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

Contents

Introduction

Russian legislation allows the use of phonograms, videograms and videophonograms (further referred to as PhVVph)[1] as evidence in administrative, arbitration, criminal and civil proceedings, regardless of the form – analog or digital, and the method of their presentation – a file in the memory of a video recording device, publication on a social network, etc.

Such evidence may include PhVVph recorded:

– as part of operational investigative activities;

– by an investigator or an expert during conducting investigative actions and taking minutes of court sessions;

– by other participants in the process (an accused, a victim, a witness, a plaintiff, a defendant, etc.);

– by various general-purpose automated systems for collecting and processing audio and visual information: video surveillance, telephone recordings, etc.

However, even a cursory review of the texts of procedural laws indicates a lack of uniformity, even in naming objects containing evidentiary audiovisual information.

For example, the result of recording audio information on a tangible medium (further referred to as a phonogram) is called:

– audio recording (Russian Administrative Procedural Code, Russian Civil Code, Russian Criminal Procedural Code);

– audio materials (Russian Code of Administrative Offenses);

– audio recording materials (Russian Criminal Procedural Code);

– sound recording materials (Russian Code of Administrative Offenses);

– phonogram (OIA law[2], Russian Civil Code, Russian Code of Administrative Offenses).

The result of recording visual or audiovisual information (further referred to as a videogram or a videophonogram, respectively) is referred to as:

– videogram (OIA law);

– video recording (Russian Administrative Procedural Code, Russian Criminal Procedural Code);

– video materials (Russian Code of Administrative Offences);

– the materials of the video recording (Russian Code of Administrative Offences).

Procedural laws do not distinguish between a videogram and a videophonogram, or between digital or analog PhVVphs, although these differences objectively exist and may affect the processing of audio-visual information with evidentiary value, as well as its verification and evaluation as evidence. Consider the following example. An investigator

---

1 According to the wording of GOST 13699-91 “Recording and reproduction of information. Terms and definitions”. https://clck.ru/3QH6Ac

2 Here and further – Federal law “On investigative activity” of 12.08.1995 No. 144-FZ (OIA law).

asked an expert if there were traces of editing on a "video recording" and submitted the videophonogram for examination. The expert, in accordance with the "letter" of the question, studied the video in the videophonogram, but ignored the sound, which, according to the case file, contained evidentiary information and was edited (Zubov, Timoshenko, 2014).

This is not surprising, given that regulatory legal acts – both laws and departmental instructions, guides, recommendations, etc. – lack even the basic concepts of PhVVphs such as the concepts of electronic and digital evidence. In the procedural laws and resolutions of the higher courts, these concepts are customarily equaled to information presented "in electronic form" (Russian Code of Administrative Offenses); on "electronic media" (Russian Criminal Procedural Code); or "electronic documents" (Russian Criminal Procedural Code and Russian Administrative Procedural Code). At the same time, there is also no explicit definition of the term "electronic media" in the texts of regulatory legal acts. Its meaning is revealed through context and indirect indications. As a rule, "electronic media" is understood as a device for recording, storage and use of digital data exclusively.

The Law "On information, information technologies and information protection"[3] gives the following definition of an "electronic document": "documented information presented in electronic form, that is, in a form suitable for human perception using electronic computers, as well as for transmission over information and telecommunication networks or for processing in information systems". It is not applicable to digital PhVVphs, since digital PhVVphs, the electronic origin of which is beyond doubt, can be recorded or reproduced without using a computer. It is equally important that, while the Russian Criminal Procedural Code classifies PhVVphs as "other documents", other procedural laws classify documents as written evidence, to which PhVVphs clearly do not belong.

A more precise definition of an "electronic document" is contained in the Law "On arbitration (arbitration proceedings) in the Russian Federation"[4]: "an electronic document transmitted through communication channels – information prepared, sent, received or stored using electronic, magnetic, optical or similar means, including electronic data exchange and e-mail".

Thus, one can state that Russian legislation lacks a single, universal, exhaustive legal definition of "electronic evidence" (further referred to as EE) and does not reflect the generic features and classification of EE. This prevents an understanding of the specific features of using this type of evidence in court proceedings and their objective assessment in terms of admissibility and reliability. It also hinders creating practical guides for investigators and experts working with this type of evidence.

---

3 On information, information technologies and information protection. No. 149-FZ of 27.07.2006. (2006). KonsultantPlyus. https://clck.ru/3QH6Dq

4 On arbitration (arbitration proceedings) in the Russian Federation. No. 382- FZ of 29.12.2015 (ed. of 08.08.2024). KonsultantPlyus. https://clck.ru/3QH6YV

A similar situation is observed in the publications of Russian practicing lawyers and legal scholars (Voronin, 2021; Malyk, 2023; Politsian, 2022; Cheretskikh, 2023), who also cannot come to a consensus on EE. Some do not see the difference between digital and electronic evidence, others classify them as different types, but both note the imperfection of Russian legislation regarding the use of EE and, as a rule, speak of the need to view EE as a separate type.

