UDC 621.391 **doi: 10.26906/SUNZ.2019.6.129**

A. Shyshatskyi[1], O. Sova[2], Yu. Zhuravskyi[3], O. Nalapko[1], Yu. Sokil[4], Yu. Ryndin[5]

[1] Central Research Institute of Weapons and Military Equipment of Armed Forces of Ukraine, Kyiv
[2] Military institute of telecommunications and information named after Heroes of Krut, Kyiv, Ukraine
[3] Zhytomyr Military Institute named after S. P. Korolev, Zhytomyr, Ukraine
[4] Military unit A0661, Khmelnytskyi, Ukraine
[5] Military Academy, Odesa, Ukraine

ANALYSIS OF APPROACHES OF INFLUENCE OF ELECTRONIC WARFARE MEANS ON THE ON THE NETWORK-CENTRIC CONTROL SYSTEM

Abstract. The intensive development of information and control technologies, as well as their integration into a single information space, leads to an increase in the role of such technologies in the processes of control of troops (forces) and weapons, including high-precision ones. At the same time, the electronic material base of the information infrastructure created within the concept of network-centric warfare is potentially vulnerable to electronic warfare. In this article, the authors analyze the approaches to the influence of electronic warfare on network-centric control systems. In the course of the study, the authors solved the following interrelated tasks: identified information restrictions on the implementation of the network-centric war concept; the prospects for the development of electronic warfare systems that are focused on disruption of the operation of network-centric systems of military control and the prospective scientific and methodological approaches to substantiate the methods of radio-electronic influence on network-centric control systems. In the course of this research, the authors used the basic principles of electronic warfare theory, signal theory, communication theory, queuing systems and classical methods of scientific cognition - analysis and synthesis. According to the results of the study, the following conclusions can be drawn: perspective directions for the development of radio-electronic influences, oriented on the transport layer of communication networks, can be implemented as complexes of territorially distributed means of electronic control, implementing fundamentally new methods of suppression, and special software and bookmarks software (viruses) that are introduced into the telecommunications network equipment. It should be noted that the use of all the above radio-electronic effects is advisable only against packet networks with advanced topology. The use of such influences against networks with tree topology is pointless given the possibility of attaining the suppression effect of "classical" channel suppression.

Keywords: electronic warfare, use of tools, performance evaluation, open systems interaction model, telecommunication equipment.

Introduction

The intensive development of information and other advanced technologies, as well as their integration into the information and control systems of the armed forces of the leading countries of the world, the continuation of the implementation of the principles of "network-centric concept" of military and weapons control, become the most important factor that determines the course and outcome of modern armed struggle. At the same time, the radio-electronic material base of the "network-centric concept" information infrastructure of conducting a modern armed struggle is potentially vulnerable to the influence of radio-electronic suppression (RES) and it is a direct object of such influence [1-3].

Nowadays, significant progress has been achieved in the development of RES in leading countries of the world, which has increased the capabilities of the latter [4, 5].

The purpose of this research is to analyze approaches to the impact of electronic warfare on network-centric systems.

Presentation of the main material

1. Information restrictions on the implementation of the concept of network-centric war. Some experts point to the impossibility of collecting and analyzing the amount of information that is necessary to make an adequate network-centric war possible. Other experts argue that the mass integration of forces and resources into a single network-centric environment can cause problems with information security [6, 7].

Most experts agree that technology can dictate its terms of military strategy and argue that over-reliance on high technology can present a new vulnerability that can be used by adversaries.

In addition, the following issues arise:

– on the compatibility of the information systems of the combined forces

– the availability of sufficient bandwidth of communication channels and computing resources to create an adequate information model of network-centric war;

– the possibility of managing large amounts of information during the course of the network of the central war.

The experience of using the concept of network-centered war in local wars has shown a number of its problematic aspects. The main ones include the following [8]:

– reassessment of a person's ability to adequately process of a large amount of conflicting information;

– insufficient consideration of the rapidity of the situation on the battlefield;

– a simplified vision of the enemy and, ultimately, his underestimation;

– excessive dependence on information;

- accelerating the process of combat management to such an extent that the speed of decision-making by a

© Shyshatskyi A., Sova O., Zhuravskyi Yu., Nalapko O., Sokil Yu., Ryndin Yu., 2019

person is a "weak link" in the process of commanding troops ";

– the vulnerability of hardware and software in military systems to the impact of RES and IT weapons.

Nowadays, the practical implementation of technical solutions for the management of the network-centric war has led to the information overload of decision-makers.

Let's consider the features of combat in the network-centric war.

Acceleration of the process of combat management. Apologists for the concept of network-centered wars believe that information advantage will lead to decision-making advantages and allow parallel and continuous operations.

Excessive dependence on the information.

The value of vast information resources as a way of developing and conducting effective military operations can be overestimated, as well as the fact that the process of making important military decisions cannot be reduced to a thoughtful analysis of information. Several experts argue that discussions on the transformation of the armed forces are focused on the benefits of information and that the types of armed forces, national security and intelligence agencies have not properly examined the risks associated with the military doctrine that underlies the information.

The following problematic issues, which were identified during the practical application of these systems [1-18]:

– reliance on modern information systems can lead to unreasonable self-confidence of decision-makers;

– quantitative changes in information and its analysis very often lead to changes in the behavior of individuals and organizations, which sometimes leads to opposite results;

– a situation, which is characterized by a wealth of information and capabilities can change the value of the information, make it possible to review the goals of the military mission, and possibly increase the likelihood of making erroneous decisions.

The software is designed to process information, determination of the position of the enemy and their troops, a set of objectives, alarm, as well as to coordinate and control the actions of crews and unmanned combat vehicles on land, at sea and in the air.

For example, according to experts, to work a promising combat system of the ground forces will require 31 million lines of computer program codes [1, 2, 5, 18]. In addition, many combat systems that work with their own equipment will eventually be integrated into network systems. However, as the complexity of network system components increases, we will need to process information from systems whose capabilities and reliability are not always known.

In the article [6] it is emphasized that most often when there is a problem of compatibility in complex systems, there is a desire to achieve greater visibility, to expand the management from a single center and to set higher criteria. Not only are these ineffective, but they also increase the likelihood of technical crashes, user errors, and other downtimes. Normal technical failures occur naturally in complex systems. At the same time, the frequency of failures increases in proportion to the number of information links in the system.

Insufficient consideration of poorly formalized factors in the psychological, cultural and religious spheres.

The experience of recent military conflicts clearly demonstrates that in the conduct of a network-centered war it is necessary to take into account many of those factors that cannot be explicitly registered by intelligence sensors and formalized in the framework of combat models.

Based on an analysis of the results of recent wars, RAND (Research and Development is US strategic research center) staff concluded that "… as remote devices become more sophisticated, there is a likelihood that a potential enemy will develop counter-technology and become more prepared in matters of protection organization, shelter equipment, fraud and application of RES systems. With all this in mind, the network effect will actually turn into a reduction in awareness and, ultimately, a reduction in situational awareness on the battlefield "[8].

