UDC 356/358

I. Maiboroda

K. Vlasov

M. Hlushchenko

APPLICATION AND DEVELOPMENT PROSPECTS OF MOBILE RADIOELECTRONIC INTELLEGENCE MEANS OF TACTICAL LINK OF THE SECTOR OF SECURITY AND DEFENCE FORCES OF UKRAINE

The purpose of the article is to assess the capabilities of mobile electronic intelligence means of the tactical link of the sector of security and defence forces of Ukraine, to develop recommendations on the prospects for their development, to analyse the use of electronic intelligence systems and means of the russian federation army during the so-called "Special Military Operation" against Ukraine.

The capabilities of means of radio-electronic intelligence in service with the Armed Forces of Ukraine and the National Guard of Ukraine are presented. A comparative analysis of the tactical and technical characteristics of Ukrainian and foreign-made equipment is carried out, as well as a brief analysis of the radio-electronic warfare equipment of the aggressor country and the results of their use. On the basis of the analysis, recommendations are made on the prospects for the use and development of electronic intelligence means of the tactical link of the forces of the security and defence sector of Ukraine.

Keywords: *electronic warfare, radio-electronic intelligence means, direction-finding systems and complexes.*

Statement of the problem. Any modem army in the world that claims to be effective on the battlefield in future must take into account the development of electronic warfare (EW), i.e. flexibly change its doctrine, structure, methods of training and recruitment. This is also driven by new military technologies, the importance of which is constantly growing, because every weapon system depends on interacting sensors, and without them it loses its effectiveness. Accordingly, this development leads to an increase in the effectiveness of certain types of weapons or military equipment in general [1].

In a high-tech battlefield and with the widespread use of digital technologies, traditional military power does not solve everything. Very often, disabling or suppressing the enemy's electronics, communications and control equipment is enough to disarm them, but it requires timely and accurate detection. These are the tasks assigned to one of the main components of electronic warfare (EW) – radio-electronic intelligence (signals intelligence (SIGINT)), which, in turn, is divided into strategic SIGINT and tactical SIGINT. While strategic signals intelligence is mainly conducted during the period of preparation for war or strategic operations, tactical signals intelligence is conducted continuously and purposefully directly during hostilities.

Tactical radio-electronic intelligence (SIGINT) is considered to be one of the main types of information provision to troops by continuously tracking the electromagnetic radiation of numerous military devices and systems of the enemy for various purposes [2]. It provides important information for the conduct of hostilities by the sector of the security and defence forces of Ukraine. This information can be obtained in the tactical command and control level through the use of means of radio-electronic intelligence (SIGINT), the technical basis of which is the following: passive devices for searching, intercepting and analysing radio emissions and direction finding of electromagnetic radiation sources; active radar and laser surveillance, detection and recognition devices; optoelectronic devices and other devices for recording physical fields of objects.

Dominance in the electromagnetic space gives an advantage over the enemy in controlling troops and weapons. Electronic warfare and radio-

electronic intelligence [signals intelligence (SIGINT)], which are among the leading elements of current wars and armed conflicts and, not by chance, have perhaps the highest development of dynamics among all modern types of weapons, should help in this. Therefore, in the context of the war with the aggressor country, whose army still has both quantitative and qualitative superiority over the Ukrainian army, in particular in electronic warfare, the development of its own capabilities in this area is of particular importance for the Ukrainian security forces.

Analysis of recent research and publications. The experience of armed conflicts of recent decades, taking into account the experience of the Joint Forces Operation (ATO) in the East of Ukraine and the hostilities as a result of the armed aggression of the russian federation (rf) against Ukraine in February 2022 [3, 4, 5], convincingly demonstrates the significant role radio-electronic intelligence in achieving the goal of an armed conflict and in war in general. The success of solving the main tasks of operations is largely determined by the effectiveness of disorganising the enemy's command and control systems and weapons, as well as protecting their own troops (forces) and facilities from damage by all types of weapons.