1. Causes of legal uncertainty of electronic evidences

There are several key factors causing the legal uncertainty of EE.

First and foremost, there is the variety of EE forms and types that do not correspond to the written form of recording evidentiary information accepted in procedural practice.

The evidences, which is currently commonly referred to as electronic, include: electronic documents per se, including electronic images of written documents; correspondence in e-mail applications and messengers; files of various formats; databases, metadata; server logs, etc. Some of them can be represented: in physical form (on a tangible medium, for example, in the external memory of a sound or video recording device); in virtual form (for example, a videophonogram in the YouTube[5] Internet service). At the same time, evidentiary information can be relatively easily, often deceptively easily, transferred from one medium to another and exist in many indistinguishable copies; its reproduction and perception in some cases are impossible without the use of software and hardware, the use of which often requires the user to have special knowledge in the field of information technologies.

All this undoubtedly complicates the identification, collection, receipt, classification and description of EE in the protocol, as well as the unification of approaches to their assessment. It also necessitates the use of various verification technologies, including those unknown for the participants in the process: electronic signatures (Russian Administrative Procedural Code, Russian Civil Code, Russian Code of Administrative Offences, Russian Criminal Procedural Code, Law on electronic signature[6]); hash functions (GOST R ISO/IEC 27037[7], GOST R 57429[8]); a unique set of technical characteristics and metadata of PhVVphs; UUID[9].

---

5 The foreign person owning the YouTube informational resource violates the legislation of the Russian Federation

6 On electronic signature. No. 63-FZ of 06.04.2011. KonsultantPlyus. https://clck.ru/3QH6dk

7 State Standard. (2012). Information technology. Methods and means of ensuring security. Guidelines for the identification, collection, receipt and storage of evidences provided in a digital form (GOST R ISO/IEC 27037-2014 (ISO/IEC 27037:2012)). Rosstandart. https://clck.ru/3QH6hR

8 State Standard. (2017). Forensic computer and technical expertise (GOST R 57429-2017). Rosstandart. https://clck.ru/3QH6ji

9 UUID is a universally unique identifier of digital data.

Secondly, there is a lack of competence of persons, who make video sound recordings; who carry out procedural recording of EE; who are involved as experts in order to confirm the accuracy of the recorded information; and the judges. Incompetence lies in a lack of understanding of the EE nature as a whole, as well as in the inability, in particular, to identify "potentially criminalistically significant information ... that does not and cannot have a direct causal relationship with the crime event, is not included in the subject of proof, but which is objectively necessary for the proper resolution of the case and contributes to solving diagnostic, classification and identification tasks" [10]. For example:

– Investigators, judges, and other participants in the process who do not have special knowledge tend to overly rely on the alleged "objectivity" of the video image, believing that it shows the facts as they really are ("naive realism"), since their personal experience is insufficient to form a critical attitude towards the perception of recorded audiovisual information.

– 37 % of the interrogated investigators do not know what the hash sum of the data contained in the file is; only one investigator uses the hash sum as a way to protect the file from modification (Shikhalieva, 2025). In investigative documentation, so rarely contain the hash sum of video and audio data that it cannot be considered a statistically significant event[11].

– During the examination, an expert did not take into account that, according to the audio file metadata, the audio was recorded using the iOS version, which appeared several months after the events recorded on the phonogram; another expert did not notice that the audio file content changed two days after the investigator drew up the protocol and recorded the audio file on an optical disc.

– The authors of the "Instructions for record keeping in the arbitration courts of the Russian Federation (first, appellate and cassation instances)"[12] not only lack understanding how the recording quality of a phonogram is assessed, but are also unable to correctly specify the unit of measurement of the recording information speed and the standard signal sampling rate: "The recording quality is 128 Kb/s, sampling rate 44 kHz, stereo mode". Apparently, the Instructions do not provide means of verifying recorded phonograms[13].

– Increasingly, videograms and videophonograms used in evidence have metadata or video- and audiodata distorted and (or) modified as a result of transmission using Internet messengers.

---

10 Yalyshev, S. A. (1999). Criminological registration: tutorial. Moscow: Academy for the management of the Russian Ministry of Internal Affairs. P. 37.

11 Based on over 30 years of the author's experience of providing phonovideoscopic expertise and studies.

12 Approved by Resolution of the Plenum of the Supreme Arbitration Court of the Russian Federation No. 100 of December 25, 2013. KonsultantPlyus. https://clck.ru/3QH6qE

13 Verification of phonograms is establishing the identity of two sets of sound data.

– "... a typical silent scene rounded up the 'tour' for cadets, young investigators and operations staff along several floors with hundreds of racks of identical equipment in the Rostelecom PJSC data center after the question "If your computer system is distributed in the cloud infrastructure of the data center, what and how will you inspect and exact here in accordance with the Criminal Procedural Code? Where will you keep the items exacted?" (Zemskova, Minakov, 2023).

