UDC 343.1
DOI: 10.63341/naia-herald/3.2025.74

The problem of legitimacy in law enforcement activities under conditions of insufficient legislative regulation of confidential cooperation

Natalia Kulitska*
Postgraduate Student
National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
https://orcid.org/0009-0004-3295-2070

■ **Abstract.** For the effective investigation of serious or particularly serious crimes, covert investigative (search) actions are conducted, involving individuals who confidentially cooperate with law enforcement agencies. This study aimed to examine the legal parameters governing the admissibility of the results of covert investigative (search) actions as a particularly sensitive form of evidence collection, with emphasis on balancing operational expediency and procedural legality within criminal proceedings. The methodological basis of the study included a systematic analysis of Ukrainian legislative acts, as well as comparative legal methods, which made it possible to assess the effectiveness of the practical application of legislative provisions. In the context of insufficient legislative regulation of confidential cooperation with law enforcement bodies, it was necessary to analyse potential errors that may lead to the recognition of evidence as inadmissible. Attention was drawn to the possibility of conducting covert investigative (search) actions solely during the investigation of crimes of a certain degree of gravity, and subject to the proper procedure for obtaining the necessary authorisation. The article also highlighted the need for proper formalisation of the involvement of individuals confidentially cooperating with law enforcement authorities in covert investigative (search) actions, and outlines the information that must be specified in the ruling authorising such a decision. Issues concerning the declassification of protocols prepared on the basis of covert investigative (search) actions and the decisions authorising their conduct have been examined, with particular attention given to the absence of a mechanism for declassifying rulings of an investigating judge granting permission for such actions and the problems arising as a result. A mechanism has been proposed for verifying the legality of covert investigative (search) actions in cases where no ruling by an investigating judge exists to authorise such actions, or where such a ruling remains classified. The problematic issues explored in this article, together with the specified conditions for using the evidence obtained, provide a useful tool for the practical work of detectives, investigators, and operational units of law enforcement agencies

■ **Keywords:** admissibility of evidence; documentation of covert investigative (search) actions; involvement of individuals; time limits; law enforcement officers; declassification

■ Introduction

Covert investigative (search) actions (hereinafter CISAs) are a type of investigative (search) action, information about the fact and methods of which is not subject to disclosure, except in cases provided

■ **Suggested Citation:**
Kulitska, N. (2025). The problem of legitimacy in law enforcement activities under conditions of insufficient legislative regulation of confidential cooperation. *Scientific Journal of the National Academy of Internal Affairs,* 30(3), 74-86. doi: 10.63341/naia-herald/3.2025.74.
■ *Corresponding author
■ Received: 28.05.2025; Revised: 23.08.2025; Accepted: 29.09.2025

for by the Criminal Procedure Code of Ukraine[1]. According to the CPC, CISAs are conducted only in cases where information about a criminal offence and the person who committed it cannot be obtained by other means. In the context of corruption-related criminal offences, law enforcement officers at the initial stage of investigation have limited time to obtain authorisation to conduct CISAs, to properly involve an individual (often the complainant) in such actions, and to carry them out competently. The lack of time is caused by offenders' awareness of law enforcement activities and their establishment of strict deadlines for receiving bribes. Owing to time constraints, the insufficient legislative regulation of confidential cooperation, and the need for rapid decision-making, law enforcement officers may make mistakes that could subsequently result in evidence being declared inadmissible or irrelevant. For this reason, this article summarises practical experience, analyses the legislation, and identifies the key conditions that must be observed when preparing, conducting, and using the results of CISAs.

Between 2012 and 2015, after the regulation permitting the conduct of CISAs during pre-trial investigation was introduced, these provisions were not implemented in practice, and only up to 7% of the results of CISAs were used by prosecutors to substantiate charges in court (Serhieieva, 2016). However, by 2020, the situation had changed, and law enforcement officers began to submit applications for the conduct of CISAs much more actively, particularly during investigations of corruption offences. For example, in 2020, investigating judges of the High Anti-Corruption Court considered 1,995 applications for authorisation to conduct CISAs, of which 81% were granted (High Anti-Corruption Court, 2021). According to the findings of J. Matijašević & S. Zarubica (2020), one reason for this may be that modern society increasingly faces serious forms of crime in which offenders employ advanced technological means, thereby compelling law enforcement officers to resort to CISAs in order to obtain evidence of criminal activity, albeit at the expense of the privacy of certain individuals.

CISAs have become an effective tool for collecting evidence in criminal proceedings, and when applied appropriately and in a timely manner, they enable law enforcement officers and prosecutors to record information that could not otherwise be obtained – for example, conversations between suspects, surveillance of their actions, or access to data exchanged electronically. Alongside the conduct of CISAs, the use of undercover agents is also considered an effective method of gathering evidence. According to J.J. Dragojlović & N. Filipović (2022), this constitutes the most effective tactic for carrying out covert operations. For this reason, this article analyses the proper procedure for involving individuals in confidential cooperation. In addition to the effectiveness of CISAs, it is equally important to maintain a balance between restricting human rights in the course of such actions and the necessity of gathering evidence during pre-trial investigation. As M.M. Pohoretskyi (2023) notes, it is crucial to adhere to standards ensuring a balance between private and public interests and to uphold the principle of proportionality, whereby any interference must remain proportionate to a legitimate aim.

In the academic literature, many studies have examined individual conditions for the use of CISAs, yet relatively few scholars have identified all the conditions under which CISAs may be applied. Among this limited group is H.R. Kret (2021), who observed that if the legal classification of a criminal offence is altered from a serious or particularly serious crime to a less serious one, the results of CISAs may nonetheless be used within the given criminal proceedings. Significant evidentiary gaps present in the process of deciding whether to declassify investigating judges' rulings authorising CISAs were studied by O.V. Heselev (2019), who pointed to the lack of regulation in this area and the resulting consequences. The issue of granting admission and access to state secrets for individuals cooperating with law enforcement agencies on a confidential basis was explored in a doctoral dissertation by Ya. Talyzina (2022). The researcher concluded that the absence of such admission and access to state secrets should not affect the admissibility of the evidence in question.

This study aimed to establish an algorithm of actions and the main requirements of the CPC[2] that law enforcement officers must follow when conducting CISAs in order to ensure that the evidence obtained is recognised as admissible.

