibilities of its using in preliminary investigating crimes are revealed.

Key words: electronic document, workflow, electronic digital signature, criminal proceedings, investigation, investigator, evidence.

На современном этапе развития общества трудно себе представить жизнь без ставших уже привычными мобильной связи, компьютерной техники, сети Интернет, локальных сетей и т.д. Однако все эти достижения научно-технического прогресса в сфере коммуникаций, высоких технологий и компьютерной техники зачастую не используются в деятельности сотрудников правоохранительных органов. Проведенный анализ законов и ведомственных нормативных актов, регламентирующих процесс раскрытия и расследования преступлений в органах внутренних дел, доказывает обоснованность высказанного утверждения.

Так, обращаясь к приказу МВД России от 18 июня 2010 г. № 445 «О некоторых вопросах обеспечения органов предварительного следствия в системе Министерства внутренних дел Российской Федерации отдельными материально-техническими средствами»[1], отметим, что в нем закреплены нормы обеспечения вычислительной, криминалистической и иной техникой органов предварительного следствия в системе МВД. К числу таких средств наряду со ставшими уже давно всем привычными персональными компьютерами отнесены съемный жесткий диск, сканер, картридер многоформатный, устройство Bluetooth, видеокамера цифровая с жестким диском HDD, DVD-проектор и т.д. Однако в условиях ежегодного роста преступности этого уже оказывается недостаточно. Более того, положения приказа все еще остаются в большей части декларированными.

Существование криминалистических банков данных и учетов на современном этапе не оказывает решающего воздействия на процесс раскрытия и расследования преступлений по ряду причин - зарегистрированными субъектами и пользователями банков данных является небольшое число сотрудников ОВД и, как правило, сотрудники органов расследования в эту группу не входят, что негативно сказывается на эффективности использования криминалистических, розыскных, справочных и иных учетов ОВД следственными подразделениями. Второй причиной можно назвать низкую квалификацию субъектов расследования и их нежелание использовать передовой опыт. И наконец, законодатель в достаточной степени не регламентирует использование достижений в области информационных технологий при производстве расследования.

Однако большим шагом вперед, как нам представляется, можно считать принятие Правительством Российской Федерации национального проекта «Электронная Россия», с помощью которого получило свое развитие довольно большое число концепций и программ использования информационных технологий в различных отраслях, ведомствах и министерствах.

В целях совершенствования информационного обеспечения органов внутренних дел Российской Федерации и внутренних войск МВД России, определения основных приоритетов, принципов и направлений его развития, активизации научно-исследовательской и опытно-кон-

структорской деятельности в области информатизации в 2008 г.[2] была принята Концепция информатизации органов внутренних дел Российской Федерации и внутренних войск МВД России до 2012 г.[3] Концепция определяла цели, задачи, принципы и основные направления в области информатизации органов внутренних дел и внутренних войск МВД России, учитывала тенденции развития информационных технологий как в Российской Федерации, так и за рубежом, особенности и возможности их применения в деятельности МВД России.

По мнению законодателя, в первую очередь должны быть решены следующие задачи:

совершенствования информационного обеспечения органов внутренних дел на основе реконструкции и оборудования объектов органов внутренних дел новыми и перспективными телекоммуникационными и программно-техническими комплексами с использованием современных телекоммуникационных, информационных и биометрических технологий;

создания интегрированной универсальной транспортной среды связи органов внутренних дел на базе единых технологий, схемных решений и наборов типовых программно-аппаратных средств;

организации санкционированного оперативного доступа сотрудников органов внутренних дел к информационным ресурсам общего и специального назначения в режиме реального времени;

организации информационного и телекоммуникационного взаимодействия с другими правоохранительными органами, органами государственной и исполнительной власти;

обеспечения технической возможности информационного обмена МВД России в процессе межгосударственного сотрудничества правоохранительных органов в борьбе с преступностью;

уменьшения трудоемкости и финансовых затрат при накоплении и обработке информации, а также значительного сокращения времени получения требуемой информации сотрудниками органов внутренних дел в процессе оперативно-служебной деятельности.