2. Prospects for the development of RES systems, which are focused on the disruption of the operation of network-centered military control systems. The perspective approaches, which are presented in this section are based on the authors' scientific research on the substantiation of new approaches to radio-electronic influences, focused on disruption of the functioning of network-centric military control systems.

The basis of this material was based on the review work on the general military-applied principles of disruption of the functioning of network-centric systems of military control [10, 11], as well as work [11-21] with the theoretical substantiation of new methods and technologies of RES, which are oriented against the unified networks of communication the core of the network-centric environment.

Perspective approaches to influence network-centric control systems.

The main paradigm of warfare in the coming decades will be based on the concept of network-centered combat management based on the integration of functionally interconnected subsystems: information, sensory intelligence and combat, which is based on a single network-centric environment. The basis of such a control system is the information subsystem, which integrates the subsystems of intelligence and combat influence.

The analysis of the use of the network-centric principle of management reveals the main tendencies in changing the nature of the military confrontation between technically advanced states in the future [10-35]:

– the ever-growing threat of a pre-emptive complex strike by the enemy with fire and precision instruments coupled with information and radio-electronic influences on the information infrastructure;

– moving to the selective defeat of objects in the territory of the enemy of mainly critical infrastructure of

the country and its armed forces with the use of precision weapons;

– increasing the role of intelligence, operational disguise and protection of troops, the population and objects of the rear from promising means of destruction;

– the rapid nature of ground-to-air combat, dramatic changes in the situation and methods of action of troops;

– conducting information, psychological, camouflage (primarily misinformation) and other special operations to gain and maintain global information and psychological advantage;

– radio-electronic suppression of elements of control systems of troops and weapons, application of software and hardware, economic methods of combat, etc.;

– expanding the scope of space assets for intelligence, command and control of ground, air and naval forces;

– increasing the use of unmanned, robotic and remotely controlled weapons and warfare at all levels;

– expanding the scope of special forces for sabotage-terrorist and reconnaissance-sabotage operations in the deep rear of troops.

The main features of the system of armed struggle in the implementation of the network-centric principle of management will be the following [10]:

– the devices of armed struggle are information-rich and contain elements of networked information infrastructure;

– the duration of the decision cycle is reduced, there is a need to take into account additional factors in the management process, which requires an increase in information system throughput;

– making management decisions, which are based on automated support systems, which are based on information intelligent systems;

– hardware and software tools, that enable interaction within telecommunication networks, form a complex network global information infrastructure;

– elements of network infrastructure (devices of armed struggle, security, control and communication) consist of information and computing systems of various levels of complexity and organization.

At the same time, the network-centric control system will be vulnerable in the following areas [10]:

– destruction of information flows circulating between elements of the system;

– reducing the speed of information exchange between the elements of the system, which will dramatically increase the duration of the cycle "detection-identification-target-lesion" and to minimize the effectiveness of the network is the centric management principle;

– providing sufficiently massive and long-term disabling of network-forming tools.

Thus, in order to implement the aforementioned areas of destructive influence on network-centric control systems, it is necessary to take measures to improve and coordinate the actions of intelligence systems, complexes and devices of RES, communication, control and devices of defeat, to create a directional weapon capable of disrupting the work of automated databases and local area networks, disable the main controls, communications and intelligence of the enemy.

Let us consider one of the promising areas of destructive influence on military control systems based on the network-centric principle, which is relatively easy to put into practice in the near term.

The network management information subsystem is made up of computing systems of varying complexity, which integrate communication networks into a single network-centric environment. One of the main features of the control system, which characterizes their ability to function on purpose, is the stability of the communication system.

Thus, reducing the stability of the communication system due to the integrated use of conventional and high-precision weapons, complexes and tools RES will violate the network management principle.

Modern control systems can be divided into three layers of a network-centric environment, which is formed by the communication system [11, 31]:

1. Physical layer (technical infrastructure of communication systems);

2. Semantic layer (data);

3. Syntax layer (data transfer protocols).

This approach allows us to identify the following impacts [10, 12]:

– effects on the physical layer, which is aimed at the real infrastructure of information and computer systems, data transmission systems and implying their physical destruction;

– effects on the semantic layer, which is related to the violation of the integrity and correctness of information;

– effects on the syntax layer, which is aimed at data corruption and violation of the logic of the systems.

Impacts on the semantic and syntactic layer appear to be simpler, more accessible and relatively easily implemented mechanisms than effects at the physical level using conventional and high-precision weapons.

In this regard, their development is receiving increasing attention. The modern approach to the influence on the semantic and syntactic layers of the network-centric environment involves a complex balanced use of RES complexes and devices, while carrying out measures to protect their management systems and information resources [10].

In view of the insufficiently developed theoretical framework for such actions, the simplest, most expedient way of influencing RES on the radio communication network within the communication system is to simplify their stability in the interests of disturbing the syntactic layer of the network-centric environment of the enemy [10].

However, an analysis of the use of existing "traditional" tactics of suppression and the use of complexes and tools of RES showed that they are not effective enough while using the enemy network-centric management principle.

In the hierarchical control system, when the impact of the RES devices at any level of the hierarchical control system, the passage of information to the

affected tool is blocked and, as a consequence, the non-fulfillment of a combat task by him [10].

Thus, the forms and methods of application of RES complexes and facilities developed prior to the emergence of the network-centric control concept will be ineffective against armed formations operated through a single network-centric environment. In such a system, it is almost impossible to completely block information and control channels.

In order to disrupt such a system, it is necessary to exclude all channels of control and transmission of information or to disable all technical or military devices. In fact, the effect can be achieved if a significant segment is blocked in the system or the transmission of information on any channels in a certain area or zone is excluded. The solution of this problem requires the development of new complexes and tools of RES and, accordingly, new forms and methods of their application [10].

Summarizing the above, we can make the following conclusions [10]:

– the existing approach to the impact of RES on individual elements of the communication system as the basis of a network-centric environment is ineffective;

– by influencing the information infrastructure of a network-centered military control system, the technical basis of which is communication systems and automatic control systems, it is possible to achieve a significant effect of the defeat of this system.

The influence of the territorially distributed heterogeneous grouping of RES will allow you to realize the following of the main directions of counteraction to the control systems, which are constructed in accordance with the network center principle, which was formulated earlier [10]:

– destruction of information flows, which are transmitted in a network-centric environment;

– reducing the speed of information exchange between elements of the network-centric system;

– providing sufficiently massive and long-term disabling of network-forming tools.

The researches, which are presented in the works [11-21] show that the most effective for destructive impact on network-centered military control systems will be the defeat of the space segment of the information subsystem, which, on the one hand, performs global information security functions, and on the other is built on the base of the radio communications and consequently vulnerable to the RES use.

