



YAKHNO IHOR

Adjunct,

Kyiv Institute of the National Guard of Ukraine

<https://orcid.org/0009-0006-0046-7163>



PAVLOV DMYTRII

Candidate of Military Sciences, Senior Researcher,

Professor of the Department of State Security,

Kyiv Institute of the National Guard of Ukraine

<https://orcid.org/0000-0002-4586-6399>

OPPORTUNITIES AND PROBLEMS OF USING RADIO-ELECTRONIC INTELLIGENCE WHEN PERFORMING TASKS IN ENSURING PUBLIC SAFETY AND PROTECTION OF OBJECTS

The possibilities and challenges of using electronic intelligence to ensure public safety and protect important government facilities amid increasing non-military threats have been explored. Recent trends in the spread of drones and remote-controlled explosive devices operating via radio communication channels have also been considered.

The goal is highlighted – exploring the possibilities and identifying the problematic issues of using electronic intelligence in ensuring the implementation of state security measures, such as: ensuring public safety and protecting important facilities in situations involving threats related to the spread of unmanned systems and remote-controlled explosive devices that operate using radio communication channels, as well as substantiating ways to improve the effectiveness of electronic intelligence to create situational awareness for the leadership.

The capabilities of electronic intelligence for detecting, recognizing, identifying, and tracking unmanned systems and radio-controlled explosive devices based on evaluating radio signal parameters have been analyzed. The role of electronic intelligence in building situational awareness for leadership has been determined.

The main problematic issues of a technical, organizational, and legal nature related to the use of electronic intelligence in the field of public safety have been considered. The need to integrate electronic intelligence tools with other surveillance systems, as well as to create a unified information space, has been substantiated.

Keywords: *state security; electronic intelligence; public safety; protection of especially important state facilities; protection of state power facilities; detection of radio-controlled devices.*

Problem Statement. Under contemporary conditions of the development of information and communication technologies and the widespread availability of technical means for remote control, there is a significant transformation in the nature of threats to public security (PS) and to important objects subject to protection, especially particularly important state objects, state authorities, and critical infrastructure facilities.

Current trends include:

- the proliferation of the use of radio-controlled unmanned systems (UAS), primarily unmanned aerial vehicles (UAVs);
- the steady increase in the number and types of explosive devices (EDs), the control or initiation of

which is carried out using radio communication channels.

The availability of commercial unmanned platforms, radio signal transmission means, and software-hardware means for remote control significantly increases the likelihood of their use not only for civilian purposes but also for unlawful ones.

These technical means may be used to conduct reconnaissance of important protected objects, deliver dangerous items, remotely detonate EDs, or perform other actions that pose a threat to the lives and health of citizens and the functioning of important protected objects. The use of radio communication channels to transmit control signals or initiate the detonation of EDs makes their



timely detection by traditional security measures more difficult, since radio signals can be transmitted across different frequency ranges and using different communication protocols.

In this regard, ensuring the timely detection, identification, recognition, and tracking of UAVs and remote control means of EDs that operate using radio communication channels becomes particularly relevant when protecting important objects, ensuring PS, preventing offences, preserving the life and health of citizens of Ukraine, etc. This will make it possible to establish sources of radio control in time with the aid of appropriate technical means, carry out their neutralisation, and take the necessary measures to protect the population and objects under protection.

The task of identifying the sources of radio control of technical means is achieved by analysing the radioelectronic environment, through continuous searching for and detecting their radio signals, i.e., conducting Signals Intelligence (SIGINT), the systematic collection, processing, analysis, and substantiation of information about the functioning of sources of radio emissions.

At the same time, analysis of the practice of performing such tasks indicates that, to date, there are a number of unresolved issues, namely:

- a shortage of scientifically grounded approaches to organising the search for, detection, recognition, identification, and tracking of UAVs and remote control means of EDs operating using radio communication channels under conditions of a complex radioelectronic environment;

- insufficiently studied issues related to integrating SIGINT means with technical surveillance systems of important protected objects, followed by the formation of a single information space to ensure an appropriate level of situational awareness of command personnel;

- the need to clarify organisational and staffing decisions regarding the use of SIGINT units in the interests of ensuring PS, and the methods of their interaction with other components of the security sector;

- the lack of agreed approaches to assessing the effectiveness of using SIGINT means, and the criteria for their performance in the specified field limits the possibilities for their practical use.

