ISSN 2786–6920
SCIENTIFIC BULLETIN OF THE KYIV INSTITUTE OF THE NATIONAL GUARD OF UKRAINE No 1 2025

UDC 343.98 DOI 10.59226/2786-6920.1.2025.143-150

NATALIA KOMISSAROVA

Candidate of of Juridical Sciences, Associate Professor,
Head of the Department of State Security of the
Kyiv Institute of the National Guard of Ukraine
https://orcid.org/0000-0001-6895-6891

SERHII SLYVKIN

Higher education student
of the Kyiv Institute of the National Guard of Ukraine
https://orcid.org/0009-0008-8865-0994

THREATS TO STATE SECURITY RESULTING FROM THE ACTIVITIES OF SUBVERSION AND INTELLIGENCE GROUPS: LEGAL AND ORGANIZATIONAL ASPECTS

The article analyzes threats to Ukraine's national security arising from the activities of sabotage and reconnaissance groups (SRGs) in the context of modern hybrid warfare. It reveals the main directions of the destructive impact of SRGs—physical, informational, social, and economic in nature. It is argued that Ukraine's legal framework has significant gaps in countering SRGs, which reduces the effectiveness of the state's response to these threats. Problems of coordination between the Armed Forces of Ukraine, the Security Service of Ukraine, and the National Guard of Ukraine in the field of counter-sabotage operations are identified. The article proposes ways to improve legislation and organizational support for countering SRGs, including the establishment of a unified interagency management center and the adoption of a special regulatory legal act. The study is based on an analysis of the national context and international experience, enabling the formation of a comprehensive approach to neutralizing sabotage threats.

Keywords*: national security; sabotage and reconnaissance groups; legal framework; interagency coordination; hybrid warfare.*

Statement of the problem. The modern hybrid war waged by the Russian Federation against Ukraine is accompanied by the active use of sabotage and reconnaissance groups (SRGs). Their activities pose a serious threat to national security, as saboteurs not only inflict physical damage but also destabilize the internal situation through information attacks and psychological pressure.

Since the beginning of the full-scale invasion in 2022, the Security Service of Ukraine (SBU) has repeatedly reported the detection and neutralization of SRGs operating in frontline territories and even in rear regions of Ukraine [1].

The activities of sabotage and reconnaissance groups (SRGs) are aimed at undermining the economy, destroying critical infrastructure facilities, disrupting military command and control systems, conducting information operations, and creating panic among the population. An important element of SRG operations is the use of information pressure and the spread of fake news to undermine the morale of society. The actions of saboteurs in frontline zones pose a particular danger due to limited control and rapid response capabilities in these areas.

Despite active countermeasures, serious problems remain in the detection and neutralization of sabotage and reconnaissance groups (SRGs), related both to legislative gaps and insufficient coordination among security agencies. The Law of Ukraine "On Combating Terrorism" does not contain clear definitions or provisions regarding countering SRGs, creating legal loopholes in the fight against them. Furthermore, although the Anti-Terrorism Center under the Security Service of Ukraine (SBU) performs coordination functions in combating terrorism, the lack of specific focus on SRGs may lead to reduced effectiveness of coordination between the Armed Forces of Ukraine (AFU), the SBU, and the National Guard of Ukraine in the event of a sabotage threat [2].

Analysis of Recent Scientific Research and Publications. Between 2022 and 2025, the number of studies dedicated to the threats posed by sabotage and reconnaissance groups (SRGs) in the context of hybrid warfare has significantly increased in both Ukrainian and international academic circles. Special attention is given to the legal regulation of countering SRGs, organizational cooperation among security agencies, and the experiences of foreign countries in combating similar forms of threats..

Specifically, the works of M.O. Borovyk, O.H. Trembovetskyi, and D.Yu. Hulevatyi examine practical aspects of detecting and neutralizing sabotage and reconnaissance groups (SRGs) by the National Police and the Border Guard Service, emphasizing the need for clear coordination among different agencies [3, 4]. The analysis of NATO's "Resolute Support" operation in Afghanistan demonstrates that effective counteraction against SRGs is possible only with the establishment of unified interagency command centers with a clear division of responsibilities [5].

