Protection of primary tangible media as evidence against cyberattacks

Oleksandr Bobarchuk[1,*,†], Oleh Briahin[2,†], Svitlana Halchenko[1,†], Rat Berdibayev[3,†], Maryna Holovatenko[1,†] and Iryna Les[1,†]

[1] *National Aviation University, Liubomyra Huzara Ave. 1, Kyiv, 03058, Ukraine*

[2] *Department of Strategic Investigations of the National Police of Ukraine, Akademika Bogomoltsa Str., 10, Kyiv, 01601, Ukraine*

[3] *Almaty University of Power Engineering and Telecommunications, Baitursynov Str., 126, Almaty, 050013, Kazakhstan*

Abstract

Due to the continuous development of information technology and the growing number of cyber threats, the importance of protecting primary media is becoming especially relevant in the field of cybersecurity. This issue examines and explores strategies and technologies to protect these media. In the case of cyberattacks, they can be not only targets of attack but also potential sources of evidence for further investigation. Primary physical media, such as hard drives, flash memory, CDs, and DVDs, store large amounts of data that can be critical to the functioning of organizations and personal privacy. Protecting these media involves using a wide range of measures, including data encryption, the use of biometric identification methods, and regular security audits. During attacks on information systems, attackers may try to delete, modify, or steal data. However, if adequate protection is applied, these media can preserve data integrity and act as electronic evidence. This approach allows law enforcement agencies to effectively conduct investigations and provide evidence for litigation. The authors found the task of "reading" certain norms of the criminal procedural legislation of Ukraine through the eyes of specialists in the field of recording, reproduction and protection of information interesting and relevant. Where necessary, the issues were extended to such popular data carriers as semiconductor USB flash drives (hereinafter referred to as USB Flash drives, abbreviated as UFD). The results of the task will help, in our opinion, to start the formation (in some cases – necessary) of a multidisciplinary approach to determining the true content of such concepts as evidence, source of evidence, material medium of information, primary medium, etc. The subject of this work is the study of the junction of these "impossibilities" – a more detailed acquaintance with the characteristics of evidence for cases where the source of evidence is a digital medium on which factual data on conversations and actions of persons or other information are recorded during the implementation of operational and search activities, pre-trial investigation and trial. In other words, we will be interested in certain types of documents within the meaning of Article 99 of the Criminal Procedure Code (CPC) of Ukraine.

Keywords

primary storage media, proof, source of evidence, cyberattack, cybersecurity, semiconductor USB flash drive, UFD

1. Duality of the concept of "document"

The discussion of the duality of the concept of "document" in the context of criminal proceedings emphasizes the importance of cybersecurity when dealing with electronic materials, such as storage media and electronic documents. Ensuring the confidentiality, integrity and availability of this data becomes a key aspect to maintain its legal weight and reliability.

CH&CMiGIN'24: Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, January 24–27, 2024, Kyiv, Ukraine

* Corresponding author.

† These authors contributed equally.

a.bobarchuk@gmail.com (O. Bobarchuk); ob112467@gmail.com (O. Briahin); smgalchenko@gmail.com (S. Halchenko); r.berdybaev@aues.kz (R. Berdibayev); marina4513125@ukr.net (M. Holovatenko); iryna.les@npp.nau.edu.ua (I. Les)

0000-0003-3176-7231 (O. Bobarchuk); 0009-0004-5333-946X (O. Briahin); 0000-0003-0531-1572 (S. Halchenko); 0000-0002-8341-9645 (R. Berdibayev); 0000-0002-6958-4767 (M. Holovatenko); 0000-0003-0596-3749 (I. Les)

Thus, from a procedural point of view, evidence is factual data, and a document is considered a procedural source of evidence (Article 84 of the CPC). Part one of Article 99 of the CPC defines a document as a material object specially created for the purpose of storing information, which contains information recorded with the help of written signs, sound, images, etc., which can be used as evidence of a fact or circumstances established during criminal proceedings.

At our discretion, we have chosen those types of documents from those specified in Article 99 of the Code of Criminal Procedure, which may be of interest to our study, namely:

- materials of photography, sound recording, video recording and other information carriers (including electronic) – subparagraph 1 of part two;
- data carriers on which procedural actions are recorded with the help of technical means (annexes to the protocols of procedural actions drawn up in accordance with the procedure provided for by the CPC) – subparagraph 3 of part two;
- materials that record factual data on unlawful acts of individuals and groups of persons collected by operational units in compliance with the requirements of the Law of Ukraine "On Operational Investigative Activities" [1] with the above restrictions – the second paragraph of part two.

Separately in Art. 105 of the CPC are also indicated in the form of annexes to the protocols:

- audio and video recording of the procedural action, – subparagraph 3 of part two;
- computer data carriers and other materials explaining the content of the protocol – subparagraph 4 of part two.

In the following presentation, we propose to adopt the following symbols for the two dimensions of the dualistic nature of such documents:

- procedural (in this dimension, we will talk about the document from a procedural, normative point of view);
- scientific and technical (in this dimension we will talk about the document as a product of certain basic information technologies).

The proposed division does not separate or oppose the procedural and scientific-technical essence of the document, but aims to present them comprehensively, to get closer to the truth in their understanding within the limits available today.