Однако до сих пор какого-либо серьезного сдвига в работе следственных подразделений ОВД не произошло, как нам представляется, по причине того, что поставленные задачи не в достаточной степени регламентированы ведомственными нормативными актами. Под большим вопросом также остается такая обширная область, как сфера программного обеспечения, которая в вышеназванных документах не затрагивается даже в части указания принципов и целей его функционирования.

В контексте сказанного хотелось бы остановиться на том, что процесс внедрения информационных технологий в ОВД необходим не только в сфере глобального взаимодействия между государствами, органами государственной власти при расследовании преступлений, как это следует из указанных документов, что, несомненно, правильно и востребовано практикой, но и в повседневной работе органов расследования - при производстве процессуальных действий и оперативно-розыскных мероприятий. Однако такие положения практически лишены правовой основы.

В данной статье мы затронем лишь отдельные аспекты повышения эффективности процесса расследования преступлений с использованием информационных технологий, а именно возможности использования электронного документооборота и электронной цифровой подписи (далее - ЭЦП) при проведении следователем процессуальных действий.

Для раскрытия сущности использования ЭЦП в качестве разновидности подписи необходимо обратиться к понятию документа как основного элемента фиксации хода и результатов производства процессуальных действий и принятия решений в ходе уголовного судопроизводства.

Понятие документа закреплено в Федеральном законе от 29 декабря 1994 г. № 78-ФЗ "О библиотечном деле»[4] (в иных законах приведено схожее понятие); «документ - материальный объект с зафиксированной на нем информацией в виде текста, звукозаписи или изображения, предназначенный для передачи во времени и пространстве в целях хранения и общественного использования». Согласно данному определению вряд ли стоит признать, что текст, хранящийся в оперативной памяти цифрового устройства, является документом, так как сама оперативная память, т.е. носитель информации, не имеет назначения для передачи во времени и пространстве - она выполняет иные функции.

В контексте излагаемых рассуждений считаем целесообразным обратиться к понятию электронного документа, официальное толкование которого закреплено в ст. 3 Федерального закона от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи»[5]. Электронный документ - это документ, в котором информация представлена в электронно-цифровой форме (данный закон утрачивает силу с 1 июля 2013 г. в связи с принятием Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи», в котором понятия электронного документа не содержится)[6]. В приведенном понятии используется словосочетание «электронно-цифровая форма», однако при изучении вышеуказанного закона раскрыть сущность этой формы и само-

го документа в целом не удается. В некоторой степени позиция законодателя оправдывается тем, что информация кодируется в виде цифр «1» и «О», т.е. двухразрядной системы, которые представлены в электронной форме, однако все большее распространение сегодня получают 32- и 64-разрядные системы, где для кодировки используются латинские буквы.

Еще одно понятие электронного документа приведено в Законе от 29 июля 2006 г. «Об информации, информационных технологиях и о защите информации» (далее - Закон «Об информации»)[7] - 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.

Несмотря на достаточно четкое и обоснованное определение электронного документа, отдельные авторы в своих диссертационных исследованиях предлагают весьма специфические определения рассматриваемых понятий, которые, как представляется, имеют неоднозначное толкование. Так, Л.Б. Краснова в своей диссертации предлагает следующие понятия: «*Электронный документ* - один или несколько взаимосвязанных по установленному правилу файлов, содержащих совокупность электронно-цифровых объектов, отражающих сведения о лицах, предметах, фактах, событиях, явлениях и процессах; отражающих реквизиты, позволяющие подтвердить его подлинность и целостность; имеющих возможность представления в форме, пригодной для восприятия человеком. *Электронно-цифровой объект* - помеченная система дискретных электронных сигналов, несущих какую-либо информацию, параметры которой представлены в форме, пригодной для ее автоматизированной обработки, хранения и передачи с использованием средств вычислительной техники (компьютеров)»[8].