Materials and Methods

To achieve the stated aim, the study employed the following principal methods. The method of dogmatic (formal-legal) analysis was applied to examine the current legislation of Ukraine, which made it possible to systematise legal norms and identify their gaps. In addition, the method of comparative jurisprudence was used to analyse the experience of applying the provisions of the Criminal Procedure Code of Ukraine in practice[3]. The methods of synthesis and induction were also employed to examine the various

[1] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.
[2] Ibidem, 2012.
[3] Ibidem, 2012.

conditions for the use of the results of covert investigative (search) actions, to generalise them, and to present the findings in this article. Finally, the case study method was applied to assess the effectiveness of the implementation of Ukrainian legislation. For example, the practical observations of O.V. Heselev (2019) were analysed, which pointed to the impossibility of prosecutors influencing decisions on declassifying rulings authorising CISAs. The theoretical framework of the study was based on the criteria of admissibility of evidence identified by A.V. Panov & D.R. Tyshchenko (2024): legality (obtained in a lawful manner and in compliance with all procedural rules), reliability (being accurate and fact-based), relevance (pertaining to the subject of the case), and fairness (not obtained through violations of human rights).

The source base of the study included: the Criminal Procedure Code of Ukraine[1], which sets out the fundamental norms to be observed; internal instructions[2], which define in greater detail the procedure for conducting CISAs; and court rulings, which reflect established judicial practice and made it possible to analyse errors committed in practice and to formulate, on their basis, the conditions that must be adhered to. For example, a ruling of the Supreme Court[3] established the requirement to disclose not only the materials of CISAs but also the decision granting permission for their conduct. These sources were selected because, when forming an operational algorithm, it is necessary to take into account the requirements set by law. The analysis of court proceedings made it possible to consider the "vision" of the court as the final link in the criminal process, and to assess the decisions taken by law enforcement officers.

Results and Discussion

The absence of a definition of the term "results of CISAs" in the CPC[4] has sparked debate among scholars and practitioners regarding its interpretation. Based on an analysis of the provisions of the CPC and the Instruction on the Organisation of Covert Investigative (Search) Actions and the Use of Their Results in Criminal Proceedings[5], D. Serhieieva (2016) proposes considering the results of CISAs in both broad and narrow senses. In the broad sense, the results of CISAs are any data obtained in the course of their conduct. In the narrow sense, the results of CISAs are materially recorded sources containing such data, as well as physical objects, including documents, arising in the course of their conduct.

M.V. Bahrii & V.V. Lutsyk (2017), in analysing the concepts of "results of CISAs" and "materials of CISAs", concluded that these notions are identical. The scholars proposed their own definition of "results of CISAs", which is persuasive, as it captures the essence of the information obtained during the conduct of CISAs and summarises it concisely. It is therefore recommended for use in further research. According to their definition, the results of CISAs are the information obtained by persons who conducted or were involved in the conduct of CISAs and recorded in a procedurally prescribed form (sources of such information), as well as objects, items, or documents seized during their conduct that may be relevant to establishing the circumstances of the criminal proceedings.

When planning the conduct of CISAs, law enforcement officers seek confidential assistance from individuals with the aim of involving them in such actions. The purpose of such involvement is to enhance the effectiveness of CISAs and to obtain indisputable evidence during their execution. If, in the course of conducting CISAs, the pre-trial investigation body manages to record evidence of the criminal activity of certain persons, the results become significant evidence through which the prosecution may secure a conviction in court. For this reason, it is crucial to adhere to the conditions that ensure the subsequent admissibility of CISA results, namely: compliance with the CPC[6] requirements for obtaining authorisation to conduct CISAs; the confidential involvement of individuals in their conduct; the prescribed forms and methods of their implementation; and the proper drafting of protocols recording their results.

Procedural conditions for conducting CISAs are the legally established fundamental rules (requirements) that ensure the lawfulness and validity of their conduct, the achievement of their purpose, and the fulfilment of the tasks of criminal proceedings. These procedural conditions determine the legitimacy of such actions and, consequently, the possibility of using their results in criminal proceedings. A breach of the procedural conditions for conducting CISAs renders their results inadmissible as evidence (Bahrii & Lutsyk, 2017).

Several conditions can be identified under which the results of CISAs obtained through confidential

[1] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.
[2] Instructions on the Organisation of Covert Investigative (Search) Actions and the Use of their Results in Criminal Proceedings. (2012, November). Retrieved from https://zakon.rada.gov.ua/laws/show/v0114900-12#Text.
[3] Resolution of the Supreme Court in the Case No. 671/463/15-к. (2017, March). Retrieved from https://dl.if.court.gov.ua/sud0906/pres-centr/1/357697/.
[4] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.
[5] Instructions on the Organisation of Covert Investigative (Search) Actions and the Use of their Results in Criminal Proceedings. (2012, November). Retrieved from https://zakon.rada.gov.ua/laws/show/v0114900-12#Text.
[6] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.

cooperation may be used. The first condition is the investigation of a serious or particularly serious criminal offence. According to the provisions of the CPC,[1] CISAs may be conducted exclusively in criminal proceedings concerning serious or particularly serious crimes – that is, offences punishable by imprisonment for a term of five years or more, or by a principal fine exceeding twenty-five thousand tax-free minimum incomes of citizens. This provision indicates that investigators or prosecutors may apply to an investigating judge for authorisation to conduct CISAs, or independently decide to conduct them, solely in relation to serious or particularly serious criminal offences.

In cases where the classification of an offence is requalified from serious or particularly serious to non-serious, evidence obtained through covert investigative (search) actions may be used in proof, provided that at the time authorisation was granted and the actions conducted, the Unified Register of Pre-Trial Investigations contained information on the offence under its initial legal classification as serious or particularly serious. In such circumstances, as noted by the Supreme Court, there is no violation of the requirements of Part 2, Article 246 of the CPC[2], despite the fact that during the pre-trial investigation the offence was subsequently reclassified as non-serious[3].

On this matter, M.V. Bahrii & V.V. Lutsyk (2017) take the opposite view and support those authors who argue that the correct solution would be to disregard the results of CISAs when making decisions in criminal proceedings if, after their conduct, the offence is reclassified from serious or particularly serious to non-serious. However, if at the time of entering the information into the Unified Register of Pre-Trial Investigations there were grounds to believe that a serious or particularly serious offence was being committed, and the initial classification was not deliberately "overstated", then the results of CISAs conducted before it became apparent that the actions should be reclassified as a less serious criminal offence may be admissible.