Thus, existing gaps in theoretical development, methodological support, and practical approaches to SIGINT use necessitate further research in this area, thereby substantiating the relevance of the article's topic and defining its purpose.

Analysis of recent research and publications.

The issues of detecting and countering threats

associated with the use of UAS and the remote control of explosive devices operating via radio communication channels have, in recent years, been actively studied in scientific works by both foreign and domestic scholars. In particular, current scientific studies have demonstrated the effectiveness of passive radio-frequency monitoring methods for detecting and identifying unmanned aerial vehicles using signal parameters of their control channels [1–3].

In works [1, 2], the feasibility of using machine learning methods for classifying UAV radio signals is demonstrated, thereby enabling higher recognition accuracy even under jamming conditions. Article [3] examines approaches to passive detection, tracking, and countering UAVs using radio-frequency sensors.

At the same time, it should be noted that similar principles can also be applied to detecting means of remote control of explosive devices that use standard or specialized radio communication channels for control. This necessitates expanding the functional capabilities of SIGINT systems to monitor the radio-frequency spectrum in order to detect potentially dangerous signals in a timely manner.

Domestic scientific works place significant emphasis on the development and application of SIGINT and radioelectronic monitoring means. In particular, in the work by I. Maiboroda, K. Vlasov, M. Hlushchenko [4], the capabilities and prospects of developing mobile SIGINT assets are considered, and their role in ensuring timely acquisition of information about the radioelectronic environment is defined.

In the article by S. P. Leshchenko, A. A. Adamenko, V. A. Lupandina, G. V. Mehelbei [5], approaches to building information support systems for countering UAVs are substantiated based on the integrated use of radiotechnical reconnaissance and electronic warfare means, which directly affects the formation of situational awareness of command personnel.

In addition, in the work by S. A. Shabeti [6], the use of radioelectronic monitoring tools in conditions of information confrontation is considered, particularly with respect to detecting and analyzing radio signals as sources of information about potential threats.

Thus, the results of the studies presented indicate that the application of SIGINT means creates prerequisites for improving the level of situational awareness of command personnel through the timely detection, recognition, and

tracking of UAVs and means of remote control of explosive devices operating using radio communication channels.

At the same time, analysis of scientific research shows that the issue of applying SIGINT capabilities to implement measures of state security—namely, directly in the interests of ensuring PS and protecting important objects – has been insufficiently addressed. Most scientific works are devoted to its use in the military sphere, whereas problems of adapting the relevant technologies to the needs of law-enforcement activity and security systems for important objects remain insufficiently studied. This necessitates further scientific research into the feasibility of using SIGINT to detect and identify technical means that use radio communication channels, in the interests of ensuring PS and protecting important objects, as well as to identify problematic issues related to implementing such means in the specified field of activity.

In addition, further scientific elaboration is required regarding the integration of SIGINT means with other surveillance systems, the organization of effective information support, and maintaining an appropriate level of situational awareness of command personnel, as well as considering legal aspects of using SIGINT means. This necessitates conducting comprehensive research in this direction.

Statement of the Task. The purpose of the article is to study the capabilities and identify problematic issues of using SIGINT in the interests of ensuring PS and protecting important objects under conditions of the proliferation of threats associated with the use of UAVs and means of remote control of explosive devices operating using radio communication channels, as well as to substantiate the directions for improving the effectiveness of using SIGINT for forming situational awareness of command personnel.

Presentation of the Main Material. Trends in the application of UAVs and means of remote control of explosive devices operating using radio communication channels have become widespread due to the availability of component-based solutions, the development of wireless communication technologies, and the ability to adapt them to various application scenarios.

As a rule, for control, open or semi-closed radio communication channels are used (GSM (English Global System for Mobile Communications, global system for mobile communications), Wi-Fi (English Wireless Fidelity, wireless local area communication technology), ISM (English

Industrial, Scientific, and Medical, parts of the radio-frequency spectrum intended for industrial, scientific, and medical use rather than telecommunications), LTE (English Long Term Evolution) / 5G (English 5th Generation, mobile communication standards), etc.), which makes it possible for them to be detected by SIGINT means [1–3].

