Scientific Journal of the Military University of Land Forces
ISSN: 2544-7122 (print), 2545-0719 (online)
2020, Volume 52, Number 1(195), Pages 121-134
DOI: 10.5604/01.3001.0014.0268

Original article

Application of spread spectrum transmission in the aspect of radio communications security

Robert Król

Special Operations Component Command, Poland,
e-mail: ro.krol@ron.mil.pl

INFORMATIONS

Article history:

Submited: 24 July 2018

Accepted: 8 November 2018

Published: 16 March 2020

ABSTRACT

This publication considers the use of spread spectrum transmissions in the aspect of threats to radio communications security. Numerous restrictions related to the previous use of specific operating modes of VHF, UHF and KF radio stations with reference to the possibilities of counteracting on the part of a potential enemy using the most modern EW (electronic warfare) systems, as well as those based on the procedures of the Russian Federation Armed Forces.

KEYWORDS

communication security, operating modes used in radio communications of the Polish Armed Forces, frequency hopping (FH), sincgars, havequick, narrowband and broadband hopping

Introduction

Considering that the security of information transfer is one of the main technical and operational requirements of the organization of the communications system, it was considered appropriate to try to explain the role of radio communications from the tactical unit (ZT) level to the platoon level.

In short, the basis adopted for planning communications systems at all levels of the Polish Armed Forces (regardless of the branch) is the NATO principle of PACE:

1) P – PRIMARY communication,
2) A – ALTERNATE communication,
3) C – CONTINGENCY communication,
4) E – EMERGENCY communication.

In order to limit the volume of the study, the author assumed that all communications systems (without going into details due to the explicit content of the article) from the highest level to the battalion level (equivalent) in the superior-subordinate relationship are planned according to the following scheme:

1. P – teleinformatic classified networks based on the stationary infrastructure of the Ministry of National Defense.
2. A – teleinformatic classified and unclassified (using encryption) networks based on VSAT systems or VPN tunnels using the infrastructure of commercial operators.
3. C – radio communications (KF to the unit level – Mechanized Brigade/Armored Brigade, equivalent, KF and VHF in the unit-battalion relationship).
4. E – unclassified telephone communication based on STUP, satellite and GSM telephony.

The following scheme has been assumed for the purpose of further considerations on the top-down brigade-regiment (equivalent) relationship:

1) P – radio communications (KF, VHF),
2) A – radio communications (UHF TACSAT),
3) C – satellite telephony (according to difficulty in tracking and jamming),
4) E – GSM telephony.

It is obvious that people with specialist knowledge in the field of communications system planning could ask a question – "Why didn't the author include wired communications both in field and connected to STUP on the lower levels of command (including the battalion top-down one)?" The author decided to focus on maneuvering activities since they apparently explain the essence of the role of radio communications in the above relationship.

Due to the fact that some readers have not explored the broadly understood issue of communications system security, it is worth mentioning the requirements of communications systems at all levels, i.e., timeliness, faithfulness and concealedness precisely defined in the literature on the subject, and the concept of communication security itself as an element of technical and operational conditions.

In the article *Technical aspects of communications system security in combat operations at the tactical level* one can find a definition of the security of the communications system identified with counteracting the hostile reconnaissance. Security is characterized as "a state of non-threat, peace, certainty" [1, p. 147], while its synonyms include [2, p. 25]: "certainty, peace, tranquility, balance, stability, assurance". In the NATO terminology, security is defined by [3, p. 315-6; 4, p. 31]:

1. "The state achieved when certain information, equipment, personnel, activities and devices are protected against espionage, sabotage, subversion and terrorism, as well as against loss and disclosure of the secret."
2. "Undertakings necessary to provide protection against espionage, sabotage, subversion and terrorism, as well as against loss and disclosure of the secret."

Communications Security (COMSEC) – this is "a set of organizational and technical measures (including the use of cryptographic security measures, appropriate transmission techniques and physical security measures) to prevent unauthorized access to information that may come from the monitoring of technical means of communication" [5, p. 402].

Security of communication includes "a set of conditions ensuring the elimination or maximum limitation of radio-electronic and fire enemy influence on the elements of communications network and information conveyed therein" [6, p. 22], as well as "the entirety of

organizational, technical and operational measures that secure the communications system before being recognized by the enemy, 'the loss of information' and disinformation" [7, p. 27].

Furthermore, security of communications comprises "undertakings in the field of telecommunications equipment security that prevent unauthorized access to relevant information that can be obtained from them, or ensuring the reliability of these devices. (…) It refers to cryptographic, transmission and emission, procedural, physical, personal, as well as of documents and IT system security" [4, p. 8].