The above emphasis on "potentially criminalistically significant information" is not accidental. The current level of development of digital signal processing technologies, including artificial intelligence, makes it possible to modify or fabricate PhVVphs without leaving any traces (Zubov, Zubova, 2023; Bodrov, Lebedeva, 2024). In this regard, while assessing the recorded information reliability, it is particularly important to establish the conformity of the PhVVphs content and technical characteristics with the circumstances of their creation, known and reflected in the procedural documents (Voznyuk, Denisov, 2017). For example, experts, with the participation of the author of this article, have repeatedly managed to establish the fact that the court session phonogram was replaced by another phonogram that had no traces of modification, but was recorded at another time in a different sound environment that did not correspond to the courtroom[14].

The third factor is the EE vulnerability, which manifests itself, among other things, in the following:

– Distortion, destruction, blocking of access to information, as well as loss, destruction or malfunction of the information carrier because of user errors, failure of technical and software tools of information systems, exposure to natural phenomena or other events, including those not aimed at changing information (GOST R 50922-2006[15]).

– A large set of methods and means of EE deliberate destruction or concealment: using both standard and special software, including malicious ones; by completely overwriting the hard disk; by formatting the media; by encryption or electromagnetic force exposure (GOST R 50922-2006).

– Difficulties in implementing measures to ensure the EE protection from intentional and unintended effects, including electromagnetic and (or) other physical effects, carried out, among other things, for criminal purposes (GOST R 50922-2006). "... (D)ue to the high volatility of information in digital media and systems, the detection of digital traces of a crime during repeated or additional inspection over time will in most cases be unlikely" (Zemskova, Minakov, 2023).

Fourthly, the "paper" recording of evidentiary information adopted in procedural practice does not correspond to the PhVVphs nature; the latter contain information about

[14] Laboratory of audiovisual documents. VKontakte. https://clck.ru/3QH6ra

[15] State Standard. (2006). Information protection. Key terms and definitions (GOST R 50922-2006). Rosstandart. https://clck.ru/3QH6uJ

video and audio events in duration that one cannot view as a whole at any given time and adequately reflect in a written document. In this regard, an expert is often assigned to establish the verbatim content of the PhVVphs and provide a so-called storyboard – hard copies of the video images with a textual description of their content. This does not allow one to fully convey "the intonation and nuances of a person's presentation of thoughts, the expressiveness of speech and the tone of conversation, facial expressions, gestures, emotional state, attitudes of the video participants to the phrases, actions, and reactions of other participants in the events" (Vlasov, 2024).

2. Methodology for the formation of the conceptual apparatus and classification of electronic evidences

Obviously, one may determine the place of digital PhVVphs in the EE series only if there is a system of fully encompassing notions, definitions and terms related to the area under consideration and constituting the conceptual apparatus of the EE.

A serious obstacle to the formation of the EE conceptual apparatus is the existence of many inconsistent descriptions of the same concept. A clear example of this heterogeneity is the different interpretations of the concept of "electronic document" in legislation (see above) and in the current state standards:

– "electronic document: a document on a machine-readable medium, requiring computer equipment to use"[16];

– "electronic document: an information object consisting of two parts:

– a prop containing identifying attributes (title, time and place of creation, information about the author, etc.) and an electronic digital signature,

– meaningful, including textual, numerical and (or) graphical information that is processed as a single whole"[17];

– "electronic document: a form of presentation of a document as a set of interrelated implementations in an electronic environment and their corresponding interrelated implementations in a digital environment"[18];

– "electronic document: a document whose information is presented in electronic form"[19];

---

16 State Standard. (2001). Electronic publications. Main types and issuance information (GOST 7.83-2001). Rosstandart. https://clck.ru/3QH6wz

17 State Standard. (2001). Information technologies to support product lifecycle. Terminological dictionary. Part 1. Stages of the product life cycle (GOST R 50.1.031-2001). Rosstandart. https://clck.ru/3QH6za

18 State Standard. (2004). Information technology. Electronic information exchange. Terms and definitions (GOST R 52292-2004). Rosstandart. https://clck.ru/3QH77t

19 State Standard. (2013). System of standards in information, librarianship, and publishing. Record keeping and archiving. Terms and definitions (GOST R 7.0.8-2013). Rosstandart. https://clck.ru/3QH7AR

– "electronic document: a document in digital form, the use of which requires computer means or other specialized devices for reproducing text, sound, and images"[20].

The variety of definitions is largely due to the fact that individual standards and laws have a limited scope of application and are focused on solving problems in specific areas of human activity. Therefore, it is logical to begin the formation of the EE conceptual apparatus by defining the main task for which it is used. This task is to ensure a uniform understanding and interpretation of the generic and specific characteristics of EE, the relationships and processes formed or applied in the collection, verification and evaluation of evidentiary information, including using the means and methods of forensic examination.