This necessitates developing and implementing effective approaches to detecting, recognising, identifying, and tracking such means in real time; this makes SIGINT an important tool for these tasks, enabling the acquisition of information about radio emission parameters, the determination of signal source locations, and classification.

In view of this, it is expedient to consider the features of the radioelectronic environment in which the specified means operate, as well as the characteristic signal features that can be used to detect them.

1. Features of the Radioelectronic Environment and Signal Features of UAVs and Means of Remote Control of Explosive Devices Operating Using Radio Communication Channels.

The radioelectronic environment of modern facilities is characterised by a high density of signals of various purposes, which creates complex conditions for detecting potentially dangerous sources of radio emissions. Under such conditions, special importance is placed on isolating the signal features of radio signals inherent to UAVs and to remote control of explosive devices operating over radio communication channels.

The main features that can be used to identify UAVs and means of remote control of explosive devices operating using radio communication channels include:

- characteristic frequency ranges of operation of the specified technical means (e.g., 2.4 GHz, 5.8 GHz);
- the structure of the radio signal (type of modulation, bandwidth, etc.);
- time parameters of radio signal transmission;
- features of data exchange protocols between the operator (a likely malicious actor) and the UAV, explosive device remote control means, etc.

Studies show that combining radio-frequency signal analysis with machine learning algorithms increases the probability of identifying emission sources and determining their UAV origin [1, 2]. This is especially relevant in conditions where signal masking is deliberately employed or where civilian communication standards are used.

2. Capabilities of SIGINT in Detecting and Tracking Radio Emission Sources.

Based on consideration of the features of the radioelectronic environment, the practical capabilities of SIGINT for detecting and tracking radio emission sources are defined.

SIGINT ensures the implementation of a set of functions important for exposing modern UAVs and means of remote control of explosive devices operating using radio communication channels:

- detecting the presence of radio emission from potentially dangerous radio emission sources;
- determining the parameters of radio signals of potentially dangerous radio emission sources with subsequent identification;
- direction finding of radio emission sources;
- tracking radio emission sources in dynamics;
- generating information for making managerial decisions.

The use of passive SIGINT means enables covert surveillance without creating additional electromagnetic load, which is an important factor in ensuring PS. In addition, such means can be effectively used to detect both UAVs and remote-controlled explosive devices, since both types of potentially dangerous technical means rely on radio channels [3].

Ukrainian researchers also emphasise the importance of using mobile SIGINT complexes, which provide flexibility and prompt response to changes in the radioelectronic and operational situation, including changes in radio-frequency environment parameters, the appearance of new radio emission sources, the movement of UAVs, and activating means of remote control of explosive devices [4]. This is especially relevant for protecting facilities with a large territory or complex configuration.

3. The Role of SIGINT in Forming Situational Awareness of Command Personnel.

The results of SIGINT operations acquire practical value only if they are effectively used in the command and control of forces and assets involved in protecting important objects and ensuring PS. The effectiveness of threat countermeasures depends significantly on command personnel's situational awareness. In this context, SIGINT is one of the sources of information on the current situation.

Situational awareness involves command personnel having a holistic understanding of the current situation, including existing threats, their characteristics, and the possible development of events. The data obtained through SIGINT makes it possible to:

- timely detection of real and potential threats from potentially dangerous radiotechnical means;

- assess the nature and level of danger posed by potentially dangerous radiotechnical means;
- forecast the development of the situation regarding their probable use;
- make well-founded command decisions.

As noted in [5], integration of SIGINT data with other information sources (video surveillance, radar, security systems) makes it possible to form a single information space, which significantly increases the effectiveness of command and control of forces and assets involved in performing tasks for protecting important objects and ensuring PS when carrying out tasks to protect against real and potential non-military threats.

Thus, SIGINT plays a key role in providing information support for command and control and in enhancing situational awareness.

4. Problematic Issues of Using SIGINT.

Despite its significant potential, the use of SIGINT to ensure PS and protect important objects is hampered by several problematic issues that limit its effectiveness.

