THE LAW ENFORCEMENT BY THE BODIES OF PRELIMINARY INVESTIGATION AND INQUIRY

DOI 10.52468/2542-1514.2025.9(4).109-118

MODELS OF THE INVESTIGATOR'S USE OF MODERN INFORMATION SOURCES OF ORIENTING AND EVIDENTIARY VALUE**

Dmitry V. Voronkov, Anna M. Sosnovikova
Ural State Law University named after V.F. Yakovlev, Yekaterinburg, Russia

Article info
Received –
2025 January 11
Accepted –
2025 September 20
Available online –
2025 December 20

Keywords
Forensic technology, digitalization of forensics, computer information, expert-analytical system, automated complex, decision support system, SigVer, mobile directory

Subject. The authors reveal the main groups of modern technologies that can be used to improve the effectiveness of investigative activities, to describe the ways of their penetration into forensic practice and to outline the value of information that can be obtained as a result of their application. The relevance of this work is due to the fact that scientific and technological progress affects all spheres of society, including law enforcement, in this regard, special attention today among the professional community deserve the issues of competent implementation of technical achievements in the practice of detection and investigation of crimes.

The purpose of this study was to prove that the introduction of modern technologies only after the prior enshrinement of the possibility of their use in the law, is currently irrational. Such an approach is not conditioned by the existing rules and negatively affects the effectiveness of investigative activities.

The methodology. The authors used the interdisciplinary approach, methods of analogy, analysis and synthesis.

The main results. As a result of the study, four groups of technologies were identified: complexes aimed at automation; decision support systems; means of working with computer information; other technologies that increase the efficiency of traditional processes. In each group, specific technologies that are most in demand in today's practice are described. Based on this, the basic principles that can guide the introduction of new technologies in investigative activities are formulated: the presumption of free determination of technical means for the production of investigative actions; restriction of human rights only by judicial authorization; autonomy of decisions of an official; preservation of the value of information while maintaining its integrity.

Conclusions. According to the results of the conducted research it is concluded that the reliance on the proposed principles, as well as the action by analogy with the considered specific models will allow investigators to successfully determine how to adapt the new technology to solve the problems of detection and investigation of crimes.

** The research was supported by the Russian Science Foundation grant No. 23-78-10011 “Conceptual and applied aspects of developing practice-oriented digital projects of forensic significance” (https://rscf.ru/en/project/23-78-10011/).

1. Introduction

Widespread digitization means that scientist in the field of criminalictics today are researching a fairly broad range of technologies in terms of their possible application to the practice of detecting and investigating crimes [1; 2], however, this requires a qualified response from legislators: legal regulation where necessary, and the introduction of discretionary regulation where possible. It is very important to find a balance between protecting the rights of participants in criminal proceedings through regulatory regulation and preserving the status of the Criminal Procedure Code of the Russian Federation as a law, rather than a reference book or instruction manual [3, p. 42; 4].

The purpose of this work is to comprehensively study some groups of modern technologies, developing optimal models for their implementation in criminalistic practice. To this end, we characterized the main groups of applied or potential technologies; described the legal mechanisms for their implementation; and considered the significance that information obtained through such technologies may acquire.

We used a general scientific dialectical method, logical methods of analysis when considering individual examples of technologies, synthesis when grouping them, and analogy when referring to models according to which already implemented technologies are applied. The work was based on an interdisciplinary approach, which allowed us to combine knowledge from jurisprudence with achievements in computer science.

2. Automation technologies

Today, Russia faces the pressing issue of a shortage of personnel in the law enforcement sector, which, given the persistently high crime rate, places a significant burden on employees, much of which is routine in nature. Modern investigators spend a significant part of their working time on mechanical operations related to the preparation and re-preparation of documents, rather than on obtaining and examining evidence. This problem can be solved by introducing automated systems into the practice of criminal investigation.

To speed up the process of drawing up protocols of investigative actions and court hearings, as well as expert conclusions, it is advisable to use *transcribers* – systems for converting spoken language into text [5, p. 70; 6]. Their use will allow investigators to focus on their own actions and the behavior of other participants, recording everything with a voice recorder or video camera, and then not wasting time and energy retyping what has been recorded into the protocol. As a result, not only will the quality of the investigative action itself improve, but energy will also be conserved for in-depth analytical work.

