Original article
UDC 343.9
doi 10.46741/2686-9764.2026.73.1.006

Information System in the Arsenal of Investigative (Search) Activities of Subjects of Disclosure and Investigation of Crimes of Previous Years: Objects, Means, Techniques, Technologies (Based on Foreign Publications)

NIKOLAI G. SHURUKHNOV
Research Institute of the Federal Penitentiary Service of Russia, Moscow, Russia,
Tula Institute (branch) of the All-Russian State University of Justice (RLA of the Ministry of Justice of Russia), Tula, Russia
matros49@mail.ru, https://orcid.org/0000-0003-1132-760X

Abstract

Introduction: the article considers situations of suspension of the preliminary investigation provided for by criminal procedure legislation, an information search system on the Internet, open sources in the disclosure and investigation of crimes of previous years. The levels of the Internet (visible network, deep network, darknet), objects, tools, tactics, methods, technologies for searching, collecting and analyzing information from publicly available resources are analyzed using OSINT (Open Source Intelligence) – intelligence based on legal sources. *Purpose*: to analyze the capabilities of the OSINT information system in investigative activities. *Methods*: system analysis, classification, and technology description. *Results*: the essence of active and passive data collection is revealed, their differences are shown, the main principle is to use open sources without restrictions, with mandatory compliance with the provisions of laws on personal data and copyrights. The content of the search, processing, analysis, and dissemination of the information received for the purpose of disclosing illegal acts committed in the past is analyzed. Special attention is focused on the complex of OSINT methods and techniques and search tactics. Attention is drawn to the requirements for tactical techniques aimed at ensuring the secrecy of designated activities that contribute to the search for the suspect, the accused. *Conclusions:* the article contributes to the development of criminalistic methods and tactics of investigative activities, adapting OSINT's foreign experience to Russian realities. The materials can be used by investigators, operatives, and analysts in solving cold cases, as well as in the educational process of law schools.

Keywords: crimes of the past; investigative activities; information; open sources of intelligence; search; techniques.

5.1.4. Criminal law sciences.

For citation: Shurukhnov N.G. Information system in the arsenal of investigative (search) activities of subjects of disclosure and investigation of crimes of previous years: objects, means, techniques, technologies (based on foreign publications). *Penitentiary Science*, 2026, vol. 20, no. 1 (73), pp. 46–53. doi 10.46741/2686-9764.2026.73.1.006.

Introduction

Considering investigative activity of an investigator, we mean two investigative situations: when an investigation is underway and when the preliminary investigation is suspended in accordance with the provisions of Article 208 of the Criminal Procedure Code of the Russian Federation. They differ in the form of criminal procedure [1; 2], means, powers, rights and obligations of subjects participating in pre-trial proceedings.

The main content of the first investigative situation is based on evidence indicating the existence of a crime, but there is no factual information about the perpetrator, and it is not possible to obtain such information at this time interval. Due to this circumstance, the crime remains unsolved. During the preliminary investigation (before its suspension), the investigator performs search actions aimed at establishing location of the accused or suspected by implementing all possible procedural actions (including investigative ones). If, at the same time, the location of the accused or suspected is unknown, he/she instructs investigative bodies in a separate resolution to carry out a search (Part 1 of Article 210 of the Criminal Procedure Code of the Russian Federation). The law establishes a rule under which "the search for the suspected or accused may be announced both during the preliminary investigation and simultaneously with its suspension" (Part 2 of Article 210 of the Criminal Procedure Code of the Russian Federation) [3, pp. 598-606; 4; 5].

The investigator's decision to declare a search for the accused before making a decision to suspend the preliminary investigation makes it possible to effectively use the combination of the investigator's procedural capabilities to establish the location of the accused with law enforcement intelligence aimed at finding him. The mutual exchange of information obtained during the course of investigative actions and information obtained during the production of public and secret operational search activities allows the subjects of interaction to choose the most optimal option for further search actions.

It should be said that the investigative (search) activity of an investigator is meaningful, or at least it should be, with a range of various means, primarily investigative actions, with a search focus – various types of inspections, interrogations, monitoring and recording of negotiations, obtaining information about subscriber connections and (or) subscriber devices [6, pp. 521–535; 7]. A set of organizational, operational, investigative, and administrative measures to carry out the search is carried out by authorized officials of the bodies of inquiry to whom the resolution is addressed.