It should be noted that such dualism is inherent not only in the above-mentioned types of information products, but also in other information products, for which their formation and life cycle are determined not only by physical phenomena, algorithms and programs, but also by legislative and (or) regulatory acts (state and other types of secrets, information that is an object of intellectual property, etc.). Such types of information are proposed to be referred to as information with a special procedural status (hereinafter referred to as ISPS). Thus, the main feature of ISPS is the mandatory combination of scientific, technical and regulatory components in the characteristics of the information product.

In this regard, it is important to consider cybersecurity aspects, as electronic forms of documents, such as computer storage media, can be the target of cyberattacks or unauthorized access. Ensuring the protection, confidentiality and integrity of this electronic data is a key element in ensuring its legal weight and credibility when used in legal proceedings.

1.1. Procedural dimension

In order to determine the properties of such documents in the first dimension, it would be necessary to further detail the main procedural characteristics (propriety, admissibility) in order to find those

of them that can be unambiguously attributed to the selected types of documents. Such studies have been conducted and are being conducted within the framework of the disciplinary approach [2, 3].

However, the authors chose another, in our opinion, more practical method, which is used in many fields of science and technology – the method of modeling, in which a model is created according to known characteristics and its analysis is carried out within certain limitations. Such characteristics were found in the provisions of the Criminal Procedure Code, the Law of Ukraine "On Operational Investigative Activities" and the Instruction on the Organization of Covert Investigative (Search) Actions and the Use of Their Results in Criminal Proceedings [4] (hereinafter referred to as the Instruction of the CISA).

For further solution of the task set before us, we propose to divide these characteristics (signs) into conditional and unconditional. It should be noted additionally that the following classification is not a classical approach to detailing the features of evidence within the framework of a disciplinary, legal approach, but is a conscious step towards formalizing the characteristics of certain types of documents given in the criminal procedural legislation. If, after the formalization of the requirements, it is possible to translate them into technical requirements for the data carrier and produce it, it is possible to talk about such a medium as "ideal" for recording information during operational and search activities, pre-trial investigation, etc.

The course and results of the classification are presented below.

Documents are material evidence if they contain signs of material evidence (Article 98 of the CPC). Thus, the unconditional feature of material evidence is its "materiality". This property of the document, as material evidence (material object), became decisive in the further consideration of the subject of the article.

Other, already conditional, characteristics of a document – material evidence – should be considered those characteristics that are determined by the provisions of the CPC, the Law of Ukraine "On Operational Investigative Activities" and the Instruction of the CISA in relation to such documents. We have grouped them into species with the following names:

1. Characteristics of the procedural content of the document:

- the presence in the object of information that can be used as evidence of a fact or circumstances established during criminal proceedings - part one of Art. 99 CPC;
- protocols on the conduct of covert investigative (search) actions, audio or video recordings, photographs, other results obtained through the use of technical means, things and documents seized during their conduct or their copies may be used in evidence on the same grounds as the results of other investigative (search) actions during pre-trial investigation - part one of Art. 256 CPC.

2. Characteristics of the procedural authenticity of the document:

- a party to criminal proceedings, a victim, a representative of a legal entity in respect of which the proceedings are conducted, are obliged to provide the court with the original document, the original of the electronic document is its reflection, which is given the same meaning as the document – part three of Art. 99 CPC;
- the materials of criminal proceedings contain original copies of technical data carriers of the recorded procedural action, backup copies of which are stored separately – part three of Art. 107 CPC;
- technical means used during covert investigative (search) actions, as well as primary carriers of the information obtained, must be stored until the court verdict comes into force – part two of Art. 266 CPC.

3. Characteristics of the overall procedural capacity of the document:

- a duplicate of a document (a document made in the same way as its original) may be recognized by the court as an original document - part four of Art. 99 CPC;
- the party is obliged to provide the other party with the opportunity to inspect or copy the original documents, the content of which was proved in the manner prescribed by this Article (Art. 99 of the CPC) - part seven of Art. 99 CPC;
- fixation with the help of technical means of procedural action on an information carrier is one of the forms of recording criminal proceedings - paragraph 2 of part one of Art. 103 CPC;
- annexes to the protocols must be duly produced, packed for the purpose of safe keeping, as well as certified by the signatures of the investigator, prosecutor, specialist, other persons who participated in the production and/or seizure of such annexes - part three of Art. 105 CPC;
- the content of information obtained as a result of retrieval of information from electronic information systems or their parts shall be recorded on the appropriate medium by the person who carried out the removal and is obliged to ensure the processing, storage or transmission of information – part two of Art. 265 CPC;
- recording the results of covert investigative (search) actions should be carried out in such a way that it is always possible to establish the reliability of these results by expert means, - paragraph 4.8 of the Instruction of the CISA;
- the prosecutor shall take measures to preserve the things and documents obtained during covert investigative (search) actions, which he plans to use in criminal proceedings - part four of Art. 252 CPC;
- if the prosecutor intends to use as evidence during the trial the information obtained as a result of interference with private communication, or a certain fragment thereof, he is obliged to ensure the preservation of all information or instruct the investigator to ensure the preservation - part one of Art. 259 CPC;
- making copies of protocols on the conduct of covert investigative (search) actions and annexes to them is not allowed - part three of Art. 254 CPC;
- declassified material media that the prosecutor intends to use as evidence during the trial shall be stored at the discretion of the prosecutor in his official safe or in the investigator's safe on the instructions of the prosecutor - paragraph 5.29 of the CISA Instruction;
- information, things and documents obtained as a result of covert investigative (search) actions, which the prosecutor does not consider necessary for further pre-trial investigation, must be immediately destroyed on the basis of his decision, the destruction of information, things and documents is carried out under the control of the prosecutor - parts one, four of Art. 255 CPC;
- information carriers and technical means by means of which information was obtained may be the subject of research by relevant specialists or experts in the manner prescribed by this Code – part three of Art. 266 CPC;
- employees (employees) of operational units - executors of covert investigative (search) actions - must take the necessary measures to ensure the safety and integrity of the received materials (protection against unauthorized interference, deformation, demagnetization, discoloration, erasure, etc.) in the period before their transfer to the prosecutor – paragraph 4.9 of the Instruction of the CISA;
- information obtained as a result of operative search activity concerning personal life, honour and dignity of a person, if it does not contain information about the commission of actions prohibited by law, shall not be subject to storage and shall be destroyed - part twelve of Article 9 of the Law of Ukraine "On Operative Investigative Activity".