The main ones of these include:

Technical problems:

- difficulty in detecting signals in a dense radio-frequency environment in urban environments and areas of active use of wireless technologies (Wi-Fi, LTE, /5G, etc.), a high level of electromagnetic noise and mutual interference is formed. This makes it difficult to isolate radio emission sources (in particular, weak or short-duration ones), reduces the probability of their detection, and increases the risk of erroneous classification.

- the need to process large volumes of data in real time-SIGINT means carrying out continuous wideband monitoring, generating significant data streams (spectral snapshots, IQ samples (In-phase/Quadrature—representation of a signal in two components), signal signatures). Analysing them requires high-performance computing resources and effective algorithms (filtering, detection, classification); otherwise, delays arise, which critically affect the timeliness of response.

- limited accuracy in determining the coordinates of radio emission sources in conditions of dense urban development – dense construction causes multipath propagation, signal reflections, and signal shadowing. This leads to errors in direction-finding methods, causes shifts in coordinate estimates, and reduces the reliability of localisation, especially for low-power or moving sources.

Organisational problems:

- lack of unified approaches to integrating heterogeneous surveillance systems—different

systems (SIGINT, video surveillance, sensor networks, etc.) are often built on the basis of incompatible standards and protocols. This complicates data exchange, their harmonisation, and the formation of a single picture of the situation, which reduces the effectiveness of management and action coordination.

- possible insufficient number of personnel in the SIGINT direction and an insufficient level of their professional training – the limited number of specialists with the necessary knowledge (radiotechnology, signal processing, analytics) leads to an overload of available personnel. An insufficient level of training or the absence of systematic training reduces the quality of data analysis and the effectiveness of using SIGINT means.

- limitations of resources for deploying modern SIGINT systems – the high cost of equipment, software, and its maintenance limits the ability to implement modern complexes. Additional impacts come from modernisation costs of infrastructure, personnel training, and supporting the continuous operation of the systems.

Legal problems:

- lack of a regulatory framework regarding the use of SIGINT in carrying out measures to ensure public security and when protecting important state facilities;

- the need to comply with requirements for protecting information and confidentiality – during SIGINT activities, data may be obtained that contains personal or official information. This requires strict compliance with information protection legislation to prevent unauthorised access, data leakage, and violations of citizens' rights.

As emphasised in [6], solving these problems requires a comprehensive approach that includes improving the regulatory and legal framework, developing technical means, and training specialists.

Conclusions and Prospects for Further Research. As a result of the conducted analysis, it has been established that the rapid growth in the availability of unmanned technologies and radio-control means increases the level of threats to protected objects and to public security overall. The use of such means is characterised by high mobility, covert operation, and the possibility of using standard radio communication channels, which significantly complicates their timely detection by traditional means.

It is substantiated that one of the most effective tools for detecting and countering such means is signal intelligence (SIGINT), which ensures:

- detection of control signals of unmanned systems and means of remote control of explosive devices that operate using radio communication channels;

- recognition of signal types (analogue/digital, communication protocols, modulation characteristics, etc.), which subsequently enables the identification of emission sources (operators of unmanned systems, relays, explosive-device radio channels, etc.) and tracking of targets through continuous monitoring of signal parameters (frequency, power, direction, time characteristics).

The use of signal intelligence means makes it possible to:

- carry out continuous monitoring of the radio-frequency spectrum within defined zones;

- determine key signal parameters (frequency, bandwidth, modulation type, protocol identifiers) and establish the location of radio emission sources using direction-finding methods, ensuring early detection of unmanned systems and radio-controlled explosive devices; reduce the response time to probable threats from radio-controlled devices.

The use of signal intelligence also increases situational awareness by forming an up-to-date picture of the radioelectronic environment.

- allows integration of data with video surveillance, radar, unmanned system detectors, creating a single information space.

At the same time, a number of problematic issues accompanying the use of signal intelligence in the specified field have been identified, in particular, technical, organisational, and legal limitations.

Further research should be aimed at:

- determining the conditions and factors that affect the effectiveness of fulfilling service-combat tasks by signal intelligence units;

- developing a set of indicators (criteria) for evaluating the effectiveness of fulfilling the tasks of conducting signal intelligence.