Reducing the quality of space grouping will lead to multiple problems in the performance of the information subsystem, as well as in the application of many types of weapons and military equipment, since it is the space segment, including space systems intelligence, communications, navigation, topo-geodetic and meteorological, the information and control circuit that underlies the architecture of the global information subsystem.

In this case, the implementation of the defeat of various components of such information and control circuit will lead to the impossibility of each of the systems to provide the performance of all or part of its inherent functions. In particular, we can distinguish [10]:

– in space exploration, the inability to transmit, with due time, messages on object detection, targeting and operational control of impact results, as well as data for determining the devices of the used impact;

– in space communication systems, the inability to provide, with specified quality, the transmission of combat command messages, to exchange data between military formations and governing bodies, including the prompt transfer to data control points for the preparation of strikes, and their result;

– in space topo-geodetic systems, the inability to transmit communications to ensure that military authorities of all levels have reliable topographic and geodetic data with given timeliness, to provide troops with special maps and photo documents of the terrain, as well as to prevent access to digital information arrays in the interests of targeting systems;

– in space radio navigation systems, the suppression will result in the failure of the radio navigation systems and, accordingly, the impossibility of creating navigation fields used in determining the location of military formations, combat and other equipment, shocks and devices of destruction.

Thus, taking into account the specifics of the modern transition to the implementation of the network-centric principle of management, it is interesting to use the existing REF complexes and facilities as a basis for defeating such a system of military control.

3. Prospective scientific and methodological approaches to the substantiation of methods of radio-electronic influence on network-centric control systems.

Based on the above arguments, it is possible to formulate a number of approaches to the technological implementation of the destructive impact on communication systems that form the network-centric environment of the network-centered control system.

Given the specifics of the modern transition to the implementation of the network-centric control principle, it is interesting to use radio-electronic influences based on the development of forms and methods of using existing RES complexes and facilities as a basis for the defeat of such a system of military control [10, 11].

Until recently, most of the work on RES was devoted to solve the problems of suppressing individual lines of communication, that is, suppressing at the physical level the model of interaction of open systems OSI (Open Systems Interconnection).

There are some researches, which are dedicated to the suppression of the radio networks, considering their structure, logic and the value of the transmitted information. However, by analyzing the possibilities of using “traditional” RES facilities, we can conclude that their impact is possible on other objects of the transport subsystem of the OSI model (physical, channel, network and transport levels).

Physical-electronic impact objects have traditionally been radio-electronic means and communication channels. At the link layer, such objects

include multiple access channels for the formation of separate networks (for example, based on TDMA, ALOHA, DVB-RSC).

Objects of electronic effects on the OSI network layer include components, transport channels of the combined network connection, routing and signaling protocols to ensure their functioning.

At the transport level, the objects of influence should include protocols and firmware to ensure the quality of service of the transmitted information flows over the integrated communications network.

The impact of RESs leads to various negative effects at different levels of OSI, the main ones of which are presented in Fig. 1.

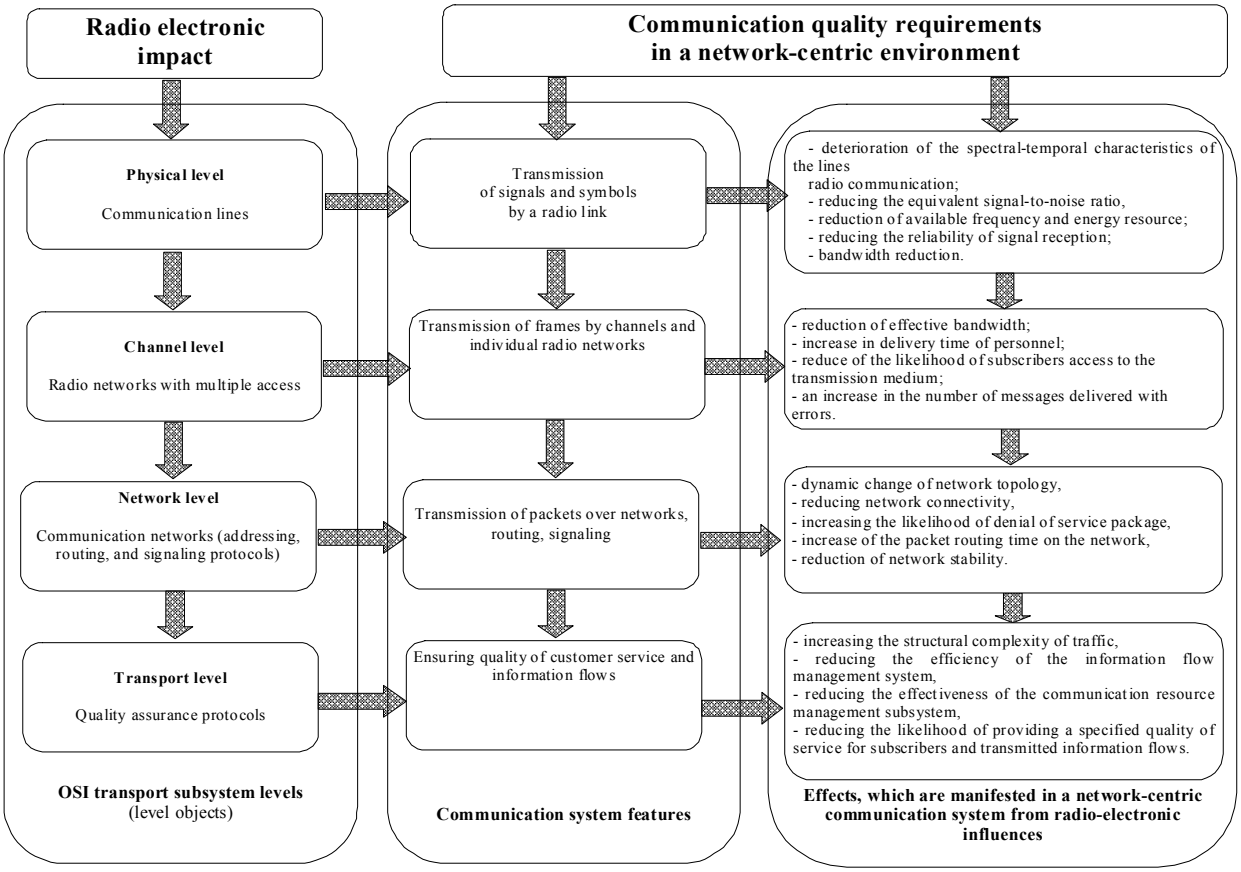

Fig. 1. The main negative effects that can cause radio-electronic effects at different levels of the transport subsystem of the OSI model [10, 11]

In this case, the direct object of influence will be the individual radio lines and radio networks operating within the integrated communications networks. Thus, promising ways to suppress integrated communications networks will use the effects of the destructive effects of radio-electronic influences on the physical layer as a basis for the formation of suppression effects at the higher levels of the OSI channel, network and transport models [10] (Fig. 2).