Думается, данные определения не могут быть использованы в уголовно-процессуальном законодательстве РФ в связи с тем, что они раскрывают лишь одну сторону сущности электронного документа, а это затрудняет использование данного понятия в процессе расследования.

В подтверждение данных слов и учитывая практическую деятельность правоохранительных органов, отметим, что на месте проведения следственных действий наиболее часто встречаются иные формы электронных документов: компьютерные файлы и каталоги (текстовые и графические), различные сетевые интернет-протоколы, электронная почта, сообщения в мобильных телекоммуникационных сетях и т.д.[9] В специальной литературе, посвященной вопросам классификации электронных документов, существуют следующие подходы к рассмотрению данной проблемы.

Так, Т.Э. Кукарникова в своей диссертации «Электронный документ в уголовном процессе и криминалистике» предлагает следующую классификацию:

по форме существования - электронные документы, существующие в компьютерной системе, могут быть классифицированы на материальные и виртуальные;

источнику происхождения - электронные документы, создаваемые пользователем и самой системой (т.е. самой электронной средой);

содержанию - электронные документы могут быть файлами, содержащими текстовую информацию, графику, анимацию, видеоряд, а также информацию, записанную специальными кодами или обозначениями;

степени защищенности - открытые/закрытые электронные документы[10].

В свою очередь, В.А. Мещеряков ввел понятие «виртуальный документ» и определил его как «совокупность информационных объектов, создаваемую в результате взаимодействия пользователя с электронной информационной системой»[11].

Однако, констатируя тот факт, что до настоящего времени пока еще не выработан общепризнанный подход к определению термина «электронный документ», вызывающий некоторые трудности в правовом регулировании соответствующих отношений, на данном этапе развития науки следует исключить упоминание в УПК РФ[12] различных видов «электронной информации», но закрепить методы и правила по ее обработке и использованию.

Основываясь на вышеизложенных рассуждениях и опираясь на Закон «Об информации...», считаем, что не имеет смысла уточнять в законодательных актах форму и вид предоставления информации, потому что это будет вносить неопределенность в понятие ее сущности и ограничивать ее использование.

В связи с этим предлагаем следующую редакцию ч. 8 ст. 166 УПК РФ: «К протоколу прилагаются фото-, аудио-, видео- и иные носители информации, на которых зафиксированы сведения, полученные при производстве следственного действия».

Кратко осветив понятие электронного документа, необходимо остановиться на том, что в настоящее время одним из приоритетных направлений государственной политики является качественное и количественное увеличение электронного документооборота с использованием

сети Интернет между различными государственными органами и населением. В свою очередь, соглашаясь с позицией А.В. Николаева, отметим, что Интернет является еще и элементом структуры в системе информационного обеспечения раскрытия и расследования преступлений[13].

В настоящее время определенные перспективы развития открываются в связи с реализацией концепции развития единой информационно-телекоммуникационной системы органов внутренних дел (далее - ЕИТКС МВД России), одним из положений которой выступает обеспечение перевода в электронную форму различных процедур взаимодействия с гражданами и организациями, а также предоставление электронных сервисов оказания услуг населению. Указанную функцию предполагается реализовать за счет организации в установленном порядке взаимодействия закрытой части Правоохранительного портала, формируемой с использованием технических возможностей ЕИТКС ОВД, и открытой части Правоохранительного портала Российской Федерации, функционирующей по каналам связи сети Интернет, создаваемого в рамках ФЦП «Электронная Россия (2002-2010 гг.)»[14], однако до настоящего времени закрытая часть такого портала не функционирует. Но приведенные положения концепции не конкретизируют применение указанных функций в практической деятельности органов внутренних дел. Частично это сделано в приказе МВД России от 12 декабря 2011 г. N° 1221 «Об утверждении Административного регламента системы Министерства внутренних дел Российской Федерации по предоставлению государственной услуги по осуществлению приема граждан, обеспечению своевременного и в полном объеме рассмотрения устных и письменных обращений граждан, принятию по ним решений и направлению заявителям ответов в установленный законодательством Российской Федерации срок»[15], где утверждается, что для приема обращений в форме электронных сообщений (интернет-обращений) применяется программное обеспечение, предусматривающее обязательное заполнение заявителем реквизитов, необходимых для работы с обращениями. Интернет-обращение распечатывается, дальнейшая работа с ним ведется как с письменным обращением. Как видно, интернет-технологии применяются лишь для получения документов от граждан, но в дальнейшем они обрабатываются в обычном порядке, что несколько непонятно, если обратиться к государственному стандарту (ГОСТ) от 1 июля 1987 г. № 6104-84 «Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники»[16] и постановлению Госстандарта от 24 сентября 1986 г. № 2781 «Методические указания по внедрению и применению ГОСТ 6104-84»[17], где указано, что вышеназванные документы могут обладать юридической силой.