1. Radio transmission with FH spread spectrum

For readers who have not yet explored the technical problems of radio transmission with spread spectrum, the author decided to bring closer the essence of the purpose of further consideration in terms of the operational capability of radio equipment in the Polish Armed Forces, and consequently its impact on communications security. In this respect, a more inquisitive analysis of Shannon's theorem on the communication channel capacity was considered right.

$$C = B \cdot \lg_2 (1 + N / S) \tag{1}$$

where:

C – the channel capacity in bits per second,

B – width of the channel in Hertz,

S – signal strength,

N – noise power.

The above formula shows that the capacity increases with the bandwidth and also the increase in the S/N ratio. If the noise is much stronger than the signal $S/N < 1$, the above formula is simplified to:

$$C = 1.44 \cdot B \cdot S / N \tag{2}$$

which as a result of the rearrangement leads to:

$$B = 0.69 \cdot C \cdot S / N \tag{3}$$

The above formula proves that by expanding the frequency band, the value N increases in relation to S, leading a situation in which $N > S$ [8, p. 201].

The classification of basic methods of signal scattering, which include:

a) DS – direct sequence,

b) FH – frequency hopping,

c) TH – time hopping.

The FH emission consists in the fact that the carrier frequency changes in steps in a wide band according to the algorithm defined by a pseudo-random sequence. The pseudo-random sequences are different for different users. The FH signal is unevenly spread over the entire width of the frequency band occupied, but it is concentrated around many randomly selected carrier frequencies on which data is transmitted.

Two FH methods – fast (used in VHF radios) and slow (used in KF relations) are distinguished. Simply put, the fast FH is the multiple change of the carrier frequency f(t) during the data bit (Fig. 1).

The slow FH is the inverse of the previously described method, that is, changes in carrier frequencies occur once per several bits of the data sequence d(t) (Fig. 2).

Fast frequency hopping (Fig. 1) – changes in carrier frequency f(t) occur repeatedly over the data bit duration (e.g., $T_h = T_b / 3T_b$ – the duration of data T_h bit – the period of carrier frequency changes). The distance between consecutive carrier frequencies is assumed to be $\Delta f = 1 / T_h$. Figures 3 and 4 show the spectrum of the distributed signals sFH(f) when $T_h = T_b / 3 \Rightarrow \Delta f = 1 / T_h = 3 / T_b$ and when $T_h = T_b / 7 \Rightarrow \Delta f = 1 / T_h = 7 / T_b$.

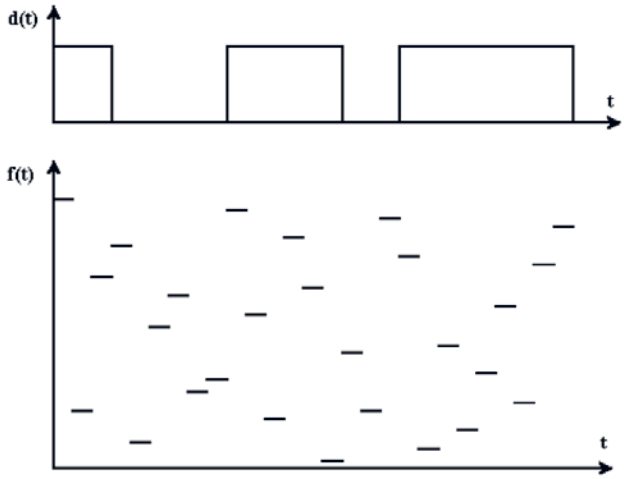

Fig. 1. Fast frequency hopping
Source: [9, p. 3].

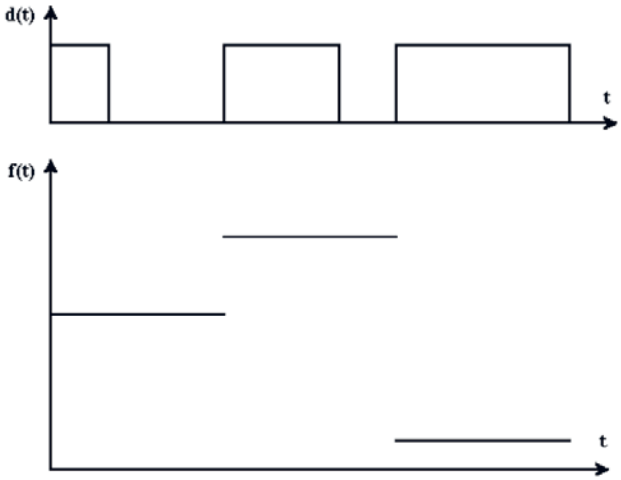

Fig. 2. Slow frequency hopping
Source: [9, p. 3].

