UDC 519.25
DOI: 10.15587/2706-5448.2022.261874
Article type «Reports on Research Projects»

Oleg Sova

ANALYSIS OF CONDITIONS AND FACTORS AFFECTING CYBER SECURITY IN THE SPECIAL PURPOSE INFORMATION AND TELECOMMUNICATION SYSTEM

The increase in the number of cases of failure of information and telecommunication networks due to cyber attacks determines the need to protect them from this type of attacks. The issue of increasing cyber security in the conditions of conducting operations by groups of troops (forces) is very important. Due to the armed conflict in the East of Ukraine, the military-political instability in the Middle East, the struggle for influence on world financial and energy flows, the global military-political instability is intensifying. This is due to an increase in the number of communication devices in information and telecommunication networks, as well as an increase in the number of possible attacks that can be used to disrupt the operation of an information and telecommunication network. Considering the above, the object of research is a special purpose information and telecommunication system. The subject of research is cyber security of a special purpose information and telecommunication system. Classical methods of scientific knowledge, namely analysis and synthesis, were used during the research. The research identifies factors that affect cyber security in a special purpose information and telecommunications system. All this must be taken into account while planning and deploying a special purpose information and telecommunication system. The analysis of the consequences of the impact on the information and telecommunications system of special purpose of modern devices of defeat and the impact of devices of radio-electronic suppression and other factors was carried out. A typical special purpose information and telecommunication system does not fully meet the requirements for constant readiness to ensure the management of troops (forces), stability, mobility and throughput. A formalized description of the task of improving cyber security in a special purpose information and telecommunications network is provided. The components that affect the level of cyber security of the special purpose information and telecommunication network during the group's operations have been established. The impact of the specified conditions and factors must be reflected: in the planning documents during the planning of the deployment and operation of the group's information and telecommunications system; in the software, during operational management.

Keywords: *cyber security, radio-electronic environment, special purpose information and telecommunication system, operational management, cyber security.*

Received date: 17.05.2022
Accepted date: 20.07.2022
Published date: 25.07.2022

How to cite
Sova, O. (2022). Analysis of conditions and factors affecting cyber security in the special purpose information and telecommunication system. Technology Audit and Production Reserves, 4 (2 (66)), 25–28. doi: http://doi.org/10.15587/2706-5448.2022.261874

1. Introduction

Due to the armed conflict in the East of Ukraine, the military-political instability in the Middle East, the struggle for influence on world financial and energy flows, the global military-political instability is intensifying. The leading states are increasing military spending, intensifying the development of new types of weapons, and increasing the intensity of military exercises.

The military doctrine of Ukraine in the new edition defines that the threat of the use of military force against Ukraine can be implemented according to the following scenarios [1–3]:

– full-scale armed aggression of the Russian Federation against Ukraine with land, air-space, and sea operations with decisive military and political goals;
– a separate special operation of the Russian Federation against Ukraine with the use of military units and/or units, fire strikes, information, information and psychological operations (actions) in combination with the use of non-military measures, including peacekeeping forces in the absence of a relevant decision of the UN Security Council;
– blockade of seaports, coastline or airspace of Ukraine with the use of military force, violation of Ukraine's communications by the Russian Federation;
– an armed conflict within the state, inspired by the Russian Federation with an effort to separate from Ukraine administrative and territorial units in the eastern and southern regions of Ukraine, with the participation of armed formations not provided for by law, terrorist

ISSN 2664-9969

groups in cooperation with political, non-governmental, ethnic, religious or other organizations;
– armed conflict on the state border of Ukraine, in particular border armed incidents (provocations, skirmishes) with regular or irregular forces of the Russian Federation, armed formations not provided for by law;
– terrorist acts on the territory of Ukraine or against citizens of Ukraine, attacks on the lives of state or public figures, representatives of foreign countries (committed with the aim of provoking war or international complications), sabotage (including on critical infrastructure facilities). Also explosions, set off in the premises of state authorities and their capture, kidnapping of citizens or hostage taking.

The aforementioned puts forward qualitatively new requirements for the construction of the Armed Forces, revision of the approaches that are currently the basis of the use of troops (forces) and the development of forms and methods of their use [4–6].

