Научная статья
УДК 34:004:343.14:343.98.062:343.98.063
EDN: https://elibrary.ru/qjhwgw
DOI: https://doi.org/10.21202/jdtl.2025.25

Место цифровых фонограмм, видеограмм и видеофонограмм в системе электронных доказательств: теоретико-методологические основы классификации

Герман Николаевич Зубов

Независимый исследователь, Санкт-Петербург, Россия

Ключевые слова

видеограмма,
видеофонограмма,
доказательства,
право,
судопроизводство,
фонограмма,
цифровая криминалистика,
цифровые технологии,
экспертиза,
электронные
доказательства

Аннотация

Цель: исследование направлено на определение места цифровых фонограмм, видеограмм и видеофонограмм в системе электронных доказательств в российском судопроизводстве с формированием единого понятийного аппарата и классификационной системы для обеспечения эффективного использования в процессуальной практике.

Методы: методологическую основу исследования составляют всеобщий диалектический метод познания, общенаучные методы (описание, сравнение, обобщение, моделирование, анализ, синтез) и частнонаучные методы. Особое внимание уделено системно-структурному анализу нормативно-правовых актов, государственных стандартов в области информационных технологий, международных документов, регламентирующих работу с цифровыми доказательствами. Применены методы криминалистического исследования, формально-юридический метод толкования норм процессуального законодательства, компаративный анализ зарубежного опыта регулирования электронных доказательств.

Результаты: в ходе исследования выявлены и систематизированы ключевые причины правовой неопределенности электронных доказательств: многообразие форм представления, высокая уязвимость данных, недостаточная компетентность субъектов доказывания, несоответствие традиционным методам фиксации доказательственной информации. Разработана оригинальная классификация электронных доказательств и цифровых фонограмм, видеограмм, видеофонограмм с использованием критериев формы представления данных, способа записи, характера носителей информации. Сформулированы универсальные определения базовых понятий: электронные доказательства, цифровые доказательства, цифровая фонограмма, видеофонограмма,

носители данных, копия цифрового доказательства. Обоснована необходимость гармонизации процессуальных норм на основе государственных стандартов информационных технологий и международного опыта.

Научная новизна: впервые разработана комплексная методология формирования понятийного аппарата и классификации электронных доказательств, основанная на интеграции государственных стандартов информационных технологий с криминалистическими и процессуальными аспектами фиксации доказательственной информации. Введены универсальные термины и определения, отсутствующие в действующем российском законодательстве, адаптированные для всех видов судопроизводства с учетом специфики цифровой среды. Предложена типовая модель работы с цифровыми доказательствами, включающая этапы идентификации, сбора, получения, сохранения, анализа и представления. Обоснована категория цифровых фонограмм, видеограмм и видеофонограмм как подвида электронных дискретных цифровых доказательств.

Практическая значимость: результаты исследования могут быть использованы для совершенствования процессуального законодательства в части регламентации работы с электронными доказательствами, разработки ведомственных инструкций и практических рекомендаций для следователей, специалистов и экспертов по идентификации, сбору, фиксации, проверке и оценке цифровых доказательств. Предложенная классификация и понятийный аппарат способствуют унификации подходов к процессуальному оформлению электронных доказательств, минимизации процессуальных ошибок, повышению компетентности субъектов доказывания, обеспечению допустимости и достоверности цифровых фонограмм, видеограмм и видеофонограмм. Материалы исследования применимы в образовательном процессе при подготовке юристов, следователей, судебных экспертов, специализирующихся в области цифровой криминалистики.

Для цитирования

Зубов, Г. Н. (2025). Место цифровых фонограмм, видеограмм и видеофонограмм в системе электронных доказательств: теоретико-методологические основы классификации. *Journal of Digital Technologies and Law*, *3*(4), 636–659. https://doi.org/10.21202/jdtl.2025.25

Содержание

Введение

Российское законодательство позволяет использовать фонограммы, видеограммы и видеофонограммы (далее – ФВиВ)[1] в качестве доказательств в административном, арбитражном, уголовном и гражданском процессе, независимо от формы – аналоговой или цифровой, и способа их представления – файл в памяти устройства видеозвукозаписи, публикация в социальной сети и др.

К таким доказательствам могут относиться ФВиВ, записанные:

– в рамках оперативно-разыскной деятельности;

– следователем или специалистом при проведении следственных действий и протоколировании судебных заседаний;

– другими участниками процесса (обвиняемый, потерпевший, свидетель, истец, ответчик и т. д.);

– различными автоматизированными системами сбора и обработки звуковой и визуальной информации общего назначения: видеонаблюдения, записи телефонных переговоров и т. п.

Однако даже беглый взгляд на тексты процессуальных законов свидетельствует об отсутствии в них единообразия хотя бы на уровне наименования объектов, содержащих доказательственную аудиовизуальную информацию.

Так, результат записи аудиоинформации на материальный носитель (далее – фонограмма) в тексте законов называется:

– аудиозаписью (АПК РФ, ГК РФ, УПК РФ);

– аудиоматериалами (КоАП РФ);

– материалами аудиозаписи (УПК РФ);

– материалами звукозаписи (КоАП РФ);

– фонограммой (Закон об ОРД[2], ГК РФ, КоАП РФ).

Результат записи визуальной или аудиовизуальной информации (далее – видеограмма или видеофонограмма соответственно) именуется:

– видеограммой (Закон об ОРД);

– видеозаписью (АПК РФ, УПК РФ);

– видеоматериалами (КоАП РФ);

– материалами видеозаписи (КоАП РФ).

Процессуальные законы не проводят различий между видеограммой и видеофонограммой, между цифровыми или аналоговыми ФВиВ, хотя эти различия объективно существуют и могут отражаться на порядке процессуального оформления имеющей доказательственное значение аудиовизуальной информации, а также на процедуре их проверки и оценки как доказательств, что можно проиллюстрировать на следующем примере. Следователь поставил перед экспертом вопрос о наличии на «видеозаписи» следов монтажа и представил на экспертизу видеофонограмму. Эксперт в соответствии с буквой вопроса провел исследование видеоряда

---

1 В соответствии с названиями, используемыми в ГОСТ 13699-91. Запись и воспроизведение информации. Термины и определения. https://clck.ru/3QH6Ac

2 Здесь и далее – Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ.

видеофонограммы, но проигнорировал звуковой ряд, который, согласно материалам дела, содержал доказательственную информацию и подвергался при этом монтажу (Зубов, Тимошенко, 2014).

Подобная ситуация не вызывает удивления, учитывая, что в нормативно-правовых актах – как в законах, так и ведомственных инструкциях, руководствах, рекомендациях и т. п. – отсутствуют даже базовые для ФВиВ понятия – электронные и цифровые доказательства. С этими понятиями в процессуальных законах и постановлениях высших судов принято отождествлять сведения, представленные: «в электронном виде» (КоАП РФ); на «электронных носителях» (УПК РФ) или «электронные документы» (ГПК и АПК РФ). При этом прямое определение термина «электронный носитель» в текстах нормативно-правовых актов также отсутствует. Его смысл раскрывается через контекст и косвенные указания. Как правило, под «электронным носителем» понимают устройство для записи, хранения и использования исключительно цифровых данных.

Определение «электронного документа», которое приводится в Законе «Об информации, информационных технологиях и о защите информации»[3]: «документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах», не применимо к цифровым ФВиВ, так как цифровые ФВиВ, электронное происхождение которых не вызывает сомнения, могут быть записаны или воспроизведены без использования ЭВМ. Не менее важно и то, что если УПК РФ причисляет ФВиВ к «иным документам», то другие процессуальные законы относят документы к письменным доказательствам, которыми ФВиВ явно не являются.

Более точное определение «электронного документа» содержится в Законе «Об арбитраже (третейском разбирательстве) в Российской Федерации»[4]: «Электронный документ, передаваемый по каналам связи, – информация, подготовленная, отправленная, полученная или хранимая с помощью электронных, магнитных, оптических или аналогичных средств, включая электронный обмен данными и электронную почту».

Таким образом, можно констатировать, что в российском законодательстве отсутствует единое, универсальное, исчерпывающее правовое определение понятия «электронные доказательства» (далее – ЭлД), не отражены родовые черты ЭлД и их классификация, что препятствует пониманию особенностей использования данного вида доказательств в судопроизводстве и их объективную оценку в части допустимости и достоверности, препятствует созданию практических руководств для следователей и специалистов по работе с данным видом доказательств.