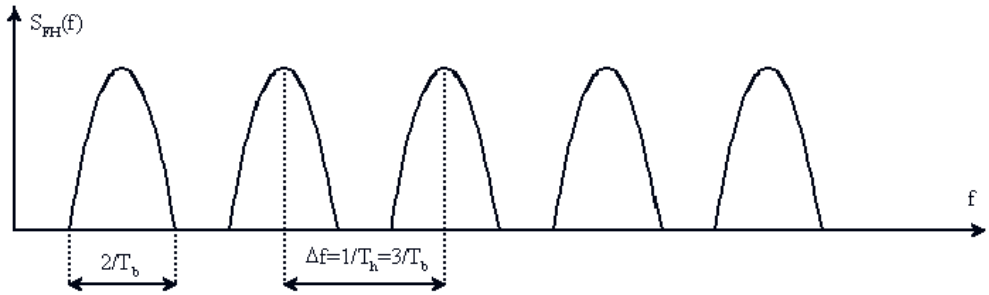

Fig. 3. Spectrum of the spread signal with fast frequency hopping $\Delta f = 3/T_b$
Source: [9, p. 4].

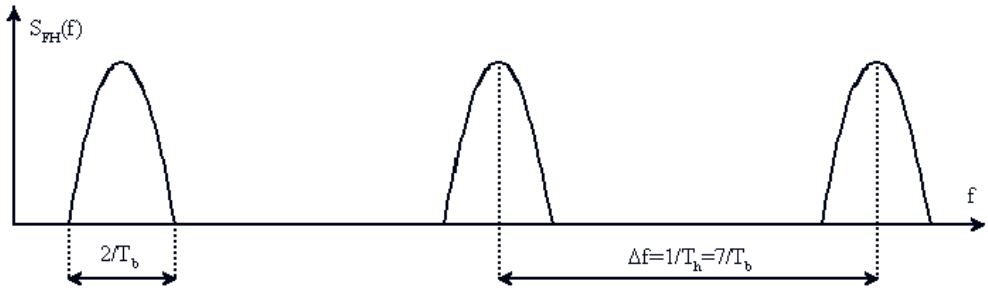

Fig. 4. Spectrum of the spread signal with fast frequency hopping $\Delta f = 7/T_b$
Source: [9, p. 4].

Slow frequency hopping (Fig. 2) – changes in carrier frequency occur every few bits of data in the data sequence d(t). In the case of slow frequency hopping, the condition $T_h >> T_b$ is usually met, and the spacing between neighboring carriers is usually assumed $\Delta f = 1/T_b$ (Fig. 5) or $\Delta f = 2/T_b$ (Fig. 6).

The bandwidth used by a single carrier is Δf; when using N carriers, the total band occupied by the signal after dispersion is $N * \Delta f$, and this means that the processing profit is N. If the transmission with a partial overlap of signals from adjacent carriers is used, it is possible to get twice as narrow space between carriers. That enables getting twice as narrow total band, but at the same time the processing profit drops twofold (N/2) [9, p. 3-5].

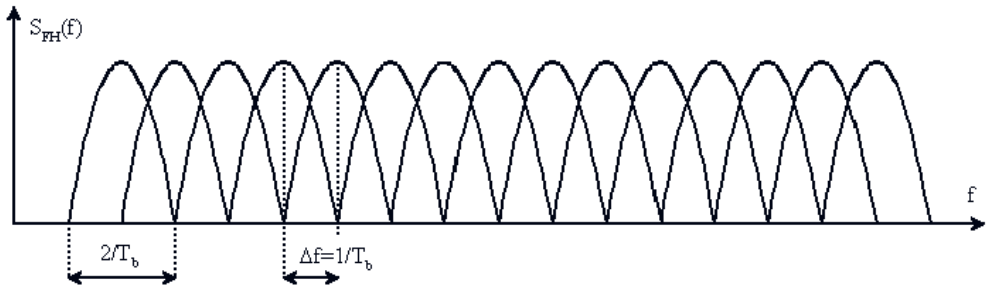

Fig. 5. The spectrum of the spread signal slow frequency hopping $\Delta f = 1/T_b$
Source: [9, p. 4].