The second important condition is the adoption of a CPC-mandated decision authorising the conduct of CISAs. In Ukraine, the life and health of individuals, their honour and dignity, as well as their inviolability and security, are recognised as the highest social values. The Constitution of Ukraine guarantees the inviolability of the home, the secrecy of correspondence, telephone conversations, telegraphic, and other communications. No one may be subjected to interference in their personal or family life, except in cases provided for by the Constitution[4]. While the Constitution[5] guarantees these rights, it also establishes exceptional circumstances in which restrictions on human rights are permissible. For example, the Constitution[6] stipulates that entry into a person's home or other property, or conducting an inspection or search therein, is permitted only by a motivated judicial decision. Exceptions to the guarantee of correspondence secrecy may be established solely by a court in cases provided for by law, for the purpose of preventing a crime or ascertaining the truth during a criminal investigation, if the information cannot be obtained by other means. For this reason, in a constitutional state, it is not prohibited to introduce certain restrictions, provided that they benefit society as a whole (Domin, 2018) and are implemented solely to achieve the objectives defined by the Constitution.

One of the legally sanctioned restrictions on human rights is the conduct of CISAs. To prevent abuse of the authority to carry out such actions, the legislature has established a logical sequence of procedural actions and decision-making algorithms for organising, conducting, and using the results of CISAs, and has prohibited the initiation or execution of any type of CISA without proper authorisation or in circumstances not envisaged by the CPC[7]. Analysing the provisions of the relevant legislation, it is possible to identify three actors who may make decisions regarding the conduct of CISAs: the investigating judge, the investigator, and the prosecutor. However, the vast majority of CISAs provided for in Chapter 21 of the CPC[8] require the prior authorisation of a judge, meaning they are subject to judicial oversight.

Judicial oversight is recognised in contemporary legal literature as an independent organisational and legal form of exercising judicial authority, a system of measures provided for by criminal procedure law aimed at implementing the constitutional functions of the judiciary. Its purpose is to prevent unlawful or unjustified restrictions on individual rights in criminal proceedings, to restore those rights, or, where necessary, to provide legal remedies. Such oversight serves as a check on potential abuse of power by the state. A distinctive feature of the role of the investigating judge is that, while exercising judicial oversight to ensure the protection of rights, freedoms, and

[1] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.
[2] Ibidem, 2012.
[3] Resolution of the Supreme Court in the Case No. 607/15414/17. (2020, April). Retrieved from https://zakononline.com.ua/court-decisions/show/88602316.
[4] Constitution of Ukraine. (1996, June). Retrieved from https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.
[5] Ibidem, 1996.
[6] Ibidem, 1996.
[7] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.
[8] Ibidem, 2012.

lawful interests of individuals, the judge does not determine the guilt or innocence of the person subject to criminal liability. Instead, the judge reviews the legality of procedural coercive measures that may infringe the constitutional principle of personal inviolability and prevents unlawful actions or decisions that violate the constitutional rights and freedoms of citizens (Drozdova & Zaritska, 2021).

In cases requiring judicial authorisation for the conduct of CISAs, the investigator, in agreement with the prosecutor, or the prosecutor independently, submits the relevant petition to the investigating judge. If the investigator or prosecutor convinces the judge that, during the conduct of CISAs, evidence may be obtained which, alone or together with other evidence, could be significant for establishing the circumstances of a criminal offence or identifying the persons who committed it, substantiates the impossibility of obtaining information about the offence and its perpetrator by other means, and provides sufficient evidence to suspect the individual in question, the judge, after verifying the seriousness of the criminal offence for which the petition is submitted and examining the details of the person concerned, will issue a reasoned ruling authorising the conduct of the CISA.

In cases where CISAs are required that do not need judicial authorisation (such as surveillance of an object or location; retrieval of information from electronic information systems whose access is not restricted by the owner, holder, or custodian, or does not involve bypassing logical security systems; or the execution of a special task to uncover the criminal activity of an organised group or criminal organisation), the investigator issues the corresponding order and notifies the prosecutor of the commencement of the CISA, or the prosecutor may make this decision independently. If the decision concerns the execution of a special task to uncover the criminal activity of an organised group or criminal organisation, the validity of the decision requires that the investigator's order be approved by the head of the pre-trial investigation authority.

The final type of CISA for which the decision to conduct it is taken exclusively by the prosecutor is crime control, which may be carried out in the following forms: controlled delivery, controlled and operational purchase, special investigative experiment, and crime scene simulation. Due to the specific nature of this type of CISA, it cannot be conducted without the involvement of a person cooperating confidentially with law enforcement or an undercover operative. Given that the prosecutor, when deciding to conduct crime control, must specify the person involved in the CISA, the investigator is required to prepare a document addressed to the prosecutor justifying the necessity of the CISA in the form of crime control and providing information about the individual whom the investigator considers should participate in the operation. When the decision to conduct a CISA is made by the investigator or prosecutor, it is essential that the official has authority in the relevant criminal proceedings – that is, they must be part of the group of investigators or prosecutors assigned to the case, and their involvement in the investigation must be recorded in the Unified Register of Pre-Trial Investigations.

It is also important to take into account the specific requirements for preparing and obtaining approval for a petition to authorise a CISA in relation to certain categories of individuals, as established in Article 480 of the CPC[1]. O.V. Shapoval (2025) presents conflicting perspectives in their study regarding the possibility of conducting CISAs in relation to a lawyer. On one hand, the scholar analyses cases in which the results of CISAs conducted on a lawyer were recognised as evidence of the lawyer's involvement in criminal activity, with the court, during the hearing, establishing that the lawyer had engaged in unlawful conduct under the guise of providing legal assistance. On the other hand, the researcher disagrees with the court's description of these facts and emphasises the necessity of conducting CISAs involving a lawyer only with the participation of a representative from the regional bar council. In some cases, O.V. Shapoval (2025) interprets the provisions of the CPC as prohibiting CISAs against lawyers entirely. It is important to note that the procedure for obtaining authorisation to conduct a CISA in relation to a lawyer involves a special petition process, namely submission by the Prosecutor General, their deputy, or the prosecutor of the Autonomous Republic of Crimea, a region, Kyiv, or Sevastopol, thereby providing additional safeguards for the protection of attorney-client privilege. Furthermore, proposed amendments requiring the involvement of a regional bar council representative in CISAs against a lawyer are not only impractical prior to implementation but could also result in the disclosure of information regarding the conduct of the CISA and are aimed primarily at preventing the effective documentation of lawyers' unlawful actions.