---

3 Об информации, информационных технологиях и о защите информации. № 149-ФЗ от 27.07.2006. (2006). КонсультантПлюс. https://clck.ru/3QH6Dq

4 Об арбитраже (третейском разбирательстве) в Российской Федерации. № 382-ФЗ от 29.12.2015 (ред. от 08.08.2024). КонсультантПлюс. https://clck.ru/3QH6YV

Аналогичная ситуация наблюдается в публикациях российских практикующих юристов и правоведов (Воронин, 2021; Малык, 2023; Полициан, 2022; Черецких, 2023), которые также не могут прийти к единому мнению в отношении ЭлД. Некоторые не видят разницы между цифровыми и электронными доказательствами, другие причисляют их к разным видам, но и те и другие отмечают несовершенство российского законодательства в части использования ЭлД и, как правило, склоняются к необходимости выделения ЭлД в отдельный вид.

1. Причины правовой неопределенности электронных доказательств

Среди факторов, обуславливающих проблемы правовой неопределенности ЭлД, можно выделить несколько ключевых.

Во-первых и прежде всего, многообразие форм и видов представления ЭлД, не соответствующих принятой в процессуальной практике письменной форме фиксации доказательственной информации.

К доказательствам, которые в настоящее время принято называть электронными, относят: собственно электронные документы, в том числе электронные образы письменных документов; переписка в электронной почте и мессенджерах; файлы различного формата; базы данных, метаданные; логи серверов и др. Часть из них может быть представлена: в физическом виде (на материальном носителе, например, во внешней памяти устройства звуко- или видеозвукозаписи); в виртуальном виде (например, видеофонограмма в интернет-сервисе YouTube[5]). При этом доказательственная информация может быть относительно просто, зачастую обманчиво просто, перенесена с одного носителя на другой и существовать во множестве неотличимых друг от друга копий, а ее воспроизведение и восприятие в некоторых случаях невозможны без использования программных и технических средств, применение которых зачастую требует от пользователя наличия специальных знаний в области информационных технологий.

Все это, безусловно, усложняет идентификацию, сбор, получение, классификацию и описание ЭлД в протоколе, а также унификацию подходов к их оценке, порождает необходимость использования различающихся, в том числе непривычных для участников процесса, технологий их проверки: электронной подписи (АПК РФ, ГК РФ, КоАП РФ, УПК РФ, Закон об электронной подписи[6]); хеш-функции (ГОСТ Р ИСО/МЭК 27037[7], ГОСТ Р 57429[8]); уникальной совокупности технических характеристик и метаданных ФВиВ; UUID[9].

---

5 Иностранное лицо, владеющее информационным ресурсом YouTube, является нарушителем законодательства Российской Федерации.

6 Об электронной подписи. № 63-ФЗ от 06.04.2011. КонсультантПлюс. https://clck.ru/3QH6dk

7 Государственный стандарт. (1991). Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме (ГОСТ Р ИСО/МЭК 27037-2014 (ISO/IEC 27037:2012)). Росстандарт. https://clck.ru/3QH6hR

8 Государственный стандарт. (2017). Судебная компьютерно-техническая экспертиза (ГОСТ Р 57429-2017). Росстандарт. https://clck.ru/3QH6ji

9 UUID (англ. universally unique identifier) – универсальный уникальный идентификатор цифровых данных.

Во-вторых, недостаточная компетентность лиц: производящих видеозвукозапись; осуществляющих процессуальную фиксацию ЭлД; привлекаемых в качестве экспертов с целью подтверждения достоверности записанной информации, и самих судей. Некомпетентность заключается в непонимании природы ЭлД в целом, а также в неспособности выделить «потенциально криминалистически значимую информацию, которая не имеет и не может иметь прямой причинно-следственной связи с событием преступления, не входит в предмет доказывания, но которая объективно необходима для правильного разрешения дела, способствует решению диагностических, классификационных и идентификационных задач»[10] в частности. Например:

– Следователи, судьи, а также другие не имеющие специальных знаний участники процесса склонны чрезмерно полагаться на предполагаемую «объективность» видеоизображения, считая, что оно показывает факты такими, какие они есть на самом деле («наивный реализм»)», так как их личный опыт недостаточен для формирования критического отношения к восприятию записанной аудиовизуальной информации.

– 37 % опрошенных следователей не знают, что собой представляет хэш-сумма содержащихся в файле данных, лишь один следователь применяет хэш-сумму как способ защиты файла от внесения изменений (Шихалиева, 2025). В документах ОРД хэш-сумма видео- и звуковых данных приводится настолько редко, что это нельзя считать статистически значимым событием[11].

– При проведении экспертизы эксперт не принял во внимание, что в соответствии с метаданными звукового файла звуковые данные были записаны с использованием версии iOS, которая появилась через несколько месяцев после записанных на фонограмме событий, другой эксперт – что содержание звукового файла изменялось через два дня после составления следователем протокола и записи звукового файла на оптический диск.

– Авторы «Инструкции по делопроизводству в арбитражных судах Российской Федерации (первой, апелляционной и кассационной инстанций)»[12] не только не представляют, как оценивается качество записи фонограммы, но и не способны корректно указать единицу измерения информационной скорости записи и значение стандартной частоты дискретизации сигнала: «Качество проведения записи 128 Кб/с, частота дискретизации 44 кГц, режим «стерео». Ожидаемо, что Инструкцией не предусмотрены средства верификации записанных фонограмм[13].

– Все чаще в доказывании используются видеограммы и видеофонограммы с искаженными и/или модифицированными в результате пересылки с использованием интернет-мессенджеров метаданными и видео- и звуковыми данными.

---

10 Ялышев, С. А. (1999). Криминалистическая регистрация: учебное пособие. Москва: Академия управления МВД РФ. С. 37.

11 На основе более чем 30-летнего опыта автора по производству фоновидеоскопических экспертиз и исследований.

12 Утверждена Постановлением Пленума Высшего Арбитражного Суда Российской Федерации № 100 от 25 декабря 2013 г. КонсультантПлюс. https://clck.ru/3QH6qE

13 Верификация фонограмм – установление тождества двух совокупностей звуковых данных.

– «…характерной немой сценой закончилась “экскурсия” для курсантов, молодых следователей и оперативных сотрудников по нескольким этажам с сотнями стоек одинакового оборудования в центре обработки данных (далее – ЦОД) ПАО “Ростелеком” после вопроса “Если ваша компьютерная система распределена в “облачной” инфраструктуре ЦОД, что и как вы здесь будете осматривать и изымать в соответствии с УПК? И где будете хранить изъятое?”» (Земскова, Минаков, 2023).

Сделанный выше акцент на «потенциально криминалистически значимой информации» неслучаен. Современный уровень развития технологий цифровой обработки сигналов, в том числе искусственного интеллекта, позволяет модифицировать ФВиВ или сфабриковать их, практически не оставляя следов (Зубов, Зубова, 2023; Бодров, Лебедева, 2024). В связи с чем особую значимость при оценке достоверности записанной информации приобретает установление соответствия содержания и технических характеристик ФВиВ известным, отраженным в процессуальных документах обстоятельствам их создания (Вознюк, Денисов, 2017). Так, специалистам при участии автора данной статьи уже неоднократно удавалось установить факт подмены фонограммы судебного заседания другой фонограммой, не имеющей следов модификации, но записанной в другое время в иной, не соответствующей залу судебного заседания звуковой обстановке[14].

В-третьих, уязвимость ЭлД, которая проявляется, в частности, в следующем:

– В искажении, уничтожении, блокировании доступа непосредственно к информации, а также утрате, уничтожении или сбое функционирования носителя информации в результате ошибок пользователя, сбое технических и программных средств информационных систем, воздействии природных явлений или иных, в том числе нецеленаправленных на изменение информации событий (ГОСТ Р 50922-2006[15]).

– В наличии большого набора способов и средств преднамеренного уничтожения или сокрытия ЭлД: с помощью как штатных, так и специальных программных средств, в том числе вредоносных; посредством полной перезаписи жесткого диска; форматированием носителя; шифрованием, а также силовым электромагнитным воздействием (ГОСТ Р 50922-2006).