Ukrainian studies in the field of national security (for example, conducted by the National Institute for Strategic Studies and Lviv State University of Internal Affairs) reveal a legal vacuum regarding the definition of sabotage and reconnaissance groups (SRGs) and criticize the fragmented nature of regulatory and legal frameworks. Additionally, publications from the Security Service of Ukraine and the Ministry of Defense provide official statistics on the detection of agent networks and operational information about SRG activities in frontline and rear areas [6].

Y. Mykhalchyshyn concludes that despite increasing awareness of the threat posed by sabotage and reconnaissance groups (SRGs), issues of legal clarification and interagency cooperation remain relevant. Therefore, further scholarly examination of these problems is a necessary prerequisite for developing an effective national security strategy [7].

The research objectives are to assess the state of Ukraine's legislative framework regarding countering sabotage and reconnaissance groups (SRGs) under martial law conditions; identify the main gaps in the legal support of counter-sabotage efforts; analyze the effectiveness of organizational cooperation among security agencies in the field of counter-sabotage; and develop proposals to improve the system for detecting and neutralizing SRGs at the legislative level and through interagency coordination.

The purpose of this article is to identify legal and organizational issues in the system of countering sabotage and reconnaissance groups (SRGs) and to substantiate ways to address them based on international experience and the analysis of current challenges.

Presentation of the Main Material. *Threats to National Security Posed by the Activities of Sabotage and Reconnaissance Groups (SRGs).* The activities of sabotage and reconnaissance groups (SRGs) represent one of the most serious threats to Ukraine's national security in the context of modern hybrid warfare. Successful sabotage operations carried out by SRGs often have not only tactical but also strategic consequences—ranging from physical damage and casualties to large-scale informational and social crises. Since the beginning of Russia's full-scale invasion in 2022, numerous incidents involving the infiltration and activity of SRGs have been recorded in both frontline and rear areas of the country [8].

The direct physical threat posed by the activities of sabotage and reconnaissance groups (SRGs) is one of the most evident. Saboteurs typically operate swiftly and locally, delivering targeted strikes on military facilities, critical infrastructure, and transportation routes. The destruction of bridges, railway hubs, ammunition depots, and logistics centers often results in delays in the delivery of equipment and supplies to the front lines, significantly affecting combat operations. For example, the destruction of the Kakhovka Hydroelectric Power Plant in June 2023 caused widespread flooding and infrastructure damage, which, according to the Security Service of Ukraine (SBU), bears all the hallmarks of sabotage.

A particular threat is posed by SRG activities aimed at eliminating command personnel and air defense units. Successful attacks on command posts and communication hubs significantly complicate troop command and coordination on the battlefield. In addition, saboteurs frequently install minefields and use explosive devices in rear areas, creating serious risks for military convoys and civilian transportation [9].

Information warfare remains a critical tool in the activities of sabotage and reconnaissance groups (SRGs). The spread of fake news, hacking of official websites, and incitement of panic via social media are all tactics used to undermine the morale of both military personnel and the civilian population. Saboteurs often disseminate disinformation about alleged successes of Russian forces, casualties among the Armed Forces of Ukraine's (AFU) leadership, or supposed betrayal by certain Ukrainian units. These attacks are designed to weaken fighting spirit and create a sense of chaos in the rear. In 2023, a series of cyberattacks on government institutions was recorded, during which malicious actors gained access to personal data of servicemembers and sensitive logistics information related to the AFU.

The social impact of SRG activity is also extremely dangerous. The spread of panic and mistrust toward the government can lead to mass unrest and acts of civil disobedience. For example, in frontline regions, there have been instances of mass protests which, according to the Security Service of Ukraine (SBU), were coordinated through enemy agent networks. Saboteurs actively use social media to coordinate their actions and mobilize the population for anti-government demonstrations.

SRG activities also cause significant economic damage. The sabotage of energy facilities and transportation infrastructure leads to the shutdown of enterprises, disruption of logistics chains, and interruptions in the supply of food and military equipment. Strikes on energy infrastructure in the Kharkiv and Zaporizhzhia regions resulted in prolonged power and water outages. In addition, attacks on fuel depots and storage facilities in the Sumy and Chernihiv regions caused fuel shortages in frontline areas, complicating the movement of equipment and the supply of frontline units.