The third important condition is the proper formalisation of the involvement of an individual in confidential cooperation. According to Article 275 of the CPC[2], an investigator has the right to involve a person who is cooperating confidentially with them in the conduct of CISAs. A similar right is granted to both the investigator and the prosecutor under

[1] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.
[2] Ibidem, 2012.

Part 6, Article 246 of the CPC[1], which provides that, by decision of the investigator or prosecutor, other persons may also be involved in conducting CISAs.

The decision to involve a person in confidential cooperation in a particular criminal proceeding is a procedural decision, and therefore, the investigator who makes it must issue a corresponding order. Attention should be paid to the CPC's prohibition on involving certain categories of persons in confidential cooperation, namely lawyers, notaries, medical professionals, clergy, and journalists, where such cooperation would involve the disclosure of professional confidential information. When examining this issue, it is important to note attempts by lawyers and bar councils to manipulate this provision, seeking to prevent lawyers from agreeing to confidential cooperation even where such cooperation would not result in the disclosure of confidential information. For this reason, it is argued that if a lawyer's confidential cooperation with law enforcement does not involve attorney–client privilege and does not use information obtained from a client, law enforcement agencies have the right to involve lawyers in confidential cooperation under Article 275 of the CPC and the Law of Ukraine "On Operative-Investigative Activities"[2] (Kulitska, 2025).

If there are grounds to change the personal details of an individual being involved in confidential cooperation, the investigator must, prior to issuing the order for their involvement, issue a separate order implementing the security measures provided for under the Law of Ukraine "On Ensuring the Safety of Persons Participating in Criminal Proceedings". In such cases, the order implementing the security measures, which contains the individual's actual details, must be stored separately from the criminal case materials, while the order for involving the individual, in which the altered personal data are recorded, is attached to the case materials.

The order to involve a person in confidential cooperation must comply with the general requirements for orders as set out in Part 5, Article 110 of the CPC[3]. Specifically, it must include an introduction, a reasoning section, and a resolutive section, containing information on: the place and time the order was issued; the full name and position of the person issuing the order; the circumstances providing grounds for the order; the reasons for issuing the order, their justification, and references to the relevant provisions of the CPC; the content of the procedural decision taken; the place and timeframe for its execution; the individual responsible for executing the order; and the possibility and procedure for appealing the order.

In addition to the information already mentioned, the order to involve a person in confidential cooperation must also include: the individual's voluntary consent to participate; the full name of the person who has agreed to cooperate; and confirmation that the individual has been warned not to provoke persons under pre-trial investigation into committing a crime. Compliance with the time limits for conducting CISAs constitutes the fourth condition. The provisions of the CPC stipulate that the overall duration of a CISA in a single criminal proceeding, for which authorisation is granted by an investigative judge, must not exceed the maximum pre-trial investigation periods established under Article 219 of the CPC. Where a CISA is conducted to determine the location of a person evading pre-trial investigation authorities, an investigative judge, or a court, and who has been declared wanted, the operation may continue until the individual's location is established. The CPC[4] further regulates that the duration of an investigative judge's authorisation for a CISA may not exceed two months, while a CISA conducted as part of a special task to uncover the criminal activity of an organised group or criminal organisation may not exceed six months. Provisions also typically allow for the extension of the CISA period if necessary.

When examining the issue of timeframes in the context of complying with the conditions necessary for the admissibility of CISA results, attention should be paid to the requirement that CISAs are conducted only after a decision authorising their execution has been issued and no later than the final day of validity of that decision. In practice, questions of legitimacy may arise if a CISA is conducted on the same day the authorisation is issued. The defence often requests information on the court's automatic allocation of motions, which records the date and time of allocation, and may focus on whether the CISA was initiated before the judge had considered the motion. Law enforcement officers must strictly control the start of a CISA and commence it only after the court hearing on the motion has taken place and authorisation has been granted. Given that the preparation of a written judicial decision authorising a CISA may take considerable time, law enforcement officers are entitled to begin the operation after receiving oral authorisation from the investigative judge during the motion hearing. The subsequent printing of the court order after

[1] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.
[2] Law of Ukraine No. 2135-XII "On Operational-Investigative Activities". (1992, February). Retrieved from https://zakon.rada.gov.ua/laws/show/2135-12#Text.
[3] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.
[4] Ibidem, 2012.

the CISA has been conducted should not constitute grounds for declaring the results of the operation inadmissible as evidence in the case.

Attention should be given to the necessity of observing the principle of "reasonable" timeframes when conducting CISAs. The concept of "reasonable" timeframes is a relatively recent development in Ukrainian criminal procedural law and theory. The legislator's intention is that participants in criminal proceedings, in each specific case, should not rely solely on the maximum time limits set out in the CPC[1], but instead should base their actions on the time objectively required to perform procedural acts and make procedural decisions (Volobuiev & Smokov, 2025). Therefore, if it becomes apparent that no results are being obtained during a CISA, it is important not to prolong the operation until the authorisation period expires, but to terminate the actions once there are grounds to conclude that the operation is unlikely to yield evidence of criminal activity by the persons concerned.

Compliance with the procedural form for recording CISA results constitutes the fifth condition. Proper documentation of a CISA is an essential prerequisite for the admissibility of its results as evidence. As a general rule, any breach of the procedure for recording the progress and outcomes of a CISA renders the resulting evidence inadmissible (Kaplina, 2024). To ensure that CISA results can be used as evidence in criminal proceedings, they must be formally recorded in material form – namely, a protocol – because the informational content alone, obtained during the operation, cannot be directly used as evidence (Serhieieva, 2017). The CPC[2] clearly stipulates that the recording of the progress and results of CISAs must comply with the general rules for documenting criminal proceedings as established by the CPC. A protocol is drawn up based on the results of a CISA, to which annexes may be attached if necessary. The CISA protocol is a written document prepared in the manner prescribed by the CPC, in which authorised persons (investigators, operative officers) record and certify the conditions and procedures of the CISA, factual information about the criminal event, the involvement of specific individuals, and other circumstances relevant to the criminal proceedings (Kudinov *et al.*, 2015).