In case the implementation of the measures taken has not yielded a positive result and at the time of the expiration of the preliminary investigation period all possible investigative actions have been carried out in the absence of the suspected or the accused, the preliminary investigation is suspended, and the investigator issues a resolution, a copy of which is sent to the prosecutor (Part 2 of Article 208 of the Criminal Procedure Code of the Russian Federation).

The second investigative situation is specific: the preliminary investigation has been suspended, no investigative actions are being carried out, however, there is enough evidence to bring an accusation against a certain person, but the investigator does not know where he/she is. If we consider private investigative situations, the first of them is related to the fact that the suspected or the accused committed intentional acts and hid from the investigation. This is also stated by the legislator in Paragraph 2 of Part 1 of Article 208 of the Criminal Procedure Code of the Russian Federation. The content of the second private investigative situation is due to a lack of information about the location of the subject due to the fact that it has not been established for other reasons. The legislator fixes in Paragraph 2 of Part 1 of Article 208 of the Criminal Procedure Code of the Russian Federation the following: "his/her location has not been established for other reasons". If the location of the accused (the suspected) has not been established for other reasons, the investigator takes measures to find him/her (Paragraph 2 of Part 1 of Article 208, Paragraph 2 of Part 2 of Article 209 of the Criminal Procedure Code of the Russian Federation).

The indicated reason for suspending the preliminary investigation is difficult to understand in theory and practice. If we proceed from general approaches, then, apparently, we are talking about reasonable doubts about the

permissibility of its deliberate evasion. With this approach, the rule of interpretation of doubts in favor of the accused is applied (Part 3 of Article 14 of the Criminal Procedure Code of the Russian Federation). But if we cite specific cases, then it cannot be ruled out that a citizen does not have the opportunity to return from another state, stay abroad, in a particular state, but if the investigator does not have a specific address, the subject of the investigation is waiting for an important response to an international request.

In these situations, the subject of the investigation issues a resolution, a copy of which is sent to the prosecutor (Part 2 of Article 208 of the Criminal Procedure Code of the Russian Federation). During this period, the investigator performs a set of duties that are defined in parts 3–8 of Article 208 of the Criminal Procedure Code of the Russian Federation. It also assigns the search to the bodies of inquiry (in accordance with the regulations of the Ministry of Internal Affairs of Russia, it carries out local, federal, interstate (CIS), and international searches). This is indicated in the decision to suspend the preliminary investigation or in a separate decision.

If the term of the preliminary investigation in a case expires, but there is a need to carry out a number of investigative actions aimed both at establishing the location of the accused and clarifying the circumstances of the crime committed, the investigator must issue a resolution to initiate a motion to extend the period of the preliminary investigation.

In accordance with Part 5 of Article 208 of the Criminal Procedure Code of the Russian Federation, the investigator continues to take necessary measures to establish the location of the fugitive accused even after the search is announced. He can receive information from people who keep in touch with the accused, are aware of his probable location, finds out the funds he lives on outside the house, and also determines whether he intends to receive a salary at his place of work, other remuneration, whether he has deposits in banks, who from his entourage owes him money and who from relatives, acquaintances provides financial assistance.

Using the information obtained about people living in other regions who may know something about the whereabouts of the fugitive accused, the investigator sends instructions to receive explanations from them.

If the investigator comes to the conclusion that the investigation needs to be suspended, he must consider the following:

– the presence of evidence in the case indicating the commission of a crime and the guilt of the fugitive suspect or accused, whose location has not been established for other reasons;

– carrying out all investigative actions, the production of which is possible in the absence of the accused;

– resolving the issue of the fate of other defendants in the case, if the crime was committed in complicity. In this case, it is important to remember that if two or more defendants are involved in a criminal case, and the grounds for suspension do not apply to all defendants, then by virtue of Part 3 of Article 208 of the Criminal Procedure Code of the Russian Federation, the investigator is entitled to separate and suspend the criminal case against individual defendants;

– resolving a set of issues related to seized property, the possibility of changing restrictions on the possession, use and disposal of property (Part 6 of Article 208 of the Criminal Procedure Code of the Russian Federation), the application of a procedural coercion measure in the form of seizure of property of persons legally responsible for the actions of the suspected and the accused (Part 7 of Article 208 of the Criminal Procedure Code of the Russian Federation); making a decision on the implementation of security measures or on full or partial cancellation (Part 8 of Article 208 of the Criminal Procedure Code of the Russian Federation);

– ensuring the safety of documents and physical evidence in the case.