The importance of the integrity of the document-material evidence guarantees its inviolability and the absence of unlawful modifications. This is a key aspect to ensure the inevitability and reliability of the facts presented in the document.

Authenticity and anonymity of the document are determined by mechanisms for determining and confirming one's authenticity, avoiding the possibility of falsification. The use of electronic signatures and other authentication methods is essential for verifying the source and authorship of a document. Encrypting the data in the document provides protection against unauthorized access, ensuring the confidentiality of information. Encryption keys must be managed and stored in trusted systems.

Protection against cyberattacks involves the use of modern antivirus programs and intrusion detection systems. The general approach to the protection of evidence documents includes a set of measures aimed at preserving their inviolability, confidentiality and authenticity. In a digital environment where cybersecurity threats are ever-increasing, effective document protection is critical to ensure the truthfulness and validity of their use in litigation [5].

1.2. Scientific and technical dimension

The combination of the listed procedural characteristics may result in the comprehension of a certain system of relationships, the elements of which are:

- persons (operative officer, party to criminal proceedings, victim, representative of the legal entity in respect of which the proceedings are conducted, specialist, expert);
- material objects (technical means, material data carriers);
- processes (fixation, copying, display, storage, destruction, authentication);
- information.

Not in the procedural, but in the scientific and technical dimension, the set of these structural objects is no different from the set of other systems (information technologies) that result in an information product. As it is known, a sufficient defining feature of the system is the difference in the interrelations of its structural elements, therefore, taking into account the given conditional and unconditional features, it is possible to talk about a separate applied information technology (subtechnology) - a system for receiving, accumulating, processing, exchanging, displaying and forming ISPS.

Again, from a scientific and technical point of view, the description of the regulation of information technology takes place at the physical (devices) and logical (programs, algorithms) levels, from the initial stage (obtaining information) to the final stage (knowledge formation). At the same time, the information subtechnology, the product of which is ISPS, can be classified as a specialized system, the functionality of which additionally includes the above-mentioned procedural characteristics.

Thus, the development of information subtechnology for creating such a product as ISPS should consist in modifying the existing information technologies in order to acquire the specified conditional and unconditional features by the final information product. Combining them into classes (procedural content, authenticity, capacity and a common feature of materiality) can be used to formalize the task for such modification, and the task should be directed from specialists in the field of criminal procedural law to specialists in the field of information technology.

From the point of view of theory, yes, but, unfortunately, it is impossible to implement such an approach in practice without detailed and close interaction, on the one hand, by specialists in the field of law who understand information technology, on the other hand, by specialists in the field of information technology, for whom the problems of procedurality are clear and relevant, on the third hand, by specialists in the protection of state secrets, who are at the same time specialists in procedural issues and information technology issues.

To solve such a complex problem, we will try to compare the life cycles of ISPS only by two approaches - procedural and scientific-technical (the features of the implementation of regime approaches are not considered in this article).

From a procedural point of view, ISPS is formed in the following way (with some peculiarities). After a person with the appropriate procedural status in one way or another receives information about a crime being prepared, or about persons preparing to commit a crime, or about the commission of a criminal offense, or after the occurrence of other events, it may be necessary to record information about conversations, actions, or other content of private or other types of communication.

After the occurrence of sufficient and (or) necessary procedural prerequisites, the task arises – in compliance with the above unconditional and conditional requirements – to obtain a material object – a medium of information with a record of those conversations, actions and other facts of private communication that carry objective information about their content and other circumstances. Such a medium, as a rule, is perceived only in the form of an appendix to the protocol, which adds the necessary procedurality to such a medium. Such a medium must be "primary", suitable for expert research, stable in time, store information (factual data) for the entire period necessary to establish the truth in criminal proceedings. In certain cases, the information from the medium, or the medium itself, must be guaranteed to be destroyed.

In the digital age, when information systems are becoming an integral part of the functioning of the public sector and cybersecurity issues are becoming extremely relevant, ISPS is becoming the object of constant cyberattacks, which requires effective strategies and measures to protect them.

Today's cyber threats are becoming more sophisticated and sophisticated. They can lead to the leakage of confidential information, the interruption of systems, or even the manipulation of important decisions. The financial, energy, medical, and other sectors require a high level of protection against these hazards.

Effective ISPS protection starts with a strong authentication and authorization system. The use of two-factor authentication and competent management of access rights can complicate the task of attackers and increase the level of security.