Given that the techniques and methods used when collecting, storing, processing, transmitting and using data constitute information technology[21], it seems logical to use definitions already contained in the state standards in the field of information technology (IT) for the EE conceptual apparatus[22].

Currently, there are several dozen such standards. The following are of the greatest interest in this study:

– GOST 15971-90 Information processing systems. Terms and definitions.

– GOST 13699-91 Recording and reproduction of information. Terms and definitions.

– GOST R 52292-2004 Information technology. Electronic information exchange. Terms and definitions.

– GOST R ISO/IEC 27037-2014 (ISO/IEC 27037:2012) Information technology. Methods and means of ensuring security. Guidelines for the identification, collection, receipt and storage of evidences provided in a digital form[23].

– GOST 33707-2016 (ISO/IEC 2382:2015) Information technologies. Dictionary.

The above standards use the "modern approach to information technology specification based on distinguishing two different aspects of phenomena: social (in this case, purpose, information, document, etc.) and technological (in this case, media, format, data, etc.)" (GOST R 52292). This is quite consistent with two different but interrelated aspects of EE fixation (Belkin, 2007). The procedural side is aimed at forming a legally binding evidence framework by reflecting the factual data, discovered by the investigator, in the procedural documents. The forensic side primarily touches upon the means and methods used at various stages of the detection and consolidation of evidentiary information.

---

20 State Standard. (2013). System of standards in information, librarianship, and publishing. Electronic publications. Main types and issuance information (GOST R 7.0.83-2013). Rosstandart. https://clck.ru/3QH7CR

21 State Standard. (1990). Information technology. Set of standards for automated systems. Terms and definitions (GOST 34.003-90). Rosstandart. https://clck.ru/3QH7EK

22 Not to be confused with the " System of standards in information, librarianship, and publishing".

23 This standard is recommended by the UN Office on Drugs and Crime for use in the investigation of cybercrimes. https://clck.ru/3QH7Pr

These stages include[24]:

1. Identifying EE – search, recognition and documentation of potential EE. During the identification process, information carriers and processing devices are identified that may contain potential EE.

2. Collecting EE – placing media with EE in a controlled environment for subsequent extraction of evidentiary information.

3. Receiving EE – creating a copy of EE.

4. Storing EE – ensuring the protection of EE from changes (falsification, damage, etc.).

5. Analyzing EE – in-depth research in order to identify evidentiary information.

6. Presenting (summarizing and explaining) the discovered factual data in a procedural document.

It is important that at all these stages "not only the evidentiary information per se is captured, but also information about the ways, methods and means of obtaining it as a necessary condition for its admissibility in the case" (Belkin, 2007).

It should also be noted that currently in Russia there is still no model for working with digital evidence during investigations, common for various law enforcement agencies.

Most of the standardized IT terms characterizing the technological/forensic side of collecting EE can be applied in the conceptual framework of EE without any changes. Missing generic and specific concepts related directly to IT can be formed by concretizing and adapting existing basic IT concepts based on "analyzing and generalizing the properties and features of objects and identifying the characteristics describing concepts" (GOST R 50.1.075[25]) (Fig. 1), including taking into account the relationship of the "information" and "data" concepts shown in Fig. 2.

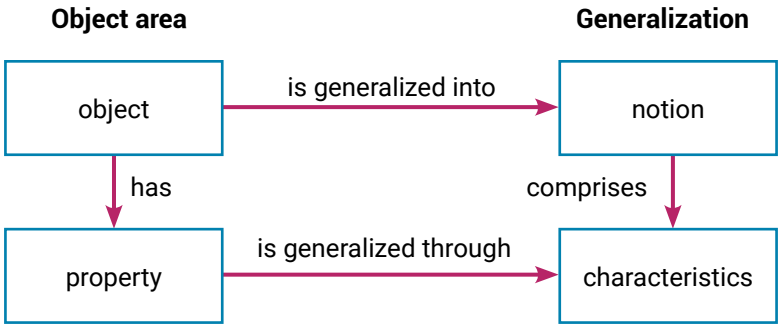

Fig. 1. Order of forming new concepts according to GOST R 50.1.075

[24] A typical integrated model for working with digital evidence is presented, para. 1-4 of which correspond to the recommendations of GOST R ISO/IEC 27037, para. 5 and 6 – to the model based on the US FBI protocol (Reedy, 2022).