In accordance with the departmental regulations of the Ministry of Internal Affairs of Russia, the decree for adjudgement of specified accused person into the Russian wanted list must contain a certificate indicating the following information:

– an identity of the suspected, the accused (with a note of the fact of changing a surname, first name (if any)); details of the document on the basis of which his/her identity was established;

– evidence confirming the fact that the suspected or the accused absconded from the investigation;

– about the persons with whom the wanted person may be hiding, the regions where he/she is most likely to be located;

– arrest of the fugitive in the case of a preventive measure not related to detention;

– persons in respect of whom orders have been issued to seize correspondence and seize it from postal and telegraphic institutions;

– a phone number that was in the personal use of the subject of the search, phone numbers that were contacted (most often) with subscribers, an email address, a name of the school (educational organization) that he/she graduated from (for searching on social networks).

Once again, we note that the investigator carries out procedural, organizational, and search activities for the search for a fugitive suspect or accused without conducting investigative actions.

Research

The information revolution in Russian society has led to the use of computer technologies by the majority of citizens. Statistics show that of the 144.2 million people living in the Russian Federation, 130.4 million actively use the Internet, with network penetration reaching 90.4%. In 2024, Russian users spent 8 hours and 21 minutes per day on the Internet. At the beginning of 2024, 219.8 million mobile subscriber connections were registered in Russia. Considering that one person can use multiple devices, the percentage of mobile connections was 152.5 [8].

The presence of a significant amount of computer equipment among citizens, the use of information technology in everyday life could not but affect the level of their use in the commission and concealment of crimes. In 2024, according to the Ministry of Internal Affairs of Russia, 765 365 crimes (369 267 – serious and especially serious) were registered, committed using information and telecommunication technologies or in the field of computer information, of which 571 369 crimes remained unsolved. In total, 1 911 300 crimes were registered in Russia in 2024 [9, pp. 2, 30-31].

Based on this, when uncovering and investigating illegal acts, it becomes important to search for computer equipment, software, and information on the Internet in order to find a fugitive suspect or accused.

The Internet is an archive of various information (for storage and transmission, without subject catalogues); it is compared to an iceberg. It is believed that what we use on a daily basis is a visible network, a small part that protrudes above the “surface of the water”. But there is a deep network under the “water”, a hidden part of the Internet where you can communicate anonymously and share files. According to this, the Internet is divided into several levels:

1. Visible network – sites that appear in the results of a regular search. This level is accessible to every user and is fully indexed.

2. Deep web is a huge archive where databases, email accounts, subscription services, and confidential information are stored. It is no longer visible and is not indexed by conventional search engines. It may include certain categories.

3. Darknet (dark web) is a hidden part of the Internet that is inaccessible through conventional search engines. Web pages are not indexed in it, and they can only be opened using special programs. The darknet has its own domains and encryption algorithms that hide not only contents of the sites, but also connection routes. This makes it more difficult to track users and website developers [10, p. 38]. Anonymity comes first here, so special programs are used for anonymized access. The darknet can be a source of concentration of information about illegal activities, the receipt of which implies the need for caution, ethical and legal norms, in particular the federal law “On personal data”. There is a lot of publicly available information in it, which is indexed by search engines. This is a source of data for the disclosure and investigation of crimes of previous years, the identification of persons involved in the illegal act, and the identification of their location.

The information system for obtaining the data of interest is OSINT (Open Source Intelligence), a system for collecting and analyzing information from publicly available resources on the Internet [12]. The starting point of the search using this system is a visible, legal network. It is about the process of collecting, evaluating, interpreting, and systematizing publicly available information.

One of the leading principles of OSINT is to obtain data only from open, accessible sources, excluding hacking, unauthorized access or

other illegal actions. An OSINT analyst (specialist) works only with what anyone can find.

The search allows you to find information and get answers to specific questions about the circumstances of the crime, the fugitive's stay in a certain territory, place of work and residence, marital status, correspondence with certain addressees, acquisition of movable and immovable property, training, advanced training in an educational organization, violation of traffic safety rules, payment of fines.

It should be said that the ability to extract information from individual sources on the Internet is highly appreciated by experts working in the digital field. It is necessary to develop this direction to identify not only locations of fugitive criminals, but also to obtain information about the committed crime in the past.

As already mentioned, the OSINT system includes open source information search, processing, analysis, and grouping to make specific decisions. These include typical open sources, such as social networks and blogs; forums and comments; public registries and databases (for example, the Unified State Register of Legal Entities, Cadastre); news sites; satellite images (Google Earth, Sentinel); domain records (Whois); data leaks published in the public domain; publications and reports; video hosting and photo stocks; and search engine data.