Publications [4, 5, 6], which dealt with electronic warfare, highlighted the tactical and technical characteristics and combat capabilities of the russian aggressor country's electronic warfare and radio-electronic intelligence [signals intelligence (SIGINT)] systems. The analysis suggests that the enemy does indeed have modern high-tech electronic warfare systems and complexes in service, but, according to US military experts, the russian way of conducting warfare on the battlefield with the use of electronic means has some limitations that generally hindered their forces. Russian systems are mostly cumbersome and best suited for stationary positions, but not for the multidimensional mobile advance that russia launched in February 2022. For their part, Ukrainian troops also have modern electronic warfare and radio-electronic intelligence, both domestic and foreign, but certainly not in the same quantity as the enemy has. In addition, Ukroboronprom Enterprises are putting more effort into the design and production of mobile small-sized systems and complexes, which are most effective in the tactical link with rapidly changing battlefield conditions.

The purpose of the article is to assess the capabilities of mobile radio-electronic intelligence means of the tactical link of sector of security and defence forces of Ukraine, to develop recommendations on the prospects for their use and development, to analyse the use of electronic warfare systems and complexes of the russian army since the beginning of full-scale aggression against Ukraine.

Summary of the main material. Radio-electronic intelligence [signals intelligence (SIGINT)] is a type of technical intelligence aimed at obtaining intelligence about the enemy by intercepting and analysing the radiation of its electronic means using special technical devices [7].

According to the principles and means of intelligence used, radio-electronic intelligence [signals intelligence (SIGINT)] is divided into Communications Intelligence, COMMINT; Electronic Intelligence, ELINT; and Measurement and Signatures Intelligence, MASINT. There are also separate types of SIGINT that use certain technical means: Radar Intelligence, RADINT, Television Intelligence, TELINT, Infrared Sets Reconnassaince, Laser Sets Reconnassaince and some others [7].

In the interests of tactical SIGINT, communications intelligence and electronic intelligence are most often conducted. In general, in cases where there is no need to separate these two types of intelligence or to emphasise their unity, the term" radio-electronic intelligence" is simply used.

Communications Intelligence (COMMINT) is conducted by intercepting radio communication signals (telephony, telegraphy, etc.). The main task of communications intelligence is to obtain information by detecting and intercepting open, coded radio transmissions, direction finding the sources of radio signals and definition of their location, processing and analysing the intercepted information to reveal its content. Communications intelligence information about enemy stations, their construction systems and the content of transmitted messages makes it possible to determine the enemy's plans and intentions, the composition and location of its groups, to define the location of their headquarters and command and control points, the location of bases and launch sites for missile weapons, etc.

Electronic Intelligence (ELINT) is conducted using radio reception, direction finding and radio signal analysis methods to detect signals from radar, telemetry and telecommand systems of their technical analysis and binding (technical object recognition). The results of this type of passive reconnaissance make it possible to: establish the frequency of the transmitting radio receivers;

determine the coordinates of radiation sources; measure the parameters of the pulse signal (repetition rate, duration, and other parameters); establish the type of signal modulation (amplitude, frequency, phase, pulse); determine the structure of the side lobes of radio wave radiation; measure the polarisation of radio waves; set the antenna scanning speed and the method of radar survey of space; analyse and record information.

According to its content, all information obtained by these types of intelligence is divided into operational and technical. Operational information includes: open or encrypted semantic information transmitted by the opposing party through various radio channels; tactical and technical data and features of intelligence on active electronic systems (tuning frequency, type of modulation and manipulation, antenna patterns, radiation power, etc.), which constitute their "electronic signature"; types of electronic systems (radio communications, radar, radio navigation, missile guidance and early detection, various telemetry data transmission systems); number of detected enemy electronic systems; location and territorial density of enemy electromagnetic energy sources.