[25] State Standard. (2011). Elaboration of standards for terms and definitions (GOST R 50.1.075-2011). Rosstandart. https://clck.ru/3QH7T9

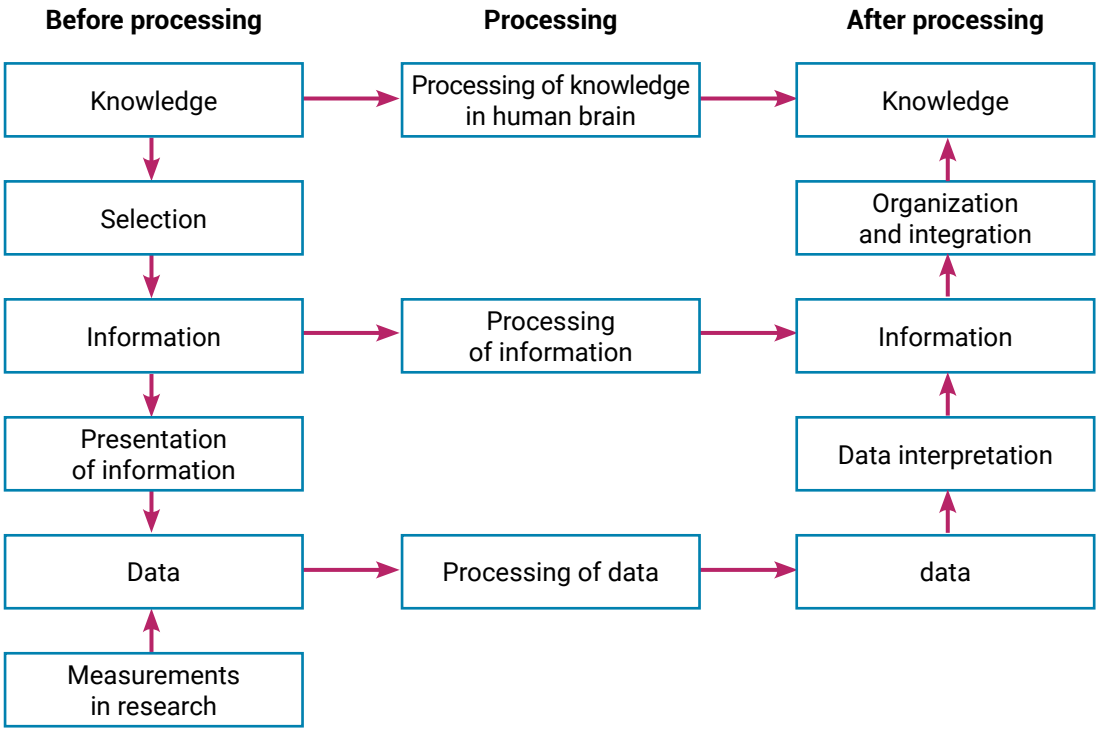

Fig. 2. A diagram reflecting the relationship between the concepts of "knowledge", "information" and "data" in accordance with ISO/IEC 2382-1:1993[26]

Using these standards and principles, it is not difficult to formulate terms and definitions universal for all types of legal proceedings, forming the basis of the EE conceptual apparatus.

GOST R 52292 provides the following definitions of "data" and "electronic environment":

– "data[27]: a formalized representation of information suitable for communication, interpretation or processing <...>;

– analog data: data represented by a physical quantity that is considered a continuous variable and whose value is directly proportional to the data or a suitable data function <...>;

– discrete data (symbolic data): data represented by symbols <...>;

– electronic environment: the environment of technical devices (hardware) operating on the basis of physical laws and used in information technology for the processing, storage and transmission of data"[28].

[26] ISO/IEC 2382-1:1993 Information technology. Dictionary. Part 1. Basic terms. Substituted with ISO/IEC 2382:2015. https://clck.ru/3QH7fj

[27] Depending on the type of information, the data can be audio, video, etc.

[28] State Standard. (2004). Information technology. Electronic information exchange. Terms and definitions (GOST R 52292-2004). Rosstandart. https://clck.ru/3QH77t

From these definitions, it follows that electronic evidence should be understood as data containing evidentiary information, stored or transmitted in a form suitable for human perception using information technology and electronic equipment.

The electronic technology mentioned in the definition includes not only computing facilities, but also electronic devices used for processing, recording, converting or transmitting information or energy using electronic components and principles of electronics. For example, for a person to perceive the sound information contained in a digital phonogram or video phonogram, it is not enough to have a DAC[29] (computing device) and a codec (information technology); it requires electronic devices designed to amplify an electrical signal and convert it into sound waves of various frequency and power.

Information technology is the techniques and methods of using computer technology in performing the functions of collecting, storing, processing, transmitting and using data (GOST 34.003-90).

It follows from the definitions of GOST R 52292 that EE can be represented in two types (Fig. 3):

– analog, in which a physical quantity takes on an infinite set of values that change continuously; and

– discrete, meaning that data exist in the form of discrete symbols, each of which can take one of a finite number of values.

That corresponds to Interpol's position on this issue: "Electronic evidence is a derivative term for two types of evidence: analog evidence and digital evidence" (Reedy, 2022).

Accordingly, digital evidence containing evidentiary information is data stored or transmitted in the form of binary code (GOST R ISO/IEC 27037); the term refers to electronic discrete evidence. The same class of evidence includes string and logical data, for example, those displayed on the screen of a voice recorder or smartphone (smartphone IMEI; phonogram title; time and geographical coordinates of the sound recording or video location; real-time clock readings of the recording device; phonogram duration; position (on/off) of the trigger or AGC[30] controls).