The search involves studying and collecting information from various sources, including social networks, trade (commercial) databases, traffic police data, and FSSP. This can be done manually or using automated tools, which include:

– Shodan-search for Internet-connected devices (cameras, routers, servers);

- Snoop-search for accounts by nickname;

– SpiderFoot– automated data collection from social networks, DNS, leaks;

– Maryam– search for information by email addresses, domains, IP;

– Alfred – analysis of links between accounts in social networks.

The OSINT advantage is that it can see connections between disparate open data.

Data processing involves the exclusion of inaccurate, incorrect, irrelevant to the subject of the search, or duplicated information. It is necessary to systematize the information received in terms of its relevance to a specific fact of interest, leading to circumstances of the crime committed in the past (the illegal act committed, the time of disappearance from the field of view of authorized officials of the investigating authorities of a particular citizen).

The analysis consists in identifying patterns that reveal the attribution of certain facts to the crime commission in the past, revealing their interrelationships, correlations between established events. Special tools for visualization and data mining, as well as language information processing, can help in this work.

In accordance with the order of the Investigative Committee of Russia No. 65 of July 31, 2014 "On organizing work to investigate criminal cases of crimes of previous years", analytical groups have been established in the central office of the Investigative Committee, the main investigative directorates and investigative directorates of the Investigative Committee for the subjects of the Russian Federation and specialized (including military) investigative departments and investigative departments equivalent to them to solve crimes of the past years. Transmitting the information received involves not only reporting to the deputy head of the investigative body of the Investigative Committee, who heads the analytical group for investigating criminal cases of crimes of previous years, but also communicating with colleagues, at its best directly with the investigator who investigated the specific crime, the preliminary investigation of which was suspended, as well as with members of the analytical group responsible for organizing the disclosure and investigation of crimes committed in the past. Joint efforts of experienced investigators and operational representatives guided by heads of the relevant investigative bodies can result in informed decision-making and preparation and implementation of notifications, guidelines, and assignments for conducting further law enforcement intelligence operations.

The OSINT objects and tools are the following:

– social networks and other platforms for online communication. It is possible to obtain or eventually track information about people's lives, their interests, plans, past lives, committed deeds, and sometimes identify illegal intentions of the search subjects;

– legal documents, such as contracts for employment and dismissal from work, acquisi-

tion, hiring of residential and industrial premises, purchase of housing, court decisions, documents of companies managing housing stock, special organizations for its provision;

– mass media, such as pages or columns of newspapers, magazines, news sites, advertisements.

Automatic collection of information through specialized programs (web scraping) helps quickly and systematically extract amounts of data. Search engines with advanced search provide more accurate results. When working with huge amounts of information, one requires tools for analyzing data (Excel, Tableau and R, etc.). They help filter out unnecessary information, establish patterns and relationships.

Before starting the search and collection of information, one needs to define a goal and forecast the desired results. This will help focus on the main thing and simplify the work. The study should be divided into logical stages, covering certain areas. When collecting information, as already mentioned, one should refer to various sources, such as search engines, social networks, and legal documents.

It is advisable to check the data obtained using several possible sources, which will increase the accuracy of results and reduce risks of obtaining false information. This is facilitated by targeted search queries. Operators, filters, and advanced search engine features will help reduce the amount of data and get more relevant results. One should study metadata of images, documents, and other files. Metadata present structured information embedded in a file that describes its properties and usage context. They are created automatically by programs or devices involved in the formation of the file, but can also be added manually. This information consists of attributes that can be divided into several categories: technical parameters (file size, type, format, resolution, codec); descriptive characteristics (name, keywords, description); administrative information (author, copyright holder, creation date, software version); geospatial attributes (GPS coordinates). Analyzing them, you can find valuable information, such as location, time indication, information about the author, and device features.

Social media profiles, online forums, blog posts, and publicly available documents can provide a comprehensive view of an object, provided a person can find digital footprints. One should record findings in detail, including timestamps, access mode, screenshots, and notes. Such systematization will increase the efficiency of the analysis and help find the stored information.

It should be noted that information collection can be passive and active.

When the search is passive, one views publicly available information and does not comment it or write personal messages. Active data collection involves direct interaction to obtain certain data. For this purpose, acquaintance is carried out on social networks, questions are asked, and chat is conducted. It is important to be an ordinary user here, for which one needs to create accounts on different platforms.