The combination of these threats highlights the multidimensional nature of SRG activity. It is not only a physical threat to military facilities and infrastructure but also a large-scale source of informational and psychological pressure on society. SRGs operate at the intersection of military, informational, and economic domains, exploiting vulnerabilities in the national security system to inflict maximum damage with minimal resources.

The absence of a unified response center and shortcomings in coordination among the Armed Forces of Ukraine (AFU), the Security Service of Ukraine (SBU), and the National Guard often lead to delays and ineffective actions in the event of a sabotage threat. In addition, insufficient legal regulation of SRG-related activities in national legislation complicates the legal classification of such actions and the determination of liability for those involved.

The activities of sabotage and reconnaissance groups (SRGs) constitute a systemic threat to Ukraine's national security. This threat encompasses physical, informational, social, and economic dimensions, requiring a comprehensive approach to the detection and neutralization of such groups. Achieving this demands a clear legal framework, effective coordination among security agencies, and modern technical means for monitoring and response.

Legal Challenges in Countering Sabotage and Reconnaissance Groups (SRGs). One of the biggest legal challenges in Ukraine is the absence of a clear definition of the term "sabotage and reconnaissance group" (SRG). The Law of Ukraine "On Combating Terrorism" (No. 638-IV dated 20.03.2003) defines terrorist acts as "threats or use of violence for political or ideological purposes," but the activities of SRGs often go beyond this definition. Sabotage and reconnaissance groups perform more complex tasks, combining reconnaissance, subversive activities, intelligence gathering on troop deployments, and even information attacks. This creates legal ambiguity,

causing SRG actions to often be classified as "treason" or "illegal armed activity," which significantly complicates the legal prosecution of saboteurs and members of their agent networks.

In many cases, individuals detained for participation in sabotage and reconnaissance groups (SRGs) are charged under articles of the Criminal Code of Ukraine that do not accurately reflect the nature of their activities. For example, members of a sabotage group uncovered in the Kharkiv region in 2022 were charged with treason, although their activities focused on gathering intelligence for artillery targeting and organizing sabotage on logistics facilities. The absence of a specific legal mechanism to combat SRGs leads to detainees often avoiding maximum penalties due to gaps in crime classification.

The insufficient adaptation of legislation to modern hybrid threats only exacerbates this problem. Contemporary warfare has long surpassed traditional combat operations—SRG activities now include information operations, cyberattacks, creating social tension, and economic disruption. Ukrainian legislation still relies on the classical definition of terrorism as an act of violence. The lack of legal tools to combat hybrid threats creates significant difficulties in responding to such attacks. For example, the Law of Ukraine "On National Security of Ukraine" (No. 2469-VIII dated 21.06.2018) recognizes the information and cyber domains as key elements of national security but contains no provisions addressing countermeasures against agent networks and information attacks coordinated by SRGs [10; 11].

Another serious issue lies in the gaps regarding the delineation of authority among security agencies in countering sabotage and reconnaissance groups (SRGs). The Law of Ukraine "On Combating Terrorism" designates the Security Service of Ukraine (SBU), Armed Forces of Ukraine (AFU), Ministry of Internal Affairs (MIA), State Border Guard Service, and National Guard as the main actors in counterterrorism. However, there is no clear division of responsibilities specifically concerning SRG counteractions. For example, while the SBU is responsible for counterintelligence and detecting agent networks, the elimination of saboteurs during combat operations remains within the competence of the AFU and the National Guard. This creates conflicts within the command chain, complicating the making of timely operational decisions in crisis situations.

In 2022, in the Kharkiv region, an incident was recorded involving the detection of an SRG engaged in artillery targeting. However, the agent network supplying the saboteurs with information remained undisclosed due to a lack of coordination between military structures and the Security Service of Ukraine (SBU). This is a direct consequence of legal gaps in regulating the actions of security agencies in the fight against SRGs.

The activities of sabotage and reconnaissance groups (SRGs) are partially regulated through existing counterterrorism measures but lack a dedicated legal framework. In 2022, the National Security and Defense Council of Ukraine (NSDC) initiated the development of the Law "On Countering Sabotage and Reconnaissance Groups," but as of 2025, this draft law has yet to be adopted. The absence of this legislation creates a legal vacuum, causing security agencies to often operate based on internal orders and temporary directives, which limits the effectiveness and speed of response to threats posed by SRGs.