Таким образом, возникает следующая проблема - является ли полученное по электронной почте заявление документом, обладающим юридической силой, и может ли оно служить поводом для возбуждения уголовного дела. Представляется, что в настоящий момент все же нет, так как в принципе достаточно тяжело идентифицировать отправителя электронного документа, в связи с чем после проверки такого заявления сотрудник ОВД должен составить рапорт в соответствии со ст. 143 УПК РФ об обнаружении признаков преступления, который и будет служить поводом для возбуждения уголовного дела. Однако если документ будет подписан с помощью электронно-цифровой подписи, то, с одной стороны, такая форма заявления будет соответствовать требованиям УПК РФ, но с другой - ч. 5 ст. 141 УПК РФ в таком случае предписывает составление того же рапорта.

Гораздо сложнее ситуация складывается с делами частного и частно-публичного обвинения, которые предполагают в качестве повода для возбуждения уголовного дела только наличие заявления от пострадавшего лица, что посредством Интернета в настоящее время сделать не представляется возможным. Более того, не совсем ясна в приведенных случаях процедура предупреждения заявителя об уголовной ответственности по ст. 306 УК РФ.

На основании вышеизложенного выглядит весьма целесообразным предложение о внесении изменений в ст. 141 УПК РФ о возможности приема заявлений в электронном виде. При этом необходимо в обязательном случае учитывать требования, предъявляемые к использованию информационных технологий в сфере уголовного судопроизводства, - законности, эффективности и достоверности.

Несмотря на существующие недостатки, следует признать, что электронный документооборот завоевывает все более прочные позиции. Для передачи запросов, например при розыске сотовых телефонов по идентификационному номеру IMEI, следователь может использовать ресурсы не только почтовой системы магистральной сети передачи данных- (МСПД) МВД России, построенной на коммуникационных узлах «Дионис», но и общераспространенных серверов www.mail.ru, www.yandex.ru. Данное положение позволит обмениваться почтовыми сообщениями не только внутри сети МВД России, но и за ее пределами, что существенно повысит эффективность рас-

крытия преступлений. Следует учитывать, что обмен электронными документами должен осуществляться с использованием современных средств защиты (электронная подпись, криптография). Использование общераспространенных серверов www.mail.ru,www.yandex.ru позволит следователю давать поручения, ориентировки, посылать фотографии и иную мультимедийную информацию непосредственно в сельские опорные пункты полиции, однако при этом должно быть соблюдено условие подключения опорного пункта к сети Интернет. Этого можно добиться путем использования сотовой сети и GPRS, которые сейчас распространены повсеместно. В свою очередь, это даст участковым уполномоченным возможность самостоятельно обращаться к существующим объектам учета в ИЦ, принимать сообщения и заявления граждан по сети Интернет, а также беспрепятственно передавать накопленный материал посредством электронной почты в дежурную часть для регистрации и последующей проверки. Все это позволяет сократить время реагирования служб и подразделений ОВД на совершенные правонарушения и соответственно повысить раскрываемость преступлений.