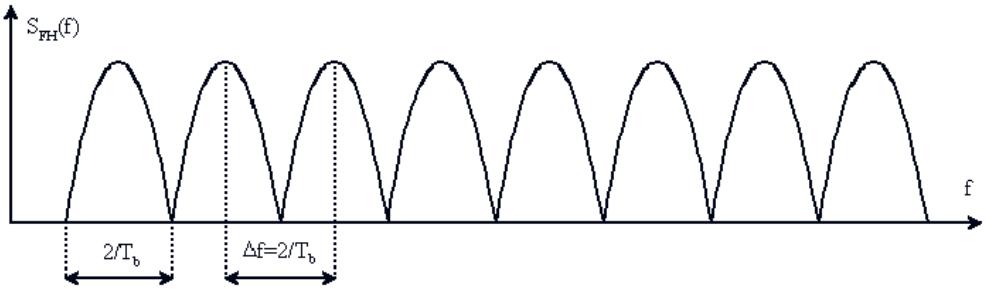

Fig. 6. Spectrum of the spread signal with slow frequency hopping $\Delta f = 2 / T_b$
Source: [9, p. 4].

In FH systems, the suppression mechanism of unwanted signals is as follows: the useful signal is at a given moment sent in a narrowband channel, the interfering signal will only sporadically overlap with the spectrum of the useful signal, and the probability of such an event is small. In this case, the suppression of the interfering signal consists in its avoidance.

In the case of scattering by frequency hopping, frequency shift keying (FSK) is usually selected as modulation. Simplified diagrams of the transmitter and receiver are shown in Figure 7.

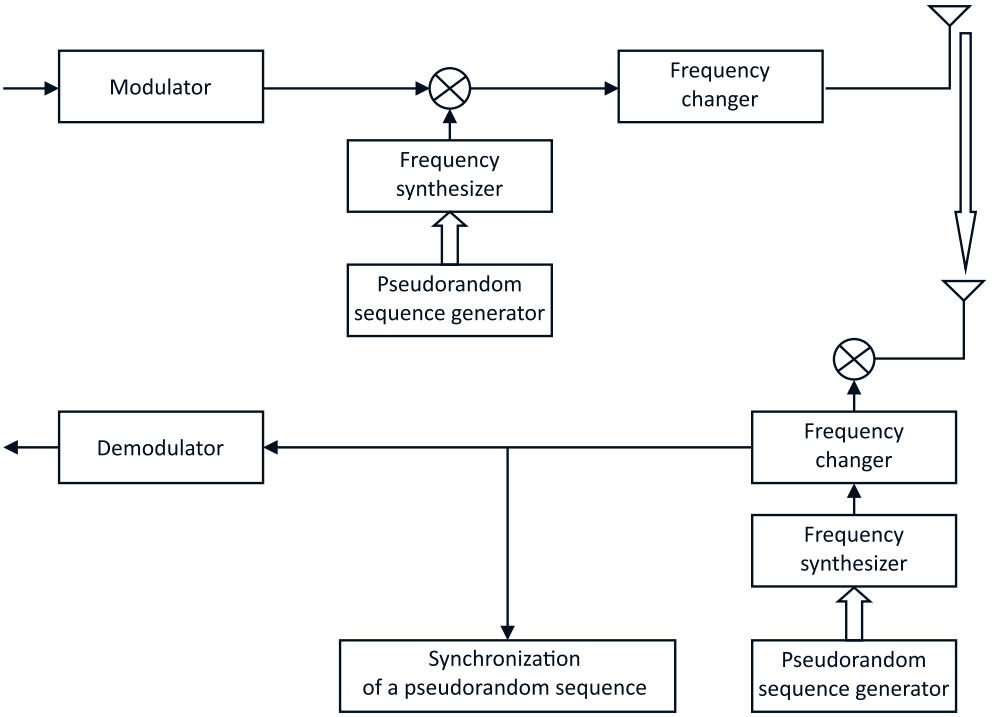

Fig. 7. FH transmitter and receiver
Source: [10].

2. Possibilities of radio stations of PR4G, F@stNet, and Falcon II/III families in the aspect of spread spectrum transmission

At present, radio stations operating in the KF, VHF and UHF range are used in the Polish Armed Forces. Therefore, the author considers it right to expose the mechanisms allowing to secure radio communications in the military range of KF (2.0-29.9999MHz), VHF (30÷87.975 MHz) and UHF (225÷399.975MHz).

The basic radio stations of the battlefield in the Polish Armed Forces are PR4G radios (including F@stNet) as well as Falcon II and III (systematic withdrawal of the first-generation radio stations results in not taking them into further considerations). These radios can work in different operating modes – from basic analogs that do not use any security mechanisms through a single-channel digital mode on a fixed frequency providing protection using COMSEC keys and protection modes against electronic combat effects, such as FH, FCS and MIX. These modes provide protection for messages sent using both COMSEC and TRANSEC keys.