Today, there are various commercial offers for transcription systems, but they have three significant drawbacks: 1) they are developed by foreign companies; 2) they are distributed on a paid basis; 3) they are aimed at the mass consumer. It is impossible to provide all law enforcement agencies with such systems, and their practical value is limited due to the lack of a built-in dictionary of special legal terms, without which the final text would require significant editing. Even machine learning methods are not entirely capable of recognizing legal speech, which can be enriched with highly specialized vocabulary. We believe that it is necessary to form a state order for the creation of a domestic transcriber that will include special terms. Even this single step will significantly reduce the volume of routine work.

Focusing on the issue of legal regulation and the significance of the information obtained, we emphasize that the systems described do not create new information; their use is purely instrumental (like computers used to prepare protocols instead of pen and paper), and therefore it is unnecessary to link their implementation to prior regulatory approval. The same applies to the content of the information obtained: the text transcribed and verified by an authorized person (investigator, expert, judge) is no different from a regular protocol (conclusion) and therefore has the same significance as such acts.

The next aspect is indirectly related to automation issues and concerns the problem of parallel document flow, when all procedural acts, accounting materials, etc. must be kept simultaneously in paper and electronic forms. The position of scholars considering the prospects of a complete transition to *electronic criminal cases* deserves attention [7–9].

The ongoing duplication of information, including information that exists only within the

system of state bodies, seems excessive. Of course, there are still regions in Russia that lag behind global digitalization processes, as well as individuals who are unfamiliar with such technologies, however, we do not propose to completely exclude paper and copying machines from the list of mandatory workplace components: by transferring all document flow in criminal cases to electronic format, it is possible to retain the option of creating paper copies of materials equivalent to digital ones in exceptional cases.

Here, the specifics of the information are no different from the traditional ones existing in criminal proceedings, and all materials stored on electronic media acquire the same significance that paper documents have today. However, the issue of legal regulation is more complicated. At the end of 2023, Article 474.2 of the Criminal Procedure Code of the Russian Federation came into force, which allows the circulation of procedural documents in electronic form, but it refers to copies of such acts, from which it follows that the documents are still initially produced on paper. In addition, the provisions of Articles 166, 189.1, etc. of the Criminal Procedure Code of the Russian Federation continue to apply, which explicitly indicate the need to sign (which follows from the context – handwritten) protocols and other procedural documents. In other words, there is currently no legal possibility for a full transition to electronic document management, although there are no technical obstacles – if necessary, other participants in the criminal process, apart from the investigator, can send a request through the GosKlyuch system to certify the accuracy of the document. We believe that the legislator's overly cautious position is unjustified and that it is necessary to intensify the transition to electronic document management, eliminating the duplication of all acts.

The next task that can be automated is the analysis of large amounts of information. In this area, *video cameras with automatic recording of offences* and built-in image recognition functions have already become quite widespread [10]. They make it possible to search for stolen cars, locate wanted persons, identify individuals committing offenses, etc.

Despite the lack of a specific provision for their use in criminal proceedings, it has been noted that the use of video surveillance cameras, including those with automatic image recognition systems, significantly increases the effectiveness of crime detection and investigation [11]. In other words, practice recognizes the admissibility of using these technical means without their direct regulation in special acts. However, an ambiguous situation arises when determining the significance of the information obtained. On the one hand, photo and video recordings themselves may have evidentiary value, as they are included in the group of other documents. Thus, if a video camera captured a criminally punishable traffic accident, this recording may form the basis for the driver's indictment; or a camera recording of a person being in a certain place at a certain time may serve as evidence of their alibi. However, the practical situations described above contradict Part 1, 2 of Article 16 of Federal Law No. 152-FZ of July 27, 2006, «On Personal Data», which establishes a general rule prohibiting the adoption of legally significant decisions based solely on the automated processing of personal data and introduces an exception in the form of direct regulation of the opposite in a special law. While the question of whether a vehicle registration number constitutes personal data is highly ambiguous, an image of a person legally has the status of biometric personal data. In this regard, it should be concluded that the direct use of evidence obtained from a video surveillance camera equipped with computer vision technology is inadmissible until such a possibility is expressly stipulated in the Criminal Procedure Code of the Russian Federation.

Another aspect of automation is related to the functional capabilities of office suites included in the basic software package. For example, when working with text files, the process of finding data of interest to the investigation can be accelerated by searching for keywords. These functions are implemented in various *expert systems* in a slightly more complex manner. In the first case, no separate sanctions for the use of automation systems by the state or the head of a law enforcement agency are required, nor are there any questions regarding the role of the information obtained, since these systems are ordinary technical means that act in the same way as a magnifying glass, which simplifies the detection of certain objects. No new information appears; the

investigator works with the information already at his disposal.

