

ИНФОРМАЦИЯ И ЦИФРОВОЙ ФОНОДОКУМЕНТ

Д.т.н., профессор В.Р.Женило (Академия управления МВД России)

Поводом написания этого доклада послужила опубликованная в журнале «Специальная техника» (№ 4 за 2001 год) статья Каретникова М.К. «Футуристический взгляд на специальные технические средства». В ней затронуты большие вопросы цифровых (компьютерных) информационных технологий, связанные с юридической и доказательной силой всех современных видов информационных данных, представляемых в цифровой компьютерной форме. И в первую очередь это касается цифровых данных, воспринимаемых с помощью зрения и слуха. Этой проблеме посвящена большая часть указанной статьи.

В упомянутой статье основное внимание уделяется закрытию цифрового документа с помощью электронной цифровой подписи (ЭЦП) и затрагивается другая весьма болезненная проблема современной криминалистики – доказательная сила цифровых звукозаписей, фотографий, видеозаписей и т.п. Кроме того, говорится о том, что современные компьютерные технологии позволяют выполнять такие изменения содержания этих файлов, что ни один эксперт не сможет найти в них следы таких манипуляций. Тем самым, вольно или невольно, но автор статьи начал повторять аналогичную историю, имевшую место в нашей стране в 60-70-е годы, больно затронувшую криминалистическую фоноскопию. Доле в том, что в момент зарождения тогда еще нового вида криминалистической экспертизы – фоноскопической – некоторые инженеры института специальной техники заявили, что они могут сделать такой монтаж магнитных (аналоговых) фонограмм, следы которого никто и ни с какими приборами обнаружить не сможет. Это заявление сыграло весьма негативную роль в принятии магнитных фонограмм как вещественного доказательства в советском уголовном процессе.

Надо признать, что проблем с электронной цифровой подписью еще очень много. Поэтому в такой весьма консервативной сфере, как юриспруденция, она будет принята еще очень не скоро. Как только ЭЦП начнет внедряться в практику, так сразу же возникнет масса проблем, наподобие современных проблем компьютерных вирусов, защиты цифровых записей (файлов) от взлома, фальсификации и т.п. На настоящем этапе ЭЦП разрабатывается в лабораторных условиях, и она еще не прошла суровой практической проверки. Не зря говорят, что современные правила уголовного процесса написаны кровью. И поэтому, видимо, еще будет пролито немало крови в прямом и переносном смысле, прежде, чем новая технология ЭЦП методом проб и ошибок найдет приемлемые формы своего существования.

Взять, хотя бы, такую простую ситуацию, как подпись одного и того же электронного документа несколькими лицами. Например, как должна выглядеть процедура подписания протокола одновременно следователем и допрашиваемым? Или как должна подписываться комплексная или комиссионная экспертиза, выполненная группой экспертов?

Прежде чем перейти к вопросу применимости ЭЦП для защиты цифровых фонограмм, остановимся сначала на самой проблеме понятия информации и документа.

Многие современные проблемы документирования в цифровых информационных технологиях связаны с тем, что понятие информации в современной культуре человечества слишком уж многозначно. И эта многозначность, а следовательно и неопределенность, создает много трудностей не только в криминалистике, но и во всей культуре (в широком смысле).

Для пояснения сказанного рассмотрим вкратце вопрос – что такое информация.

Определений понятия информация сейчас существует очень много. Некоторые рьяные кибернетики утверждают, что до Н. Винера понятие информации вообще не существовало, и, якобы, именно он ввел и придумал это понятие. Философы разных течений дают свои определения в зависимости от того, к какому течению (направлению) они принадлежат. Принципиальная отличительная суть понятия информации у одних философов заключается в том, что они говорят – до тех пор, пока сообщение не прочитано (не услышано, не воспринято) субъектом, в нем (в сообщении) информации нет. Информация, якобы, возникает в самом субъекте в момент сравнения поступившего сообщения (сигнала) на вход «компаратора» субъекта. И если «компаратор сработал», то, значит, информация получена, и она в сообщении есть. А до этого в этом сообщении (сигнале) никакой информации нет.