Так, находясь на рабочем месте в деревне М., к участковому уполномоченному обращается гражданин К. и сообщает, что 10 минут назад трое неизвестных с использованием ножа в качестве оружия совершили на него разбойное нападение и похитили сотовый телефон, после чего скрылись на автомашине ВАЗ 2112 р/з Х 100 ** (последние буквы потерпевший не запомнил). Участковый уполномоченный принимает заявление и получает объяснение от гражданина К., после чего предлагает по приметам опознать лиц, совершивших на него нападение, предварительно связавшись по каналу связи GPRS с информационным центром. Одновременно участковый уполномоченный проверяет по базе данных автомашину и ее владельца, сообщает в дежурную часть и передает посредством электронной почты ориентировку (фоторобот может быть составлен с использованием программы Faces), далее направляется запрос в компании сотовой связи, которые могут сообщить примерное местоположение сотового телефона. По полученной информации дежурный по ОВД принимает неотложные меры по розыску и задержанию лиц, совершивших преступление.

С технической стороны проведение данных мероприятий и раскрытие преступления требуют персонального компьютера и сети Интернет. ЕИТКС в данном случае может служить средством связи дежурной части с опорным пунктом, но никак не с офисами сотовых компаний. Важными моментами в приведенном примере служат передача мультимедийных сообщений, юридическая сила передаваемых документов, в частности ответов сотовых компаний, и возможность регистрации в дежурной части сообщения о преступлении, полученного в электронном виде. Эффективность внедрения и использования указанных технологий подтверждается проведенным анкетированием. На вопрос: «Необходимо ли Вам при исполнении должностных обязанностей быть всегда на связи и иметь доступ к сети ЕИТКС и Интернету вне пределов ОВД?» - 63% опрошенных ответили утвердительно, из них доля сотрудников, представляющих постовые и передвижные подразделения, составляет около 59%.

Помимо возможности использовать информацию, содержащуюся в интегрированных банках, как просто оперативную либо справочную, интересна перспектива придания юридической силы таким документам. Например, при доступе субъекта расследования к базе данных о судимостях лиц необходимо предусмотреть возможность распечатки такой информации с помощью принтера и придания ей юридической силы. Опять же данный аспект необходимо рассматривать с двух сторон. Первая составляющая - это техническая сторона. Необходимо, чтобы информация, передающаяся по локальным сетям, была достоверной и объективной, а у органов расследования имелась возможность проверки подлинности этой информации. Оптимальную возможность такой проверки предусматривает электронный документ с электронной цифровой подписью, понятие которого закреплено в ФЗ «Об электронной цифровой подписи»[18]. Электронная цифровая подпись - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе. В соответствии с Законом «Об электронной подписи»[19] электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Также хотелось бы отметить, что приказом Министерства по налогам и сборам от 3 марта 2003 г. № БГ-3-28/96 «Об утверждении Порядка доступа к конфиденциальной информации напо-

говых органов»[20] в органах МНС уже закреплена возможность составления и направления запросов в электронном виде по телекоммуникационным каналам связи, однако из-за отсутствия механизма реализации электронной цифровой подписи должностного лица (в связи с отсутствием центров сертификации и выдачи подписей в системе МВД России) данное положение так и осталось декларативным.

В свою очередь, наличие канала связи между различными ОВД позволяет дистанционно проводить следственные действия, например допрос. Для проведения допроса на значительном удалении следователя от допрашиваемого лица можно предложить следующий алгоритм проверки подлинности полученных показаний и придания свойства допустимости полученным показаниям. По окончании допроса следователь по электронной почте отправляет файл с протоколом допроса, который по прочтении подписывается допрашиваемым лицом с использованием технологии электронной цифровой подписи (в УПК РФ прямо не указано, каким видом подписи должен быть подписан документ). Однако, к сожалению, на данный момент нормы Федерального закона «Об электронной цифровой подписи» применяются недостаточно широко и по большей части являются декларированными.