By studying the technical characteristics and features of the enemy's electronic systems, it is possible to determine their scope of application and affiliation. By comparing this data with the information already known to the intelligence community through other channels, it is possible to deduce the purpose of the detected equipment. Knowing this and determining the types and number of enemy electronic means, it is possible to establish the location of military units, military bases, airfields, and other facilities. For example, having data on the number of radars for guided anti-aircraft missiles in any enemy air defence zone, it is possible to draw correct conclusions about the number of anti-aircraft missile batteries installed in that zone.

Technical information contains information about new weapons systems and control of electronic devices, as well as their electrical characteristics, which are used for the first time by the intelligence community. The purpose of obtaining technical information is to timely develop equipment and methods of signals intelligence of new weapons systems and enemy control systems. According to American experts, technical information on new electronic equipment of potential adversaries is especially necessary for the creation of effective technical means and methods of radio countermeasures and counter-radio countermeasures.

Ukraine's security and defence forces have many electronic warfare and radio-electronic intelligence systems in service, both from the old fleet (inherited after the collapse of the USSR) and new ones designed and manufactured by Ukroboronprom Enterprises. Our country has every opportunity to develop its electronic warfare capabilities, as evidenced by the successful creation in a short time and adoption by the Armed Forces of Ukraine (AFU) of the Polonez mobile UAV countermeasures system, the Anklav electronic jammer (with a range of up to 40 km, and the frequency range of signal jamming is from 400 MHz to 2500 MHz), the highly mobile all-round radar MR-18, the counter-battery radar Biskvit-KB, and the 1L221E Zoopark-2 radar complex for reconnaissance of firing positions.

The leader in the development and production of domestic radio-electronic intelligence equipment is Infozakhyst Research and Production Centre Company. Among their latest developments, which are already working to defeat the aggressor, are the PLASTUN-RP3000 portable direction finder, the Arkhont and Khortytsia-M mobile radio monitoring systems, and the Khortytsia-R UAV countermeasures system.

The PLASTUN-RP3000 small-sized tactical direction-finding system (Figure 1) is designed for direction finding of enemy's communication systems, automated high-speed radio monitoring, processing and recording of intercept data. During the development, the Research and Production Centre's specialists improved the radio reconnaissance system, taking into account the experience of combat use of the previous system. In real time, the system exchanges data to coordinate information on the location of radio sources and their characteristics to form a single reconnaissance field.

Figure 1 – PLASTUN-RP3000 Radio-electronic Intelligence Complex

Due to the modularity, dimensions and significant energy autonomy of the PLASTUN-RP3000 complex (up to 8 hours of operation from standard batteries), high mobility of tactical radio reconnaissance groups is achieved. When folded, the complex can be placed in two backpacks (total weight up to 39 kg), which provides additional convenience and concealment during movement. This makes it possible to deploy the direction-finding system in the most favourable location and quickly collect the necessary intelligence. At the same time, the system does not require a special place for deployment and has a simple interface with touchscreen screens. It successfully detects radio networks and operating frequencies of the tactical (UKF), operational and tactical (KKH) links, communication and data transmission facilities of small sabotage and reconnaissance groups. The complex is capable of determining the location of communication stations with the UKF and the coordinates of the electronic warfare station. PLASTUN-RP3000 can also record digital control and information transmission channels, the location of aircraft and UAVs, detects the methods of data transmission of counter-battery means and implements synchronous direction-finding and demodulation of frequency-modulated signals [8].

Since 2016, the PLASTUN-RP3000 tactical radio reconnaissance system has been supplied to the Armed Forces of Ukraine and has already been used to counter modern electronic warfare equipment used by the russian occupation forces in Donbas. According to the scheme of application of the system (Figure 2), two PLASTUN-RP3000 semi-sets are designed for pair operation.