According to Part 3 of Article 104 of the CPC, the protocol consists of: 1) the introductory section, which must include information on the location and time of the procedural action and its title; the person conducting the action (full name, position); all individuals present during the procedural action (full names, dates of birth, places of residence); confirmation that the participants were informed in advance of the use of technical recording devices, including their specifications and the information carriers employed; and the conditions and procedures for their use. 2) The descriptive section, which must contain details of the sequence of actions; information obtained as a result of the procedural action that is relevant to the criminal case, including any items or documents identified or provided during the action. 3) The concluding section, which must include information about the items and documents seized and the method of their identification; copies of documents prepared, as well as duplicates of information, including computer data, and the method of their identification; the manner in which participants are familiarised with the content of the protocol; and any comments or additions to the written protocol submitted by participants in the procedural action.

Scholars emphasise that CISA protocols have additional specific features. In the introductory section of the protocol, the relevant decision authorising the CISA must also be indicated – this could be a court ruling, or a resolution by the investigator or prosecutor. Protocols may be drawn up periodically, and the recording of results must be conducted in such a way that their accuracy can always be verified by expert examination. Additionally, the confidentiality regime must be maintained during the drafting of protocols and while working with them (Bahrii & Lutsyk, 2017).

It is also important to note that if an individual is involved in the execution of a CISA, the protocol must include information about their participation and their personal details. If security measures have been applied to such individuals, the protocol may record their data in a manner that ensures confidentiality, in accordance with the procedure established by law. Additionally, if a CISA is assigned to operational staff of a particular department – for example, surveillance of a person, object, or location – the protocol must record the involvement of such personnel without specifying the position or personal details o f each individual, as this information may be classified.

D. Serhieieva (2016) notes that, in many cases, CISA protocols are drafted by investigators or operational staff who did not personally conduct or participate in the operation, but merely delegated it to the direct executor. The scholar argues that this prevents the use of such a CISA in evidence. However, this view is not fully convincing, as in most instances, CISAs are carried out either by the individuals involved in their execution (such as audio or video surveillance of a person, crime monitoring, or performing a special task to uncover the activities of an organised

[1] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.
[2] Ibidem, 2012.

group or criminal organisation) or simultaneously by several operational staff members (for example, visual surveillance of a person, object, or location), making it impossible for a single executor to compile the protocol. When an individual is involved in conducting a CISA, they do not have the procedural status of an investigator authorised to draft the protocol and often lack access to state secrets, which is required for protocol preparation. In cases where multiple staff members are involved, each is responsible for a clearly defined task and does not have information on the entire operation, which is necessary for drafting the protocol.

For this reason, it is considered that the protocol based on the results of a CISA should be drafted by the investigator or an operational unit officer who either summarises the results of the CISA (in the case of visual surveillance of a person, object, or location, or performing a special task to uncover the activities of an organised group or criminal organisation) or analyses the information obtained from its execution (such as audio or video monitoring of a person, or monitoring the commission of a crime).

Another possible method of recording procedural actions, as provided by Article 103 of the CPC[1], is the use of an information carrier on which procedural actions are recorded using technical means. The issues related to this method of recording were examined by D. Serhieieva (2017), who noted that, unlike the previous Ukrainian criminal procedural legislation, which mandated the maintenance of a protocol (Article 84 of the 1960 CPC[2]), the current CPC allows an alternative form of recording procedural actions – using an information carrier with technical means (paragraph 2, part 1, Article 103 of the CPC). Such information carriers, provided they contain the data specified in part 1 of Article 99 of the CPC, are considered documents (paragraph 3, part 2, Article 99 of the CPC). At the same time, Serhieieva points out that the criminal procedural legislation does not specify in which cases this form of recording may be used. Part 2 of Article 104 of the CPC of Ukraine legislatively provides for this possibility only during an interrogation, and only if none of the participants insists that the text of the testimony be included in the protocol. Other instances of using technical recording to document the course and results of a procedural action remain the subject of limited academic discussion.

Given the specific nature of CISAs, this method of recording is not feasible. Unlike a public investigative action, it is impossible to verbally record on tape the information that is mandatory for proper documentation of a CISA, such as the date and time of the CISA, the location where it was conducted, the legal basis for its conduct, the official carrying out the action, the persons involved, the technical recording devices used, and other required details.

The declassification and disclosure of materials to the defence and the accused constitute the sixth condition. When drafting the protocol based on the results of a CISA, the investigator or operational officer assigns the appropriate security classification, which ensures that information regarding the fact of the CISA and the content of evidence obtained remains confidential. However, once the CISA has been completed and the prosecutor intends to submit the criminal case to the court and use the drafted protocols and their annexes during trial, the security classification must be removed from these documents.

L. Shcherbyna (2024) asserts that protocols and other operational documents, along with their annexes, relating to the conduct of CISAs, which are used as evidence in criminal proceedings, should generally be declassified simultaneously with the rulings of the investigating judge authorising their conduct. This requirement stems from the need to ascertain in a timely manner the legality of such actions, the lawfulness of temporarily restricting certain human rights, and their compliance with evidentiary admissibility standards, which cannot be properly assessed without considering the legal grounds and conditions under which they were carried out.

The procedure for declassifying protocols drawn up on the results of CISAs and their annexes (material information carriers containing photos, video files, photo tables, other items, and documents) is clear and properly regulated. The Instruction on the Organisation of Covert Investigative (Search) Actions and the Use of Their Results in Criminal Proceedings (hereinafter – the Instruction) provides a precise algorithm for investigators and prosecutors regarding the declassification of CISA materials. Specifically, the security classification of such materials is removed by an expert commission composed of at least three members of the body that conducted the CISA, based on a petition submitted by the head of the prosecutorial body. The submission of this petition is preceded by the issuance of a resolution to declassify the designated material carriers of classified information. This resolution is issued by the prosecutor exercising prosecutorial authority in the specific criminal case in the form of procedural guidance over the pre-trial investigation and must be approved by the head of the prosecution office[3].

[1] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.
[2] Criminal Procedural Code of Ukraine. (1960, December). Retrieved from https://zakon.rada.gov.ua/laws/show/1001-05#Text.
[3] Instructions on the Organisation of Covert Investigative (Search) Actions and the Use of their Results in Criminal Proceedings. (2012, November). Retrieved from https://zakon.rada.gov.ua/laws/show/v0114900-12#Text.

In addition to CISA protocols, documents authorising the conduct of CISAs are also subject to declassification. These may include resolutions issued by an investigator or prosecutor, or rulings of the investigating judge. Declassifying such documents is crucial for recognising the resulting evidence as admissible. Considering that resolutions issued by investigators or prosecutors are declassified according to a procedure similar to that applied to CISA protocols, it is useful to focus in greater detail on the issues that arise when declassifying investigating judge rulings.