Currently, to solve the problems of ensuring the quality of service of telecommunication networks, numerous researches are conducted on the effectiveness of functioning of communication networks and switching devices of different levels in terms of transferring traffic of complex structure (presence of self-similar properties, non-poisson distribution of the time of packet arrival, etc.), as well as routing information flows in networks with dynamically variable topology.

Researches on this topic indicate a significant reduction in the speed and efficiency of servicing these information flows when transmitting them over networks with dynamically variable topology. It is proposed to use the available results of these studies in the field of evaluation of the quality of service of telecommunication networks for the development of new solutions for the organization of radio-electronic suppression of network-centric systems [10].

At the same time, these data allow us to organize new interferences at the physical level, which, on the one hand, are not determined by existing means of protection, and on the other are focused on reducing the efficiency of the network and transport layer functioning, because they cause a number of negative effects at these levels [10].

Let's look at some of the promising areas for developing electronic effects that are focused on suppressing unified communications by taking into account the features of protocols on the OSI channel, network, and transport levels.

The main feature of the effects considered the accounting for the impact of interference, which allows us to consider dynamic transient and transient modes in the objects of suppression, as well as functional dependencies between protocols at different levels of the OSI model.

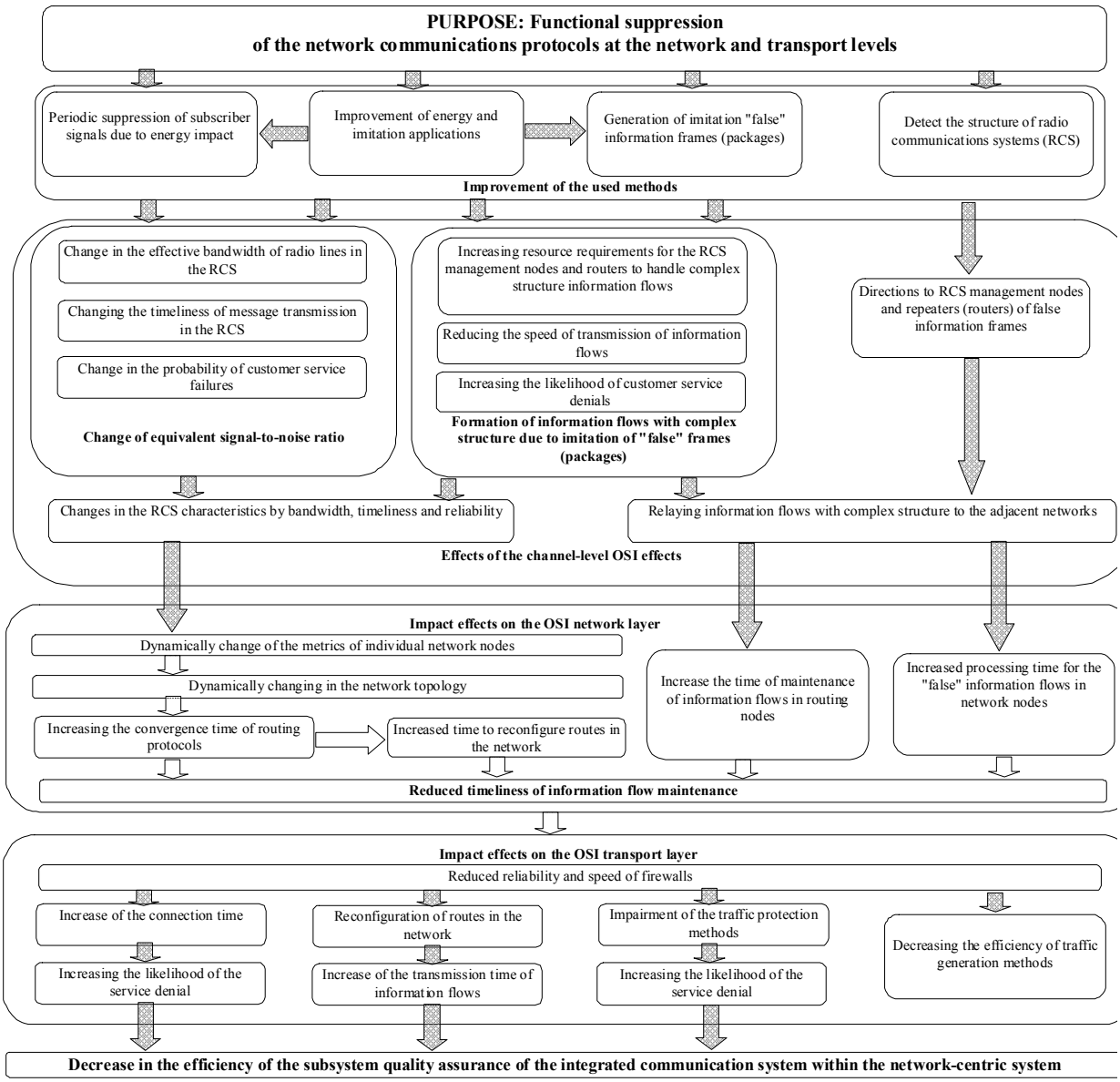

Fig. 2. Radio-electronic effects, which are oriented on the functional suppression of the networking protocols of the network-centered control system

Let's consider the main types of influences that can be applied to network-centric systems.

1. Radio-electronic influences, which are aimed at suppressing individual multiple access networks.

The researches of the possibilities of radio-electronic influences on suppression of communication protocols at the link layer, which are presented in the works [11-21], have shown the following.

It is known that packet radio networks that use a common multiple random access (MRA) channel to transmit packets have inherent instability. Such radio networks require correction during a long time of continuous operation. Thus, it is possible to implement a radio-electronic effect aimed at suppressing a radio network based on a common radio channel with a random MRA by periodically interfering with deliberate interferences and by using the specific properties of the random access method. This approach for suppression of the radio network was firstly proposed in the works [10, 11] for the networks based on the CSMA/CA and S-Aloha protocols.

The process of servicing packets in these radio networks with a random MRA was presented as a Markovian process of death-reproduction, in which the intensity of packet service is determined by the bandwidth, which, in turn, depends on the current value of the signal/interference ratio.

The simulation showed that the dynamic intermittent interference of the interference on the common channel of such radio networks leads to their demolition to their blocked status even after the removal of radio-electronic influence. In this case, the suppression effect can be achieved without the complete suppression of the channel of the MRA, and by partial reduction of its throughput, within 10-20%.

This method of radio-electronic exposure, focused on the channel layer OSI, can be implemented by "traditional" RES by introducing a dynamic interference

mode, the time parameters of which are consistent with the parameters of the protocol random MRA, which is used in the radio network [10, 11].