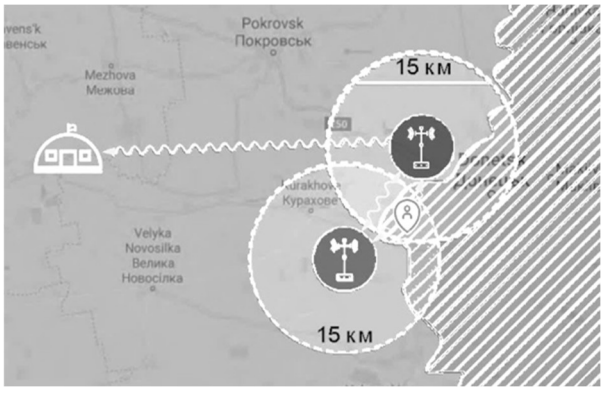

Figure 2 – Scheme of application of the complex SIGINT PLASTUN-RP3000

One of them is selected by the operator as the master, the other as the subordinate. The data from the subordinate half-set is transmitted via a radio channel or a local/Internet network to the master, where the coordinates are determined, the radio source is fixed on the map, and radio reconnaissance is carried out on a wide front. The operator chooses the type of connection between the two half-sets based on the specific situation. The operator performs a generalised analysis of the accumulated results. If a new radio source is detected, the operator can trace the history of activity at a certain frequency since the start of reconnaissance at that frequency.

The PLASTUN-RP3000-MN modification, which is supplemented with a 15 m high electromechanical mast, a multifunctional automated radio reconnaissance post and satellite communication kits, is the basis for the more powerful Arkhont system (Figure 3).

Figure 3 – Archon mobile radar station

This is a multifunctional mobile radio reconnaissance and direction-finding station for the KKH and UKF bands. It is designed to assess the electromagnetic environment, search, detect, rapidly analyse and determine the direction-finding (or coordinates when working in conjunction with a second station) of radio emissions. The complex is transported by a high-capacity passenger car towing a trailer with equipment. "The Arkhont is easy to use, provides confident direction finding of UKF signals and high performance in the military data communications range (25 MHz – 90 MHz), civilian bands (100 MHz – 500 MHz), and data communications bands (500 MHz – 3000 MHz).

The most powerful mobile radio and electronic intelligence vehicle in the Infozakhyst Research and Production Centre Company lineup is Khortytsia-M,

which is designed on a vehicle chassis with high cross-country ability and autonomy. It is capable of analysing radio signals, demodulating and decoding them, as well as automatically determining the coordinates of radio sources. The complex provides: decoding of civilian radio signals in DMR, DPMR, NDXN, FLEX, P25, A25, etc. standards; automatic determination of coordinates and spatial orientation of the complex's means; automated determination of coordinates of radio sources; establishment of a secure connection with similar communication complexes, wired connection or using a radio relay line of its own production. In addition, the system can combine its capabilities by working in conjunction with unmanned systems, for example, with a reconnaissance and strike system based on the DUCKY small reconnaissance unmanned aerial vehicle. In the case of joint use and application of unique algorithms, real-time verification of the data obtained from radio reconnaissance means with images from UAVs is achieved. This makes it possible to achieve a qualitatively new level of task performance.

In 2018, the National Guard of Ukraine (NGU) received tactical portable direction-finding systems made in the USA. The Tactical Portable Direction-Finding System TCI 903S-8 (Figure 4) is designed to search, detect, analyse signals from radio sources and determine their location in the tactical command and control chain.

Figure 4 – TCI 903S-8 direction finding system

The system allows detection and direction-finding of all signals from 20 MHz to 8000 MHz and 3 GHz/s fast scanning with simultaneous direction finding of all detected signals at a channel frequency of 25 kHz (DF First technology). The optional Universal Signal Detection (USD) makes it possible to create custom signal detectors without the need for programming [9].

The extremely easy-to-use interface with the BlackbirdNextGen Software enables capabilities such as: analysis and geolocation of several signals that have some interest from data collected in a dense signal environment; networked multi-site geolocation of emitters of interest; display of spectral and DF reports collected by the real-time system; LookbackCollection and analysis of signals of interest after the mission; generation of azimuth colour spectrograms, maps with sensor carrier beams and detection metadata displays.