Thus, a digital phonogram containing evidentiary information belongs to the class of electronic discrete digital evidence. It is digital audio data stored on a tangible medium, obtained as a result of:

– digital sound recording – digital recording of sound, or sound information, coming from a primary source or a device for reproducing sound information (Fig. 3);

---

[29] DAC (digital-analog converter) – a device for converting digital data into an analog signal.

[30] AGC – automatic signal gain control.curcuit.

– generation (synthesis) of sound using algorithms and methods of digital signal processing.

The importance of distinguishing two ways of creating a digital phonogram is due to the following:

– The need to distinguish between the actual sound recording and recording on a digital audio data carrier. The latter can be either one of the stages of sound recording (Fig. 3), or a self-sufficient process carried out in order to copy digital audio data or save the generated data (see below).

– The fact that sound synthesis can be performed using previously recorded audio signals or their components indicating time and frequency, as well as on the basis of a mathematical or generative[31] model, without using the sound recording process at all stages of phonogram creation.

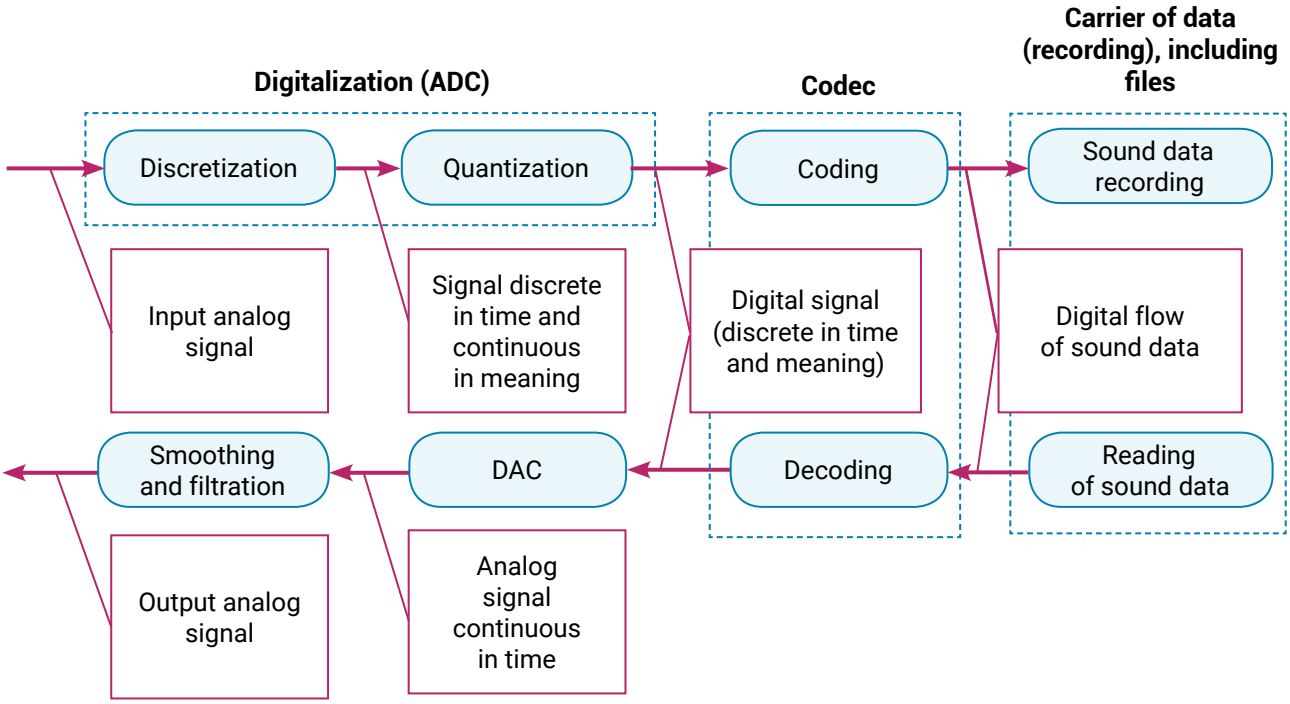

Fig. 3. Digital sound recording and sound reproduction

Source: (Zubov, 2020).

Digital audio data should be understood as the result of digitization and encoding of audio signals, presented in a form suitable for communication, interpretation or processing using electronic devices and information technologies. The recording of digital audio data on a media can be accompanied by the creation of files and metadata.

The need to mention “analog phonograms” is due, in particular, to the fact that there are aircraft still in operation, in which flight data and crew negotiations are recorded with

[31] The generative model creates training-like data based on statistical patterns, but not based on physical laws.

analog tape recorders (on magnetic tape or wire); stored in archives, there are analog phonograms and videophonograms recorded on magnetic tape, film, discs, etc.

It also follows from the above that not all currently existing phonograms can be classified as EE. For example, to record and reproduce mechanical (by recording method) analog phonograms on discs, rollers, etc., the use of electronic equipment and information technology is not necessary.