Modern communication systems are built on the basis of MIMO technologies, in which several ways can be selected for sending messages to the addressee.

In the future, the above-mentioned field of development of radio-electronic influences was developed in the form of a multi-channel queuing system with the interlocking of individual channels, modeling the MIMO communication system, which is presented in the work [18]. Periodic impact in the form of suppression of individual radio channels in a multi-channel communication system leads to a significant decrease in the quality of service of such a system and ultimately to the overloading of the system with packets and its transition to a blocked status.

The simulation performed in the work [18] showed that when the system lock criterion is fulfilled, its throughput decreases from 100% to 70%, and the service time in a multichannel radio system increases by 10-20 times relative to the level corresponding to its normal functioning.

Thus, dynamic radio-electronic influences make it possible to translate the radio network into a non-stationary mode of operation, increase the duration and depth of transients in them. Increasing the intensity of influences allows the radio networks to be locked in as a result of a decrease in the intensity of the incoming packet inflow below the critical values.

2. Radio-electronic effects, which is aimed at suppressing the integrated geographically distributed mixed communications networks.

The principle of interference with dynamically variable parameters for varying the bandwidth of channels in their working signal-to-noise ratio (to exclude the triggering of physical layer interference protection) was further developed for the development of radio-electronic influences aimed at suppressing interconnection networks features of the functioning of their protocols on the network layer of the OSI model.

In order to take into account the effects of dynamic radio-electronic impact at the network level, it was proposed to recalculate the quality of service of individual networks and radio communication channels in the network metric coefficients used by the respective protocols in solving network signaling and routing problems in it.

A mathematical model formalizing the estimation of network channel metrics in terms of dynamic interference with respect to DVB-S/S2 satellite channels is presented in the work [12]. The simulation for the DVB-S2 communication channel showed that a periodic change in the signal/interference ratio in the channel (upward and downward) leads to the issuance of channel metric change messages, which in turn lead to stopping the process of transferring and recalculating the network topology. The intensity of these messages is directly proportional to the frequency and depth of the signal-to-noise ratio and the time between individual messages can generally be approximated by an exponential distribution.

The analysis of the effects of suppression on adaptive-avalanche routing protocols (OSPF, IS-IS, EIGRP, etc.), which was carried out in the works [16-40], showed that such influence leads to an increase in the re-routing intensity of information flows and reducing the adequacy of routing tables.

The research of the process of functioning of the router with an adaptive-avalanche protocol (based on OSPF), is conducted in the work [13], showed that the probability of suppression of the communication network is determined by the intensity of failures of individual channels due to the interference, as well as by the parameter of the routing by the waiting time of the recovery time. Moreover, the size of the communication network practically does not affect the efficiency of its suppression.

There is a fundamental possibility of suppressing the communication network when it is exposed to a given intensity even on one radio channel in its composition.

In the article [22], to model the temporal parameters of radio-electronic impact, which is aimed at disrupting the operation of routing protocols without establishing a connection, a model of the functioning of the communication object in terms of communication channels failure in the form of a Markov process of transitions between the "channel failure" - "waiting for the connection recovery" - "router reconfiguration" states were developed.

The use of this model as a part of the technique of justifying the time parameters of radio-electronic influence on the routing protocol by the state of the channels (on the example of the OSPF protocol) allowed us to determine the most difficult operating conditions for this routing protocol. The simulation results show that when the time parameters of the impact and the routing protocol are agreed, the readiness of the individual router is reduced to 0.5. Due to the avalanche of adjacent message nodes changing the metrics of individual channels, each of the routers of the network reduces its availability by constantly recalculating the shortest paths. As a result, the effect of reducing stability applies to the whole network as a whole. At the same time, the network stability indicator is reduced to 0.4-0.2 by the "average network probability of information communication direction" indicator. In this case, the degree of network stability is proportional to the average length of the link.

In the article [20], to justify the temporal parameters of radio-electronic impact, which is aimed at disrupting the operation of routing protocols with connection, a model of functioning of the information direction of communication was developed, which takes into account not only the process of reconfiguration of individual routers due to the failure of channels, but also accounting for the structure connections, as well as the network approach, which is taken to backing up routes. The results of radio-impact effects simulations show that connection-based routing networks reduce their resilience by reducing the resilience of connections that pass through the affected nodes. In this case, the level of stability reduction is proportional to the number of

nodes that are affected. On the basis of this model, a technique for substantiating the time parameters of radio-electronic influence on the routing protocol with the establishment of connections was further developed, which allows to justify the time parameters of dynamic interference, which reduce the stability of the network to values below the required ones.

To confirm the adequacy of the developed scientific and methodological apparatus of substantiation of the methods of radio-electronic influence and practical confirmation of the effects of functional suppression of networks, experimental studies were conducted on the basis of the network with the OADV protocol (Ad hoc On-Demand Distance Vector), the results of which are presented in the article [19].

A comparison of the theoretical calculations and experimental data, which was obtained, makes it possible to conclude on practical confirmation of the possibility of such radio-electronic influences to perform effective functional suppression of networks.

The above-mentioned perspective directions for the development of radio-electronic influences, oriented on the network layer of the OSI model, can be implemented by territorially distributed "traditional" RES complexes due to the introduction of dynamic interference mode, the time parameters of which are consistent with the parameters of the routing protocol, which is used by the network.

Additionally, an analysis of the influence of cryptographic information security in the communication channels on the effectiveness of the considered electronic effects was conducted. This analysis has shown that the use of standard VPNs and packet-mode crypto-routers (which make up the vast majority of modern cryptographic protection solutions) is not a complication for such radio-electronic influences and allows them to maximize their functionality for suppressing both networks and individual information destinations.

3. Radio-electronic influences, which are aimed at disrupting the quality of service protocols in the integrated communications networks.

A promising area for the development of radio-electronic impacts, which were aimed at suppressing unified networks at the transport layer of the OSI model is the development of influences focused on traffic generation and disruption of service quality protocols.

Well, promising radio-electronic influences are the effects that are oriented to form a channel packet flow of a complex structure with a coefficient of variation that is greater than one and significantly different from the simplest.

The analysis of the results of modeling the processing of complex structure flows at the network switching nodes, which is presented in the articles [15-36] showed that the timeliness of processing such flows is ten times lower relative to the processing of the simplest flows. In this case, this effect is observed on high-voltage switches.

The first variant of such electronic influence is presented in the article [20] and it is based on the introduction of additional simulation traffic, which allows to generate the output stream of packets from the channel due to the structure, which is significantly different from the simplest one (coefficient of variation is greater than one). A distinctive feature of this impact is the need to introduce additional packages, which are copies of previously transferred packages, which in some cases can lead to the "destruction" of the information flow. In addition, a number of protocols (such as IPSec) number packets within a data session, enabling them to detect implemented packets in traffic. This disadvantage is deprived of the second variant of radio-electronic influence, focused on the complete interception and transformation of the structure of information flow [21]. The evaluation of the results of these radio-electronic impacts, focused on the formation of a complex traffic structure, critical to delays, showed that the stability of the network is reduced by reducing the timeliness of traffic service at its nodes and the actual blocking of nodes that transmit complex traffic. These electronic effects are a variant of complex DOS attacks.