The set in transport cases is designed to be transported to the point of deployment by vehicle, and in the field, it can be redeployed with a marching version by a tactical reconnaissance group to the required location. The scheme of combat use of the system is shown in Figure 5.

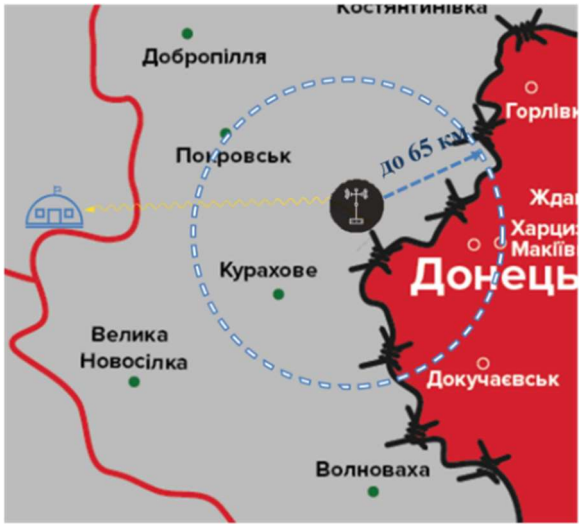

Figure 5 – Scheme of application of the TAI 903S-8 system

The system is capable of detecting enemy radiation objects at a distance of up to 65 km, which makes it possible to deploy it far enough from the line of combat contact.

The spectrogram display of the new Blackbird combines a traditional spectrogram view with an interactive overlay of the real-time detection database. Operators simply hover over any detected signal and a pop-up window will show the metadata for the intercept, including any available modulation and DF results. Operators can also define areas of interest for signal search using geolocation. The system automatically detects signals, evaluates them according to the search criteria, classifies them and records them in the detection database with an operator alert.

Based on the analysis of the capabilities of the PLASTUN-RP3000 direction-finding system and the TSI 903S-8 direction-finding system, a table of comparative characteristics was compiled (Table 1), which allows, taking into account the combat experience of their use, to draw conclusions about the effective use of these electronic warfare means in the tactical command and control link.

Table 1

Main features	PLASTUN-RP3000	TSI 903S-8
Operating frequency range	From 25 MHz up to 3000 MHz	From 1 MHz up to 7500 MHz
Instrumental direction-finding deviation error	Less than 0.5°	Less than 0.1°
Scanning speed	Over 2 GHz/s	Over 3 GHz/s
Dynamic range	Over 80 dB	Over 90 dB
Minimum direction-finding time	Less than 15 ms	3 ms
Frequency resolution in panoramic direction-finding mode	12.5 kHz	4 kHz
Mode of direction-finding of IFR signals	Yes	Yes
Radio-electronic intelligence range	Up to 15 km	Up to 65 km
System deployment time	20 min	10 min
Battery life	Up to 8 hours	Up to 12 hours
Combat calculation	2 persons	3 persons
Operating temperature range	From –20 to +45 °C	From –20 to +45 °C

It is thanks to the skilful use of these two electronic warfare systems that Ukrainian troops have been able to detect, capture or destroy a large number of enemy electronic warfare assets since 24 February 2022. Thus, in March 2022, Ukrainian soldiers captured the latest russian electronic intelligence station Thorn-MDM [10] and one of the most powerful electronic warfare stations Krasukha 4 [11], and members of the resistance movement captured the russian electronic warfare complex Rtut-BM [12]. In addition, as a result of timely detection and targeting, according to the command of the Joint Task Force SKHID the russian RB-341V Leer-3 electronic warfare system was destroyed [13]. In June 2022, Ukrainian artillery destroyed the enemy's Repellent-1 electronic warfare system deployed on the outskirts of the temporarily occupied Kherson [17], and in July, in Mykolaiv region, the Leer-2 electronic warfare system based on the chassis of the Tiger armoured vehicle [18].