Obviously, it is not difficult to form similar definitions of a videogram or videophonogram and the data contained in them.

Thus, a videophonogram should be called digital video and audio data stored on a tangible medium, obtained as a result of:

– digital video sound recording – synchronous digital recording of video and sound, or audiovisual information coming from the primary source or a reproduction device;

– generation (synthesis) of video images and sound using algorithms and methods of digital signal processing.

Let us focus separately on data carriers, which are material objects (including a physical field) intended for recording and storing data, which, due to their tangibility, are often classified as physical evidence in procedural documents. It is advisable to classify media: by the recording method (mechanical, magnetic, optical, electronic, etc.); by the form of recorded data representation (analog, digital, etc.); and by the type of information (video, audio, text, etc.). In this case, for example, a music CD is an optical carrier of digital audio data; an ordinary tape recorder with a magnetic phonogram is a magnetic carrier of analog audio data; a hard disk with digital phonograms is a magnetic carrier of digital audio data; a flash drive is a solid-state carrier.

A special case of a data carrier is a "recording medium", or "a physical body used during recording to store information signals in it or on its surface"[32], for example, a tape cassette or an optical disc.

The above example with the classification of a music CD shows that not all digital data carriers are electronic carriers. The latter should include only electronic devices of the appropriate purpose that operate with their own controller[33]: a flash drive; a hard disk; a hardware RAID array; a network storage, etc.

Apparently, it is not easy for a nonprofessional to determine whether a data carrier belongs to a certain class. Therefore, in procedural documents drawn up by a nonprofessional, it is quite acceptable to indicate, along with other identifying

---

[32] State Standard. (1991). Information recording and reproduction. Terms and definitions (GOST 13699-91). Rosstandart. https://clck.ru/3QH7or

[33] A controller (in electronic engineering) is a specialized electronic device (or its assembly) designed to automatically control a technical object (process) according to a set algorithm (program).

information, only the type of media (a hard or optical disk; a flash drive; a tape recorder) and the characteristics of its contents (an audio or video file, a magnetic or digital phonogram and so on). The classification and explication of data carriers acquires the greatest importance at the stage of assessing the admissibility and reliability of evidence, including using the means and methods of forensic examination.

It is also important to keep in mind the following significant feature of digital PhVVphs. They can be presented in a virtual form, for example, a videophonogram published on the YouTube[34] Internet service, or files with PhVVphs in a cloud storage. Therefore, at the stage of such PhVVphs' identification, their carrier cannot always be determined, and to use PhVVphs as evidence, it will be necessary to copy or export the data to an alienated medium.

Hence, the technical side of the standard procedure for exporting data from virtual to alienated media includes a number of sequential operations that can take place automatically, including without the user's knowledge and control. These may include:

– extracting data from the source environment (database, information system, etc.);

– converting data into a format which allows them to be imported and used in another system or environment;

– actual storage of data on alienated media for their further use or processing.

In other words, the PhVVphs obtained as a result of export are not always copies of those recorded on virtual media.

In this regard, it is advisable to identify a primary carrier to which audio and video signals coming directly from the original source were recorded. In other words, this is the first tangible object on which specific data were recorded. The secondary carrier is that on which the data were stored as a result of copying or exporting data from the primary or another secondary media. The primary carrier can be either embedded (inalienable) or removable (alienable); the secondary one is alienable, as a rule.

Both primary and secondary carriers can also be virtual at the same time, which the user can access via the Internet or in a similar way.

We also consider important to mention the definition of a "digital evidence copy" as a created copy of a digital evidence and a means of verifying it, which is given in GOST R ISO/IEC 27037. It follows that a copy of a digital phonogram containing evidentiary information can only be considered a phonogram obtained as a result of file-based or bitwise copying, the conformity of which can be verified either using the verification function or in another acceptable way. In the English-language specialized literature, this is also called a "forensic copy".

[34] The foreign person owning the YouTube informational resource violates the legislation of the Russian Federation.

Naturally, all these definitions are not "carved in stone" and can be replaced with synonymous ones that do not distort the essence of the described properties, processes and phenomena. For example, the verification of the immutability of files by establishing the identity of two sets of data contained in them is called "verification" in GOST R ISO/IEC 27037 and "authentication" in GOST R 57429, which does not change the meaning and content of the procedure.

3. International experience

Currently, the "branch of criminology that applies legal issues to information and communication technologies and digital devices"[35] , commonly referred to as Digital forensics, is recognized as an independent scientific discipline by many international and national organizations. These include the United Nations Office on Drugs and Crime, Interpol, the European Network of Forensic Science Institutes (ENFSI), the European Union Agency for Cybersecurity (ENISA), the American Academy of Forensic Sciences (AAFS), the Organization of Scientific Industry Committees (OSAC)[36], the UK Forensic Science Regulator, the International Organization for Standardization (ISO), and the International Electrotechnical Commission (IEC). The fundamental sciences and basic scientific directions for various subdisciplines of digital forensics currently include: biology, physics, mathematics, linguistics, as well as computer science, computer engineering, image science, acoustics, anthropology, statistics, and data science (Reedy, 2020; Rybaczewska & Sparks, 2022).