It is necessary to emphasize the synthesis of differences between individual modes of radio station operation, which despite the common denominator in the form of the possibility of spread spectrum transmission lead to incompatibility, and thus prevent cooperation between elements of the combat group. For the radio station of the PR4G family, these are:

1) FCS (*Free Channel Search*) – the operating mode consisting in searching a set of defined frequencies for a channel characterized by the highest signal-to-noise ratio,
2) FH (*Frequency Hopping*) – the frequency-hopping operating mode (selected from a set of defined sub-bands),
3) MIX (*Mixed)* – the mixed mode combining features of FCS and FH modes.

All the above-mentioned modes offer full protection of transmitted information by using the built-in encryption module based on the COMSEC key mentioned above and the TRANSEC key responsible for pseudorandom frequency selection. At this stage, it should be noted that those keys, and thus the hopping algorithm, are not identical to the Falcon II and III systems implemented in the radio stations. Reading the detailed instructions of the devices in question, which are also generally available on the global network, should be recommended to all those interested in deepening the knowledge about the radio stations in question. At the same time, the author notes that the FH mode of the PR4G family radio station allows for performing 300 hops per second. Radio stations of the Falcon II and III family (VHF and UHF – applies to both portable radio transmitters – 20W/10W and individual ones – 10W/5W):

1. SINCGARS (FM) – the frequency-hopping operating mode (selected from a set of defined sub-bands – any of the 2320 channels at intervals of 25 kHz, 100 hops per second).
2. HAVEQUICK (AM) – the frequency-hopping operating mode (selected from internal tables of channels in the radio memory determined by the network number with a 25 kHz interval between channels, the modulation/hop rate is confidential and cannot be included in the content of this publication, however, a reader familiar with the laws of physics associated with AM modulation and Doppler phenomenon, will be able to determine the order of magnitude).

Radio stations of the Falcon II and III family (KF):

1. FH NARROWBAND – frequencies: multiples of 5 kHz, the bandwidth depends on the central frequency (the coupler must be switched on).
2. FH WIDEBAND – frequencies: multiples of 100 Hz, the bandwidth between 15 kHz-1.999 MHz (the coupler must be switched off).
3. FH LIST – the list of programmed channels – frequencies: multiples of 100 Hz, number of frequencies: 5 to 50 (the coupler must be switched off).
4. LPI/LPD – the ALE 3G mode – a hybrid, which today can only be described in a classified publication.

The modulation speed cannot be included in this publication, which results from the synchronization signature which is important in the detection/tracking process and, consequently, jamming or destroying.

While discussing FH with regard to the KF Falcon II radio station family, it is worth noting that they use both TRANSEC and COMSEC keys certified by the US NSA and HARRIS commercial algorithms.

3. Methods of detection and jamming

Basically, after having discussed the theory of the spread spectrum transmission and the presentation of the equipment capabilities of the Polish Armed Forces, the author could be tempted to draw final conclusions. Unfortunately, the reader who does not have basic knowledge of the potential of the opposing party could have the wrong impression that when acting based on the latest generation equipment we do not have to worry about anything else. Unfortunately, things are not as simple as they seem.

Before specific examples related to the technical capabilities and procedures of an opponent possessing the equipment identical or close to that of the Russian Federation (RF) are presented, it has been considered appropriate to briefly explain the methods of signal detection and analysis without going into the details of physical processes that will be discussed in the next study.

Detection of FH emissions is most frequently carried out by the rapid serial scanning of the frequency band in which the FH emission transmitter operates. The simplest method to determine the presence of FH emissions is the analysis of the spectrogram for signals exceeding the previously defined coordinate threshold consisting of three elements: signal level, frequency and time. This type of display makes it possible to determine the range of frequencies and emission start and end moments used by the FH transmitter. It is also possible to use signal level information to pre-differentiate individual signal sources.

The most common method of FH emission detection is the time-frequency analysis of the spectrogram (see Fig. 8).

When choosing a specific algorithm by Bernsen, Niblack or the team of G. Baranowski, R. Urbana and K. Wilgucki (being a defacto modification of the Niblack algorithm) from the Military Institute of Communication, one can conclude that the filtration of the spectrogram is based on the determined detection threshold with simultaneous elimination of noise and constant signals allows for isolating the desired FH emission.