The situation is somewhat more complicated with expert systems, which should be considered in the next group of technologies.

3. Decision support systems

The essence of all components in this group boils down to analyzing a specific data set to provide an answer to a specific question posed by the user, which will form the basis for a human decision, including a legally significant one.

Thus, *automated expert analytical systems* not only facilitate the analysis of large amounts of information, but are also capable of taking on individual expert tasks (determining whether two signatures were made by one or different persons [12, pp. 70–72], identifying the make and model of the weapon from which a shot was fired).

The widespread use of such systems carries the risk of discrediting forensic activities, since the investigation is actually carried out not by an expert, but by a machine system. From the perspective of current criminal law, this is unacceptable, since all such automated systems, functioning on the basis of artificial intelligence technology, are characterized by the «black box» phenomenon [13], which does not allow the entire process to be traced, and therefore makes it impossible to reproduce the examination procedure step by step in order to verify the final conclusion.

Thus, the use of expert analytical systems should be limited based on the following principles:

1) The preservation in expert practice of «non-intelligent» automated systems, whose decision-making process is obvious and reproducible in manual mode, as well as semi-automated systems, where the algorithm only performs preliminary processing of raw data. For example, in the «Author» system developed by A. Yu. Komissarov, the frequency of occurrence of certain linguistic categories in the texts presented is established, after which the data obtained is subjected to statistical analysis, based on the results of which the expert independently decides whether both texts were written by the same person [14, pp. 167–172].

2) Limit the scope of application of analytical complexes to pre-expert verification. In this case, decision support systems are aimed at people who do not have special knowledge and help determine the advisability of appointing a specialized expert examination. This is precisely the approach implemented in the SigVer system for verifying forged handwritten signatures. It is expected that an investigator who suspects that a document is not authentic will upload images of a verified original and disputed signatures into the program, which will determine the probability that the disputed signature is forged. If the quantitative indicators of this probability are high enough, the investigator will order a handwriting analysis; otherwise, they will be able to accept the document as authentic.

3) Design the interface of automated systems in such a way that their output minimally restricts human freedom in decision-making. The systems in question should advise, but not replace, human decision-making. For the SigVer system mentioned above, it has been experimentally established that the greatest independence of the user's decision is achieved when the result of the program's work is presented in the form of a gradient color scale, where bright green means that the disputed signature is reliably authentic, and bright red means that it is reliably fake [15, pp. 47–48].

In summary, we emphasize that the results of automated decision support systems should only be used as a guide, as another source of information from which the authorized person draws their own conclusions. At the same time, if such systems are introduced into expert practice, they must be enshrined in the relevant certified methodological recommendations, whereas, in our opinion, their use by other entities does not require any authorization.

4. Electronic information processing technologies

The rapid pace of universal digitalization is leading to constant growth, including increased internal diversity, in the group of technologies designed to work with information stored in electronic form [16].

It is necessary to consider various software and *hardware modules designed to access this type of information* (Mobile Criminalist, Celebrite UFED, etc.). They are often used by criminal investigators or other specialists invited to seize electronic media as part of investigative activities, or by experts in the process of

forensic examination. In this regard, it is necessary that these systems be certified, comply with all technical regulations and quality standards, and be developed in Russia on domestic platforms. At the same time, there is no need for any special rules that would directly establish the right of an authorized entity to use a particular technical means from this category, just as the Criminal Procedure Code of the Russian Federation does not contain rules on what tools an investigator may use if necessary to open a safe during a search.

In terms of determining the significance of the information obtained, we emphasize that, provided all the rules for working with electronic media are followed, there is no distortion or other modification of the data, and the procedural role of the data that was inherent to it from the outset is preserved. It is important to note that the information obtained will only be meaningful if no errors have been made that could lead to the modification or loss of information. However, investigators today generally do not have sufficient expertise in this area and must seek the help of specialists or experts.

After gaining access to the information stored on the electronic medium, the task is to detect, seize, and examine criminally significant materials. In some cases, the investigator can do this himself during the inspection, but this only allows for the processing of explicit information and does not require the use of specific technological solutions. A more in-depth study of objects, allowing the detection of encrypted information, hidden communication channels, system logs, etc., is located in the sphere of separate subtypes of computer-technical expertise.