As already noted, open source search involves extracting information from publicly available resources. At the same time, the OSINT analyst should act anonymously and maintain confidentiality. If the person being searched finds out that someone is trying to find information about them, they can take appropriate measures, including deleting messages on social networks, restricting profile visibility, suspending websites, and destroying data. Anonymity will help to hide the fact of the search and surveillance in many ways. Even indirectly, one should not designate a search. In addition, if a wanted person detects surveillance, he/she may change his/her behavior or communication methods. This will significantly complicate further collection of the necessary information and thus negatively affect the level of desired awareness. Anonymity helps to avoid undesirable developments.

By compromising the search in the early stages, it can harm obtaining the information necessary to solve a crime committed in the past, to identify a new criminal conspiracy. Let the perpetrator continue his/her illegal activities, but under surveillance. Anonymity is an important component of discreet surveillance. It helps eliminate unintentional violations of ethical and legal norms, and create security for analysts and information. Hackers, terrorists, and other criminals may try to crack down on analysts and informants who participate in the search. Anonymity and confidentiality help to ensure their protection. It is necessary to eliminate data leakage and possible undesirable consequences by applying reliable privacy protection measures.

An OSINT analyst should not be identified by an IP address search. If one does not mask the real IP address using special means, the sites will fix it. Browsers collect an incredible amount of data, from the screen resolution to installed plugins. A unique fingerprint is created on their basis. It is a combination of data about the device, browser, and connection that the user uses to visit a specific site, and a set of data that help identify a file, such as an audio or video recording. The browser fingerprint gives an opportunity to track search activity regardless of the session.

To avoid a false sense of security, it is necessary to combine several tools or approaches, taking into account weaknesses of each of them.

Websites place small text files (cookies) on the device they use in order to track and remember online activities. On the one hand, it is convenient when sites save login information and contents of the shopping cart, but on the other, cookies create detailed portraits of users with information about their habits, interests, behavior and other characteristics left on a variety of sites and during different sessions. Regular clearing of cookies helps limit tracking, but there are more advanced methods, including browser and device fingerprints (using Canvas technology), that are independent of these files. Cookies can be stored in different locations and can contain quite a lot of information.

To avoid surveillance, it is important to use special browsers designed for confidential web browsing, as well as to change online behavior from time to time. It is known that files contain metadata, which are information about the file itself created by the device being used. For example, geotags, timestamps, device serial numbers, editing history, etc. can be saved. The headers of emails reveal the IP address and information about a client. In the event of a leak, metadata can reveal information about person's identity and minimize anonymity, so before publishing a file, one needs to delete them, as well as avoid communication methods that disclose metadata.

It is reasonable to choose a place of work, taking into account that in coffee shops, hotels, and transport, the Wi-Fi network often does not have a password and is not protected in any way. As a result, anyone nearby can intercept unencrypted traffic and spy on what a person is doing on the Internet. When connecting to an unsecured public Wi-Fi network, one should not log into accounts that contain confidential information, such as email, and should encrypt traffic using a reliable VPN, or better yet, keep confidential data until connected to a secure network.

The use of an account may be one of the mistakes of OSINT analysts. When searching on social networks, forums, and other online platforms, one should create anonymous one-time accounts and mask IP addresses. It is necessary to separate persons' own Internet activity and actions related to the search for facts related to the investigation of crimes of previous years.

A person can destroy his/her anonymity by accidentally revealing personal information in a chat, on a forum, or other communication platform. So, one should be extremely careful when providing data and differentiate anonymous characters. When the same logins, passwords, or similar email addresses for different accounts are used, it is rather easy to establish connections between them.

New hacking methods, exploits and vulnerabilities are constantly appearing. If one does not monitor the emergence of new threats to privacy and security, the information used may be stolen by methods that are not yet in circulation, from which they have not been protected. To prevent this from happening, one should not rely on existing knowledge; training should be continuous.

The complex of OSINT methods and techniques allows analysts to navigate the vast information space. Advanced tools help extract valuable information, perform ethical hacking and data extraction. Web scraping is designed to use a program to automatically extract data from websites. This is the main OSINT tool that helps quickly collect large amounts of information. Using scripts in programming languages like Python, he scans websites and extracts information, knows how to be where he needs to be, easily collecting the necessary data. Web scraping helps get valuable data in the digital space: from the contact list from online catalogues to useful forum data.