The issue of coordination between security agencies in countering sabotage and reconnaissance groups (SRGs) requires particular attention. In practice, the Anti-Terrorism Center under the Security Service of Ukraine (SBU) performs the coordination role among agencies, but due to the lack of clear procedures for information exchange and a unified response system, delays often occur in decision-making between military structures and the SBU. In cases of SRG infiltration into frontline areas, operational intelligence from military reconnaissance may not be transmitted to the SBU in a timely manner, reducing the effectiveness of counter-sabotage efforts.

Resolving this problem requires the establishment of a unified interagency command center under the direct leadership of the National Security and Defense Council of Ukraine (NSDC). This center would ensure coordination among the Armed Forces of Ukraine (AFU), SBU, National Guard, and Border Guard Service in countering SRGs. Such a command center should be granted authority to make operational decisions in real-time and provide direct communication links between units at the command level.

Therefore, to effectively counter sabotage and reconnaissance groups (SRGs), it is necessary to amend the legislation, develop a dedicated legal framework specifically addressing SRG countermeasures, clearly define the powers of security agencies, and establish a unified coordination system at the level of the National Security and Defense Council of Ukraine (NSDC).

Without systematic changes in the legal and organizational spheres, efforts to combat SRGs will remain fragmented and insufficiently effective.

Organizational Challenges in Countering Sabotage and Reconnaissance Groups (SRGs). Countering sabotage and reconnaissance groups (SRGs) requires a high level of coordination and responsiveness from security agencies. However, in practice, there are organizational challenges that significantly reduce the effectiveness of responses to SRG threats. Chief among these are the absence of a unified command center, weak cooperation between different agencies, and insufficient preparedness to act in critical situations.

One of the main problems lies in the absence of centralized management of operations to counter sabotage and reconnaissance groups (SRGs). The Law of Ukraine "On Combating Terrorism" assigns primary responsibility for coordinating counterterrorism measures to the Security Service of Ukraine (SBU) through the Anti-Terrorism Center. However, in practice, the SBU mainly performs counterintelligence functions and the detection of agent networks, while the physical elimination of SRGs and conducting clearance operations remain within the competence of the Armed Forces of Ukraine (AFU) and the National Guard of Ukraine.

Such a division of powers leads to conflicts of interest and duplication of tasks during actual combat operations. For example, in 2022, an SRG engaged in directing artillery fire at Ukrainian Armed Forces (AFU) positions in the Kharkiv region was neutralized by the National Guard. However, the Security Service of Ukraine (SBU) was unable to promptly access the captured equipment and communication devices because, legally, the operation was classified as a military action rather than a counterintelligence one. This situation highlights the absence of a mechanism for joint management of operations between different security agencies [12].

Another problem is the limited level of information exchange between the Security Service of Ukraine (SBU), the Armed Forces of Ukraine (AFU), and the National Guard of Ukraine (NGU). Operational data about saboteur movements, enemy group plans, and agent networks often remain within departmental circulation and are not shared in real-time between agencies. For example, in 2023, in the Donetsk region, Ukrainian forces intercepted a sabotage group planning to blow up a bridge over the Siverskyi Donets River. The military received information about the planned attack from local residents; however, due to the absence of an operational communication channel with the SBU, this information was not promptly transmitted to the Anti-Terrorism Center. This delay resulted in postponed decision-making and created a risk of mission failure.

Insufficient coordination also becomes evident in the process of operational response to threats in frontline zones. Special forces units (SBU, AFU, NGU) often operate independently, without clear information sharing or coordinated actions. In frontline areas, especially in urban environments, this can lead to "friendly fire" incidents, where units from different agencies lack effective interaction and situational awareness on the battlefield. A notable example occurred in Mariupol in early 2022. During the clearing of the city, a group of National Guard fighters engaged in a firefight with an SBU unit because both operated under different operational plans and lacked a unified coordination channel.

The absence of a unified command center for operations also affects the logistical support and technical assistance of security forces. During prolonged operations to detect and neutralize sabotage and reconnaissance groups (SRGs), units of the Armed Forces of Ukraine (AFU) and the National Guard (NGU) often face shortages of communication equipment, ammunition, and armored vehicles due to the lack of a single supply channel. Logistics units of the AFU are supplied through one system, while the NGU and Security Service of Ukraine (SBU) units are supplied through others, complicating coordination of deliveries and the rapid deployment of equipment to combat zones.