To avoid unauthorized access to sensitive information, it is important to use strong encryption to protect data in transit and at rest. Encryption becomes a barrier for attackers trying to obtain sensitive information. The use of intrusion detection and protection systems allows you to detect and eliminate potential threats in time. These systems can respond to suspicious activity and block attacks, ensuring the security of the system.

Also, the main task of protection against cyberattacks is regular security audits to identify vulnerabilities and weaknesses in the system. Activity monitoring allows you to quickly respond to potential threats and ensure business continuity.

Data backup and recovery systems play a key role in ensuring that the system is quickly restored after a cyberattack. Creating regular backups and verifying them is a necessary part of your security strategy.

In today's increasingly multiplied and sophisticated cyber threats, protecting ISPS from cyberattacks requires constant updating and refining strategies. Only a comprehensive approach that takes into account technical, organizational and human aspects can ensure reliable protection of information systems in the public sector [6].

In the scientific and technical dimension, the formation of ISPS, like any other information, occurs by converting external signals from input devices into a set of data available for processing, without which it is impossible to talk about an information product as such [7].

It should also be realized that information is a reflection of the real world in the form of its evaluation. A person can perceive and evaluate information using only his intellect (objectively, logically, using the methods of scientific cognition), emotionally (on the basis of the psychophysiological characteristics inherent in a given person), or traditionally – in this case, perception and evaluation is carried out in the format of generally accepted ethical or other criteria, established provisions and forms. In practice, as a rule, there is a combination of these three forms of perception [8]. Sounds, voices, and images are forms of information representation, which in information theory are called data [9]. Signals are considered to be the primary material carriers of information [10].

Now let's try to provide some general provisions regarding sound recording. Sound, by its nature, is the oscillatory movement of particles of an elastic medium, propagating in the form of waves. There is a certain specificity of the direct perception of such oscillatory movements by the human ear. These issues are dealt with by psychoacoustics. In our case, the scientific and technical environment offered humanity the following solution to the problem of recording and reproducing sound. With the help of specially created receivers of sound waves (microphones and other electroacoustic transducers), an electrical signal is obtained that reflects one or another characteristic of the sound wave. Everyone is probably well aware, for example, the arrow indicators for recording an audio signal [11], which display the level of the signal converted from the sound wave.

The next technological task was to invent a way to preserve the flow of such a signal in time, and then, using the reverse method of electroacoustic conversion, to reproduce sound waves from speakers. Obviously, with any implementation of this method, we will not get an identity between the directly heard voice and its reproduced copy after recording. From a scientific and technical point of view, it is possible to speak only about the identity of the electrical signals generated at the input of the recording system and at the output of the playback system.

So, let's note the existence of the first problem, which concerns the block of authentic features of any voice recording. The only primary, in the scientific and technical sense, source of sound waves is their direct natural source - the human voice, environmental sounds, etc. Receiving a signal is the first, primary procedure for displaying sound (voice).

Recording such a signal is a rather complex process, and the recording technology determines the possible type of media on which such a recording will be made.

Creating an audio recording on a flash drive is approximately as follows (Figure 1).

Sound waves are received by a sound-receiving device (microphone) and converted by the shaper into a continuous analog electrical signal that carries the course of certain characteristics of the received sound waves over time.

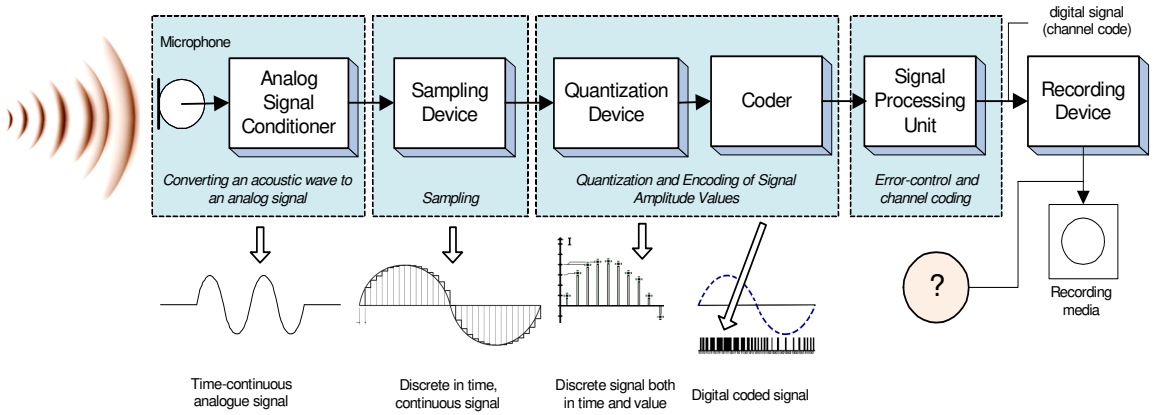

Figure 1: The process of acoustic signal recording on UFD.

It should be noted that at one time the technology of recording such an analog signal on magnetic tape was probably the last "sophisticated" technology built by analogy with writing a manuscript on paper. It was in this case that we obtained a physical medium (a magnetic tape with a magnetic signalogram, in which both the trace of the acoustic wave and the recording process itself were recorded from its beginning to its end), which, from a procedural point of view, could be considered a potentially "ideal" source of evidence without reservationsв.