В противовес этим другие философы утверждают, что информация в сообщении (сигнале) есть всегда, в независимости от того, получит (воспримет) субъект это сообщение или нет. При этом утверждается, что эта информация «сидит» (отражена) в *структуре* сообщения (сигнала). На это утверждение первые философы возражают – но тогда получается, что информация есть в любом сообщении, представляемом в той или иной материальной форме (в виде материального носителя информации). И этой информации будет бесконечно много, поскольку не оговаривается – до какого уровня детализации структуры материального носителя следует опускаться.

Например, в случае письменной речи можно ограничиться общей структурой букв, из которых составлен текст сообщения. А можно опуститься на уровень ниже и исследовать структуру отдельных букв (их начертания), выискивая индивидуальные особенности почерка, типографского шрифта в целом или отдельных символов и т.п. Или же можно изучать структуры отдельных линий для определения инструмента письма (или печати), или поверхности, на которой выполнялась рукопись или оттискивались литеры. А можно углубиться еще больше и исследовать структуру химического состава красителя пишущего инструмента. И так далее вплоть до примесей в красителе, изотопов в носителе информации и т.п. То есть, если остановиться на структу-

ре (которая, как утверждается, всегда несет информацию) молекулярного или атомарного уровня, то получается, что такое письменное сообщение будет содержать огромный объем информации (вопрос только – о чем?). Поэтому в пылу спора даже утверждается, что при бесконечном углублении в структуру носителя информации в нем информации становится бесконечно много.

Чтобы уйти от этого спорного момента некоторые философы даже предлагают ввести два понятия: потенциальной и кинетической информации (по аналогии с потенциальной и кинетической энергией).

Чтобы не приводить все, существующие в настоящее время, определения понятия информации (можно насчитать более десятка принципиально разных определений этого понятия), приведем лишь два, достаточно близко подходящих к упомянутым выше несовместимым философским определениям (течениям):

«Информация – это все то, что изменяет нас» (Г. Батесон)¹.

«Информация (от лат. informatio – разъяснение, изложение) – содержание сообщения или сигнала, сведения, рассматриваемые в процессе их передачи или восприятия; одна из *исходных* общенаучных категорий, отражающая *структуру* материи и способы ее познания, *несводимая к другим, более простым понятиям*»².

Принимая первое определение, получается, что непрочитанное письмо, действительно, информации не содержит. А даже если и прочитать письмо, то для кого-то в нем может оказаться информация, а для кого-то – нет. Но тогда, принимая это определение, получается, что внушение или гипноз, кнут или пряник тоже следует отнести к категории информации. Хотя, наверное, всякий согласится, что такое определение справедливо с той точки зрения, что некоторое сообщение для кого-то может оказаться информативным, а для кого-то – нет.

Золотую середину между определениями понятия информации, приведенными выше, занимает определение, данное К. Шенноном: «Информация – это все то, что снижает неопределенность»³.

Нечеткость любого известного определения понятия информации порождает множество алогизмов в использовании этого понятия в быту. Самый яркий из этих алогизмов сводится к тому, что дезинформацию иногда тоже называют информацией. Хотя, скорее всего, каждый из нас полагает, что информация – это всегда нечто истинное, а дезинформация – это всегда нечто ложное. Поэтому различать информацию по критерию истинно-ложно, видимо, не корректно. Информация всегда истинна. В этой части определение понятия информации через понятие структуры, приведенное выше, оказывается более корректным. Ведь структура – есть структура. Она не может быть истинной или ложной. Другое дело, что кто-то (или что-то) может изменять (искажать) эту структуру, утверждая при этом, что она полностью соответствует той или иной действительности. В таком случае правильнее было бы говорить, что структура в таком дезинформационном сообщении содержит информацию (которая всегда истинна) о некоторой действительности и о том, что эту структуру некто (или нечто) изменил в той или иной мере.

Приведенное философское отступление может показаться не принципиальным или не важным. Однако именно наша привычка или вера в одну из полярных философий не позволяет разобраться в одном из самых проблематичных в настоящее время понятий – информации. Более того, массовая некорректная интерпретация понятия информации привела даже к тому, что в некоторых странах все средства печати, радио и телевидения стали называться средствами массовой информации, вместо прессы, массмедиа⁴ и т.п., чего не было ранее до бурного роста и широкого распространения информационных технологий.