In August and September 2022 as a result of the joint work of radio intelligence and the advanced forces of the Armed Forces of Ukraine, a russian jamming station R-9344BMV, part of the automated electronic suppression complex Borysoglebsk-2, was captured: in Kharkiv region [14]; several sets of electronic warfare stations with the type index RP-377 - RP-377UVM1L Lesochek, which are designed to create interference against radio-controlled landmines [15]; the modern russian electronic warfare system Silok-M, which can automatically detect unmanned aerial vehicles, determine their coordinates, and then suppress control, telemetry and communication channels [16]. These are just a few examples of the successful work of Ukraine's security and defence forces to achieve superiority in the electromagnetic space of the battlefield.

Conclusions

One of the most significant mistakes made by the russian federation after the invasion of Ukraine was the expectation that it would dominate the electronic warfare part of the battle. Russian commanders were not only confident that Ukrainian forces had not advanced in terms of electronic warfare since 2014, but also ignored the impact of equipment and training provided by NATO. In addition, the centralised hierarchical command structure of the russian army has made it very difficult for their electronic warfare forces to adapt quickly and ensure timely debugging and repair of equipment. First of all, the occupiers faced problems in the field of intercepting and jamming communications, which is becoming an increasingly important element of military success. Thanks to our air defence forces, the russian aviation has not been able to achieve air superiority, and therefore their aircraft often remained over safe territories in russia and Belarus, which significantly limited the ability to collect signals and jam them. For their part, Ukrainian electronic warfare specialists were able to timely connect to russian communications, detect and block their signals, and blind their surveillance, which often led to the capture or destruction of the enemy's most advanced electronic warfare equipment.

Thus, it is safe to say that modern signals intelligence means in service with the security and defence forces of Ukraine perform their tasks with a high degree of efficiency. First of all, this was facilitated by the correct choice of tactics of their use, flexibility in changing their own structures and methods of recruitment and training of personnel.

Systems, complexes and means of signals intelligence must collect information on the transmission of radio and audio signals, telephone conversations, text messages and online communications. Therefore, promising solutions in this area must meet the target requirements, namely, to collect, analyse and distribute signal intelligence results to users as efficiently as possible, creating their own database. Such a system will have to not only identify individual issuers, but also determine their characteristics and capabilities within the target system and even the integrated combat system. As part of the implementation of the provisions of the Strategic Defence Bulletin of Ukraine, the leadership of the Armed Forces of Ukraine is working to create an effective system of operational control, communications, intelligence and surveillance (C4ISR) that would meet NATO standards and ensure its integration with the Defense resources management information system (DRMIS) [19].

Thus, the positive prospects for the development of signals intelligence include: a strong scientific base and state support for the creation of new modern electronic warfare means (research and production institutes, centres and associations); preservation of the production base with its further increase under state project programmes; introduction of an automated system for collecting, processing and analysing electronic intelligence data; availability of a spacecraft for space reconnaissance in order to fully integrate C4ISR with DRMIS.

The results obtained in this article can be used in further research in the process of developing and implementing instructions and regulations on the combat use of signals intelligence.

References

1. *Defense express. Chomu zasoby radioelektronnoi borotby ta rozvidky nabuvaiut dedali bilshoho znachennia* [Why means of radio-electronic warfare and intelligence are gaining more and more importance]. Retrieved from: http://surl.li/gxfib (accessed 22 November 2023) [in Ukrainian].

2. Zaitsev D., Nakonechnyi A., Pakhariev S., Lutsenko I. (2016). *Viiskova rozvidka* [Military intelligence]. Kyiv : Kyivskyi universytet. Retrieved from: http://surl.li/fqzoy (accessed 22 November 2023) [in Ukrainian].