Further, the analog signal in the sampling device becomes discrete in time, - the signal changes in time are recorded only during samples (samples), - discretely, the more frequent the samples are (the higher the sampling rate), the more "accurate" the future image of the analog signal will be. But at this stage, in any case, part of the primary analog signal is already irretrievably lost.

The quantization device converts a signal that is discrete in time, but continuous in values, into a discrete sequence of values of the signal "countdown – signal value" with the replacement of the signal magnitude with the nearest value from a set of fixed values – quantization levels.

The encoder converts this value into a number corresponding to the ordinal number of the quantization level. Error-control coding involves artificially adding so-called "control" data bits to the samples at the output of the analog-to-digital converter, which in the future will allow, if necessary, to restore the damaged count or predict its value and replace it. Channel encoding is used to match digital signals to the parameters of the recording/playback channel and also results in some modification of the digital signal.

Thus, as a result of the transformation of acoustic waves, we get a digital stream in the form of a sequence of logical "0" and "1", which carries information about the characteristics of these acoustic waves.

All these operations are performed in hardware and software devices (computer sound card, recorder-playback channel, etc.), and the user, as a rule, is given the opportunity to choose its main parameters before starting recording. For household devices, it can be just a choice of "quality" gradations (high, medium, low), for professional devices – the type of analog signal representation in digital form (PCM, CCITT A-Law, etc.), sampling rate, bit or bitrate, spatiality (mono, stereo, 5.1, etc.). The format of the future sound file (wav, mp3, ogg, etc.) is also selected.

Such a file is created by the "Create" command of the context menu in the following order – first, a file record is created for a new "empty" file with a default name and a size determined by the file type, then the data itself is written to the data region in the clusters allocated to them, and a corresponding cluster chain is created in the file allocation table. After assigning a file a given name, the previously created file record is marked as deleted and a new one is created.

A sound file, like any other, has a fixed name and a certain logical representation and corresponding read/write operations (a named block of information stored on a data carrier) and is a combination of two areas (service area and data area). In the service area there is, among other things, information about the parameters of its recording and playback algorithms, in the data area there is an array of logical "0" and "1", which were formed in the process of recording acoustic signals.

It should be noted that a rather simplified description of the processes that occur during the encoding of digital signals and their compression for representation in one or another format (compression is possible without loss and with data loss) has been given above. However, this was not done to the detriment of the idea that a digital "cast" of an audio signal is a dynamic container of various data in terms of its content and flow in time in the process of formation.

It should also be noted that, despite the external (from the user's point of view) characteristics of the file, which give it the properties of a material object (the file can be seen, analyzed, opened, deleted, copied, moved from one medium to another), in the strict sense it is not such. A material array of data on a medium is filled from the beginning of the conversation recording to its end with the results of the conversion of acoustic waves.

So, the formation and presence of a sound file already involves transferring an array of data to a medium and its location on it. But even at this final stage of the formation and storage of a sound file, there are certain features associated with the peculiarities of writing data to a particular medium. For hard magnetic disks, these are the operations of optimally placing data on the disk surface and moving it from place to place during, for example, a defragmentation operation, for optical disks, these are the operations of channel coding in the drive write path.

The protection of storage media, in particular UFD, is becoming a matter of paramount importance. These portable devices, which store large amounts of information, become the focus of cybercriminals, and therefore require a high level of protection. Important sensitive information such as personal data, corporate files, and other sensitive data can be accessed from UFD. With this in mind, ensuring the security of these devices becomes a critical task.

The use of hardware and software encryption mechanisms is a key aspect of UFD security. This ensures data confidentiality and prevents unauthorized access, even if the device is lost or stolen.

Installing systems that automatically block access to data in case of failed password attempts, or can delete information from the device remotely in the event of loss or theft, is an effective security measure. Also, constant firmware updates and regular security audits allow you to identify and fix vulnerabilities that can be used for cyberattacks.

The overall approach to UFD protection includes technical, organizational, and educational measures. Ensuring comprehensive protection of data carriers from cyberattacks is determined by the need to combat the era of digital threats and preserve the confidentiality and integrity of important information [12].

The use in the form of a UFD data carrier also has its own characteristics, the presence of which is indicated in Figure 1 in the form of an "icon" with a question mark.

The peculiarities of recording and storing data on UFD are due to the so-called "architecture" of combining memory cells located in the plane of the chip and providing access to them, as well as the peculiarity of the functioning of the memory cells themselves. Without going into detail about this issue, we note that in order to achieve the goal of this work, at least two internal algorithms are important, which are implemented by UFD manufacturers inside the devices themselves.

A feature of the first algorithm is that before writing something to a memory cell, it is necessary to erase not only this cell, but all the neighboring ones that form a block of cells. The data written in these cells is moved by the internal firmware to a new location in the UFD array.

The second algorithm is that UFD manufacturers, in order to ensure a uniform load of all cells in the array, have equipped these devices with a "wear leveling" microprogram, which in each case of data overwriting translates them into new free memory cells.

Recording an image on UFD, of course, has differences in signal formation technology, the sensor for which is a matrix of photosensitive cells of a digital camera. Algorithms for processing such signals, including their compression, are also quite complex tasks.

The formation of a complete video signal (image and sound) involves the complex processing of video and audio signals to form an appropriate digital stream, but the technological procedures for recording it on UFD do not differ from the procedures for recording audio files.