References

1. Tekin, K., Yavuz, A. G. (2021). Drone detection using machine learning methods based on RF signals. *IEEE Access*, no. 9, pp. 77165–77181. DOI: <https://doi.org/10.1109/ACCESS.2021.3082531> [in English].
2. Aydin, B., Selvi, E., & Ozdemir, M. F. (2020). Deep learning-based UAV detection using

RF signals. *IEEE Communications Letters*, no. 24 (9), pp. 2019–2023. DOI: <https://doi.org/10.1109/LCOMM.2020.3001844> [in English].

3. Guvenc, I., Koohifar, F., Singh, S., Sichitiu, M. L., & Matolak, D. W. (2018). Detection, tracking, and interdiction for amateur drones. *IEEE Communications Magazine*, no. 56 (4), pp. 75–81. DOI: <https://doi.org/10.1109/MCOM.2018.1700455> [in English].

4. Maiboroda I., Vlasov K., Hlushchenko M. (2024). Application and development prospects of mobile radioelectronic intelligence means of tactical link of the sector of security and defence forces of Ukraine. *Chest i zakon*, no. 2 (89), pp. 83–84 [in English].

5. Leshchenko S. P., Adamenko A. A., Lupandin V. A., Mehelbei H. V. (2022). *Systema*

informatsiinoho zabezpechennia protydii bezpilotnym litalnym aparatom protyvnyka pry kompleksnomu zastosuvanni zasobiv radioelektronnoi borotby [Information support system for countering enemy unmanned aerial vehicles with the integrated use of electronic warfare equipment]. *Litalni aparaty: aerodynamika, sylovi ustanovky, obladnannia, ozbroiennia ta zastosuvannia*, no. 73, pp. 31–36 [in Ukrainian].

6. Shabetia S. A. (2024). *Radioelektronni zasoby monitorynhu v umovakh informatsiinoi viiny* [Radio-electronic monitoring means in the conditions of information warfare]. *Akademichni vizii*, no. 44. Retrieved from: <https://surl.li/tgwexi> (accessed 6 March 2026) [in Ukrainian].

Стаття надійшла до редакції / Received: 14.04.2026

Прорецензовано та прийнято до друку / Reviewed and accepted for publication: 20.05.2026

Опубліковано / Published: 30.06.2026

ЯХНО ІГОР ЮРІЙОВИЧ

ад'юнкта,

Київський інститут Національної гвардії України

<https://orcid.org/0009-0006-0046-7163>

ПАВЛОВ ДМИТРІЙ ВАДИМОВИЧ

кандидат військових наук, старший науковий співробітник,

професор кафедри забезпечення державної безпеки,

Київський інститут Національної гвардії України

<https://orcid.org/0000-0002-4586-6399>

МОЖЛИВОСТІ ТА ПРОБЛЕМНІ ПИТАННЯ ЗАСТОСУВАННЯ РАДІОЕЛЕКТРОННОЇ РОЗВІДКИ ПІД ЧАС ВИКОНАННЯ ЗАВДАНЬ ІЗ ЗАБЕЗПЕЧЕННЯ ГРОМАДСЬКОЇ БЕЗПЕКИ ТА ОХОРОНИ ОБ'ЄКТІВ

Досліджено можливості та проблемні питання застосування радіоелектронної розвідки для забезпечення громадської безпеки й охорони важливих державних об'єктів в умовах зростання загроз невоєнного характеру. Розглянуто сучасні тенденції поширення безпілотних систем і засобів дистанційного керування вибуховими пристроями, що функціонують із використанням каналів радіозв'язку.

Проаналізовано можливості радіоелектронної розвідки щодо виявлення, розпізнавання, ідентифікації та супроводження безпілотних систем і радіокерованих вибухових пристроїв на підставі оцінювання параметрів радіосигналів. Визначено роль радіоелектронної розвідки у формуванні ситуаційної обізнаності керівного складу.

Висвітлено основні проблемні питання технічного, організаційного та правового характеру, пов'язані із застосуванням радіоелектронної розвідки у сфері забезпечення громадської безпеки. Обґрунтовано необхідність інтеграції засобів радіоелектронної розвідки з іншими системами спостереження, а також створення єдиного інформаційного простору.

Ключові слова: *державна безпека; радіоелектронна розвідка; громадська безпека; охорона особливо важливих державних об'єктів; охорона об'єктів державної влади; виявлення радіокерованих засобів.*