The above mentioned increases the role of the management system (MS), a component of which is the communication system (CS). Information and telecommunication systems (ITS) ensure the fulfillment of the requirements and the tasks assigned to it, but the rapid development of the forces and devices of radio electronic suppression (RES), information and cyber warfare force us to constantly adjust the ways of development of CS. At the same time, it should be noted that a number of theoretical and practical contradictions in the issues of cyber security assessment in special purpose ITS still remain poorly researched. This is confirmed by the significant imperfection and inconsistency of the current legislation in this important area, especially in the context of the need to improve the management system of the Armed Forces of Ukraine.

Because of this, it becomes obvious that the topic of research, which is aimed at increasing cyber security in special purpose ITS to the required level of performance of the assigned tasks, is relevant.

Therefore, *the object of research* is a special purpose ITS. *The subject of research* is cyber security of special purpose ITS. The purpose of the research is to analyze the conditions and factors that affect cyber security in special purpose ITS.

2. Research methodology

In the course of the conducted research, classical methods were used:
– analysis method – to solve the problem of analyzing the conditions and factors affecting the cyber security of special purpose ITS;
– synthesis method – to substantiate ways of increasing the level of security of special-purpose ITS.

3. Research results and discussion

The analysis of the existing conditions of operation of the special-purpose ITS shows that the special-purpose ITS, when brought to a higher level of combat readiness, is significantly influenced by a combination of external and internal factors.

Special purpose ITS units, depending on the purpose of its application, can conduct operations to repel armed aggression, eliminate armed conflict on the state border or within the state. At the same time, each of them will have a complex character, which combines defensive, offensive (counter-offensive), stabilization, special and other operations with the clear dominance of one of them.

The special purpose ITS is equipped and deployed in accordance with the conditions, the most important of which are [1]:
– the nature of operations;
– the role and place of subdivisions in operational construction;
– purpose, nature, scope and tasks of the operation;
– the combat composition of the groups, the operational formation of the troops and their tasks;
– adopted organization of the military management system and its structure;
– order of organization of interaction in the group;
– the degree of influence of the enemy on the communication system and units of the group;
– physical and geographical conditions of the area of hostilities (operations);
– expected flows of operational information on the main lines of communication.

Let's consider them in more detail. Depending on the nature of the group's operations, the role and place of units in the operational structure is determined. During the operation, the location and role of units may change.

The purpose, nature, scope and tasks of the grouping operation are actually the most important operational conditions and initial data for the organization of communication. They determine [1, 4, 7]: the scope, structure, topology and pace of deployment of the communication system; the order, frequency and magnitude of jumps of movements of communication nodes of control points. They also determine the greatest distance on direct communication lines in order to choose the optimal power of radio-electronic devices, frequencies and antennas.

Combat composition, operational formation of troops and their tasks.

The combat composition of the group is not permanent and is determined by the nature of the group's operation and the tasks it performs.

The group may include: combat military units; military units of military branches; military units and units of Special Forces; military units and units of operational subordination and logistics units.

A possible increase in the combat composition of the group's troops leads to an increase in the number of communication routes from control points, including with troop groups and elements of the operational structure. This complicates the process of communication planning and increases the time for its implementation, and increases the load on the communication and automation parts of the group, which in this case can be additionally strengthened at the expense of the communication parts of the central subordination.

Communication is organized with all elements of the operational construction, and in the period of the operation, when a certain element performs its main task, reinforcement and reservation of communication channels with this element should be provided for.

The combat composition of the group, the operational formation of troops in the operation determine [1, 4, 7]:
– the number of information directions and communication channels, which are organized from communication nodes of control points;

– intensity of capacity, flows of operational information circulating in these directions;
– the order of distribution and use of forces and communication devices;
– determination of a part, an element of the operational construction of troops, which perform the most important tasks according to the stages of the operation, with the aim of organizing the most stable communication with them in the specified time period;
– the distribution of digital streams of the main communication network between elements of the operational construction of troops and the necessary reinforcement of connections and parts with the necessary communication devices;
– the procedure for using digital streams and communication devices of the telecommunication network, departmental networks and communication devices of other state and non-state structures.

The organization of the military management system and its structure have been adopted.

To manage the group's troops in operations, a management system is created, which includes management bodies, control points and management tools (a communication system and sets of automation tools).

To control the troops of the group in operations, preprepared protected control points are used, which are in the operational space, and field mobile control points are also formed. Control points are located (deployed) at such a distance from the front edge that provides stable, continuous control and at the same time the protection from enemy strikes.