Scrapers serve as reliable observers who monitor any changes on websites. They promptly warn you about news and updates, which can be very convenient. Web scrapers can act as a time machine and take regular snapshots of web pages, analyzing which you can see what

has changed on them. This feature helps out if one needs to access old information or restore deleted information. The data collected through web scraping can be combined with other information and a deeper analysis can be performed.

Conclusion

The value of the OSINT information system lies in the continuity of the cycle: it gives an opportunity to constantly collect information, improve its analysis, processing, and take into account new data, including correlations and feedback. However, the system has the same disadvantages and limitations as other search tools and methods. Therefore, it is necessary to involve experienced IT specialists, professionals in the field of information technology, who at the same time are able to correctly interpret the extracted data and apply them to circumstances that reveal a crime committed in the past.

Today, special training of investigators is required to acquire relevant knowledge, skills and abilities. It is not possible to do this without developing specific programs with the direct participation of IT specialists at all stages. In addition, a special material and technical base is required, equipped with modern computers, which allows solving specific tasks by implementing automated tools, searching and collecting information from various sources.

REFERENCES

1. Gimazetdinov D.R. *Ugolovno-protsessual'naya forma: obshcheteoreticheskii, normativno-pravovoi i pravoprimenitel'nyi analiz: dis. … kand. yurid. nauk* [Criminal procedural form: general theoretical, regulatory and law enforcement analysis: Candidate of Sciences (Law) dissertation abstract]. Izhevsk, 2023. P. 598–606.
2. Rossinskii S.B. A criminal-procedural form: essence, problems, trends and prospects of development. *Aktual'nye problemy rossiiskogo prava = Actual Problems of Russian Law*, 2020, no. 9, pp. 67–79. (In Russ.).
3. Activities of the investigator in the suspended case. Search for the accused. Resumption of the preliminary investigation. In: Grigor'ev V.N., Pobedkin A.V., Yashin V.N. *Ugolovnyi protsess* [Criminal process]. Moscow, 2023. 960 p.
4. Gonchar V.V. *Teoreticheskie i pravovye aspekty rozysknoi deyatel'nosti sledovatelya* [Theoretical and legal aspects of the investigator's investigative activities]. Moscow, 2021. 162 p.
5. Lupinskaya P.A. *Resheniya v ugolovnom sudoproizvodstve. Ikh vidy, soderzhanie i formy* [Decisions in criminal proceedings. Their types, contents and forms]. Moscow, 1976. 162 p.
6. Shurukhnov N.G. Investigative activity of an investigator. In: Volynskii A.F., Lavrov V.P. (Eds.). *Kriminalistika* [Criminalistics]. Moscow, 2006. P. 521–535. (In Russ.).
7. Shurukhnov N.G., Grishin D.A. Improving the effectiveness of individual investigative actions (monitoring and recording of negotiations, obtaining information about the connection of subscribers and (or) subscriber devices). *Lobbirovanie v zakonodatel'stve = Lobbying in the Legislative Process*, 2024, vol. 3, no. 4, pp. 95–100. (In Russ.).
8. *Digital 2024: global'nyi obzornyi otchet* [Digital 2024: global overview report]. Available at: https://datareportal.com/reports/digital-2024-global-overview-report (accessed November 12, 2025).
9. The state of crime in Russia in January-December 2024. *Ministerstvo vnutrennikh del Rossiiskoi Federatsii, FKU "Glavnyi informatsionno-analiticheskii tsentr"* [Ministry of Internal Affairs of the Russian Federation, Main Information and Analytical Center]. Moscow, 2025. Available at: https://portal.tpu.ru/SHARED/n/NIKOLAENKOVS/student/risk_management/Sbornik_UOS_2024.pdf
10. *IT-spravochnik sledovatelya* [IT-investigator's handbook]. Ed. by Zuev S.V. Moscow, 2019. 232 p.
11. Meredit D. *OSINT. Rukovodstvo po sboru i analizu otkrytoi informatsii v internete* [OSINT. A guide to collecting and analyzing open information on the Internet]. Astana, 2025. 224 p.

INFORMATION ABOUT THE AUTHOR

NIKOLAI G. SHURUKHNOV – Doctor of Sciences (Law), Professor, Leading Researcher at the Research Institute of the Federal Penitentiary Service of Russia, Moscow, Russia, professor at the Department of Criminal Law and Procedure of the Tula Institute (branch) of the All-Russian State University of Justice (RLA of the Ministry of Justice of Russia), Tula, Russia, matros49@mail.ru, https://orcid.org/0000-0003-1132-760X

Received December 16, 2025