In addition, the effect of the effect is manifested in the fact that the generated information flows are transmitted further through the network, reducing the timeliness of processing in other nodes. In this way, radio-electronic impact data can suppress specific communication directions. At the same time, the level of network stability decrease under such influences is proportional to the number of modified information flows, their speed and the average length of the communication direction.

The conclusion from the article

Further promising development of the direction of creation of radio-electronic influences, focused on suppression of networks at the transport level, is the development of a complex of models reflecting the process of functioning of the Diff Serv model in ensuring the quality of service of subscribers and information flows, as well as technologies of traffic formation (traffic shaping) and technologies of parameter control and traffic policing in the conditions of directed destructive radio-electronic influences.

The presence of such models will allow us to substantiate a set of radio-electronic influences, focused on the functional suppression of modern network technologies of quality assurance of service.

Their application will not allow to provide the necessary values of indicators of the functioning of the unified communication network, namely - to reduce the probability of stability of the information direction of communication and to increase the probability of failure of service.

Perspective directions of development of radio-electronic influences, oriented on the transport layer of communication networks, can be implemented both by complexes of territorially distributed RESs, implementing new methods of suppression, and by hardware and software bookmarks and special software (viruses), which are implemented in the telecommunication equipment.

It should be noted that the use of all the above radio-electronic effects is impractical only against packet networks with advanced topology. The use of such effects against networks with tree topology is impractical, which is given the possibility of attaining the suppression effect of "classical" channel suppression.

Thus, one of the promising ways of counteracting a network-centric integrated command structure is to use the radio-electronic effects that are oriented on the syntactic layer of the network-centric environment and violate the availability of information resources of that environment by affecting the communication subsystem.

Prospective methods of radio-electronic interference suppression of the oriented networks can use the effects of destructive effects at the physical level as a basis for the formation of suppression effects at the channel, network and transport levels of the OSI model.

In this case, new at this stage of research, and sufficiently elaborated methods of radio-electronic influences, include the following:

– a method of radio-electronic impact at the channel level, which is focused on congestion of multiple access networks due to the dynamic change of the signal/interference ratio in the common radio channel;

– a channel-level radio-electronic impact method, which is aimed at congesting the multi-channel communication systems by periodically suppressing individual communication channels in such a system;

– a method of radio-electronic impact at the network level, which is aimed at reducing the efficiency of routing protocols in the network by periodically changing the bandwidth of individual communication channels, which leads to a dynamic change in the topology;

– a method of electronic influence at the transport level, which is aimed at reducing the effectiveness of quality assurance protocols in the network due to the directional formation of the complex structure of the transmitted traffic.

In general, the novelty of these methods of electronic influence is the use of "traditional interference" to generate and develop internal system conflicts in the communication system at the upper levels of its functioning. Specifically, interferences with dynamically changing parameters that lead to transient and non-stationary processes at the upper OSI levels are considered.

A new achieved effect is the suppression of the communications network as a whole, including the wired segment, by influencing radio channels as a kind of "radio-electronic impact entry point".

References

1. Cebrowski, A. K. and Garstka J. J(1998). "Network-Centric Warfare: Its Origin and Future". U.S. Naval Institute Proceedings. Annapolis (Maryland).
2. Hersprin, D. R(2008). "Rumsfeld's Wars: The Arrogance of Power. Lawrence, Kans.": University Press of Kansas.
3. Intelligence and Electronic Warfare (IEW) System Fact Sheets. Fort Huachuca, Arizona: U.S. Army Intelligence Center, 1994. 39 p. available at :: http://www.dtic.mil/dtic/tr/fulltext/u2/a390663.pdf (last accessed november 25, 2019).
4. FY 2015 budget request funds Electronic Warfare Development. PE 0604270A: Electronic Warfare Development Army. U.S. Army, 2014. 31 p. available at : http://www.globalsecurity.org/military/library/budget/fy2015/army-peds/0604270a_5_pb_2015.pdf (last accessed november 25, 2019).
5. Electronic Warfare Planning and Management Tool (EWPMT). United States Army Acquisition Support Center. 2016. available at : http://asc.army.mil/web/portfolio-item/iews-electronic-warfare-planning-and-manage ment-tool-ewpmt/ (last accessed november 25, 2019).
6. JP 3-13.1. Electronic Warfare. US Joint Chiefs of Staff, 2007. 115 p.
7. Shyshatskiy, A.V., Bashkirov, O.M. and Kostina, O.M (2015). "Development of integrated systems and data for Armed Forces", Arms and military equipment, No 1(5), pp. 35-40. available at : http://journals.uran.ua/index.php/2414-0651/issue/view/1%285%29%202015 (last accessed november 25, 2019).
8. Kalantaievska, S., Pievtsov, H., Kuvshynov, O., Shyshatskyi, A., Yarosh, S., Gatsenko, S., Zubrytskyi, H., Zhyvotovskyi, R., Petruk, S. and Zuiko, V. (2018). "Method of integral estimation of channel state in the multiantenna radio communication systems.", Eastern-European Journal of Enterprise Technologies. Vol 5, No 9 (95): pp 60–76. DOI: https://doi.org/10.15587/1729-4061.2018.144085 (last accessed november 25, 2019).
9. Zhuk, O.G., Shyshatskiy, A.V., Zhuk, P.V. and Zhyvotovskyi, R.M (2017). "Methodological substances of management of the radio-resource managing systems of military radio communication", Information Processing Systems, Vol. 5(151), pp. 16-25. https://doi.org/10.30748/soi.2017.151.02 (last accessed november 25, 2019).
10. Kuvshinov, O.V., Shyshatskiy, A.V., Lyutov, V.V and Zhuk, O.G(2017). "Analysis of ways for increasing the secrecy of broadband radiocommunication systems " Scientific works of Kharkiv National University of Air Forces, No. 1(50), pp. 24-28.
11. Popov, A.O. and Tverdokhlibov, V.V(2014). "General tendencies of development of means of electronic warfare ", Arms and military equipment, No. 4 (4), pp. 4-10.
12. Shyshatskiy, A., Kalantaievska, S., Malyk, O., Tiurnikov, M., Zhuk, P. and Pikul, R(2019). "Foundation the ways of radio electronic warfare devices development". Advanced information systems. No. 3(2). pp. 98-103.
13. Shyshatskiy, A., Yakhno, I., Malyk, O., Hatsenko, S. and Pikul, O(2019). "Method of assessment of information availability of radio inflammation sources by devices of radioelectronic recognition. Advanced information systems. 2019. No. 3(1). pp. 98-103.
14. Shyshatskiy, A., Hordiichuk, V., Sergienko, V., Mishchenko, A. and Pozdniakov, P(2019). "Analysis of technical characteristics of the radioelectronic intelligence of the Russian Federation". Системи управління, навігації та зв'язку No.1 (53). pp. 142-146. DOI: 10.26906/SUNZ.2019.1.142.