Таким образом, проведенный анализ продемонстрировал, что до настоящего времени пока еще не выработан общепризнанный подход к определению термина «электронный документ», вызывающий определенные трудности в правовом регулировании соответствующих отношений, в связи с чем следует исключить упоминание в УПК РФ различных видов «электронной информации», а закрепить методы и правила по ее обработке и использованию.

Необходимо исключить из УПК РФ вид и форму представления информации, в связи с этим предлагаем изложить ч. 8 ст. 166 УПК РФ в следующей редакции: «К протоколу прилагаются фото-, аудио-, видео- и иные носители информации, на которых зафиксированы сведения, полученные при производстве следственного действия».

которых вопросах обеспечения органов предварительного следствия в системе Министерства внутренних дел Российской Федерации отдельными материально-техническими средствами» // СПС КонсультантПлюс (документ опубликован не был). 2012.

[2] Стоит отметить, что принятая в 2002 г. приказом МВД России № 562 Концепция развития информационно-вычислительной системы МВД России на 2002-2006 гг. не достигла своей цели.

[3] Приказ МВД России от 4 апреля 2009 г. № 280 «Об утверждении Концепции информатизации органов внутренних дел Российской Федерации и внутренних войск МВД России до 2012 года» // СПС КонсультантПлюс. 2012.

[4] Федеральный закон от 29 декабря 1994 г. № 78-ФЗ О библиотечном деле» // Собрание законодательства РФ. 2002. № 2. Ст. 127.

[5] Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» // Собрание законодательства РФ. 2002. № 2. Ст. 127.

[6] В соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ данный документ был признан утратившим силу с 1 июля 2012 г. Федеральным законом от 10 июля 2012 г. № 108-ФЗ дата утраты силы перенесена на 1 июля 2013 г.

[7] Федеральный закон от 27 июля 2006 г. № 149-ФЗ Об информации, информационных технологиях и о защите информации» // Российская газета. 2006. 29 июля

[8] Краснова Л.Б. Компьютерные объекты в уголовном процессе и криминалистике: Автореф. дис. ... канд. юрид. наук. - Воронеж, 2005.

[9] Демин К.Е. Электронные носители как источники информации о личности // Информатизация и информационная безопасность правоохранительных органов. - М.: Академия управления МВД России, 2001. С. 300.

[10] Кукарникова Т.Э. Электронный документ в уголовном процессе и криминалистике. - Воронеж, 2005.

[11] Мещеряков В.А. Механизм следообразования при совершении преступлений в сфере компьютерной информации // Известия Тульского государственного университета. Сер.: Современные проблемы законодательства России, юридических наук и правоохранительной деятельности. - Тула, 2000. Вып. 3. С. 167.

[12] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ // СПС Консультант Плюс. 2012.

как элемент информационной системы раскрытия и расследования преступлений: Дис. ... канд. юрид. наук. - М.: РГБ, 2005

[14] Постановление Правительства РФ от 28 января 2002 г. № 65 «О федеральной целевой программе „Электронная Россия (2002-2010 годы)"» (ред. от 09.06.2010 г.) // Собрание законодательства РФ. 2002. № 5. С. 531.

[15] Приказ МВД России от 12 декабря 2011 г. № 1221 «Об утверждении Административного регламента системы Министерства внутренних дел Российской Федерации по предоставлению государственной услуги по осуществлению приема граждан, обеспечению своевременного и в полном объеме рассмотрения устных и письменных обращений граждан, принятию по ним решений и направлению заявителям ответов в установленный законодательством Российской Федерации срок» // СПС КонсультантПлюс. 2010.

[16] Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники: ГОСТ от 1 июля 1987 г. № 6104-84.

ГОСТ 6104-84: Постановление Госстандарта от 24 сентября 1986 г. № 2781 // СПС КонсультантПлюс. 2012.

[18] Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» // СПС КонсультантПлюс. 2011.

[19] Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» //СПС КонсультантПлюс. 2012.

[20] Приказ МНС России от 3 марта 2003 г. № БГ-3-28/96 «Об утверждении Порядка доступа к конфиденциальной информации налоговых органов» // Российская газета. 2003. 3 апр.