Certain features of signal formation also take place during the recording of telephone conversations. At first glance, the recording of a telephone conversation is just an audio recording of the voice of subscribers between whom a connection has been established in the telecommunications network. An acoustic wave sensor is also a microphone, but a telephone, and the systems for generating the corresponding digital signal operate on the same principles as described for the case of forming a digital audio signal. The first well-known feature is the artificial limitation in traditional telecommunication technologies of the frequency range of the transmitted audio signal to the limits from 300 Hz to 3400 Hz. The second feature is the presence of a number of additional algorithms for processing (converting) a digital signal – an image of a telephone conversation in the software and hardware of telecommunication and information and telecommunication networks, through which the connection was routed, and the routing change can occur not only for different connections of the same subscriber, but also during the implementation of one such connection. But even in this case, recording such data in the form of files on UFD will not differ from the one described above.

At this stage, it is possible, under certain conditions, to complete the review of those scientific and technical components of ISPS formation on UFD, without which it is impossible to talk about recording information on such a medium at all.

Based on the results, it is possible to draw the following, in our opinion, obvious conclusions.

1. To date, there is no systematic combination of procedural and scientific-technical aspects of obtaining a recording of various types of information on UFD during the implementation of operational and investigative measures and criminal proceedings. Probably, this applies to recording digital streams on other media as well.
2. One of the options for a systematic combination of these aspects is the introduction of the concept of "information with a special procedural status", the formation with the

participation of specialists (criminalists, experts, specialists in IT, information security and others) of complex requirements for a certain information sub-technology for the production of ISPS and their implementation by entities that directly receive, process and study ISPS.

In our opinion, the core of future requirements can be a combination of the specified unconditional requirement (materiality of the information carrier) on the basis of technologies for recording and storing information and the maximum possible achievement of its "primacy".

2. Primary storage medium

Understanding a certain inadmissibility in the procedural dimension of the expression "the maximum possible achievement of the primacy of the carrier", we will try to outline the boundaries and criteria of the concept of "primary carrier".

As mentioned above, from a scientific and technical point of view, the primary carrier of information is a signal. The standardized definition of the concept of "signal" is the following: a signal is a physical process, the properties of which are determined by the interaction between a material object and the means of its study [13]. Both the signal and the physical process are objects of the material world, but the question of their "materiality" in the procedural dimension is relative.

Scientists understand the property of "materiality" in several dimensions, the main of which are philosophical understanding - it concerns the concept of "matter" (it exists independently of consciousness, the opposite of spiritual), and the understanding of the sign of materiality in the form of acquiring a tangible form, material, objective property [14]. Thus, the signal and the physical process are material in the first sense, but have no attributes of materiality in the second sense. It is obvious that it is the second understanding of materiality that is the basis of the concept of a document as material evidence - a certain object or thing (material object).

In the previous section, using the example of recording a speech signal on UFD, we considered the main processes that cannot but occur during the transfer of a signal to such or any other digital medium. We have indicated at what stages there are irretrievable losses of some part of the primary signal received from the sensor (the operation of sampling an analog signal and the use of an algorithm for compressing a digital audio signal with losses). Irretrievable losses of the primary signal from its sampling are not a selectable option, while losses from compression of a digital signal may be an option, but in practice, in most cases, compression algorithms are used that provide for the irretrievable loss of parts of the signal, especially during the formation of a digital video signal and a signal in telecommunication networks. Such losses of "primacy" are inevitable.

Let's imagine that a conversation of a probable offender is being recorded. Its words in the form of acoustic vibrations are received by the sensor, converted into signals that flow from one electronic component to another, from one functional device to another, and at the end of the formed recording path must be recorded on a medium, which must be material (object, material).

The term "fixation" in this context is interesting and, in our opinion, decisive in the mutual coordination of the scientific, technical and procedural aspects of the recording. This term is quite popular in the text of the Criminal Procedure Code and mainly refers to the procedures for recording various information on a medium. The word "fixation" (from the French consolidation, establishment) means, among other things, - recording, registration, installation of something; focusing on something [15]. The use of the term "fixation" implies, probably, that there should be not only a recording, but also retention, consolidation in a specific place (in our case, in certain physical addresses) of an array of data formed directly during the investigative action (event) from its beginning to its (his) end. It is an array of data, not an electronic file. The user, performing operations with the file as with a quasi-material object (copying, moving, destroying, etc.), deals with the corresponding record on the monitor screen, but this record should be perceived only as a "package with an instruction manual" of such an array. An ordinary user cannot "see" this array directly, because the "instruction manual" is not written for it, but for software designed to view the contents of the recorded array.

Under such conditions, the minimum task of criminalists may be the introduction of a technology for obtaining and recording on a material carrier a signal (trace) that carries information about a person's speech and (or) acoustic environment in a certain place and for a certain time, with losses, without which the use of technology is impossible. The material carrier should be a system part not only of this technology, but also of the technology of ISPS formation as a whole.

It should be noted that during digital recording of images and videos, placement of these records in telecommunication and information networks, the essence of irretrievable signal losses in the recording path will change, but the requirement for the system ownership of the material data carrier of the ISPS formation technology will still be necessary.

At the same time, the consistency of the carrier's belonging to such technology should be ensured by the fulfillment of the requirements for acquiring those characteristics specified in subsection 1.1., which we called conditional (characteristics of procedural content, procedural authenticity and general procedural capacity). It is obvious that the main task of scientific and technical specialists in the process of ensuring the systemic affiliation of the carrier to the technology (their segment of work in the creation of the technology for obtaining and fixing ISPS) should be the implementation, first of all, of the characteristics of procedural authenticity.