O.V. Heselev (2019) asserts that declassifying and subsequently using these rulings during trial allows the prosecutor to evaluate the lawfulness of the actions of those conducting the CISA in terms of compliance with all conditions specified in the ruling regarding the persons involved, the location, type, and duration of such actions. It also allows the court to form an internal conviction regarding the admissibility of the evidence obtained, while ensuring adherence to the rule of law and protection of individual rights. For this reason, the panel of judges of the Supreme Court of Ukraine concluded in its ruling of 16 March 2017 in criminal case No. 671/463/15-к[1] that, in accordance with Article 290 of the CPC of Ukraine, not only the protocols recording the course and results of procedural actions but also the materials serving as the legal basis for those actions (rulings, resolutions, petitions) must be attached to the case file and disclosed to the defence. This ensures that both the defence and the court can verify the admissibility of such actions as evidence.

O.V. Heselev (2019) notes that neither the CPC[2] nor any other legislation provides a mechanism for declassifying rulings authorising the conduct of CISAs, which creates significant challenges for the prosecuting authorities in practice. Typically, once a prosecutor decides to declassify CISA protocols, they act by analogy with the provisions of the Instruction regarding the declassification of rulings. Specifically, the ruling is sent to the court that issued it and originally decided to classify it. Subsequently, the court's expert commission decides on the declassification of the ruling and, once the confidentiality mark has been removed, forwards the ruling to the prosecutor for inclusion in the criminal case file. However, given the absence of legislative regulation for this procedure, and the fact that the provisions of the Instruction[3] do not apply to the activities of courts and are not binding on investigating judges, the final decision on whether to declassify such rulings rests with the appellate court, independent of the prosecutor. Since there is no legally defined procedure for the declassification of these judicial rulings and their provision to the prosecutor for subsequent use in assessing the admissibility of evidence obtained through CISAs, judges may, and in some cases do, refuse to authorise such declassification, citing the lack of regulation in the law, even in light of the legal position expressed by the Supreme Court of Ukraine in its March 2017 ruling[4]. This entirely deprives the prosecutor of the ability not only to assess the admissibility of evidence but also to use protocols from CISAs as evidence in criminal proceedings. It also makes the prosecutor dependent both on the general situation of legal uncertainty and on the arbitrary decisions of individual investigating judges (Heselev, 2019).

In the absence of a statutory provision or a ruling of a higher court obliging investigating judges to declassify orders authorising CISAs and to provide them to the prosecutor before the completion of the pre-trial investigation, the prosecutor is placed in a situation where, in the words of L. Fuller (1999), he is "demanded to do the impossible". In this case, it involves ensuring the implementation of certain measures and taking responsibility for actions and decisions, the outcome of which is not in fact within his control (Heselev, 2019). Given this, if an investigating judge refuses to declassify an order authorising CISAs, the presiding judge may, if necessary, request the classified order for examination and, having verified the existence of a valid judicial decision, recognise as admissible the evidence obtained during the CISAs. The defence may likewise review the content of the authorising order, provided that security clearance for access to state secrets has been obtained.

Alongside this, practitioners encounter another issue. In connection with the full-scale invasion of Ukraine by the russian federation, certain law enforcement agencies and courts took measures to prevent the enemy from accessing classified documents in the event of seizing administrative buildings, which included destroying classified materials. Among these could have been court rulings granting permission to conduct CISAs. Under such circumstances, it is considered sufficient to confirm the legitimacy of conducting a CISA by obtaining a certificate from the court stating that a judge issued permission to carry out the action regarding a particular individual in a specific criminal proceeding.

[1] Resolution of the Supreme Court in the Case No. 671/463/15-к. (2017, March). Retrieved from https://dl.if.court.gov.ua/sud0906/pres-centr/1/357697/.
[2] Criminal Procedural Code of Ukraine. (1960, December). Retrieved from https://zakon.rada.gov.ua/laws/show/1001-05#Text.
[3] Instructions on the Organisation of Covert Investigative (Search) Actions and the Use of their Results in Criminal Proceedings. (2012, November). Retrieved from https://zakon.rada.gov.ua/laws/show/v0114900-12#Text.
[4] Resolution of the Supreme Court in the Case No. 671/463/15-к. (2017, March). Retrieved from https://dl.if.court.gov.ua/sud0906/pres-centr/1/357697/.

It should be noted that when granting permission to conduct a CISA, the investigative judge examines the severity of the alleged crime, the circumstances giving reason to suspect the individual of committing the offence (i.e., reviewing the available evidence and documents confirming the person's involvement), as well as whether evidence can be obtained during the CISA that, alone or together with other evidence, may be of significant importance for clarifying the circumstances of the criminal offence or identifying the persons who committed it[1]. Permission to conduct CISAs is granted by appellate-level investigative judges and judges of the High Anti-Corruption Court – judges who, in addition to legal knowledge, possess substantial professional and practical experience. Therefore, questioning the validity of their decisions without strong evidence of judicial bias constitutes an infringement on the fundamental principles of justice.

The same applies to the position regarding the need to declassify and provide the defence with access to criminal case materials that served as the basis for conducting covert investigative (search) actions, as noted by H.R. Kret (2021). However, declassifying these materials would lead to a complete reopening of the criminal proceedings and prolong the court process, which is already time-consuming. Moreover, the review of such materials would in no way affect the annulment of the court ruling granting permission to conduct the CISA, which, under the CPC[2], is not subject to appeal.

Another problematic issue that arises during the declassification of CISA materials and the decisions authorising their conduct is the use of a ruling granting permission to conduct such an action that was obtained in one criminal proceeding and later formalised in another. Obstacles to its use and to the defence's access may arise if the criminal proceeding in which the ruling was originally obtained is still under investigation, with ongoing investigative actions including CISAs, while in the criminal proceeding where the ruling has been formalised, the pre-trial investigation is already concluding. An important consideration when providing the ruling for review by the parties is the need to maintain the confidentiality of information contained in the ruling that may be unrelated to the criminal proceeding in which the materials are being disclosed to the parties. For clarity, the criminal proceeding in which the materials are opened for review can be referred to as Case B, while the proceeding in which the pre-trial investigation is still ongoing can be referred to as Case A, containing the facts and details of that investigation.

Under such circumstances, two courses of action are appropriate:

1. Instead of declassifying the ruling granting permission to conduct CISAs, use a courtissued certificate confirming that the decision was made concerning a specific individual in the relevant criminal proceeding.