From the control points of the group, information directions are created with those elements of the operational construction of the group, the management of which is entrusted to these points of directions.

Depending on the conditions of the situation, the specified distances may change, the movement of control points is carried out as necessary, including to ensure survivability.

In case of forced relocation of the control points of the group, its parts during the operation, reserve areas for their placement are provided. In order to ensure continuity and stability of management, these areas must be prepared in advance in terms of engineering and communication.

Thus, the system of control points of the group and subordinate headquarters, their mutual distance, order and frequency of movement during the operation determine:
– the areas of placement, terms of readiness and directions of movement of communication nodes of the PU group;
– the procedure for transferring connections from one control point to another and measures to ensure the continuity of control in case of movement and failure of control points;
– the choice of communication devices to ensure the management of troops on each direction of communication.

The procedure for organizing interaction in the group.

In the course of the grouping operation, communication must ensure interaction at all stages of the operation.

The most stable connection of interaction is ensured between units with military units of the Armed Forces of Ukraine during repelling airstrikes, repelling enemy attacks, including from the sea; maintaining boundaries and launching counterattacks.

In the middle of the grouping, the relationship of interaction in the operation must be provided between:
– echelons and reserves during the preparation and conduct of a counterattack, withdrawal, change of troops and transfer of responsibility for the corresponding lane;
– artillery units and reserves during operations in tank-dangerous directions;
– military units of the air forces during repelling enemy airstrikes, fighting abroad and ensuring the flight of aircraft in the flight corridors and in the zone of damage of air defense devices;
– military units of the group and naval forces during the defense of the sea coast, ensuring the sea landings, protection and defense of important objects in the operational space;
– combined military and tank units with parts of operational support during the execution of the last tasks according to the relevant types of support.

The degree of influence of the enemy on special purpose ITS is determined by:
– creation of the necessary reserves of forces and devices of communication in order to promptly restore nodes and communication lines that have failed;
– creation of detachments at communication nodes to eliminate the consequences of the enemy's use of devices of mass destruction, teams to search for transmitters of jamming that are thrown;
– planning and carrying out a set of measures aimed at countering the enemy's RES.

The physical and geographical conditions of the operation area have an important influence on the organization and functioning of the communication system. The complex topography of the area, unfavorable weather, climatic and hydrometeorological conditions lead to difficulties and increased time in relation to:
– cable laying and redundancy of radio relay and tropospheric communication lines;
– deployment of communication nodes and implementation of marches;
– organization of combat and technical support of the communication system and troops.

Expected flows of operational information on the main lines of communication determine the number and type of communication devices on these lines. At the same time, it is necessary to take into account that the number of communication types in informational directions is determined by the degrees of their importance and the capabilities of the devices of communication themselves.

In addition, while organizing communication, the following factors should be taken into account:
– availability and condition of forces and communication devices;
– availability of time allocated for planning and organizing communication.

Taking into account the above conditions and factors, cyber security are achieved by the following components:
– a description of devices and assets in cyberspace;
– cyber space audit, detection of software embedded tools, cyber threats, cyber attacks, cyber security incidents, vulnerabilities of communication and automation tools and complexes;
– prompt notification of cyber security incidents;
– prevention of cyber threats, fight against cyber attacks and elimination of the consequences of cyber security incidents;

ISSN 2664-9969

– cyber protection of assets, information and telecommunication systems against software-mathematical (cybernetic) influences of the enemy;
– ensuring network security, host and application security using cyber security tools;
– implementation of cryptographic and antivirus protection of software and hardware and software tools and systems;
– ensuring cyber security of wireless networks;
– cyber protection of departmental communication and special communication systems;
– development and modeling of cyber security measures;
– assessment of the effectiveness of cyber security of information and telecommunication systems and digital technical devices;
– organization of cooperation on cyber protection and management of the cyber security system;
– conducting departmental control (monitoring) of the state of cyber security in information and telecommunication systems.

The conducted analysis of the literature [8–10] on this topic allows to conclude about the need to develop new methods that allow assessing cyber security in a special purpose information and telecommunication system and as a result provide recommendations for improving cyber security. A formalized statement of the task of improving the state of cyber security can be shown by the expression:

$$K_s \in \{K_r, K_{sur}, K_{im}, K_{cs}\} \to \max,$$

where K_r is the reliability coefficient of the communication system; K_{sur} is the survivability coefficient of the communication system; K_{im} is the immunity coefficient of the communication system; K_{cs} is the cyber security coefficient of the communication system.