– Сложности реализации мер по обеспечению защиты ЭлД от преднамеренного и непреднамеренного воздействия, в том числе электромагнитного и (или) воздействия другой физической природы, осуществляемого в том числе в криминальных целях (ГОСТ Р 50922-2006). «…из-за высокой волатильности информации в цифровых средствах и системах обнаружение цифровых следов преступления при повторном либо дополнительном осмотре по прошествии времени в большинстве случаев будет маловероятным» (Земскова, Минаков, 2023).

В-четвертых, принятая в процессуальной практике «бумажная» фиксация доказательственной информации не соответствует природе ФВиВ, содержащих информацию о длящихся видео- и звуковых событиях, которые невозможно в каждый момент

---

14 Лаборатория аудиовизуальных документов. ВКонтакте. https://clck.ru/3QH6ra

15 Государственный стандарт. (2006). Защита информации. Основные термины и определения (ГОСТ Р 50922-2006). Росстандарт. https://clck.ru/3QH6uJ

времени обозреть в целом и адекватно отразить в виде письменного документа. В связи с чем перед экспертом зачастую ставится задача установления дословного содержания ФВиВ и представления так называемой раскадровки – твердых копий изображения видеокадров с текстовым описанием их содержания. Что не позволяет в полной мере передать «интонацию и нюансы изложения мыслей человеком, выразительность его речи и тон разговора, мимику, жесты, эмоциональное состояние, отношение участников видеозаписи к произносимым фразам, действия, реакции других участников событий» (Власов, 2024).

2. Методология формирования понятийного аппарата и классификации электронных доказательств

Очевидно, что определить место цифровых ФВиВ в ряду ЭлД возможно только при наличии системы полномерно охватывающих понятий, определений и терминов, относящихся к рассматриваемой предметной области и составляющих понятийный аппарат ЭлД.

Серьезным препятствием на пути формирования понятийного аппарата ЭлД является существование множества несогласованных между собой описаний одного и того же понятия. Наглядным примером такой неоднородности являются различные интерпретации понятия «электронный документ» как в законодательстве (см. выше), так и в действующих государственных стандартах:

– «электронный документ: Документ на машиночитаемом носителе, для использования которого необходимы средства вычислительной техники»[16];

– «документ электронный: Информационный объект, состоящий из двух частей:

– реквизитной, содержащей идентифицирующие атрибуты (имя, время и место создания, данные об авторе и т. д.) и электронную цифровую подпись,

– содержательной, включающей в себя текстовую, числовую и/или графическую информацию, которая обрабатывается в качестве единого целого»[17];

– «электронный документ: Форма представления документа в виде множества взаимосвязанных реализаций в электронной среде и соответствующих им взаимосвязанных реализаций в цифровой среде»[18];

– «электронный документ: Документ, информация которого представлена в электронной форме»[19];

---

16 Государственный стандарт. (2001). Электронные издания. Основные виды и выходные сведения (ГОСТ 7.83-2001). Росстандарт. https://clck.ru/3QH6wz

17 Государственный стандарт. (2001). Информационные технологии поддержки жизненного цикла продукции. Терминологический словарь. Часть 1. Стадии жизненного цикла продукции ГОСТ Р 50.1.031-2001. Росстандарт. https://clck.ru/3QH6za

18 Государственный стандарт. (2004). Информационная технология. Электронный обмен информацией. Термины и определения (ГОСТ Р 52292-2004). Росстандарт. https://clck.ru/3QH77t

19 Государственный стандарт. (2013). Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения (ГОСТ Р 7.0.8-2013). Росстандарт. https://clck.ru/3QH7AR

– «электронный документ: Документ в цифровой форме, для использования которого необходимы средства вычислительной техники или иные специализированные устройства для воспроизведения текста, звука, изображения»[20].

Разнообразие определений во многом связано с тем, что отдельные стандарты и законы имеют ограниченную сферу применения и ориентированы на решение задач в конкретных областях человеческой деятельности. Поэтому формирование понятийного аппарата ЭлД логично начать с определения основной задачи, для решения которой он используется. Эта задача заключается в обеспечении единообразного понимания, толкования родовых и видовых характеристик ЭлД, взаимосвязей и процессов, образующихся или применяемых как при собирании доказательственной информации, так и ее проверки и оценки, в том числе с использованием средств и методов судебной экспертизы.

Учитывая, что приемы, способы и методы, задействованные при выполнении функций сбора, хранения, обработки, передачи и использовании данных, составляют информационную технологию[21], представляется логичным использовать в понятийном аппарате ЭлД определений, уже закрепленных в государственных стандартах, относящихся к сфере информационных технологий (ИТ)[22].

Таких стандартов сейчас насчитывается несколько десятков. Наибольший интерес в рамках данной статьи представляют следующее:

– ГОСТ 15971-90 Системы обработки информации. Термины и определения.

– ГОСТ 13699-91 Запись и воспроизведение информации. Термины и определения.

– ГОСТ Р 52292-2004 Информационная технология. Электронный обмен информацией. Термины и определения.

– ГОСТ Р ИСО/МЭК 27037-2014 (ISO/IEC 27037:2012) Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме[23].

– ГОСТ 33707-2016 (ISO/IEC 2382:2015) Информационные технологии. Словарь.

Принятый в перечисленных стандартах «современный подход к спецификации информационных технологий основан на разделении двух разных аспектов явлений: социального (в данном случае назначение, информация, документ и т. д.) и технологического (в данном случае носитель, формат, данные и т. д.)» (ГОСТ Р 52292), что вполне согласуется с наличием двух различающихся, но взаимосвязанных сторон фиксации ЭлД (Белкин, 2007). Процессуальной стороны, целью которой является формирование имеющей юридическую силу доказательственной базы посредством отражения в процессуальных документах обнаруженных следователем фактических данных. Криминалистической, затрагивающей, прежде всего, средства и методы, используемые на различных этапах обнаружения и закрепления доказательственной информации.

---

20 Государственный стандарт. (2013). Система стандартов по информации, библиотечному и издательскому делу. Электронные издания. Основные виды и выходные сведения (ГОСТ Р 7.0.83-2013). Росстандарт. https://clck.ru/3QH7CR

21 Государственный стандарт. (1990). Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения (ГОСТ 34.003-90). Росстандарт. https://clck.ru/3QH7EK

22 Не следует путать с «системой стандартов по информации, библиотечному и издательскому делу».

23 Данный стандарт рекомендован Управлением ООН по наркотикам и преступности для использования при расследовании киберпреступлений. https://clck.ru/3QH7Pr

К этим этапам относятся[24]:

1. Идентификация ЭлД – поиск, распознавание и документирование потенциальных ЭлД. В процессе идентификации определяются носители информации и устройства обработки, которые могут содержать потенциальные ЭлД.

2. Сбор ЭлД – перемещение носителей с ЭлД в контролируемую среду для последующего извлечения доказательной информации.

3. Получение ЭлД – создание копии ЭлД.

4. Сохранение ЭлД – обеспечение защиты ЭлД от изменений (фальсификации, повреждения и т. п.).

5. Анализ ЭлД – углубленное исследование с целью выявления доказательственной информации.

6. Представление (краткое изложение и объяснение) обнаруженных фактических данных в процессуальном документе.

Важно, что на всех перечисленных этапах «запечатлевается не только сама доказательственная информация, но и информация о путях, способах и средствах ее получения как необходимое условие ее допустимости по делу» (Белкин, 2007).

Следует также отметить, что в настоящее время в России все еще не принята единая для различных правоохранительных органов модель работы с цифровыми доказательствами при проведении расследований.

Большая часть стандартизированных терминов ИТ, характеризующих технологическую/криминалистическую сторону собирания ЭлД, может быть применена в понятийном аппарате ЭлД без всяких изменений. Недостающие родовые и видовые понятия, относящиеся непосредственно к ЭлД, могут быть сформированы путем конкретизации и адаптации существующих базовых понятий ИТ на основе «анализа и обобщения свойств и признаков объектов, выявления характеристик, описывающих понятия» (ГОСТ Р 50.1.075[25]) (рис. 1), в том числе с учетом соотношения понятий «информация» и «данные», представленных на рис. 2.