2. Review the ruling granting permission to CISAs after it has been declassified, during which a copy of the ruling should be produced with information unrelated to Case B masked. This is necessary to prevent any adverse impact on the ongoing investigation of Case A if the copy is provided to the parties for inspection. Following this review, the masked ruling should be provided to the parties in Case B for inspection and copying in accordance with Article 290 of the CPC[3], while the original ruling should be kept separately from the case materials.

In addition to providing the defence with access to the protocols of CISAs and the rulings authorising them, the prosecutor must also make available the investigator's order regarding the use of confidential cooperation with a specific individual in the relevant criminal proceeding. This individual was involved in conducting CISAs such as audio and video monitoring, supervision of criminal acts, and the execution of special tasks to uncover the criminal activities of an organised group or criminal organisation. In other words, this person directly interacted with the individuals who were later formally notified of suspicion of committing a crime.

If information regarding the true identities of such individuals has been altered, the prosecutor and the court must take measures to prevent the defence and the accused from establishing these identities during court examination, for example, by asking questions that could reveal personal information about these individuals. In addition to the necessity of declassifying the aforementioned documents, the defence often insists on formalising security clearance and access to state secrets for individuals involved in conducting CISAs, arguing that failure to do so may constitute a violation of Article 517 of the CPC. However, researchers S.R. Tahiiev *et al.* (2023) disagree with this position. Their findings indicate that, despite persistent demands by the defence, judges across different jurisdictions generally consider that granting clearance to involved individuals is not required.

The issue of whether materials from CISAs should be classified as state secrets was examined by A.A. Kohut (2024), who established criteria for information to qualify as a state secret. Kohut concluded

[1] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.
[2] Ibidem, 2012.
[3] Ibidem, 2012.

that materials from CISAs do not meet the requirements for classified information as defined in the Law of Ukraine "On State Secrets"[1]. The scholar argues that the confidentiality of CISAs can, in the vast majority of cases, be equated with the confidentiality of decisions to conduct searches, and that protection as pre-trial investigation data is sufficient. The issue raised by the researcher is highly debatable and requires more detailed study and discussion, as the Law sets out general criteria for information that may be classified as a state secret, and the more detailed description provided in the Register of Information Constituting a State Secret[2] leaves no doubt regarding the appropriateness of classifying particular information as a state secret.

Thus, in criminal proceedings, materials from CISAs – particularly protocols, decisions authorising their conduct, and orders involving confidential collaborators – must be disclosed to the parties, while ensuring the protection of personal data. If the real identities of such individuals have been altered, the court and the prosecutor are obliged to prevent their disclosure during court examination. Although the defence frequently insists on granting security clearance for those conducting CISAs, both judicial practice and academic research indicate that such a measure is unnecessary.

Conclusions

This article has analysed Ukrainian legislation as well as practical experience in conducting CISAs, including those involving individuals who confidentially cooperate with law enforcement agencies. The analysis reveals that, at present, Ukraine lacks legislative regulation concerning the declassification of judicial rulings granting permission to conduct CISAs, which creates an obstacle when examining the legality of such actions during court proceedings. The study also highlighted the necessity of properly formalising confidential cooperation with individuals who are subsequently planned to be involved in CISAs, as well as adhering to the procedural requirements for authorising such actions and respecting the prescribed timeframes.

The findings indicate a clear need for legislative regulation governing the involvement of individuals in CISAs and the declassification of judicial rulings authorising such actions. In summarising the results and the identified parameters for the admissibility of evidence obtained through covert investigative (search) actions, it should be emphasised that compliance with these conditions – both when obtaining authorisation for such actions and during their execution, including the preparation of protocols – must constitute an inviolable element of law enforcement practice. This is essential not only for the proper collection of evidence establishing the culpability of a given individual but also for fostering a culture of trust in law enforcement personnel, who must avoid acting *extra legem* in the course of their duties.

The lack of publicly available statistics from law enforcement agencies regarding the granting of authorisations for CISAs, the practical implementation of such authorisations, and related court decisions limits the ability to fully examine the appropriateness of the statutory timeframes and the conditions necessary for recognising the resulting evidence as admissible in court. Further research is required to delineate the concepts of "involvement of an individual in CISAs" and "use of confidential cooperation", as well as to clarify the prosecutor's powers in this context and to develop a regulatory framework for the removal of secrecy classifications from judicial rulings granting authorisation for CISAs.

Acknowledgements

None.

Funding

The study was not funded.

Conflict of Interest

None.

References

[1] Bahrii, M.V., & Lutsyk, V.V. (2017). *Procedural aspects of covert information gathering: Domestic and foreign experience*. Kharkiv: Pravo.

[2] Domin, Yu.M. (2018). Certain aspects of the use of results of covert investigative (search) actions. *Legal Ukraine*, 8, 31-39.

[3] Dragojlović, J., & Filipović, N. (2022). Undercover investigator in legislation of the United States and the United Kingdom. *Culture of Polissia*, 19(1), 62-78 doi: 10.51738/Kpolisa2022.19.1r.4df.

[1] Law of Ukraine No. 3855-XII "On State Secrets". (1994, January). Retrieved from https://zakon.rada.gov.ua/laws/show/3855-12/ed19940121#Text.

[2] Order of the Security Service of Ukraine No. 383 "On the Approval of the Summary of Information Constituting a State Secret". (2020, December). Retrieved from https://zakon.rada.gov.ua/laws/show/z0052-21#n13.