Thus, the solution of the problem of authenticity (in the language of the CPC – original, primacy) of the material medium of information is reduced to the formalization of the task for specialists in the field of information technology, recording and reproduction and protection of information regarding the development of the technology for the formation of ISPS, in which the systemic affiliation of the carrier to this technology is a prerequisite.

Meeting the requirements for the primacy, originality of the ISPS carrier is not an easy task for several reasons. Despite the fact that the integration of the medium into the recording technology already takes place at a certain level (writing a file in the form of an array of data to an optical disk is carried out according to its own technology, and writing this file to a hard disk is different from writing to UFD), consideration of the signs of primacy in the conditions of system affiliation of the ISPS medium should take into account, at least, two circumstances.

The first is determined by the fact that the resulting data array can be presented only in the form of an electronic file (the possibilities of manipulating files - both with their service details and with their data arrays are widely known), the understanding of the second requires additional explanations.

When considering the issues of transferring the data array to the medium, the authors deliberately made a certain substitution of concepts, which is also present in the criminal procedural legislation - the data array recorded on the medium is identified with the medium itself in the procedural dimension. But in the strict sense, the data array and its carrier are different objects, and they have different histories. The authors did not make a mistake in describing the processes of getting an array of data onto the medium and holding it. However, in the described procedure, it was understood that we chose a "blank" medium for recording, wrote an array of data on it and obtained a material object – a source of evidence, under certain conditions – a primary medium.

First, let's imagine (in practice, such a case is hardly possible) that in the described way we first received an audio file on UFD – a recording of a conversation between a probable offender, on the second day we received a video recording of a meeting between his two comrades on the same medium, and on the third day – a recording of a telephone conversation between a probable offender and one of these two comrades. For all three records, UFD becomes the primary physical medium, but it is one. As a result of each covert investigative (search) action, a protocol was drawn up. How do I connect one medium to three protocols? The answer is no, only to one.

The following is a more realistic example. Let's imagine that there is a multi-day documentation of criminal activity, for example, a corrupt bribe-taker. If one medium is used for each documented episode (issuing a certificate "about something" to a visitor for a bribe, the number of visitors per day is 20 people, the documentation period is 30 days), the cost of such documentation can be considerable. If you record several episodes on the same medium, it is possible that the problem described for the first imaginary case will occur.

The next example is even more realistic. Recording and documentation are performed on the computer's hard disk for various objects, and the hard disk acquires the characteristics of a primary carrier for a number of criminal proceedings and operational-search cases. The practical use of such a hard drive in this capacity is extremely difficult, if not impossible. Taking into account the above, it can be concluded that the unconditional identification of the formed data array and the medium on which it was recorded is incorrect. So, the second circumstance is that it is correct to call the primary carrier not the entire medium, but the array of data recorded on it using the ISPS formation technology.

Awareness and acceptance of these circumstances as an objective reality will require, in our opinion, a slight adjustment of several concepts of criminal procedural legislation, but neglecting them may lead to a layer of problems during the further development and detailing of procedural requirements for recording information on a medium.

Solving the problem of the primacy of the medium in the proposed way (systematic combination of the medium with the technology) will allow for a wider use of the currently available applications of information technologies, such as a guaranteed electronic digital signature with, for example, "binding" special official information to the received data array (details of the permission of the investigating judge, executing unit, date and time of recording, etc.), adding geographical coordinates to the recorded data array (binding to a place), which will significantly increase the evidentiary value of the information obtained, while greatly simplifying its expert study.

It is obvious that the data carrier itself, in the case of its system integration into the technology of ISPS formation, must have specific properties in relation to:

- recording an array of data;
- retention of the recorded array of data;
- logical and physical layer structures;
- policies for access to and operations with data arrays on media.

An analysis of the modern market of recording equipment potentially suitable for use in operational and investigative work has revealed the means that are closest in their characteristics to the specified basic requirements - small-sized recording devices of the "Edic" type and the like [16]. But they also have, in our opinion, some fundamental shortcomings that do not make it possible to fully use them for the formation of ISPS. For each of the products, the disadvantages are different, but they are related to each other in one way – the recording medium (built-in or external) is integrated into the recording device, and not into the ISPS formation technology.

On today's market, there are also quite a few ways to protect information on UFD, but each of the protection methods implements one or another component of the selected information security policy [17], none of which, according to our research, meets the requirements of ISPS generation and processing technology.

The information security policy for the formation and processing of ISPS, taking into account these specific requirements, is under development, but the products of the corporation "TrusCont" (Israel) [18] and patents of Ukraine [19–21] can be considered as its separate elements.

3. Conclusions

We propose to consider the presented materials and the results obtained as a "step forward" of scientific and technical specialists to specialists in criminalistics in order to achieve an optimal solution to problematic issues that are at the intersection of two relevant disciplines.

We believe that the main conclusions of this work should be the following provisions.

1. The introduction of the concept of "information with a special procedural status" and the formalization of the requirements for its receipt is relevant and is aimed at:

- scientifically grounded optimization of duality of information products obtained with the use of modern information technologies for the implementation of tasks of operational and investigative activities and criminal proceedings;
- significant simplification of expert research of digital records, increasing their reliability;
- increasing the potential of the material carrier of information as a procedural object;
- dissemination of the expected achievements from the developed information sub-technologies for obtaining ISPS to other spheres of public relations, such as the protection of personal data, licensed information, intellectual property, various types of information with limited access, etc.