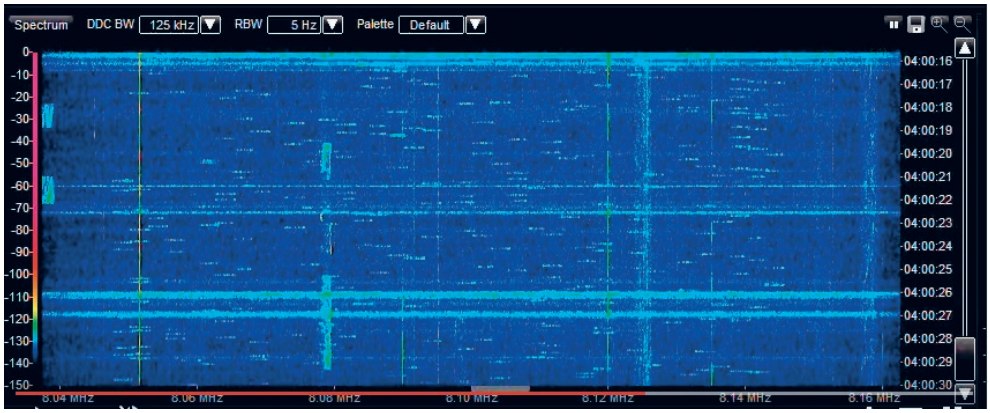

Fig. 8. Time-frequency spectrogram
Source: Own elaboration – study of FH emission differences using a spectrum analyzer.

The analysis of the possibilities of a potential enemy in procedural and equipment terms has been carried out.

According to the latest Russian definition, "radio-electronic warfare is a set of coordinated activities aimed at radio-electronic strike on radio-electronic and IT objects of the enemy, radio-electronic protection of own radio and electronic objects, counteracting the enemy's technical means of reconnaissance, as well as radio-electronic and IT support of own forces" [11].

The Russians are constantly emphasizing the growing importance of this domain in the modern battlefield. According to them, experience from modern wars and conflicts indicates that the use of forces and means of EW can increase the potential of land forces up to two times, reduce the loss of air forces up to six times, and combat vessels up to three times. In this very simple way, the distance that separates Russia from Western countries can be reduced.

According to the Russian data, the contribution of the Radio-Electronic Warfare Forces in performing such tasks as disorganization of the command and control system of weapons can be greater than 70 percent. Effective protection of own troops and objects against enemy attacks using precision weapons and information war systems is impossible without EW. It is also emphasized that the radio-electronic fight should not only concern the military sphere, but also cover civilian systems using electromagnetic energy. Moreover, the Russian doctrine envisages not only the application of EW systems for operational support of certain types of combat actions (e.g., land ones), but also for conducting independent operations, for example to disorganize the command and control systems of the opponent's combat measures. At the same time, the Russians intend to introduce completely new ways of using EW forces in combat actions, including massive electronic-fire and electronic blow, and the use of drones for this purpose.

It is for this reason that Russia has been intensively introducing new multipurpose radio-electronic systems of 'impact on the enemy in all areas (in space, air, land and sea) and the entire depth of its troops', as well as EW systems – capable to electronically secure own forces during the times of peace and war. These EW devices operate according to completely new rules and are built in a new technology, together with traditional systems they are to increase the efficiency of own forces up to five times.

Due to the development program and the saturation of the Armed Forces with modern equipment of the Radio-Electronic Warfare, systems such as 'Borisogliebsk-2', 'Djugonist', 'Infauna', Krasucha-2, 'Murmansk-BN' and 'Swiet-KU' were introduced already in 2015. There was also implemented a new version of the Mi-8MTPR-1 helicopters equipped with the 'Ryczag-AW' EW complex, capable of, among others, electronic protection of own aircrafts against the operation of antiaircraft systems guided by radars in the radius of 600 km. In the meantime, the assembly of 'Chibiny' EW complexes was commenced on Su-34 fighter-bombers and 'Witiebsk' sets on modernized Su-25SM attack aircrafts of the Aerospace Forces. Selected elements of the 'Witiebsk' complex were additionally installed on Ka-52, Mi-28, Mi-8MT, Mi-26 and Mi-26T2 helicopters. In the years 2016-2017, the Aerospace Forces also included three Ił-22PP aircrafts modernized for EW operations (interference and reconnaissance).

The Russians are aware of the advantages that the United States and NATO have gained in terms of tactics and the use of precision weapons. The radio-electronic warfare is to be a panacea for the weaknesses of the Armed Forces of the Russian Federation. A propaganda campaign has begun, the task of which is to exaggerate the capabilities of Russian EW systems. On the other hand, however, actual actions were also started – paying special attention to further equipping and training of EW forces. This is increasingly apparent in the scenarios of military maneuvers that take place on the territory of the Russian Federation. A model example of such policy was the Kawkaz-2016 strategic maneuvers" [11].

In the author's opinion, an indispensable element of subsequent considerations is the attempt of general characteristics of selected devices and EW measures of the Russian Federation included in the Table 1.