The study of computer information can also be carried out by the investigator to solve other tasks not related to the seized electronic media. As already mentioned, digitalization has become widespread. One of the consequences of this has been the aggregation of large amounts of various information about individuals on the Internet. A significant amount of this information is posted by users themselves on their own initiative, while some of it becomes publicly available as a result of unintentional human actions or illegal breaches of the confidentiality of various electronic databases.

All this information can be obtained using specialized *OSINT* software services through dorks (optimized search engine queries), bots in messengers, or independent software (the latter is more common for Linux-based operating systems). This area has attracted considerable attention from criminalists in recent years [17–20], and its admissibility is assessed ambiguously. However, it seems that in this case there is no reason to talk about a violation of citizens' rights to personal and family privacy, since all the information that can be accessed by a criminal investigator is already in the public domain, and the aforementioned and many other specialized services are only focused on its detection and systematization.

However, in modern conditions, information obtained through OSINT must be approached with caution, since deepfakes – distorted photos, video images, and audio recordings of real people's voices – are becoming widespread. Various organizations and research teams are creating deepfake recognition systems [21], but their use is currently only possible in the context of expert research. There is a risk that investigators will discover false information that will influence their decisions. In any case, information collected through OSINT, even if this technology does not require special regulatory approval, can only be used as a guide and, for example, to study the personality of the person being questioned as part of preliminary preparation for investigative actions.

5. Other technologies

Firstly, **drones** (unmanned aerial vehicles) deserve attention, as they allow for the photographing of extended (e.g., corpses) and large-scale (e.g., motor vehicle or railway accident sites) objects without distortion and without the need for large-scale lifting equipment. They can be used to inspect and record crime scenes where it is unsafe for humans to be present (fire sites, explosion sites), as well as directly dangerous objects. At the same time, drones are just modified photo and video cameras, so there is no need to separately establish their applicability in the practice of solving and investigating crimes, and the information obtained can have evidentiary value when attached to the protocol in the form of an illustrative table.

Secondly, continuing the theme of photographic recording, *stereo cameras with a 360°*

coverage function have significant potential [22, p. 34]. Such devices can be installed in the center of the site of the upcoming investigative action, as well as in the projection of this point above the ground (using a drone or fixed to the ceiling), thereby capturing in a single frame the entire space that potentially contains criminally significant information. Subsequent examination of such photographs increases the chance of discovering important details that may have been overlooked during fieldwork, which, on the one hand, can minimize the negative consequences of investigative errors and, on the other hand, provide greater clarity of the situation for other participants in the criminal process (mainly the court). The legal regime for the use of such cameras and the significance of the images obtained are similar to those of drones.

Finally, the last technology that we would like to focus on in this study is based on the fact that almost everyone has a smartphone. The use of mobile reference systems is very useful in terms of improving the effectiveness of investigative activities. The authors of this work have created a mobile application called «CrimLib – Investigator's Reference book», which contains brief criminalistic and forensic recommendations and algorithms for examining and describing various objects; organizing investigations; appointing experts; interrogating suspects on various criminal charges; etc. This reference book and similar projects [23] can be used by novice investigators to minimize errors in their work. At the same time, mobile phones are now ubiquitous, do not take up much space, and are lightweight, while electronic services support regular updates by qualified industry representatives. This gives mobile reference guides an advantage over paper books or Internet resources.

6. Conclusion

Of course, our review is far from exhaustive in terms of the new technological tools that can assist investigators, but based on the above, we can formulate general principles for the use of modern sources of evidence and guidance in criminal investigation.

1) Guided by their own sense of justice, investigators should be guided by the provisions of Part 6 of Article 164 of the Criminal Procedure Code of the Russian Federation, which establishes their right to freely use technical means in the course of investigative actions, notifying other participants of this and reflecting this fact in the protocol.

2) If the use of any technology may restrict the legal rights and freedoms of a person, but the investigative action does not imply such a possibility (is carried out without court approval), then the use of the specified technology is unacceptable.

3) All decisions of the investigator, especially those of legal significance, must be independent in nature; their replacement by the results of an information system is unacceptable.

4) If the use of technology does not lead to the modernization, distortion, or other essential transformation of the original information, then its significance in the process of proving should not change; otherwise, its use is permissible only as a guide.