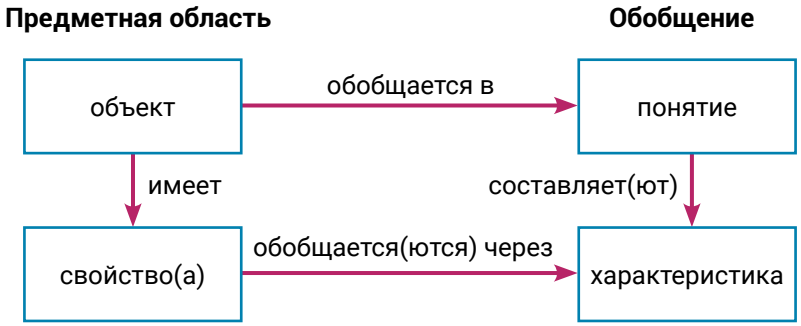

Рис. 1. Порядок формирования новых понятий в соответствии с ГОСТ Р 50.1.075

[24] Представлена типовая интегрированная модель работы с цифровыми доказательствами, пп. 1–4 которой соответствуют рекомендациям ГОСТ Р ИСО/МЭК 27037, пп. 5 и 6 – модели, основанной на протоколе ФБР США (Reedy, 2022).

[25] Государственный стандарт. (2011). Разработка стандартов на термины и определения (ГОСТ Р 50.1.075-2011). Росстандарт. https://clck.ru/3QH7T9

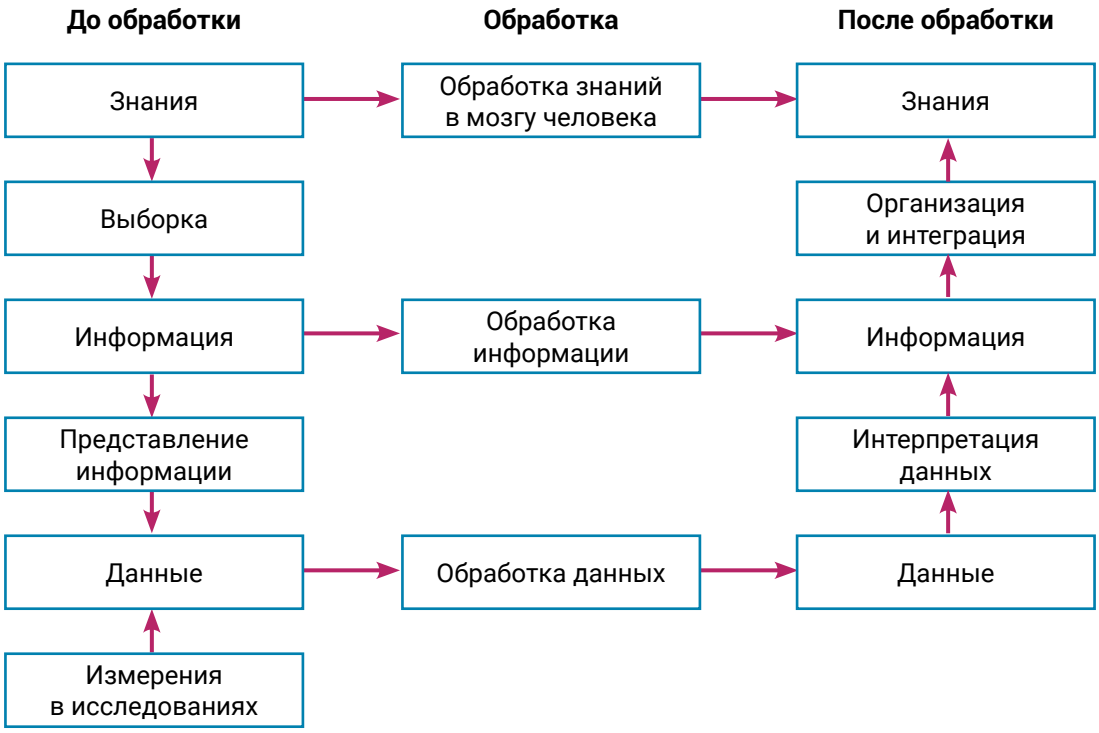

Рис. 2. Схема, отражающая соотношение понятий «знания», «информация» и «данные» в соответствии с ISO/IEC 2382-1:1993[26]

Если воспользоваться указанными стандартами и принципами, то не составит труда сформулировать универсальные для всех видов судопроизводства термины и определения, составляющие основу понятийного аппарата ЭлД.

Из определений «данных» и «электронной среды», которые приводятся в ГОСТ Р 52292:

– «данные[27]: Интерпретируемое формализованным способом представление информации, пригодное для коммуникации, интерпретации или обработки <...>;

– аналоговые данные: Данные, представленные физической величиной, которая считается непрерывной переменной и значение которой прямо пропорционально данным или подходящей функции данных <...>;

– дискретные данные (символьные данные): Данные, представленные при помощи символов <...>;

– электронная среда: Среда технических устройств (аппаратных средств), функционирующих на основе физических законов и используемых в информационной технологии при обработке, хранении и передаче данных»[28],

[26] ISO/IEC 2382-1:1993 Информационные технологии. Словарь. Часть 1. Основные термины. Заменен на ISO/IEC 2382:2015. https://clck.ru/3QH7fj

[27] В зависимости от вида информации, данные могут быть звуковыми, видео и т. п.

[28] Государственный стандарт. (2004). Информационная технология. Электронный обмен информацией. Термины и определения (ГОСТ Р 52292-2004). Росстандарт. https://clck.ru/3QH77t

следует, что под электронными доказательствами следует понимать содержащие доказательственную информацию данные, хранящиеся или передаваемые в виде, пригодном для восприятия человеком с использованием информационных технологий и средств электронной техники.

К упоминаемой в определении электронной технике относятся не только вычислительные средства, но и электронные устройства, служащие для обработки, записи, преобразования или передачи информации или энергии с использованием электронных компонентов и принципов электроники. Например, для восприятия человеком звуковой информации, содержащейся в цифровой фонограмме или видеофонограмме, недостаточно иметь ЦАП[29] (вычислительное средство) и кодек (информационную технологию), для этого требуются электронные устройства, предназначенные для усиления электрического сигнала и его преобразования в звуковые волны разной частоты и мощности.

Информационная технология представляет собой приемы, способы и методы применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных (ГОСТ 34.003-90).

Из определений ГОСТ Р 52292 следует, что ЭлД могут быть представлены в двух видах:

– Аналоговом, при котором физическая величина принимает бесконечное множество значений, изменяющихся непрерывно.

– Дискретном, означающем, что данные существуют в виде дискретных символов, каждый из которых может принимать одно из конечного числа значений.

Это соответствует позиции Интерпола по данному вопросу: «“Электронные доказательства” – это производный термин для двух типов доказательств: “аналоговые доказательства” и “цифровые доказательства”» (Reedy, 2022).

Соответственно, цифровые доказательства, содержащие доказательственную информацию данные, хранящиеся или передаваемые в виде двоичного кода (ГОСТ Р ИСО/МЭК 27037), относятся к электронным дискретным доказательствам. Этому же классу доказательств принадлежат данные строкового и логического типа, например, отображаемые на экране диктофона или смартфона: IMEI смартфона; имя фонограммы; время и географические координаты места звукозаписи или видеосъемки; показания часов реального времени устройства записи; длительность фонограммы; положение (вкл/выкл) органов управления, отвечающих за работу акустопуска или АРУ[30].

Таким образом, содержащая доказательственную информацию цифровая фонограмма относится к классу электронных дискретных цифровых доказательств и представляет собой сохраненные на материальном носителе цифровые звуковые данные, полученные в результате:

– цифровой звукозаписи – цифровой записи звука, или звуковой информации, поступающей от первоисточника или устройства воспроизведения звуковой информации (рис. 3);

– генерации (синтеза) звука с использованием алгоритмов и методов цифровой обработки сигналов.

---

[29] ЦАП (цифро-аналоговый преобразователь) – устройство для преобразования цифровых данных в аналоговый сигнал.

[30] АРУ – автоматическая регулировка усиления сигнала.

Важность выделения двух способов создания цифровой фонограммы обусловлена следующим:

– Необходимостью различения собственно звукозаписи и записи на носитель цифровых звуковых данных. Последняя может быть как одним из этапов звукозаписи (рис. 3), так и самодостаточным процессом, осуществляемым с целью копирования цифровых звуковых данных или сохранения сгенерированных данных (см. ниже).

– Тем, что синтез звука может производиться как с использованием ранее записанных звуковых сигналов или их временных и частотных составляющих, так и на основе математической или генеративной[31] модели, без применения процесса звукозаписи на всех этапах создания фонограммы.