A separate issue is the lack of a unified database on the activities of sabotage and reconnaissance groups (SRGs) and agent networks. The Security Service of Ukraine (SBU) and the Armed Forces of Ukraine (AFU) maintain separate operational data systems that are not integrated into a single information network. This complicates the identification of saboteurs operating under the cover of civilian populations. For instance, in 2023, an SRG operated in the Kharkiv region for two months using forged documents. Military intelligence provided information to the AFU, but due to the lack of an operational communication link with the SBU, the group continued its activities until it was accidentally discovered during a checkpoint inspection.

Another significant problem remains the absence of a unified system for accounting and coordinating agent activities in rear areas. Sabotage and reconnaissance groups (SRGs) often receive support from local agents who provide shelter, information about movement routes, and logistical assistance. In practice, the Security Service of Ukraine (SBU) and military intelligence operate separately in this sphere, leading to duplicated efforts and a loss of a comprehensive picture of the operational environment.

In summary, the key organizational problems in countering sabotage and reconnaissance groups (SRGs) remain the absence of a unified command center, weak coordination between agencies, lack of an operational communication channel, and fragmented logistical support. To address these issues, it is necessary to establish a single interagency center under the leadership of the National Security and Defense Council (NSDC), which would ensure continuous information exchange, operational planning, and real-time coordination of actions among security agencies. Integrating databases between the Security Service of Ukraine (SBU), the Armed Forces of Ukraine (AFU), and the National Guard of Ukraine (NGU), creating a unified communication channel, and centralizing logistical support will significantly enhance the effectiveness of countering SRGs and enable rapid response to threats in frontline zones.

Improvement of the Legal and Organizational Framework for Countering Sabotage and Reconnaissance Groups (SRGs). Effective counteraction against sabotage and reconnaissance groups (SRGs) requires not only the improvement of operational and tactical training of security forces but also the establishment of a reliable legal and organizational foundation. Currently, the legal framework for countering SRGs remains fragmented and insufficiently adapted to the realities of modern hybrid warfare. The lack of a clear definition of SRGs, legal norms regarding the use of force, as well as weak coordination between agencies, significantly complicate the fight against saboteurs at the operational level.

First and foremost, it is necessary to amend the current legislation to provide a clear legal classification of the activities of sabotage and reconnaissance groups (SRGs). The Law of Ukraine "On Combating Terrorism" should include a definition of SRGs as organized groups acting under the direction of foreign states or non-state entities with the purpose of gathering intelligence, conducting sabotage, and destabilizing the internal situation in the country. Such a classification will enable clear determination of response mechanisms and the procedures for the use of force upon detection of SRGs.

In addition, it is advisable to enact a separate law titled “On Countering Sabotage and Reconnaissance Groups,” which should establish the procedures for detection, neutralization, and criminal liability of SRG members. The law should also provide a clear framework for coordination between the Armed Forces of Ukraine (AFU), the Security Service of Ukraine (SBU), and the National Guard of Ukraine (NGU) during counter-sabotage operations. It is important to define a legal mechanism for the use of force against SRGs that protects service members from risks of exceeding their authority or legal liability.

Besides legislative changes, it is necessary to establish a unified command center for countering sabotage and reconnaissance groups (SRGs). Currently, the Anti-Terrorist Center under the Security Service of Ukraine (SBU) primarily performs a coordinating function but does not possess direct operational authority to respond to threats in frontline areas. To ensure timely response to sabotage threats, it is advisable to create a Joint Counter-Sabotage Center (JCSC) under the direct leadership of the National Security and Defense Council of Ukraine (NSDC). The JCSC should have direct authority to coordinate operations among the Armed Forces of Ukraine (AFU), the SBU, the National Guard of Ukraine (NGU), and other security agencies, including territorial defense units and the State Border Guard Service.

The center must operate in real time, ensuring uninterrupted information exchange between agencies. To achieve this, it is necessary to create a unified electronic database on the activities of sabotage and reconnaissance groups (SRGs), agent networks, and intelligence on enemy operations. Integrating data from military intelligence, counterintelligence, and operational services will allow for identifying connections between agent networks, tracking the movements of saboteurs, and preventing future attacks on critical infrastructure.