At the same time, for each technology in different investigative situations, a unique assessment of the possibility of its use, the limits and significance of such use must be made. Science can only prepare recommendations that will never take into account the full diversity of life situations. However, relying on the examples considered and acting by analogy can significantly help individual investigators in adapting to the processes of digitalization.

ISSN 2658-4050 (Online)

REFERENCES

1. Kruger E., Porter G., Birch P., Bizo L., Kennedy M. The dimensions of “forensic biosecurity” in genetic and facial contexts. *Security Journal*, 2024, vol. 37, iss. 4, pp. 1746–1768. DOI: 10.1057/s41284-024-00445-1.

2. Harshith P., Ramakrishnan P. Exploring the Potential of Augmented Reality for Forensic Crime Scene Reconstruction: A Review. *International Journal Of Trendy Research In Engineering And Technology*, 2023, vol. 7, iss. 3, pp. 28–34. DOI: 10.54473/IJTRET.2023.7305.

3. Rossinskiy S.B. Criminal Procedure Code of the Russian Federation: the embodiment of the “high” purpose of the criminal procedural form or a “memo” for illiterate law enforcers. *Zakony Rossii: opyt, analiz, praktika*, 2021, no. 6, pp. 42–46. (In Russ.).

4. Pobedkin A.V. Criminal procedural code: a form of live law or a “soul-less” instruction. *Biblioteka kriminalista = Criminalist's Library*, 2017, no. 3 (32), pp. 101–111. (In Russ.).

5. Sotnikov K.I. On the possibilities of introducing transcription into the practice of interrogation at the stage of preliminary investigation of crimes. *Yuridicheskie issledovaniya = Legal Studies*, 2023, no. 11, pp. 66–75. DOI: 10.25136/2409-7136.2023.11.68738. (In Russ.).

6. Vakhmyanina N.B., Ivanov E.A. Possibility to Use of Transcription Software in Investigative Activities. *Rossiiskii sledovatel’ = Russian Investigator*, 2019, no. 2, pp. 6–9. (In Russ.).

7. Zuev S.V. Information-Technological Process of Criminal Proceedings: A Matter of Time, in: *Tekhnologii XXI veka v yurisprudentsii*, Proceedings of the Sixth All-Russian Scientific and Practical Conference (Yekaterinburg, May 24, 2024), Yekaterinburg, 2024, pp. 77–82. (In Russ.).

8. Singarimbun D.A., Pakpahan K. Implementation of the Electronic Criminal Case File Transfer System. *YURISDIKSI: Jurnal Wacana Hukum dan Sains*, 2024, vol. 20, no. 1, pp. 58–65. DOI: 10.55173/yurisdiksi.v20i1.229.

9. Qin H., Chen L., Mou L. The development of China’s electronic case file regulations and its future implications. *Computer Law & Security Review*, 2024, vol. 52, art. 105930. DOI: 10.1016/j.clsr.2023.105930.

10. Shyam R., Singh Y. Automatic Face Recognition in Digital World. *Advances in Computer Science and Information Technology*, 2022, vol. 2, no. 1, pp. 64–70.

11. Tsurluy O.Yu. Synchronization of the Criminalistic Science, Law Enforcement, Laws And Technologies: A Required And Inevitable Process. *Rossiiskii sledovatel' = Russian Investigator*, 2024, no. 4, pp. 24–28. DOI: 10.18572/1812-3783-2024-4-24-28. (In Russ.).

12. Bakhteev D.V. Computer Vision and Pattern Recognition in Forensic Science. *Rossiiskoe pravo: obrazovanie, praktika, nauka = Russian Law: Education, Practice, Researches*, 2019, no. 3 (111), pp. 66–74. DOI: 10.34076/2410-2709-2019-3-66-74. (In Russ.).

13. Suman R.R., Mall R., Sukumaran S., Satpathy M. Extracting State Models for Black-Box Software Components. *Journal of Object Technology*, 2010, vol. 9, no. 3, pp. 79–103. DOI: 10.5381/jot.2010.9.3.a3.

14. Komissarov A.Yu. *Forensic Examination of Written Speech Using a Computer*, Doct. Diss. Moscow, 2001. 225 p. (In Russ.).

15. Bakhteev D.V., Tsvetkova A.D. Interface in Intelligent Decision Support System as a Decision-Making Factor on Example of Signature Verification Project, in: *Tekhnologii XXI veka v yurisprudentsii*, Proceedings of the Fifth International scientific and practical conference (Yekaterinburg, May 19, 2023), Yekaterinburg, KrimLib Criminology Development Assistance Center Publ., 2023, pp. 43–50. (In Russ.).