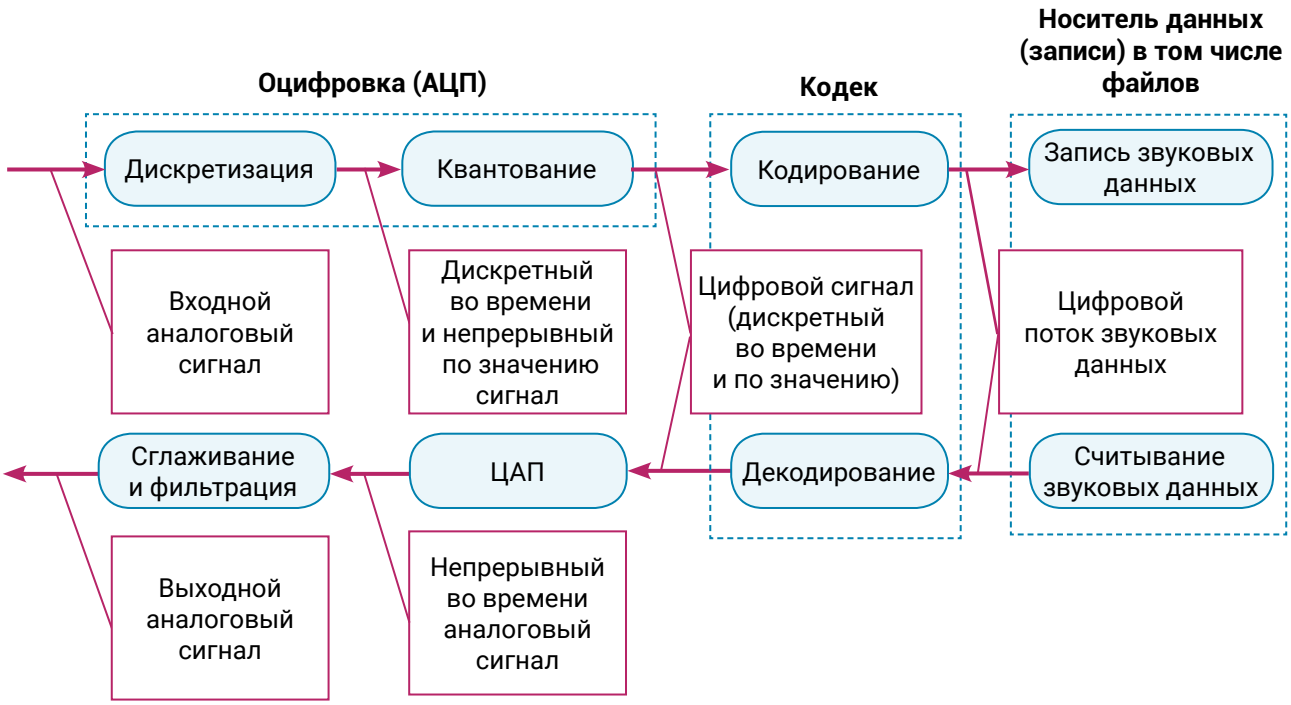

Рис. 3. Схема цифровой звукозаписи и воспроизведения звука

Источник: (Зубов, 2020).

Под цифровыми звуковыми данными следует понимать результат оцифровки и кодирования звуковых сигналов, представленный в виде, пригодном для коммуникации, интерпретации или обработки с использованием электронных устройств и информационных технологий. При этом запись цифровых звуковых данных на носитель может сопровождаться созданием файлов и метаданных.

Необходимость упоминания «аналоговых фонограмм» обусловлена, в частности, тем, что в эксплуатации до сих пор находятся самолеты, регистрация полетных данных и переговоров экипажа которых производится аналоговыми магнитофонами (на

[31] Генеративная модель создает данные, подобные обучающим, на основе статистических закономерностей, но не основываясь на физических законах.

магнитную ленту или проволоку), в архивах хранятся являющиеся предметом авторского права аналоговые фонограммы и видеофонограммы, записанные на магнитной ленте, кинопленке, грампластинках и др.

Из вышесказанного также следует, что не все существующие в настоящее время фонограммы могут быть отнесены к ЭлД. Так, для записи и воспроизведения механических (по способу записи) аналоговых фонограмм, представленных на дисках, валиках и т. п., применение электронной техники и информационных технологий не является необходимостью.

Очевидно, не составит большого труда по аналогии сформировать определения для видеограммы или видеофонограммы и содержащихся в них данных. Так, видеофонограммой следует называть сохраненные на материальном носителе цифровые видео- и звуковые данные, полученные в результате:

– цифровой видеозвукозаписи – синхронной цифровой записи видеоизображения и звука, или аудиовизуальной информации, поступающей от первоисточника или устройства ее воспроизведения;

– генерации (синтеза) видеоизображения и звука с использованием алгоритмов и методов цифровой обработки сигналов.

Отдельно остановимся на носителях данных, представляющих собой материальные объекты (включая физическое поле), предназначенные для записи и хранения данных, которые в процессуальных документах в силу своей осязаемости нередко причисляют к вещественным доказательствам. Классификацию носителей целесообразно производить: по способу записи (механический, магнитный, оптический, электронный и т. п.); по форме представления записанных данных (аналоговые, цифровые и т. п.) и виду информации (видео-, звуковые, текстовые и т. п.). В таком случае, например, музыкальный компакт-диск является оптическим носителем цифровых звуковых данных; обычная магнитофонная кассета с магнитной фонограммой – магнитным носителем аналоговых звуковых данных; жесткий диск с цифровыми фонограммами – магнитным носителем цифровых звуковых данных; флэш-накопитель – твердотельным носителем.

Частным случаем носителя данных является «носитель записи», или «физическое тело, используемое при записи для сохранения в нем или на его поверхности сигналов информации»[32], например, магнитофонная кассета или оптический диск.

Вышеприведенный пример с классификацией музыкального компакт-диска показывает, что далеко не все носители цифровых данных являются электронными носителями. К последним следует относить только электронные устройства соответствующего назначения, функционирующие под управлением собственного контроллера[33]: флеш-накопитель; жесткий диск; аппаратный RAID-массив; сетевое хранилище и т. п.

Безусловно, неспециалисту будет непросто определить принадлежность носителя данных к определенному классу, поэтому в процессуальных документах,

---

32 Государственный стандарт. (1991). Запись и воспроизведение информации. Термины и определения (ГОСТ 13699-91). Росстандарт. https://clck.ru/3QH7or

33 Контроллер (в электронной технике) – специализированное электронное устройство (или его узел), предназначенное для автоматического управления техническим объектом (процессом) по заданному алгоритму (программе).

составленных несведущим лицом, вполне допустимо указание, наряду с другими идентифицирующими сведениями, только типа носителя: жесткий или оптический диск; флеш-накопитель; магнитофонная кассета и характеристики его содержания – звуковой или видеофайл, магнитная или цифровая фонограмма и т. д. Наибольшее значение классификация и экспликация носителей данных приобретает на этапе оценки допустимости и достоверности доказательств, в том числе с применением средств и методов судебной экспертизы.

Также важно иметь в виду следующую значимую особенность цифровых ФВиВ. Они могут быть представлены в виртуальном виде, например, видеофонограмма, опубликованная в интернет-сервисе YouTube[34], или файлы с ФВиВ – в облачном хранилище. Поэтому на этапе идентификации таких ФВиВ их носитель не всегда может быть определен, а для использования ФВиВ в качестве доказательств потребуется копирование или экспорт данных на отчуждаемый носитель.

При этом техническая сторона типовой процедуры экспорта данных с виртуального на отчуждаемый носитель включает ряд последовательно выполняемых операций, которые могут происходить в автоматическом режиме, в том числе без ведома пользователя и контроля с его стороны:

– Извлечение данных из исходной среды (базы данных, информационной системы и т. п.).

– Преобразование данных в формат, который позволяет им быть импортированными и использованными в другой системе или среде.

– Собственно сохранение данных на отчуждаемом носителе для их дальнейшего использования или обработки.

Иначе говоря, полученные в результате экспорта ФВиВ далеко не всегда являются копиями записанных на виртуальном носителе.

В связи с этим целесообразно выделили два вида носителей: (1) первичный носитель, на который производится запись звуковых и видеосигналов, поступающих непосредственно от первоисточника. Другими словами, это первый материальный объект, на котором конкретные данные были записаны; (2) вторичный носитель, на котором ФВиВ оказываются в результате копирования или экспорта данных с первичного или другого вторичного носителя. Первичный носитель при этом может быть как встроенным (неотчуждаемым), так и съемным (отчуждаемым). Вторичный, как правило, бывает отчуждаемым. И первичный, и вторичный носители могут также одновременно являться и виртуальными, доступ пользователя к которым осуществляется с помощью Интернета или подобным образом.