2. The key issue for the successful and procedural justified application of modern technologies of recording and reproduction of information in criminal proceedings is the solution of problematic issues of the "primacy" of the material medium of information.

3. Resolving issues that are in the planes of contact between different spheres of activity (criminal procedure, information technology, protection of information with limited access, etc.) is possible only through a dialogue between specialists in these areas, and the proposed solutions should be the result of consensus.

4. Reaching a consensus in solving the problematic issues of the primacy of a material medium in criminal proceedings and ensuring that it acquires other necessary procedural characteristics for the case of such most common media as UFD can be proposed by domestic experts, which is extremely important for ensuring guarantees of independent and objective establishment of the truth.

The protection of primary tangible media is becoming a key element in today's digital world, where cyber threats are constantly evolving. The above strategies and approaches prove to be effective in preventing cyberattacks and ensuring reliable information protection.

Effective security measures include not only responding to current threats, but also proactively considering possible attacks. Analyzing potential risks and improving security measures is an important component to ensure reliable protection of evidentiary information.

Protection should be focused not only on prevention, but also on timely detection of possible threats. Intrusion monitoring and detection systems allow you to quickly respond to events and minimize possible consequences.

The use of modern encryption methods and authentication systems guarantees the confidentiality and authenticity of information. Secure media are becoming an important piece of evidence that can be used in the event of a cyberattack. Preparing for possible incidents and quickly restoring the system is an important part of the protection strategy. Backups and recovery planning help you avoid big losses in the event of a successful cyberattack.

In general, effective protection of primary physical media from cyberattacks requires a combination of technical measures, management strategies and personnel training. This not only helps to ensure the security of information, but also creates the possibility of using this information as evidence in the event of a potential cyberattack.

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] The Law of Ukraine "On operative investigative activity", 2023. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text.

[2] I. Yu. Kailo. Conditions of admissibility of documents in criminal procedural evidence, Law and society 5(2) (2015) 230–237. URL http://www.pravoisuspilstvo.org.ua/archive/2015/5_2_2015/part_1/40.pdf.

[3] A. Slobodzyan, Document as a source of evidence in criminal proceedings, Scientific journal of the National Academy of the Prosecutor's Office of Ukraine 1 (2014) 184–190. URL: http://www.chasopysnapu.gp.gov.ua/chasopys/ua/pdf/1-2014/184-slobodzan.pdf.
[4] Instructions on the organization of undercover investigative (search) actions and the use of their results in criminal proceedings, approved by the order of the Prosecutor General's Office of Ukraine, the Ministry of Internal Affairs of Ukraine, the Security Service of Ukraine, the Administration of the State Border Service of Ukraine, the Ministry of Finance of Ukraine, the Ministry of Justice of Ukraine dated November 16, 2012 No. 114/1042/516/1199/936/1687/5, as of November 16, 2012. URL: http://zakon3.rada.gov.ua/laws/show/v0114900-12.
[5] G. Cascavilla, D. A. Tamburri, W.-J. Van Den Heuvel, Cybercrimethreat intelligence: A systematic multi-vocal literature review, Computers & security 105 (2021) 102258.
[6] G. Edwards, Cybercrimes Investigators Handbook. Hoboken, New Jersey: John Wiley & Sons, Incorporated, 2020.
[7] Information processes. Receiving Information, 2022. URL: http://surl.li/ovjsh.
[8] E. Bern, Introduction to psychiatry and psychoanalysis, Just about complicated, 2022.
[9] Signal, 2023. URL: http://surl.li/ovkcz.
[10] Information, 2023. URL: http://surl.li/otlr.
[11] STUDER A810 Professional Tape Recorder, 2022. URL: http://theaudioarchive.com/TAA_Tape_Studer_A810.htm.
[12] M. A. Al-garadi, K. D. Varathan, S. D. Ravana, Cybercrime detection in online communications: The experimental case of cyberbullying detection in the Twitter network, Computers in human behavior 63 (2016) 433–443.
[13] DSTU 2681-94. The state system of ensuring the unity of measurements. Metrology. Terms and definitions.
[14] Dictionary of the Ukrainian language: in 11 volumes, Kyiv, Naukova dumka, 1970—1980.
[15] Dictionary of foreign words, 2022. URL: http://slovopedia.org.ua/ 36/53412/250161.html.
[16] Recorders, 2022. URL: http://alex-ua.com/dictaphone.
[17] [Information security policy, 2022. URL: http://surl.li/avyop.
[18] TrusCont USB Copy Protection, 2022. URL: https://www.truscont.com/usb-copy-protection/usb-protection.
[19] G. M. Rozorinov, O. V. Bryagin, Patent 98851 Ukraine, IPC GO6F 12/14. The method of protecting information from unauthorized use, Publ. 12.05.2015, Bull. No. 9.
[20] G. M. Rozorinov, O. V. Bryagin, Patent 100204 Ukraine, IPC GO6F 12/14. The method of protecting information from unauthorized use, Publ. 10.07.2015, Bull. No. 13.
[21] G. M. Rozorinov, O. V. Bryagin, Patent 100582 Ukraine, IPC GO6F 12/14. The method of protecting information from unauthorized use, Publ. 27.07.2015, Bull. No. 14.