Table 1. Radio-electronic warfare measures of the Russian Federation Armed Forces

No.	Name of the complex/set	Type of carrier	Capabilities and purpose	Comments
1.	Boriso-glebsk-2	MTLB	Reconnaissance of and interference with radio, satellite and radio-navigation systems. Up to 30 interfering stations can be controlled. Preparation time for work from the marching position – 15 min.	Mobile control system: R-300KMW Interference systems: P-37BMW P-330BMW P-34BMW P325-UMW Crew: 4 (including 2 EW operators).
2.	Djugonist		System supervising the work of own troops in terms of passive radio-electronic defense.	The bandwidth from 0,1 MHz to 18 GHz), tracking accuracy 23°.
3.	Infauna	K1SZ1 (modelled on a BTR-80)	Reconnaissance of and interference with the enemy's means of communication, as well as protection of own forces against radio-controlled explosive devices.	Airborne troops.

No.	Name of the complex/set	Type of carrier	Capabilities and purpose	Comments
4.	Karsucha-4S	KaMAZ	Reconnaissance and interference on the wide band. Designed to protect ground-based objects from being detected primarily by aerial radiolocation stations of early detection aircraft, multi-purpose radars of tactical multi-role combat aircrafts, on-board drone radars, ground radars, and radiolocation systems of reconnaissance satellites.	Detection range of radiolocation stations and on-board radars – up to 300 km.
5.	Lieer-3	BSR Orlan-10	Reconnaissance of and interference with GSM telephony systems.	2×Orlan-10. The power interfering transmitters – 10 W. Interference radius – up to 6 km.
6.	Rtuć-BM	MTLB	Interference with VHF radio communication. The main purpose is to distort fuses of approaching missiles and artillery shells. Time to prepare for work from the marching position – 10 min.	2 operators. Continuous operation up to 6 hours 1 vehicle at 50 ha.
7.	Swiet-KU	KaMAZ Ford Transit	Reconnaissance of and interference with radio and radiolocation systems. It allows for tracking various types of emission, analyze them and determine computing the coordinates of the sources of these signals. The "Swiet-KU" complex can block itself by interfering with the GSM, CDMA2000 and UMTS mobile telephony networks.	The bandwidth from 25 MHz to 18 GHz. Tracking accuracy in the 30-100 MHz band – 5°, 1-3 GHz – 2°.
8.	Żitiel	Ził + trailer	Reconnaissance of and interference with Inmarsat and Iridium satellite communications systems as well as base stations of the GSM 1900 standard mobile telephony network, and jamming of GPS navigational equipment using the NAVSTAR satellite system. The complex does not have the capacity of selective distortion. Before starting work, there is a need to send a warning to own units located in the system operating range.	The bandwidth from 01 to 2 GHz. The scope of interfering with ground measures – up to 15 km, air ones – up to 200 km. R-330 KMK remote control kit.
9.	Murmańsk	Kamaz	Interference with KF radio systems at distances of up to 5000 km. This is not a mobile system. The service needs up to 72 "sunny" hours to spread the antenna set on four telescopic masts with the height of 32 meters.	Edge, extensive. Range up to 5000 km. 7×KaMAZ.

Source: Own elaboration based on: [11].

Conclusions

The study presents the basics of knowledge necessary to better understand the specifics of radio communications security in the aspect of using systems based on the spread spectrum transmission in the field of FH, and thus the possibility of using the capabilities of the equipment in combat operations most effectively. It can be followed by the assumption that the issues under consideration are keeping those responsible for planning communications systems at all levels of command awake at night. According to the author, there is no doubt that today the radio communications security is identical with the safety not only of users and service of command vehicles but in the broader context of the Armed Forces, since all those who use radio means do not perform tasks in isolation. In this case, there must be synergy of procedures, rules for the protection of information, as well as the skills and experience of the professional staff. Detailed characteristics of radio equipment have been deliberately omitted, as it is available in the literature on the subject.

The most important advantages of spread spectrum transmissions in terms of communications security include:

– low spectral density of the signal being sent,
– reduced probability of detection of signals being transmitted,
– increase in resistance to targeted interference.

When analyzing the theory of detection and interference, and, in particular, the possibilities of modern EW set of our eastern neighbor, it should be realized that over the last six years not only did it learn lessons, but also achieved or has been on its way to achieving an advantage in this respect. We must not forget about scheduled planning. In a relationship based on a single channel or modes, even of the latest generation, with automatic connection set-up. If some of the media noise comes down to the dimension of propaganda activities, it should be realized that this type of troops, like few others, is very disciplined and organized. Another problem may be the fact that the Russian Federation does not care about losses among civilians (which has already been proved several times), and in the case of lack of possibilities of interference with our communication systems, they will proceed to destroy them and, due to savings and shortages of precision weapons, they may move on to surface destruction.