Также важным видится определение «копии цифрового доказательства» как созданной копии цифрового доказательства и средства ее верификации, которое приводится в ГОСТ Р ИСО/МЭК 27037. Из него следует, что копией цифровой фонограммы, содержащей доказательную информацию, можно считать лишь фонограмму, полученную в результате файлового или побитового копирования, соответствие которой оригиналу можно проверить или с помощью функции верификации, или иным приемлемым способом. В англоязычной специализированной литературе такую копию также называют «криминалистической копией» (Forensic Copy).

[34] Иностранное лицо, владеющее информационным ресурсом YouTube, является нарушителем законодательства Российской Федерации.

Естественно, все эти определения не «отлиты в граните» и могут быть заменены на синонимичные, не искажающие сути описываемых свойств, процессов и явлений. Так, проверка неизменности файлов, проводимая посредством установления тождества двух совокупностей содержащихся в них данных, называемая в ГОСТ Р ИСО/МЭК 27037 верификацией, в ГОСТ Р 57429 именуется аутентификацией, что не меняет смысла и содержания данной процедуры.

3. Международный опыт

В настоящее время «отрасль криминалистики, которая применяет вопросы права к информационно-коммуникационным технологиям и цифровым устройствам»[35] и которую принято называть цифровой криминалистикой (Digital forensics), признана самостоятельной научной дисциплиной многими международными и национальными организациями, включая: Управление ООН по наркотикам и преступности, Интерпол, Европейскую сеть институтов судебной экспертизы (ENFSI), Агентство Европейского союза по кибербезопасности (European Union Agency for Cybersecurity - ENISA), Американскую академию судебной экспертизы (AAFS), Организацию научных отраслевых комитетов (OSAC)[36], Регулятор судебной экспертизы Великобритании (Forensic Science Regulator), Международную организацию по стандартизации (ISO) и Международную электротехническую комиссию (IEC). При этом к фундаментальным наукам и базовым научным направлениям для различных субдисциплин цифровой криминалистики в настоящее время относят: биологию, физику, математику, лингвистику, а также информатику, компьютерную инженерию, науку об изображениях, акустику, антропологию, статистику и науку о данных (Reedy, 2020; Rybaczewska & Sparks, 2022).

Достаточно полное представление о текущем состоянии цифровой криминалистики о методах и процедурах, относящихся к работе с цифровыми доказательствами, можно получить из общедоступных публикаций вышеперечисленных организаций. Следует отметить, что особенности работы с ФВиВ в перечисленных документах не конкретизируются.

В 2020 г. вышло в свет учебно-методическое пособие «Киберпреступность»[37], состоящее из 14 модулей, которое является результатом совместной работы Управления ООН по наркотикам и преступности, и ведущих специалистов из более чем 25 стран мира. В модуле 4 «Введение в цифровую криминалистику» указанного пособия представлен обзор современного состояния цифровой криминалистики, рассматриваются, в частности, стандарты цифровой криминалистики, процесс проведения экспертизы цифровых доказательств и общие практические методы экспертного исследования, а также передовая практика в области цифровой криминалистики.

---

35 Управление ООН по наркотикам и преступности. (2020). Серия Университетских Модулей «Киберпреступность». https://clck.ru/3QH7sy

36 Учреждена Национальным институтом стандартов и технологий США (NIST) для разработки специализированных стандартов судебной экспертизы.

37 Управление ООН по наркотикам и преступности. (2020). Серия Университетских Модулей «Киберпреступность». https://clck.ru/3QH7sy

Анализ тенденций, проблем и достижений Интерпола и правоохранительных органов разных стран в области сбора, анализа и использования цифровых доказательств при расследовании преступлений приводится в «Обзоре цифровых доказательств» (Interpol review of digital evidence) за 2016–2019 и 2019–2022 гг. (Reedy, 2020; 2022; Tripathi & Meshram, 2022; Insa, 2007).

В 2019 г. опубликованы «Глобальные руководящие принципы Интерпола по криминалистическим лабораториям, предназначенным для работы с цифровыми доказательствами» (INTERPOL Global Guidelines for Digital Forensics Laboratories)[38]. Документ является руководством по созданию, управлению и работе лабораторий цифровой криминалистики в соответствии с едиными стандартами, обеспечивающими допустимость электронных доказательств в судах, включая международные.

В Руководстве ENISA 2014 г. для служб быстрого реагирования на компьютерные инциденты[39] основное внимание уделяется порядку работы с цифровыми доказательствами, начиная с прибытия на место преступления и заканчивая оценкой и представлением цифровых доказательств.

В Руководстве по передовой практике экспертизы (Best Practice Manual) Европейской сети судебно-экспертных институтов (ENFSI) по проведению судебных исследований цифровых технологий (версия 1, 2015 г.)[40] отражен типовой процесс проведения судебной экспертизы цифровых доказательств, стандарты и универсальные методы экспертного исследования, а также передовая практика в области цифровой криминалистики, включая подготовку персонала, которые в совокупности должны обеспечить надежность и сопоставимость результатов судебных экспертиз.

В отчете NIST IR 8387 (сентябрь 2022 г.) (Guttman et al., 2022; Turner, 2005; Romaniuk, 2024), подготовленном в партнерстве с Национальным институтом юстиции США (NIJ) и предназначенном для специалистов по управлению доказательствами, изложены практические рекомендации по сохранению цифровых доказательств и уникальные особенности последних.

В качестве ключевых проблем, с которыми приходится сталкиваться специалистам правоохранительных органов, в упомянутых документах указаны: шифрование данных, облачные сервисы, распределенное хранение, интернет вещей, искусственный интеллект, нехватка квалифицированных специалистов, различия в национальном законодательстве. А среди главных рекомендаций – гармонизация правовых норм, инвестиции в обучение специалистов и оснащение лабораторий, развитие совместимых технологий исследования цифровых доказательств.

Подчеркивается, что «каждое дело, связанное с цифровыми доказательствами, ставит новые задачи, которые специалисты по цифровым доказательствам должны уметь решать. Будущий специалист по цифровым доказательствам должен обладать знаниями и навыками для решения криминалистических вопросов в рамках конкретного дела» (Reedy, 2020; An, 2017; Awwad, 2025; Hosmer, 2006; Maurer, 2004).

---

38 Interpol. (2019). INTERPOL Global guidelines for digital forensics laboratories. https://clck.ru/3QH7zA

39 Electronic evidence – a basic guide for First Responders Good practice material for CERT first responders. (2014). European Union Agency for Network and Information Security.

40 Best Practice Manual for the Forensic Examination of Digital Technology ENFSI-BPM-FIT-01 Version 01 – November 2015. (2016). ENFSI. https://clck.ru/3QH83b

Нельзя не упомянуть, что, кроме адаптированного к российским условиям ГОСТ Р ИСО/МЭК 27037, ИСО/МЭК опубликовали дополнительные, не имеющие российских аналогов международные стандарты, которые охватывают: достоверность и надежность инструментов и методов цифровой судебной экспертизы – ISO/IEC 27041:2015, «Руководство по обеспечению пригодности и соответствия метода расследования инцидентов» (Information technology. Security techniques. Guidance on assuring suitability and adequacy of incident investigative method), а также этапы исследования и интерпретации процесса цифровой судебной экспертизы (ISO/IEC 27042:2015, «Руководство по анализу и интерпретации цифровых свидетельств» (Information technology. Security techniques. Guidelines for the analysis and interpretation of digital evidence).

Таким образом, в мире накоплен богатый опыт разработки нормативных актов – инструкций, руководств, а также стандартов и учебных материалов по созданию и функционированию лабораторий цифровой криминалистки и работе с цифровыми доказательствами при расследовании преступлений. При этом понятие «электронные доказательства» в современных нормативных документах и стандартах практически не используется, поскольку особенности исследования аналоговых доказательств, составляющих, наряду с цифровыми, массив «электронных», давно известны и изучены.

Заключение

Цифровые фонограммы, видеограммы и видеофонограммы занимают значимое место в системе ЭлД, представляя собой весьма уязвимые источники аудиовизуальной информации, которые требуют специализированного подхода к их фиксации, проверке и оценке в судопроизводстве.