The limitations of the mentioned research are the need to create an extensive system of cyber intelligence in ITS, which will allow monitoring the changes of the specified indicators in real time.

The direction of further research should be considered the development of methods for increasing the cyber security of special purpose information and telecommunication networks.

4. Conclusions

The research identifies factors that affect cyber security in a special purpose information and telecommunication system. All this must be taken into account while planning and deploying a special purpose information and telecommunication system.

The analysis of the consequences of the impact on the special purpose information and telecommunication system of modern devices of defeat and the impact of RES and other factors was carried out. The analysis showed that a typical special purpose information and telecommunication system does not fully meet the requirements for constant readiness to ensure the management of troops (forces), stability, mobility and bandwidth.

A formalized description of the task of improving cyber security in a special purpose information and telecommunication network is provided. The components that affect the level of cyber security of the special purpose information and telecommunication network during the group's operations have been established.

The impact of the specified conditions and factors should be reflected:
– in planning documents during planning of the deployment and operation of the group's information and telecommunication system;
– in the software, during operational management.

Conflict of interest

The author declares that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

References

1. Shishatckii, A. V., Bashkirov, O. M., Kostina, O. M. (2015). Rozvitok integrovanikh sistem zv'iazku ta peredachi danikh dlia potreb Zbroinikh Sil. *Ozbroennia ta viiskova tekhnika, 1 (5)*, 35–40.
2. Timchuk, S. (2017). Methods of Complex Data Processing from Technical Means of Monitoring. *Path of Science, 3 (3)*, 4.1–4.9. doi: http://doi.org/10.22178/pos.20-4
3. Sokolov, K. O., Gudima, O. P., Tkachenko, V. A., Shiiatii, O. B. (2015). Osnovni napriami stvorennia IT-infrastrukturi Ministerstva oboroni Ukraini. *Zbirnik naukovikh pratc Tcentru voenno-strategichnikh doslidzhen, 3 (6)*, 26–30.
4. Shevchenko, D. G. (2020). The set of indicators of the cyber security system in information and telecommunication networks of the armed forces of Ukraine. *Suchasni informatciini tekhnologii u sferi bezpeki ta oboroni, 38 (2)*, 57–62. doi: https://doi.org/10.33099/2311-7249/2020-38-2-57-62
5. Makarenko, S. I. (2017). Perspektivy i problemnye voprosy razvitiia setei sviazi spetcialnogo naznacheniia. *Sistemy upravleniia, sviazi i bezopasnosti, 2*, 18–68.
6. Zuiev, P., Zhyvotovskyi, R., Zvieriev, O., Hatsenko, S., Kuprii, V., Nakonechnyi, O. (2020). Development of complex methodology of processing heterogeneous data in intelligent decision support systems. *Eastern-European Journal of Enterprise Technologies, 4 (9 (106))*, 14–23. doi: http://doi.org/10.15587/1729-4061.2020.208554
7. Brownlee, J. (2011). *Clever algorithms: nature-inspired programming recipes.* LuLu, 441.
8. Gorokhovatsky, V., Stiahlyk, N., Tsarevska, V. (2021). Combination method of accelerated metric data search in image classification problems. *Advanced Information Systems, 5 (3)*, 5–12. doi: http://doi.org/10.20998/2522-9052.2021.3.01
9. Meleshko, Y., Drieiev, O., Drieieva, H. (2020). Method of identification bot profiles based on neural networks in recommendation systems. *Advanced Information Systems, 4 (2)*, 24–28. doi: https://doi.org/10.20998/2522-9052.2020.2.05
10. Rybak, V. A., Akhmad, Sh. (2016). Analiticheskii obzor i sravnenie sushchestvuiushchikh tekhnologii podderzhki priniatiia reshenii. *Sistemnyi analiz i prikladnaia informatika, 3*, 12–18.

Oleg Sova, *Doctor of Technical Sciences, Senior Researcher, Head of Department of Automated Control Systems, Military Institute of Telecommunications and Information Technologies named after Heroes of Kruty, Kyiv, Ukraine, ORCID: https://orcid.org/0000-0002-7200-8955, e-mail: soy_135@ukr.net*