3. Shamanov D., Sorokin A. (2024). *Analiz suchasnykh metodiv radioelektronnoi borotby* [Analysis of modern methods of radio-electronic warfare Control, navigation and communication systems]. *Systemy upravlinnia, navihatsii ta zviazku*. Poltava : PNTU, vol. 1 (75), pp. 211–214. DOI: https://doi.org/10.26906/SUNZ.2024.1.211 [in Ukrainian].

4. *Zasoby radioelektronnoi borotby voroha* [Means of radio-electronic warfare of the enemy]. Retrieved from: http://surl.li/uhbux (accessed 22 November 2024) [in Ukrainian].

5. Alimpiiev A. M., Pievtsov H. V., Hryb D. A. (2015). *Dovidnyk uchasnyka ATO: ozbroiennia i viiskova tekhnika zbroinykh syl rosiiskoi federatsii* [Handbook of ATO participants: weapons and military equipment of the armed forces of the russian federation]. Kharkiv : Original [in Ukrainian].

6. *Defense express. Radioelektronna borotba: analiz arsenalu rosii* [Radio electronic warfare: analysis of russia's arsenal]. Retrieved from: http://surl.li/svtdn (accessed 22 November 2023) [in Ukrainian].

7. Ministerstvo oborony Ukrainy (2004). *Slovnyk osnovnykh terminiv ta skorochen, yaki vykorystovuiutsia v NATO* [Dictionary of basic terms and abbreviations used in NATO]. Kyiv : MP Lesia [in Ukrainian].

8. *Infozakhyst. Malohabarytnyi taktychnyi pelenhatsiinyi kompleks PLASTUN-RP3000* [Small-sized tactical direction finding system PLASTUN-RP3000]. Retrieved from: http://surl.li/svtlk (accessed 22 November 2023) [in Ukrainian].

9. *Taktychna perenosna systema pelenhatsii TSI 903S-8* [TSI 903S-8 tactical portable direction finding system]. Retrieved from: http://surl.li/vztnbf (accessed 22 November 2023) [in Ukrainian].

10. *Zaxid.net. Biitsi ZSU zakhopyly novitniu stantsiiu rozvidky rosiian "Torn"* [Armed Forces fighters captured the newest intelligence station of the russians "Torn"]. Retrieved from: http://surl.li/svtpn (accessed 22 November 2023) [in Ukrainian].

11. *The WarZone. Ukrainski viiskovi zakhopyly odnu z naipotuzhnishykh rosiiskykh stantsii REB Krasukha-4* [The Ukrainian military seized one of the most powerful russian EW stations Krasukha-4]. Retrieved from: http://surl.li/svtsd (accessed 22 November 2023) [in Ukrainian].

12. *Doroslyi pohliad na svit. Uchasnyky rukhu oporu zakhopyly rosiiskyi kompleks REB "Rtut-BM"* [The members of the resistance movement seized the russian complex of EW "Rtut-BM"]. Retrieved from: http://surl.li/svttk (accessed 22 November 2023) [in Ukrainian].

13. *Armiiainform. Ukrainski viiskovi znyshchyly rosiiskyi kompleks radioelektronnoi borotby "Leier-3"* [The Ukrainian military destroyed the russian complex of radio-electronic warfare "Layer-3"]. Retrieved from: http://surl.li/svtvm (accessed 22 November 2023) [in Ukrainian].

14. *Militarnyi. Viiskovi zakhopyly stantsiiu "R-934BMV" kompleksu "Borysohlebsk-2" rosiiskoi federatsii* [The military seized the R-934BMV station of the Borysoglebsk-2 complex of the russian federation]. Retrieved from: http://surl.li/svtxy (accessed 22 November 2023) [in Ukrainian].

15. *Defense express. ZSU zakhopyly odrazu dvi ridkisni stantsii REB armii rf RP-377 priamo v zavodskii upakovtsi* [The Armed Forces seized two rare EW stations of the russian army directly in the factory packaging]. Retrieved from: http://surl.li/ksvbq (accessed 22 November 2023) [in Ukrainian].