Отсутствие в нормативно-правовых актах четких определений и классификации ЭлД и ФВиВ приводит к правовой неопределенности, ошибкам в процессуальной практике и снижению эффективности использования таких доказательств в целом.

Предложенная в статье методология формирования понятийного аппарата ЭлД в целом и ФВиВ в частности на основе существующих государственных стандартов, относящихся к области информационных технологий, позволяет создать универсальные термины и определения, адаптированные для всех видов судопроизводства.

Дальнейшие исследования в этой области должны быть направлены на разработку предельно четких и детализированных рекомендаций, руководств и инструкций для специалистов и следователей по идентификации, сбору, получению, сохранению и анализу ЭлД, в том числе с использованием зарубежного опыта.

В перспективе требуется совершенствование процессуальных норм, включая введение обязательных требований к компетентности специалистов и обязательного их привлечения к расследованию на самых ранних этапах.

Список литературы

Белкин, А. Р. (2007). *Теория доказывания в уголовном судопроизводстве*. Москва: Норма.

Бодров, Н. Ф., Лебедева, А. К. (2024). Анализ судебной практики установления обстоятельств в случаях противоправного распространения генеративного контента, созданного с помощью технологий искусственного интеллекта. *Юридические исследования*, *11*. EDN: https://elibrary.ru/TLSBYY. DOI: https://doi.org/10.25136/2409-7136.2024.11.72540

Власов, О. О. (2024). Классификация задач криминалистической экспертизы видеозаписей. *Теория и практика судебной экспертизы*, *19*(2), 14–25. EDN: https://elibrary.ru/XQEHZW. DOI: https://doi.org/10.30764/1819-2785-2024-2-14-25

Вознюк, М. А., Денисов, Ю. А. (2017). Экспертная диагностика обстоятельств изготовления цифровых видео- и звукозаписей: аналитический обзор. *Теория и практика судебной экспертизы*, *12*(1), 48–71. EDN: https://elibrary.ru/YHMVEL. DOI: https://doi.org/10.30764/64/1819-2785-2017-12-1-48-71

Воронин, М. И. (2021). Особенности оценки электронных (цифровых) доказательств. *Актуальные проблемы российского права*, *8*(129), 118–128. EDN: https://elibrary.ru/ncpirv. DOI: https://doi.org/10.17803/1994-1471.2021.129.8.118-128

Земскова, А. В., Минаков, С. С. (2023). Особенности применения инструментальных средств для поиска и документирования компьютерной информации в ходе следственных действий по осмотру. *Вестник экономической безопасности*, *2*, 74–85. EDN: https://elibrary.ru/hcvgtp. DOI: https://doi.org/10.24412/2414-3995-2023-2-74-85

Зубов, Г. Н. (2020). Актуализация понятия «специальные технические средства для негласного получения информации» в фоновидеоскопической экспертизе. *Вестник криминалистики*, *2*(74), 52–60. https://elibrary.ru/rnbdma

Зубов, Г. Н., Зубова, П. И. (2023). Фальсификация звуковой информации с использованием технологий искусственного интеллекта. Особенности технического исследования. *Вестник криминалистики*, *3*(87), 5–26. https://elibrary.ru/qvhfrw

Зубов, Г. Н., Тимошенко А. А. (2014). Использование в доказывании цифровых аудио и видеофонограмм. *Уголовный процесс*, *2*(110), 52–61. https://elibrary.ru/ruqikd

Малык, А. В. (2023). Формирование и природа электронных доказательств. *Вестник Воронежского государственного университета. Серия: Право*, *3*(54), 45–51. EDN: https://elibrary.ru/atlajw. DOI: https://doi.org/10.17308/law/1995-5502/2023/3/45-51

Полициан, Д. А. (2022). «Цифровое» и «электронное» доказательство – pro et contra: проблемы терминологии. *Российский судья*, *7*, 38–44. EDN: https://elibrary.ru/fvlsvs. DOI: https://doi.org/10.18572/1812-3791-2022-7-38-44

Черецких, А. В. (2023). Цифровые (электронные) доказательства в уголовном процессе. *Правопорядок: история, теория, практика*, *4*(39), 110–117. EDN: https://elibrary.ru/ptaemv. DOI: https://doi.org/10.47475/2311-696X-2023-39-4-110-117

Шихалиева, С. З. (2025). Отсутствие хэш-суммы как процессуальная ошибка, возникающая в судебной экспертизе при исследовании объектов в цифровой форме. *Правовое государство: теория и практика*, *21.1*(79), 256–263. EDN: https://elibrary.ru/bntuwa. DOI: https://doi.org/10.33184/pravgos-2025.1.28

An, S. S. (2017). The admissibility of digital evidence. *Korean Lawyers Association Journal*, *66*(1), 5–56. https://doi.org/10.17007/klaj.2017.66.1.001

Awwad, A. (2025). Digital evidence in forensic accounting: A study in Saudi Arabia. *Journal of Accounting and Finance in Emerging Economies*, *5*(1), 23–31. https://doi.org/10.1177/097215092501001

Hosmer, C. (2006). Digital evidence bag. *Communications of the ACM*, *49*(2), 69–70. https://doi.org/10.1145/1113034.1113072

Maurer, U. (2004). New approaches to digital evidence. *Proceedings of the IEEE*, *92*(6), 933–947. https://doi.org/10.1109/jproc.2004.827358

Guttman, B., White, D. R., & Walraven, T. (2022). Digital Evidence Preservation Considerations for Evidence Handlers. *NIST Interagency Report NIST IR 8387*. https://doi.org/10.6028/NIST.IR.8387

Insa, F. (2007). The admissibility of electronic evidence in court (A.E.E.C.). *Computer Law & Security Review*, *23*(5), 409–418. https://doi.org/10.1016/j.clsr.2007.07.002

Reedy, P. (2020). Interpol review of digital evidence for 2016–2019. *Forensic Science International: Synergy*. https://doi.org/10.1016/j.fsisyn.2020.01.015

Reedy, P. (2022). Interpol review of digital evidence for 2019–2022. *Forensic Science International: Synergy*. https://doi.org/10.1016/j.fsisyn.2022.100313

Romaniuk, V. V. (2024). Criteria for the admissibility of digital (electronic) evidence in criminal proceedings. *Problems of Legal Regulation*, *59*(2), 47–56. https://doi.org/10.32782/2524-0374/2024-2-10

Rybaczewska, M., & Sparks, L. (2022). Digital evidence and online consumer engagement. *Journal of Retailing and Consumer Services*, *65*, Article 102889. https://doi.org/10.1016/j.jretconser.2022.102889

Tripathi, S., & Meshram, B. B. (2022). Digital evidence for database tamper detection. *Advances in Multidisciplinary and Scientific Research Journal Publication*, *1*(1), 185–190. https://doi.org/10.22624/aims/crp-bk3-p30

Turner, P. (2005). Unification of digital evidence from disparate sources (Digital Evidence Bags). *Digital Investigation*, *2*(3), 223–228. https://doi.org/10.1016/j.diin.2005.07.001

Сведения об авторе

Зубов Герман Николаевич – независимый исследователь, независимый судебный эксперт
Адрес: 195027, Россия, г. Санкт-Петербург, пр. Энергетиков, 10а
E-mail: hzubov@yandex.ru
ORCID ID: https://orcid.org/0000-0002-9504-1715
РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?spin=5528-9035

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.07.45 / Право и научно-технический прогресс
Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 25 сентября 2025 г.
Дата одобрения после рецензирования – 8 октября 2025 г.
Дата принятия к опубликованию – 20 декабря 2025 г.
Дата онлайн-размещения – 25 декабря 2025 г.

Research article
UDC 34:004:343.14:343.98.062:343.98.063
EDN: https://elibrary.ru/qjhwgw
DOI: https://doi.org/10.21202/jdtl.2025.25

Place of Digital Phonograms, Videograms, and Videophonograms in the System of Electronic Evidences: Theoretical and Methodological Principles of Classification

German N. Zubov
Independent researcher, Saint Petersburg, Russia

Keywords

digital forensics,
digital technology,
electronic evidence,
evidence,
expertise,
law,
legal proceedings,
phonogram,
videogram,
videophonogram

Abstract

Objective: to determine the place of digital phonograms, videograms and videophonograms in the system of electronic evidence in Russian judicial proceedings, to form a unified conceptual framework and classification system to ensure effective use in procedural practice.