15. Shyshatskiy, A., Yakhno I., Malyk, O. and Hatsenko, S(2019). "Foundation of the factors affecting the planning and management of the radioelectronic developmen". Системи управління, навігації та зв'язку No.1 (53). pp. 162-167. DOI: 10.26906/SUNZ.2019.1.162.
16. Kopylov, A. V(2011). "On the weaknesses of the American concept of "network-centric wars (operations)"". Military thought. No. 7. pp. 53-62.
17. Sidorin, A. N. Prishchepov, V. M. and Akulenko, V. P(2013). "The US Armed Forces in the 21st Century: Military Theoretical Labor". Moscow : Kuchkovo field; War book, 800 p.
18. Makarenko, S. I(2016). "Radio-electronic informational effects on communication networks of a network-centric control system". Bulletin of the Air Force Academy. No. 3 (27). pp. 108-117.
19. Antonovich, P.I., Makarenko, S.I., Mikhailov, R.L. and Ushanev, K.V(2014). "Promising methods of destructive impact on military control systems in a single information space. Bulletin of the Academy of Military Sciences. No. 3 (48). pp. 93-101. — available at : http://www.avnrf.ru/attachments/ article/669/AVN-3(48)_001-184.pdf (last accessed November 25, 2019).
20. Makarenko, S.I(2012). "Evaluation of the quality of service of a packet radio network in an unsteady mode under the influence of external destabilizing factors". Journal of Radio Electronics. No. 6. p.2. — available at : http://jre.cplire.ru/jre/jun12/9/text.pdf (last accessed November 25, 2019).
21. Makarenko, S.I(2011). "Suppression of packet radio networks with random multiple access due to destabilization of their state". Journal of Radio Electronics. No 9. p. 2. available at : http://jre.cplire.ru/jre/sep11/4/text.pdf (last accessed November 25, 2019).
22. Makarenko, S. I., Mikhailov, R. L. and Novikov, E. A(2014). "Research of channel and network parameters of a communication channel in a dynamically changing signal-noise situation". Journal of Radioelectronics. No. 10.— available at : http://jre.cplire.ru/jre/oct14/3/text.pdf (last accessed November 25, 2019).
23. Makarenko, S. I. and Mikhailov, R. L(2016). "Information conflicts - analysis of work and research methodology". Management, communication and security systems. No 3. pp. 95-178. — available at : http://sccs.intelgr.com/archive/2016-03/04-Makarenko.pdf (last accessed November 25, 2019).
24. Makarenko, S. I., Afanasyev, O. V., Baranov, I. A. and Samofalov, D. V(2016). "Experimental studies of the reaction of the communication network and the effects of rerouting information flows under dynamic changes in the signal-noise situation" Journal of Radio Electronics. No. 4.— available at : http://jre.cplire.ru/jre/apr16/4/text.pdf . (last accessed November 25, 2019).
25. Mikhailov, R. L. and Makarenko, S. I(2013). "Assessment of the stability of a communication network under the influence of destabilizing factors on it". Radio engineering and telecommunication systems. No.4. pp. 69-79.
26. Makarenko, S. I(2015). "Time of convergence of routing protocols in case of network failures". Management, communication and security systems. Np. 2. pp. 45-98. — available at : http://sccs.intelgr.com/archive/2015-02/03-Makarenko.pdf (last accessed November 25, 2019).
27. Makarenko, S.I. and Mikhailov, R.L. "Adaptation of signaling parameters in the routing protocol with the establishment of connections under the influence of destabilizing factors on the network". Control, communication and security systems. 2015. No. 1. pp. 98-126. — available at : http://sccs.intelgr.com/archive/2015-01/07-Makarenko.pdf (last accessed November 25, 2019).
28. Makarenko, S. I(2015). "A dynamic model of a communication system under the conditions of a functionally multilevel information conflict of observation and suppression". Control, Communication and Security Systems. No. 3. pp. 122-185. — available at : http://journals.intelgr.com/sccs/archive/2015-03/07-Makarenko.pdf (last accessed November 25, 2019).
29. Makarenko, S. I(2014). "Intentional formation of the information flow of a complex structure due to the introduction of additional simulation traffic into the communication system." Cybersecurity issues. No. 3 (4). pp. 7-13.
30. Makarenko, S. I., Korovin, V. Mand Ushanev, K. V(2016). "Traffic conversion operator for deliberately increasing the structural complexity of information flows". Control, Communication and Security Systems. No 4. pp. 77-109. — available at : http://sccs.intelgr.com/archive/2016-04/04-Makarenko.pdf (last accessed November 25, 2019).
31. Makarenko, S. I., Ryumshin, K. Yu. and Mikhailov, R. L(2014). "A model of the functioning of a communication network object in conditions of limited reliability of communication channels". Information Systems and Technologies. No. 6 (86). pp. 139-147.
32. Shyshatskiy, A., Zhuravskyi Yu., Kuvshinov, O., Hurskyi, T., Vozniak, R., Pikul, R. and Pikul, O(2019). "Vector-space approach to evaluation of the efficiency of use of radioelectronic controls". Advanced information systems. No 3(3). pp. 68-75. DOI: 10.20998/2522-9052.2019.3.10.
33. Gurskyi, T. G., Zhuk, O. G., Krivenko, O. V. and Shyshatskyi, A. V(2016). "Directions of improvement of facilities of radio communication with pseudorandom reconstruction of the working frequency. Collection of scientific works of MITI. No. 1. pp. 25-34.) available at: http://www.viti.edu.ua/index.php?view=coll_2016_1 (last accessed November 25, 2019).
34. Shyshatskyi, A.V., Lutov V. V. and Zhuk, O. G(2015). "Analysis of ways of increasing the efficiency of radio communication systems with orthogonal frequency multiplexing". Scientific and technical journal "Arms and military equipment.". – K.: CSIAM AF of Ukraine. No. 4(8) p.22-26: available at : http://nbuv.gov.ua/UJRN/ovt_2015_4_5. (last accessed November 25, 2019).
35. Shyshatskyi, A. V., Olshanskyi, V. V. and Zhyvotovskyi, R. M(2016). "Algorithm of the choosing working frequencies for facilities of military radio communication in the conditions of intentional interference". Systems of armament and military equipment. No. 2. - P. 62-66. available at: http://www.hups.mil.gov.ua/periodic-app/article/16881 (last accessed November 25, 2019).
36. Shyshatskyi, A.V. and Zhuk, P.V. (2017) "Perspective of signal-code designs for wireless communication systems of the standard 5G. Scientific-practical conference "Priority directions of development of telecommunication systems and networks of special purpose". Application of subdivisions, complexes, communication facilities and automation in ATO" 9 – 10 november 2017 year (Reports and abstracts), Kyiv: MITI, pp.269-270. available at: http://www.viti.edu.ua/files/zbk/2017/1/c_2017_1.pdf (last accessed November 25, 2019).