[4] Drozdova, O.V., & Zaritska, K.H. (2021). Investigating judge as a guarantor of ensuring the legality and justification of restrictions on constitutional human rights and freedoms during covert investigative (search) actions (CISA). *Scientific Papers of the National University "Odessa Law Academy"*, 29, 98-107. doi: 10.32837/npnuola.v28i29.721.
[5] Fuller, L. (1999). *The morality of law*. Kyiv: Sphera.
[6] Heselev, O.V. (2019). Problematic issues of declassification and use in criminal proceedings of decisions of an investigating judge on the permission to hold secret investigators (wanted) actions. *Legal Ukraine*, 3, 29-38.
[7] Higher Anti-Corruption Court. (2021). *Generalisation of judicial practice on the consideration by investigating judges of the High Anti-Corruption Court of applications for permission to conduct covert investigative (search) actions and operational-search measures*. Retrieved from https://hcac.court.gov.ua/userfiles/media/new_folder_for_uploads/hcac/statistics/reviews/review_CIA_OSM.pdf.
[8] Kaplina, O.V. (2024). Proper recording of carrying out of covert investigatory (detective) actions as a prerequisite for using their results as evidence in law enforcement activities. *Legal Scientific Electronic Journal*, 5, 441-445. doi: 10.32782/2524-0374/2024-5/109.
[9] Kohut, A.A. (2024). On the justification of classifying materials related to covert investigative (search) actions as state secrets. *Legal Scientific Electronic Journal*, 2, 426-428. doi: 10.32782/2524-0374/2024-2/105.
[10] Kret, H.R. (2021). Use of the results of covert investigative (search) actions in criminal proceedings. *Scientific Notes of the V.I. Vernadsky Tavria National University. Series: Legal Sciences*, 4, 88-93. doi: 10.32838/TNU-2707-0581/2021.4/14.
[11] Kudinov, S.S., Shekhavtsov, R.M., Drozdov, O.M., & Hrynenko, S.O. (2015). *Covert investigative (search) activities and the use of the results of operational-search activities in criminal proceedings*. Kharkiv: Oberih.
[12] Kulitska, N. (2025). Problems of normative and legal regulation of engaging lawyers in confidential cooperation. *KELM*, 1(69), 172-179. doi: 10.51647/kelm.2025.1.25.
[13] Matijašević, J., & Zarubica, S. (2020). Types and conditions for the application of special investigative measures and preventive security measures by security services. *Pravo – Teorija i Praksa*, 37(4), 26-41. doi: 10.5937/ptp2004026M.
[14] Panov, A.V., & Tyshchenko, D.R. (2024). Admissibility of evidence in echr practice as a guarantee of a fair trial. *Legal Scientific Electronic Journal*, 3, 476-478. doi: 10.32782/2524-0374/2024-3/114.
[15] Pohoretskyi, M.M. (2023). Guarantees of human rights when interfering in private communication during confidential investigations in the practice of the security service of Ukraine: Problem issues. *Criminal Justice Bulletin*, 3-4, 103-122. doi: 10.17721/2413-5372.2023.3-4/103-122.
[16] Serhieieva, D. (2016). Use of the results of covert investigative (search) activities in evidence: on improving the provisions of the current Criminal Procedure Code of Ukraine. *South Ukrainian Law Journal*, 1, 105-107.
[17] Serhieieva, D. (2017). The applying of the results of secret investigative (search) actions to obtain certain types of evidence in criminal proceeding: Problematic issues. *Law of Ukraine*, 12, 49-61.
[18] Shapoval, O.V. (2025). Topical issues of ensuring guarantees of legal professional activity during the conduct of covert investigative (detective) actions against defense attorneys in criminal proceedings. *Legal Scientific Electronic Journal*, 7, 214-216. doi: 10.32782/2524-0374/2025-7/48.
[19] Shcherbyna, L. (2024). Consequences of non-disclosure of the investigative judge's approvals, on the basis of which covert investigative (search) action, operational search and counter-intelligence measures were carry out, for criminal procedural evidence. *Law Journal*, 3, 294-304. doi: 10.32782/yuv.v3.2024.36.
[20] Tahiiev, S.R., Puzyrov, M.S., & Ivashko, S.V. (2023). Covert investigative (search) activities in war conditions: Selected theoretical and practical aspects (part II). *Electronic Scientific Publication "Analytical and Comparative Law"*, 2, 454-459. doi: 10.24144/2788-6018.2023.02.79.
[21] Talyzina Ya.O. (2022). *Regulatory support and implementation of confidential cooperation in criminal proceedings*. (Doctoral dissertation, Research Institute for the Study of Crime Problems Named After Academician V.V. Stashys National Academy of Legal Sciences of Ukraine, Kharkiv, Ukraine).
[22] Volobuiev, A.F., & Smokov, S.M. (2025). Procedural terms in criminal proceedings: Problematic issues. *Electronic Scientific Publication "Analytical and Comparative Law"*, 1, 702-707. doi: 10.24144/2788-6018.2025.01.117.

Проблема легітимності правоохоронної діяльності в умовах дефіциту законодавчого регламентування конфіденційного співробітництва

Наталя Куліцька
Аспірант
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
https://orcid.org/0009-0004-3295-2070

■ **Анотація.** Для ефективного розслідування тяжкого чи особливо тяжкого злочину проводять негласні слідчі (розшукові) дії, до яких залучають осіб, що конфіденційно співпрацюють з правоохоронними органами. Метою статті було дослідження юридичних параметрів допустимості результатів негласних слідчих (розшукових) дій як особливо чутливої форми збирання доказів з акцентом на баланс між оперативною доцільністю та процесуальною законністю в умовах кримінального провадження. Методологічна основа дослідження охоплювала системний аналіз законодавчих актів України, а також методи порівняльного правознавства, які дали змогу оцінити ефективність практичного використання норм законодавства. В умовах дефіциту законодавчого регламентування конфіденційного співробітництва правоохоронних органів необхідним є аналіз помилок, які можуть призвести до визнання доказів недопустимими. Акцентовано на можливості проведення негласних слідчих (розшукових) дій виключно під час розслідування злочинів певної категорії тяжкості та з дотриманням процедури отримання відповідного дозволу на їх проведення. Увагу спрямовано на необхідність належного оформлення залучення особи, яка конфіденційно співпрацює з правоохоронними органами, до проведення негласних слідчих (розшукових) дій, а також окреслено відомості, які мають бути зазначені в постанові про прийняття такого рішення. Досліджено питання розсекречення протоколів, складених за результатами проведення негласних слідчих (розшукових) дій та рішень про їх проведення, а також зосереджено увагу на відсутності механізму розсекречення ухвал слідчого судді про надання дозволу на проведення негласних слідчих (розшукових) дій та проблеми, які виникають у зв'язку з цим. Запропоновано механізм перевірки законності проведення негласних слідчих (розшукових) дій у разі відсутності ухвали слідчого судді про надання дозволу на проведення таких дій або нерозсекречування такої ухвали. Проблемні питання, які досліджено в цій статті, й виокремлені умови використання здобутих доказів стануть корисним інструментом у практичній роботі детективів, слідчих та оперативних підрозділів правоохоронних органів

■ **Ключові слова:** допустимість доказів; фіксація негласних слідчих (розшукових) дій; залучення особи; строки; працівники правоохоронних органів; розсекречування