Publicly available publications of the above organizations provide a rather comprehensive picture of the current state of digital forensics, its methods and procedures related to working with digital evidence. It should be noted that the features of working with the PhVVphs are not specified in the listed documents.

In 2020, a manual "Cybercrime"[37] consisting of 14 modules was published, as a result of the joint work of the United Nations Office on Drugs and Crime and leading experts from more than 25 countries around the world. Module 4 of this manual, "Introduction to digital forensics", provides an overview of the current state of digital forensics, in particular, the digital forensics standards, the process of examining digital evidence and general practical methods of expert research, as well as best practices in the field of digital forensics.

---

35 United Nations Office on Drugs and Crime. (2020). "Cybercrime" – a series of university modules. https://clck.ru/3QH7sy

36 Adopted by the US National Institute of Standards and Technology (NIST) for the development of specialized standards of forensic examination.

37 United Nations Office on Drugs and Crime. (2020). "Cybercrime" – a series of university modules. https://clck.ru/3QH7sy

An analysis of trends, problems, and achievements of Interpol and law enforcement agencies in different countries in the field of collecting, analyzing, and using digital evidence in crime investigations is provided in the Interpol review of digital evidence for 2016–2019 and 2019–2022 (Reedy, 2020; 2022; Tripathi & Meshram, 2022; Insa, 2007).

In 2019, Interpol published Global Guidelines for Digital Forensics Laboratories[38]. The document is a guide to the creation, management and operation of digital forensics laboratories in accordance with common standards that ensure the admissibility of electronic evidence in courts, including international ones.

The 2014 ENISA guide for first responders to computer incidents[39] focuses on how to handle digital evidence, starting with arrival at the crime scene and ending with the assessment and presentation of digital evidence.

The Best Practice Manual of the European Network of Forensic Science Institutes (ENFSI), devoted to conducting digital forensic research (version 1, 2015)[40], reflects the standard procedure of forensic examination of digital evidence, standards and universal methods of expert research, as well as best practices in the field of digital forensics, including staff training. Taken together, these should ensure the reliability and comparability of the results of forensic examinations.

The NIST IR 8387 (September 2022) report (Guttman et al., 2022; Turner, 2005; Romaniuk, 2024), prepared in partnership with the US National Institute of Justice (NIJ) and aimed at professionals in evidence management, provides practical recommendations for preserving digital evidence and describes their unique features.

The key problems faced by law enforcement specialists include data encryption, cloud services, distributed storage, the Internet of Things, artificial intelligence, a shortage of qualified specialists, and differences in national legislations. The main recommendations include the harmonization of legal norms, investments in training specialists and equipping laboratories, and the development of compatible technologies for examining digital evidence.

It is emphasized that “every case involving digital evidence poses new challenges that digital evidence specialists must be able to solve. A future digital evidence specialist must have the knowledge and skills to solve forensic issues in a specific case” (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

It should be mentioned that, in addition to GOST R ISO/IEC 27037 adapted to Russian conditions, ISO/IEC published additional international standards that have no Russian analogues. They cover reliability of digital forensic examination tools and methods – ISO/IEC 27041:2015 "Information technology. Security techniques. Guidance on assuring suitability and adequacy of incident investigative method", as well as the stages of research and interpretation of the digital forensic examination process – ISO/IEC 27042:2015 "Information technology. Security techniques. Guidelines for the analysis and interpretation of digital evidence".

Thus, the world has accumulated a wealth of experience in developing regulations – instructions, manuals, as well as standards and training materials on the creation and operation of digital forensics laboratories and working with digital evidence in the investigation of crimes. At the same time, the concept of "electronic evidence" is practically not used in modern regulatory documents and standards, since the features of studying analog evidence have long been known and studied and, together with digital evidence, they constitute an array of "electronic" evidence.

Conclusions

Digital phonograms, videograms, and videophonograms occupy a significant place in the EE system, representing highly vulnerable sources of audiovisual information that require a specialized approach to their recording, verification, and evaluation in court proceedings.

The lack of clear definitions and classifications of EE and PhVVphs in regulatory legal acts leads to legal uncertainty, errors in procedural practice and a decreased effectiveness of using such evidence in general.

The proposed methodology for the formation of the conceptual apparatus of the EE in general and PhVVphs in particular, based on existing state standards in the field of information technology, makes it possible to create universal terms and definitions adapted for all types of legal proceedings.

Further research in this area should be aimed at developing utmost clear and detailed recommendations, guidelines and instructions for experts and investigators on the identification, collection, receipt, preservation and analysis of EE, including using foreign experience.

In the future, it is necessary to improve the procedural rules, including the introduction of mandatory requirements for the competence of specialists and their mandatory involvement in the earliest stages of investigation.

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

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

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.