16. Zaichenko K.S. Digitalization of Economies And Society: Global Trends. *Aktual'ni problemi ekonomiki = Actual Problems of Economics*, 2023, no. 9 (267), pp. 21–30. DOI: 10.32752/1993-6788-2023-1-267-21-30. (In Ukrainian).

17. Bessonov A.A. The Use of Information From Open Sources of Information (OSINT) in the Disclosure of Crimes, in: *Aktual'nye voprosy teorii i praktiki operativno-razysknoi deyatel'nosti*, Collection of scientific papers of the Interdepartmental scientific and practical conference (Moscow, Semtember 16, 2022), Moscow, Kikot Moscow University of the Ministry of the Interior of Russia Publ., 2022, pp. 40–45. (In Russ.).

18. Ivanov V.Yu. Using OSINT in Detecting and Investigating Crimes. *Vestnik Ural'skogo yuridicheskogo instituta MVD Rossii = Bulletin of the Ural Law Institute of the Ministry of the of the Interior of the Russian Federation*, 2023, no. 1 (37), pp. 62–66. (In Russ.).

19. Yangaeva M.O., Pavlenko N.O. OSINT. Obtaining Forensic Significant Information From the Internet. *Altaiskii yuridicheskii vestnik = Altai Law Journal*, 2022, no. 2 (38), pp. 131–135. (In Russ.).

20. Yadav A., Kumar A., Singh V. Open-source intelligence: a comprehensive review of the current state, appli-

cations and future perspectives in cyber security. *Artificial Intelligence Review*, 2023, vol. 56, no. 11, pp. 12407–12438. DOI: 10.1007/s10462-023-10454-y.

21. Bodrov N.F., Lebedeva A.K. Deepfakes as an Object of Forensic Examination, in: *Natsional'nye i mezhdunarodnye tendentsii i perspektivy razvitiya sudebnoi ekspertizy*, Collection of reports of the Scientific and Practical Conference with international participation (Nizhny Novgorod, May 22–23, 2024), Nizhny Novgorod, Lobachevsky State University of Nizhny Novgorod Publ., 2024, pp. 42–50. (In Russ.).

22. Arsenteva S.S., Morozov S.A. Using the Spherical Fixation Method of the Place of Incident. *Vestnik Chelyabinskogo gosudarstvennogo universiteta. Seriya: Pravo = Bulletin of Chelyabinsk State University. Series: Law*, 2019, vol. 4, iss. 2, pp. 33–36. DOI: 10.24411/2618-8236-2019-14204. (In Russ.).

23. Khuzhaev A.T., Vasil'ev A.I. Mobile Application «Directory of The Investigator of The Ministry of Emergency Situations», in: *Aktual'nye problemy obespecheniya bezopasnosti v Rossiiskoi Federatsii*, Collection of materials from the Days of Science with international participation, dedicated to the 90th anniversary of the Civil Defense of Russia (Yekaterinburg, May 30, 2022), in 2 parts, Yekaterinburg, UISFS of EMERCOM of Russia Publ., 2022, pt. 1, pp. 204–
209. (In Russ.).

INFORMATION ABOUT AUTHORS

Dmitry V. Voronkov – Doctor of Law, Associate Professor; Head, Department of Criminalistics named after I.F. Gerasimov; Head, Laboratory of Digital Technologies in Criminalistics
Ural State Law University named after V.F. Yakovlev
21, Komsomol'skaya ul., Yekaterinburg, 620066, Russia
E-mail: ae@crimlib.info
ORCID: 0000-0002-0869-601X
RSCI SPIN-code: 8301-7165

Anna M. Sosnovikova – Junior researcher, Digital Technologies in Criminalistics
Ural State Law University named after V.F. Yakovlev
21, Komsomol'skaya ul., Yekaterinburg, 620066, Russia
E-mail: at@crimlib.info
ORCID: 0000-0002-1631-9265
RSCI SPIN-code: 7460-5805

BIBLIOGRAPHIC DESCRIPTION

Voronkov D.V., Sosnovikova A.M. Models of the investigator's use of modern information sources of orienting and evidentiary value. *Pravoprimenenie = Law Enforcement Review*, 2025, vol. 9, no. 4, pp. 109–118. DOI: 10.52468/2542-1514.2025.9(4). 109-118. (In Russ.).