То, что понятие «информация» относится к категории идеального, шокирует очень многих. Это свойство идеальности предельно явно проявилось с появлением и разграничением понятий hardware и software в цифровых информационных технологиях. Как это ни парадоксально, но громадные полезные достижения в этой области оказались не только ненужными, но они еще проявили и некоторые болезненные и нерешенные проблемы, например, современной криминалистики, которая ранее, особенно в советское время, вся строилась исключительно на материалистическом философском веровании. Так, например, с позиции современного определения понятия следа стало практически невозможным использование цифровых информационных технологий для фиксации следов преступления с помощью цифровых фотокамер, магнитофонов и видеокамер. Суды отказываются принимать в качестве вещественных доказательств файлы с записями изображения или звука,

¹ “Information – that which changes us” (Gregory Bateson). Это определение взято из электронного словаря Web Dictionary of Cybernetics and Systems.

² Математический энциклопедический словарь. Москва, Советская энциклопедия, 1988, с. 821. Следует заметить, что в этом же словаре, но на странице 245 дается такое «определение»: «Информация (от лат. informatio – разъяснение, изложение) – основное понятие кибернетики». Вот, в общем-то, и все. Далее идут лишь разъяснения, но не определения. Однако и в этих разъяснениях говорится о том, что современное представление понятия «информации» пока еще интуитивно, и в науке оно еще окончательно не сформировано. В этой же статье приводятся очень интересные аналогии из других научных областей, где также существуют ключевые понятия, которые нельзя определить через иные – более простые понятия. Например, дать определение – что такое время, масса, энергия, пространство, площадь или объем никто не может. Но, тем не менее, человечество успешно пользуется этими понятиями и, более того, умеет измерять их значения количественно. Хотя, в природе таких эталонов и единиц измерения как секунда, метр или грамм не существует. Все эти единицы придумал человек для удобства хранения или передачи информации о тех или иных объектах или явлениях, которые он использует в своей жизни.

³ “Information – that which reduces uncertainty” (Claude Shannon). Это определение взято из электронного словаря Web Dictionary of Cybernetics and Systems.

⁴ The media - mass communications, eg television, radio, the press (A.S.Hornby. Oxford Advanced Learner's Dictionary of Current English // Special edition for the USSR, Volume II, Moscow - Oxford, 1982).

поскольку содержимое этих файлов можно изменять (редактировать), практически не оставляя никаких следов монтажа.

Нескончаемый антагонизм полярных философий приглушил реальное решение вопроса соотношения материального и идеального. В контексте темы данного доклада можно сказать так: не бывает материи без структуры, но и не бывает структуры без материи. Обе они «равнопервичны» и равноценны.

Простейший пример. Одна и та же структура молекулы, но с разными атомами придает химическому веществу разные свойства. Но и наоборот, изомеры, состоящие из одних и тех же атомов (с их одинаковым составом), но по-разному структурированные, тоже придают химическому веществу разные свойства. И поэтому говорить о том, что важнее – структура или атомарный (или молекулярный) состав – попросту некорректно. Все важно.

В этой связи, последнее философское отступление. Культура человечества не зря придумала две алгебры. Одну для описания законов, так сказать, материального мира, где $A+A=2A$. С помощью этой алгебры описываются все законы сохранения энергии, вещества, импульса, момента импульса и т.п. И вторую алгебру – для описания законов, скажем так, идеального мира, где $A+A=A$ и $A*A=A$, – это алгебра логики и теории множеств.

Теория информации, помимо обычной алгебры весьма активно использует, во-первых, теорию множеств и алгебру логики, а, во-вторых, теорию вероятностей, которая, в свою очередь, базируется на теории множеств.

Вот в такой «философской атмосфере» оказалась современная криминалистика (да и не только она), у которой важнейший ее объект – структура следа оказалась, благодаря современной цифровой информационной технологии, полностью оторванной от материального носителя и перенесена в чисто идеальную форму – цифровой компьютерный файл. Информация в файле, грубо говоря, «сидит» в битовой структуре файла. Но сами биты, как и файл в целом, не относятся к категории материального.

Решить проблему защищенности компьютерного файла от возможных фальсификаций (чтобы ему можно было бы придать статус документа) в настоящее время пытаются с помощью, так называемой, электронной цифровой подписи (ЭЦП). Но такая защита цифрового файла не отвечает всем требованиям криминалистики. Такая защита, например, не гарантирует создание нового документа, тоже защищенного с помощью ЭЦП, который был бы составлен из отдельных фрагментов разных речевых сигналов, извлеченных из совершенно других документов, тоже защищенных с помощью ЭЦП.