Methods: the research is based on the universal dialectical method of cognition, general scientific methods (description, comparison, generalization, modeling, analysis, synthesis), and specific scientific methods. Special attention was paid to the system-structural analysis of regulatory legal acts, state standards in the field of information technology, and international documents regulating work with digital evidence. The author applied methods of criminalistic research, a formal legal method of interpreting procedural norms, and a comparative analysis of foreign experience in regulating electronic evidence.

Results: the study identified and systematized the key reasons for the legal uncertainty of electronic evidence: a variety of representation forms, high data vulnerability, insufficient competence of the proving subjects, and inconsistency with traditional methods of evidence recording. The author developed an original classification of electronic evidence and digital phonograms, videograms, and videophonograms, using criteria such as the form of data presentation, recording method, and nature of information media. Universal definitions of the basic concepts are formulated: electronic evidence, digital evidence, digital phonogram,

videophonogram, data carriers, a copy of digital evidence. The necessity is substantiated to harmonize procedural norms based on state standards of information technologies and international experience.

Scientific novelty: for the first time, a comprehensive methodology was developed to form the conceptual apparatus and classification of electronic evidence, integrating state standards on information technology with criminalistic and procedural aspects of evidence recording. Universal terms and definitions were introduced, which had been absent in the current Russian legislation. They were adapted for all types of legal proceedings, taking into account the specifics of the digital environment. A typical model of working with digital evidence was proposed, with identification, collection, receipt, preservation, analysis and presentation stages. The category of digital phonograms, videograms and videophonograms was proved to be a subtype of electronic discrete digital evidence.

Practical significance: the results can be used to improve procedural legislation regarding the regulation of work with electronic evidence. They can help to develop departmental instructions and practical recommendations for investigators, specialists and experts on the identification, collection, fixation, verification and evaluation of digital evidence. The proposed classification and conceptual framework contribute to the unification of approaches to the procedural design of electronic evidence. The result is minimizing procedural errors, increasing the competence of the proving subjects, and ensuring the admissibility and reliability of digital phonograms, videograms and videophonograms. The research materials are applicable in the training of lawyers, investigators, and forensic experts specializing in digital forensics

For citation

Zubov, G. N. (2025). Place of Digital Phonograms, Videograms, and Videophonograms in the System of Electronic Evidences: Theoretical and Methodological Principles of Classification. *Journal of Digital Technologies and Law, 3*(4), 636–659. https://doi.org/10.21202/jdtl.2025.25

References

An, S. S. (2017). The admissibility of digital evidence. *Korean Lawyers Association Journal*, *66*(1), 5–56. https://doi.org/10.17007/klaj.2017.66.1.001

Awwad, A. (2025). Digital evidence in forensic accounting: A study in Saudi Arabia. *Journal of Accounting and Finance in Emerging Economies*, *5*(1), 23–31. https://doi.org/10.1177/097215092501001

Belkin, A. R. (2007). *Theory of proving in criminal judicial procedure*. Moscow: Norma. (In Russ.).

Bodrov, N. F., & Lebedeva, A. K. (2024). Analysis of the case law establishing circumstances of illegal distribution of generative content created using artificial intelligence. *Legal Studies*, *11*. (In Russ.). https://doi.org/10.25136/2409-7136.2024.11.72540

Cheretskikh, A. V. (2023). Digital (electronic) evidence in criminal proceedings. *Legal Order: History, Theory, Practice*, *4*(39), 110–117. (In Russ.). https://doi.org/10.47475/2311-696X-2023-39-4-110-117

Guttman, B., White, D. R., & Walraven, T. (2022). Digital Evidence Preservation Considerations for Evidence Handlers. *NIST Interagency Report NIST IR 8387*. https://doi.org/10.6028/NIST.IR.8387

Hosmer, C. (2006). Digital evidence bag. *Communications of the ACM*, *49*(2), 69–70. https://doi.org/10.1145/1113034.1113072

Insa, F. (2007). The admissibility of electronic evidence in court (A.E.E.C.). *Computer Law & Security Review*, *23*(5), 409–418. https://doi.org/10.1016/j.clsr.2007.07.002

Malyk, A. V. (2023). Formation and nature of electronic evidence. *Proceedings of Voronezh State University. Series: Pravo*, *3*(54), 45–51. (In Russ.). https://doi.org/10.17308/law/1995-5502/2023/3/45-51

Maurer, U. (2004). New approaches to digital evidence. *Proceedings of the IEEE*, *92*(6), 933–947. https://doi.org/10.1109/jproc.2004.827358

Politsan, D. A. (2022). "Digital" and "Electronic" evidence – pro et contra: problems of terminology. *Rossiyskiy sudya*, *7*, 38–44. (In Russ.). https://doi.org/10.18572/1812-3791-2022-7-38-44

Reedy, P. (2020). Interpol review of digital evidence for 2016–2019. *Forensic Science International: Synergy*. https://doi.org/10.1016/j.fsisyn.2020.01.015

Reedy, P. (2022). Interpol review of digital evidence for 2019–2022. *Forensic Science International: Synergy*. https://doi.org/10.1016/j.fsisyn.2022.100313

Romaniuk, V. V. (2024). Criteria for the admissibility of digital (electronic) evidence in criminal proceedings. *Problems of Legal Regulation*, *59*(2), 47–56. https://doi.org/10.32782/2524-0374/2024-2-10

Rybaczewska, M., & Sparks, L. (2022). Digital evidence and online consumer engagement. *Journal of Retailing and Consumer Services*, *65*, Article 102889. https://doi.org/10.1016/j.jretconser.2022.102889

Shikhaliyeva, S. Z. (2025). The absence of a hash sum as a procedural error arising in a forensic examination when analysing objects in a digital form. *The Rule-Of-Law State: Theory and Practice*, *21.1*(79), 256–263. (In Russ.). https://doi.org/10.33184/pravgos-2025.1.28

Tripathi, S., & Meshram, B. B. (2022). Digital evidence for database tamper detection. *Advances in Multidisciplinary and Scientific Research Journal Publication*, *1*(1), 185–190. https://doi.org/10.22624/aims/crp-bk3-p30

Turner, P. (2005). Unification of digital evidence from disparate sources (Digital Evidence Bags). *Digital Investigation*, *2*(3), 223–228. https://doi.org/10.1016/j.diin.2005.07.001

Vlasov, O. O. (2024). Classification of tasks for forensic video analysis. *Theory and Practice of Forensic Science*, *19*(2), 14–25. (In Russ.). https://doi.org/10.30764/1819-2785-2024-2-14-25

Voronin, M. I. (2021). Characteristics of electronic (digital) evidence assessment. *Actual Problems of Russian Law*, *8*(129), 118–128. (In Russ.). https://doi.org/10.17803/1994-1471.2021.129.8.118-128

Voznyuk, M. A., & Denisov, Yu. A. (2017). Forensic diagnostics of the circumstances of digital video and audio production: analytical review. *Theory and Practice of Forensic Science*, *12*(1), 48–71. (In Russ.). https://doi.org/10.30764/64/1819-2785-2017-12-1-48-71

Zemskova, A. V., & Minakov, S. S. (2023). Features of the use of tools for searching and documenting computer information during investigative actions on inspection. *Vestnik economicheskoy bezopasnosti*, *2*, 74–85. (In Russ.). https://doi.org/10.24412/2414-3995-2023-2-74-85

Zubov, G. N. (2020). Actualizing the concept of "special technical means for covert obtaining of information" in the photovideoscopic expertise. *Vestnik kriminalistiki*, *2*(74), 52–60. (In Russ.).

Zubov, G. N., Timoshenko, A. A. (2014). Using digital audio- and videophonograms in proving. *Ugolovniy protsess*, *2*(110), 52–61. (In Russ.).

Zubov, G. N., Zubova, P. I. (2023). Falsification of audio information using artificial intelligence technologies. Features of technical research. *Vestnik kriminalistiki*, *3*(87), 5–26. (In Russ.).

Author information

German N. Zubov – independent researcher, independent legal expert
Address: 10A Energetikov Str., Saint Petersburg, Russia
E-mail: hzubov@yandex.ru
ORCID ID: https://orcid.org/0000-0002-9504-1715
RSCI Author ID: https://www.elibrary.ru/author_items.asp?spin=5528-9035

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – September 25, 2025
Date of approval – October 8, 2025
Date of acceptance – December 20, 2025
Date of online placement – December 25, 2025