The main disadvantage of using FH systems and devices during peacetime is the lack of proper knowledge and skills among both planners and the equipment users of the lowest level.

Considering the fact that due to the possibility of overpowering systems based on GPS navigation (SAASM is not yet widespread), satellite links, and GSM, we are left only with KF communication, thus the training discipline, especially in the field of correspondence, use of equipment, including individual VHF radio stations must be definitely increased.

The only disadvantage, apart from the aspect of the human factor described above, which may contribute to the disclosure of the procedures and capabilities of the equipment, is the low data transmission rate – both in the case of KF and VHF. Hence the solution seems to be the correct format of the report instead of extensive presentations in the pptx format.

Acknowledgement

No acknowledgement and potential founding was reported by the author.

Conflict of interests

The author declared no conflict of interests.

Author contributions

The author contributed to the interpretation of results and writing of the paper. The author read and approved the final manuscript.

Ethical statement

The research complies with all national and international ethical requirements.

ORCID

Robert Król https://orcid.org/0000-0002-6134-9033

References

1. Urbanek A. *Ilustrowany leksykon teleinformatyka*. Warszawa: IDG; 2001.
2. Żmigrodzki P. *Słownik synonimów i antonimów*. Wrocław: Europa; 2007.
3. *AAP-6 Słownik terminów i definicji NATO*. Agencja Standaryzacji NATO; 2006.
4. *AAP-31(A) Słownik terminów i definicji dotyczący systemów łączności i informatyki NATO*. STANAG 5064. Agencja Standaryzacji NATO; 2001.
5. *Regulamin działań Wojsk Lądowych*. Warszawa: Dowództwo Wojsk Lądowych. Pion Szkolenia; 2008.
6. Mazurkiewicz J. *Leksykon łączności wojskowej*. Warszawa: AON; 1996.
7. Guziewicz L, Kielar M, Łukasiewicz H. *Łączność w oddziałach i pododdziałach zmechanizowanych oraz dane taktyczno-techniczne sprzętu łączności*. Wrocław: Wyższa Szkoła Oficerska Wojsk Lądowych imienia generała Tadeusza Kościuszki; 2004.
8. Chojcan J, Dustor A. *Transmisja danych z rozproszonym widmem.* Zeszyty Naukowe Politechniki Śląskiej. 2000.
9. Chaciński H. *Badanie łącza Bluetooth*. Warszawa: Politechnika Warszawska; 2005.
10. Mąka W. *Projektowanie u analiza usług sieciowych. Wykład 10. Radiowe systemy transmisyjne*, [online]. PJWSTK, 2006. Available at: http://edu.pjwstk.edu.pl/wyklady/psk2/scb/main82.html [Accessed: 15 May 2018].
11. Dura M. *Walka Radioelektroniczna rosyjską odpowiedzią na przewagę NATO? [ANALIZA]*, [online]. Portal Defence24.pl. 4 May 2017. Available at: http://www.defence24.pl/walka-radioelektroniczna-rosyjska-odpowiedzia-na-przewage-nato-analiza [Accessed: 16 May 2018].

Biographical note

Robert Król – MA, a professional soldier interested in the issues of ICT security in the context of conducting special operations. As part of this issue, he pays special attention to the practical use of the capabilities of the possessed equipment, as well as their increase through the creation of integrated systems based on both the most modern military and commercial equipment.

Zastosowanie transmisji z widmem rozproszonym w aspekcie bezpieczeństwa łączności radiowej

STRESZCZENIE W niniejszej publikacji poddano pod rozwagę wykorzystanie transmisji z widmem rozproszonym w aspekcie zagrożeń bezpieczeństwa łączności radiowej. Wskazano na liczne ograniczenia związane z dotychczasowym wykorzystywaniem określonych trybów pracy radiostacji VHF, UHF oraz KF w odniesieniu do możliwości przeciwdziałania ze strony potencjalnego przeciwnika wykorzystującego najnowocześniejsze systemy WRE, a także bazujące na procedurach SZ Federacji Rosyjskiej.

SŁOWA KLUCZOWE bezpieczeństwo łączności, tryby pracy wykorzystywane w łączności radiowej SZ RP, frequency hopping (FH), sincgars, havequick, hopping wąsko- i szerokopasmowy

How to cite this paper

Król R. *Application of spread spectrum transmission in the aspect of radio communications security*. Scientific Journal of the Military University of Land Forces. 2020;52;1(195):121-34.

DOI: http://dx.doi.org/10.5604/01.3001.0014.0268