37. Romanenko, I. O., Shyshatskyi, A.V., Zhyvotovskyi, R. M. and Petruk, S.M (2017). "The concept of the organization of interaction of elements of military radio communication systems". Science and Technology of the Air Force of the Armed Forces of Ukraine. No 1. pp. 97-100.
38. Romanenko, I. O., Zhyvotovskyi, R. M., Petruk, S.M., Shyshatskyi, A.V. and Voloshin, O.O (2017). "Mathematical model of load distribution in special purpose telecommunication networks". Information processing systems. No.3. p. 61-71.
39. Shyshatskyi, A.V(2017). "The technique of choosing operating frequencies in a complex electromagnetic environment. Management", Navigation and Communication Systems Collection of Scientific Papers of the Yuri Kondratyuk National Technical University. No. 1(41).pp. 146-149.
40. Zhuravskyi, Y.V. and Kirilluk, V.A(2015). "The suppression factor of radio communication systems with pseudorandom frequency change.Problems of creation, testing, application and operation of complex information systems: coll. Sciences. wash. - Zhytomyr : ZVY, Issue. 10, pp. 141-147.
41. Zhuravskyi, Y.V. Zhovnovatyuk, R.M., Nosova, G.D. and Zavada, A.A(2015). "Analysis of the influence of radio-masking measures on intelligence protection of electronic means". Problems of creation,testing, application and operation of complex information systems. - Zhytomyr: ZVY. Issue. 10. pp. 43–50.
42. Sova O.Ya., Romanuk, V.A. Zuk, P.V. and Umanec, Ya. L(2012). "Synthesis methodology of smart nodes management systems of perspective mobile radio networks with dynamic topology". Collection of scientific works of HUPS. No 3. pp. 51 – 60.
43. Salnik, S.V., Salnik, V.V., Sova, O. Ya. and Stampkovskaya, Ya.A (2016). "Model of invasion of mobile radio networks of the class MANET". Proceedings of Kharkiv National University of the Air Force. No.(46). pp. 79-84.
44. Sova, O. Ya(2015). "An intelligent model for ensuring the radio connectivity of MANET mobile network nodes". Weapons systems and military equipment. No. 2(42). pp. 134-151.
45. Salnik, S.V., Salnik, V.V., Simonenko, O.A. and Sova, O. Ya(2015). "A method for detecting intrusions into mobile radio networks based on neural networks". Science and Technology of the Air Force of the Armed Forces of Ukraine. No. 4(21). pp. 82-90.
46. Sova, O. Ya., Minochkin, D.A., Romanyuk, V.A. and Zhuk, P.V(2015). "Model of organization of information resources of intelligent management systems of nodes of mobile radio networks of the class MANET". Science and Technology of the Air Force of the Armed Forces of Ukraine. No. 2(19). pp. 51-57.
47. Symonenko, O.A., Osurko, V.M., Minochkin, D.A. and Sova, O. Ya(2015)."Threats of secure transmission of information in mobile radio networks of the class MANET and methods of their elimination". Science and Technology of the Air Force of the Armed Forces of Ukraine. No. 1(18). pp. 109-113.
48. Sova, O. Ya., Romanyuk, V.A., Stampkovskaya, Ya.A. and Simonenko, O.A (2014). "Coordination of target functions of intelligent MANET tactical radio control systems". Proceedings of Kharkiv National University of the Air Force. No 3(40). pp. 85-92.
49. Simonenko, O.A., Sova, O. Ya., Romanyuk, V.A. and Umanec, Ya. L(2014). "Analysis of existing agent platforms for the construction of MANET nodes management systems for mobile radio networks". Information processing systems. No. 1(117). pp. 200-203.
50. Kravchuk, S.A., Minochkin, D.A. and Sova, O. Ya(2013). "Analysis of directions of increasing the efficiency of functioning of modern satellite communication systems". Science and Technology of the Air Force of the Armed Forces of Ukraine. No. 2(11). pp. 140-147.

Received (Надійшла) 24.09.2019
Accepted for publication (Прийнята до друку) 20.11.2019

Аналіз підходів впливу засобів радіоелектронного подавлення на мережецентричну систему управління

А. В. Шишацький, О. Я. Сова, Ю. В. Журавський, О. Л. Налапко, Ю. М. Сокіл, Ю. І. Риндін

Анотація. Інтенсивний розвиток інформаційних та управляючих технологій, а також їх інтеграція в єдиний інформаційний простір приводить до підвищення ролі таких технологій у процесах управління військами (силами) та зброєю, у тому числі високоточною. Разом із тим, радіоелектронна матеріальна основа інформаційної інфраструктури, що створюється в рамках концепції мережецентричної війни, є потенційно уразливою для засобів радіоелектронної боротьби. В зазначеній статті авторами проведено аналіз підходів щодо впливу засобів радіоелектронної боротьби на мережецентричні системи управління. Авторами в ході проведення зазначеного дослідження вирішені наступні взаємопов'язані завдання: визначено інформаційні обмеження щодо реалізація концепції мережецентричної війни; визначено перспективи розвитку систем радіоелектронної боротьби, що орієнтовані на порушення функціонування мережецентричних систем військового управління та визначено перспективні науково-методичні підходи до обгрунтування способів радіоелектронного впливу на мережецентричні системи управління. В ході зазначеного дослідження авторами використані основні положення теорії радіоелектронної боротьби, теорії сигналів, теорії зв'язку, систем масового обслуговування та класичні методи наукового пізнання – аналізу та синтезу. За результатами проведеного дослідження можна зробити наступні висновки: перспективні напрямки розробки радіоелектронних впливів, орієнтованих на транспортний рівень мереж зв'язку, можуть бути реалізовані як комплексами територіально розподілених засобів радіоелектронної боротьби, що реалізують принципово нові способи подавлення, так і апаратно-програмними закладками і спеціальними програмними засобами (вірусами), які впроваджуються в телекомунікаційне обладнання мережі. Необхідно відзначити, що застосування всіх вищевказаних радіоелектронних впливів доцільно виключно проти пакетних мереж з розвиненою топологією. Застосування подібних впливів проти мереж з деревовидної топологією безглуздо зважаючи на можливість досягнення ефекту придушення "класичним" придушенням каналів.

Ключові слова: радіоелектронна боротьба, застосування засобів, оцінювання ефективності, модель взаємодії відкритих систем, телекомунікаційне обладнання.