Particular attention should be given to improving the system of operational response to SRG threats in frontline zones. Currently, the Armed Forces of Ukraine (AFU) and the National Guard operate in the combat zone based on their own operational directives, which often leads to uncoordinated actions. The establishment of a unified operational headquarters within the Joint

Counter-Sabotage Center (JCSC) will enable conducting comprehensive operations involving special forces, unmanned aerial vehicles (UAVs), and electronic warfare (EW) assets.

Special attention should be given to the legal regulation of the use of force during counter-sabotage operations in peacetime. Currently, the use of weapons against SRGs is governed by general rules on the lawful use of force, which creates legal uncertainty. To address this issue, it is necessary to adopt a regulatory act that will establish the procedure for the use of weapons and electronic warfare (EW) means in the event of detecting an SRG. This will allow servicemen to act within the law without the risk of prosecution for exceeding their authority.

In addition to legal reforms, it is necessary to strengthen the personnel support and material-technical base of the units involved in countering SRGs. This is especially true for special forces units (SBU, Armed Forces of Ukraine, National Guard), which play a key role in detecting and neutralizing SRGs. Enhancing the level of training and supplying modern communication equipment, night vision devices, and strike UAVs will significantly improve the effectiveness of combat operations against SRGs.

The informational component also requires improvement. SRGs often use social networks and messengers to coordinate their actions and recruit agents among the local population. To counter these threats, it is advisable to establish an information unit within the Joint Counter-Sabotage Center (JCSC), which would be responsible for detecting and blocking information channels related to SRG activities. Additionally, monitoring of suspicious financial transactions and online activities of suspected individuals should be implemented.

Thus, the improvement of the legal and organizational framework for countering sabotage and reconnaissance groups (SRGs) should include the adoption of a dedicated law on SRGs, the establishment of a unified operations management center under the National Security and Defense Council (NSDC), the enhancement of regulations regarding the use of force, and the strengthening of the material and technical support for security agencies. A comprehensive approach that combines legal, organizational, and technical measures will enable the creation of an effective counter-sabotage system and protect Ukraine's national security from threats posed by SRGs.

Conclusions and directions for future research. Analysis of current challenges in Ukraine's national security sphere demonstrates that the activities of sabotage and reconnaissance groups (SRGs) represent one of the greatest threats in the context of hybrid warfare. The identified issues in the legal and organizational support for combating SRGs require a systematic approach to their resolution at the levels of legislation, interagency coordination, and technical provision of security forces.

Among the key problems are legal uncertainty regarding the activities of sabotage and reconnaissance groups (SRGs), the lack of a unified coordination system between the Armed Forces of Ukraine (AFU), the Security Service of Ukraine (SBU), and the National Guard, as well as weak integration of information databases and communication channels. The absence of a clear legal framework for the use of force against SRGs during peacetime also complicates the response to threats in frontline areas.

To improve the legal framework, it is necessary to amend the Law of Ukraine "On Combating Terrorism" by establishing a clear definition of sabotage and reconnaissance groups (SRGs) and mechanisms for holding individuals accountable for participation in their activities. The adoption of a separate law "On Countering Sabotage and Reconnaissance Groups" will regulate the use of force and coordination between agencies during counter-sabotage operations.

In the field of organizing counter-sabotage efforts, it is necessary to establish a Joint Counter-Sabotage Center (JCSC) under the leadership of the National Security and Defense Council of Ukraine (NSDC). The center should ensure the operational exchange of information between agencies, integration of databases, and centralized management of operations to detect and neutralize sabotage and reconnaissance groups (SRGs) in frontline zones.

Special attention should be given to the technical support of special forces units, including electronic warfare systems, unmanned aerial vehicles (UAVs), and modern communication systems. Strengthening intelligence operations and improving methods of informational counteraction will enable more effective detection of enemy agent networks and disruption of sabotage and reconnaissance groups (SRGs) activities at the preparatory stage of their operations.

Thus, effective counteraction against sabotage and reconnaissance groups (SRGs) requires a comprehensive approach that combines legal

regulation, organizational coordination, and technological support of security forces. Implementing these measures will enhance Ukraine's national security and ensure prompt response to SRG threats both in the combat zone and rear areas.