Электронная цифровая подпись – это, можно сказать, новый вид старого оформления магнитных фонограмм. ЭЦП не снимает проблемы аутентичности (подлинности, неподдельности) фонограмм. Рассмотрим этот вопрос чуть подробнее.

ЭЦП – это еще лишь зарождающийся элемент новой формы документирования. Теоретически и на еще не широком практическом опыте использования ЭЦП, вроде бы, подтверждается ее перспективность. Однако, что произойдет с технологией ЭЦП после реально широкого ее внедрения, и особенно после закрытия с помощью ЭЦП очень важных, дорогих и т.п. сведений, когда компьютерные вирусописатели, воры и взломщики займутся ЭЦП вплотную, предсказать очень сложно. Но, даже предполагая, что ЭЦП будет успешно жить так, как предполагают ее разработчики, можно с уверенностью сказать, что ЭЦП не решит криминалистические проблемы современной цифровой информационной технологии.

Можно приводить много доводов в «некриминалистичности» ЭЦП. Приведем лишь один – простейший. Предположим, что мы имеем цифровой электронный документ, в который внедрен такой цифровой информационный объект, как стандартный звуковой файл (например, в WAV формате).

Да, судя по идеологии ЭЦП, содержимое этого документа нельзя будет изменить ни на один бит, не оставив следа в защитной структуре. Но, несмотря на это, любой эксперт фоноскопист все равно может столкнуться с вопросом – а нет ли признаков монтажа во внедренном и закрытом с помощью ЭЦП цифровой фонограмме речи? Ведь остаются две возможности фальсификации этого внедренного звукового файла – *до* создания документа и *после*.

Если посмотреть на экспертную практику, то с уверенностью можно сказать, что и раньше практически все аналоговые фонограммы, поступавшие на криминалистическое исследование в том или ином виде, всегда были документально оформлены. Фонограммы на криминалистическое исследование поступают или от следственных органов или от оперативных служб разных правоохранительных органов. То есть, всегда эти фонограммы документально оформлены. А если это не так, то заключение эксперта просто не будет иметь никакой юридической силы. И поэтому его заключение не будет являться юридическим документом.

ЭЦП всего лишь позволяет эксперту принимать на исследование не вещественные доказательства, как ранее в традиционном понимании, а цифровые файлы, которые даже не вещественны (не материальны). Поэтому, как и раньше, следовательно, например, назначивший фоноскопическую экспертизу, может вполне обоснованно задать традиционный вопрос – а нет ли во внедренном в цифровой документ звуковом файле, закрытом с помощью ЭЦП, признаков монтажа?

Это пример ситуации «до». А вот пример возможной ситуации «после».

Некий злоумышленник, имея аутентичную цифровую фонограмму, закрытую с помощью ЭЦП, копирует ее (цифровым методом или заново оцифровывая воспроизводимый из документа звук), и затем, применяя цифровые информационные технологии, монтирует из нее новую (фальсифицированную) фонограмму. Фальсифицированную фонограмму он закрывает своей ЭЦП и заявляет, что его фонограмма аутентична.

В подобном случае, при хорошо сделанном компьютерном монтаже цифровых фонограмм эксперт фоноскопист, в принципе, может столкнуться с неразрешимостью поставленной перед ним задачи обнаружения признаков монтажа. И все это потому, что если злоумышленнику повезет с техническими характеристиками цифровой фонограммы, он сможет тасовать отдельные ее фрагменты как колоду карт.

Таким образом, говорить о защите цифрового звукового файла на уровне материального носителя информации бессмысленно, поскольку само понятие «файл» никак не привязано к материальному носителю информации. В таком случае остается только одно – говорить о защите звукового файла на уровне его структуры.

Можно предложить множество способов синтеза и подмешивания в структуру речевого сигнала защитного сигнала. Некоторые из этих структур должны быть полностью описаны в открытой печати и, более того, стандартизованы для быстрого их обнаружения общедоступными средствами и методами, например, с помощью обычных сонограмм. Но некоторые защитные структуры не должны быть не только широко опубликованы, но не должен даже излагаться и сам принцип формирования этих структур, чтобы снизить вероятность их распознавания, синтеза и вычитания из оригинальных фонодокументов.

Возможные способы защиты цифровых фонограмм изложены в других докладах в данном сборнике.