16. *Doroslyi pohliad na svit. Ukrainski biitsi zakhopyly suchasnyi rosiiskyi kompleks REB "Sylok-M1"* [Ukrainian fighters captured the modern russian missile defense complex "Sylock-M1"]. Retrieved from: http://surl.li/svvjv (accessed 22 November 2023) [in Ukrainian].

17. *Armiiainform. "Repellent-1": shcho vidomo pro znyshchennia rosiiskoho kompleksu REB* ["Repellent-1": what is known about the destroyed russian EW complex]. Retrieved from: http://surl.li/svvls (accessed 22 November 2023) [in Ukrainian].

18. *Defense express. Znyshchennia kompleksu REB armii rf "Leier-2"* [The EW complex of the russian army "Layer-2" was destroyed]. Retrieved from: http://surl.li/svvpl (accessed 22 November 2023) [in Ukrainian].

19. *Ukaz Prezydenta Ukrainy "Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy "Pro Stratehichnyi oboronnyi biuleten Ukrainy" № 240/2016* [Decree of the President of Ukraine on the decision of the National Security and Defense Council of Ukraine "On the Strategic Defense Bulletin of Ukraine" activity no. 240/2016]. (2016, May 20). Retrieved from: http://surl.li/svvtp (accessed 22 November 2023) [in Ukrainian].

The article was submitted to the editorial office on 10.05.2024

УДК 356/358

І. М. Майборода, К. В. Власов, М. О. Глущенко

ЗАСТОСУВАННЯ І ПЕРСПЕКТИВИ РОЗВИТКУ МОБІЛЬНИХ ЗАСОБІВ РАДІОЕЛЕКТРОННОЇ РОЗВІДКИ ТАКТИЧНОЇ ЛАНКИ СИЛ СЕКТОРУ БЕЗПЕКИ ТА ОБОРОНИ УКРАЇНИ

Радіоелектронна розвідка – одна з найважливіших частин державної та воєнної розвідки різних країн і є основним, а в багатьох випадках єдиним способом добування розвідувальної інформації. За різними оцінками засобами радіоелектронної розвідки добувається до 90 % первинної інформації. Мета статті – оцінити можливості мобільних засобів радіоелектронної розвідки тактичної ланки сил сектору безпеки і оборони України, розробити рекомендації щодо перспектив їхнього розвитку, проаналізувати застосування систем та засобів радіоелектронної розвідки армії російської федерації під час проведення так званої «спеціальної воєнної операції» проти України.

У статті наведено можливості засобів радіоелектронної розвідки, що перебувають на озброєнні у Збройних Силах України та Національній гвардії України. Проведено порівняльний аналіз тактико-технічних характеристик засобів українського та іноземного виробництва, а також стислий аналіз засобів радіоелектронної боротьби країни-агресорки та результатів їхнього застосування. На основі проведеного аналізу визначено рекомендації щодо перспектив застосування і розвитку засобів радіоелектронної розвідки тактичної ланки сил сектору безпеки і оборони України.

Одержані у статті результати можуть бути використані у процесі розроблення і введення в дію належним чином інструкцій та положень з бойового застосування засобів радіоелектронної розвідки.

Ключові слова: *радіоелектронна боротьба, засоби радіоелектронної розвідки, комплекси та системи пеленгації.*

Maiboroda Ihor – Candidate of Military Sciences, Associate Professor, Associate Professor of the Department of Military Communications and Informatisation of the National Academy of the National Guard of Ukraine
https://orcid.org//0000-0002-8389-6994

Vlasov Kostiantyn – Senior Lecturer at the Department of Military Communications and Informatisation of the National Academy of the National Guard of Ukraine
https://orcid.org/0000-0002-6311-0499

Hlushchenko Mykola – Senior Lecturer at the Department of Military Communications and Informatisation of the National Academy of the National Guard of Ukraine
https://orcid.org/0000-0003-3448-0965