References

1. UKRINFORM. Vasyl Maliuk: SBU vykryla 11 ahenturnykh merezh z pochatku 2024 roku [The Security Service of Ukraine uncovered 11 agent networks since the beginning of 2024]. Retrieved from: https://surl.lu/ksuhob (accessed 03 January 2024) [in Ukrainian].

2. Zakon Ukrainy: "Pro borotbu z teroryzmom" No 638-IV vid 20 March 2003 [Law of Ukraine "On Combating Terrorism" activity 2003, March 20 No. 638-IV]. Retrieved from: https://surl.li/wblayc (accessed 5 January 2025) [in Ukrainian].

3. Borovyk M. O. (2024). *Protydiia dyversiino-rozviduvalnym hrupam protyvnyka pidrozdilamy Natsionalnoi politsii Ukrainy v umovakh voiennoho stanu* [Countering enemy sabotage and reconnaissance groups by units of the National Police of Ukraine under martial law]. *Naukovyi visnyk Lvivskoho derzhavnoho universytetu vnutrishnikh sprav.* No 2. pp. 45–58 [in Ukrainian].

4. Trembovetskyi O. H., Hulevatyi D. Yu. (2018). *Metodyka roboty shtabu prykordonnoho zahonu shchodo poshuku i likvidatsii dyversiino-rozviduvalnykh hrup protyvnyka* [Methodology of border guard headquarters operations for detecting and eliminating enemy sabotage and reconnaissance groups]. *Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrain.* No 4. pp. 119–127 [in Ukrainian].

5. *Operatsiia "Resolute Support" v Afhanistani: dosvid borotby z dyversiino-rozviduvalnymy hrupamy* [Operation "Resolute Support" in Afghanistan: Experience in countering sabotage and reconnaissance groups]. Retrieved from: nato.int. (accessed 03 January 2025) [in Ukrainian].

6. Sukhodolia O. M., Bobro D. H., Ivaniuta S. P., Kondratov S. I. (2019). *Orhanizatsiini ta pravovi aspekty zabezpechennia bezpeky i stiikosti krytychnoi infrastruktury Ukrainy* [Organizational and legal aspects of ensuring the security and resilience of Ukraine's critical infrastructure] analit. dop. Kyiv : NISD 224 p. [in Ukrainian].

7. Mykhalchyshyn Yu. (2021). *Kontrrozvidka v Ukraini vid UNR do sohodennia* [Counterintelligence in Ukraine from the UNR to the present day]. Lviv : SPOLOM. 79 p. [in Ukrainian].

8. *TSN. Diialnist rozvidnykiv-dyversantiv boiovykiv posylylasia odrazu na kilkokh napriamkakh* [The activities of the militants' reconnaissance and sabotage units have intensified in several areas at once]. Retrieved from: https://surl.lu/veulwz (accessed 03 January 2025) [in Ukrainian].

9. *MVS. Hvardiitsi pokrashchuvaly navychky protydii dyversiino-rozviduvalnym hrupam* [Guardsmen improved their skills in countering sabotage and reconnaissance groups]. Retrieved from: https://surl.li/arvjys (accessed 03 January 2025) [in Ukrainian].

10. Zakon Ukrainy: "Pro natsionalnu bezpeku Ukrainy" No 2469-VIII vid 21.06.2018 [Law of Ukraine "On the National Security of Ukraine" activity 2018, June 21 No 2469-VIII]. Retrieved from: https://surl.li/cwtnnx (accessed 5 January 2025) [in Ukrainian].

11. Chaika Ye. S. (2024). *Normatyvno-pravove rehuliuvannia kontrrozviduvalnoho zabezpechennia v Ukraini* [Regulatory and legal regulation of counterintelligence support in Ukraine]. *Akademichni vizii*. No 29. DOI: https://doi.org/10.5281/zenodo.10874942.

12. Viter D., Tsevelov O., Bezbakh V. (2021). *Robota shtabu orhanu okhorony kordonu pid chas orhanizatsii protydii dyversiino-rozviduvalnym hrupam* [The work of the border guard headquarters during the organization of counteraction to sabotage and reconnaissance groups]. Zbirnyk naukovykh prats Tsentru voienno-stratehichnykh doslidzhen Natsionalnoho universytete oborony Ukrainy. No 3(73), pp. 53–59.

Received: 08.04.2025
Revised: 16.04.2025
Accepted: 26.04.2025