Robot technological system of analysis of cybersecurity information systems and communication networks

E A Maksimova¹,³, ⁶, N P Sadovnikova¹, V V Baranov ², Yu Yu Gromov³, O S Lauta⁴, L V Tret'yakova⁵

¹Department of Information Security, Volgograd State University, 100 Universitetskaya, Volgograd, 400062, Russia
²Department of Information Security, South Russian state Polytechnic University NPI named after M. I Platov, Enlightenment 132, Novocherkassk, 346428, Russia
³Institute of Automation and Information Technology, Tambov State Technical University, 1 Leningradskayastr,Tambov, 392036, Russia
⁴Department of Information Security, Military Academy on Communications n.a.Budenny, 3 Tikhoreckiyave., St Petersburg, 194064, Russia
⁵Department of Information Security, Sevastopol state University, 33Universitetskaya str, Sevastopol, 299053, Russian
⁶E-mail: maksimova@volsu.ru

Abstract. The article presents the authors’ views on the organization of the modern system of cybersecurity. We considered the tasks, assigned to the monitoring subsystem and reconnaissance of cyberspace as a source of preventive hardware and software effects on the opposing side. The shortcomings of the existing structures of such subsystems are analyzed and the requirements to the intelligent automated system of cybersecurity are specified. The article offers hardware and software solutions, based on the development of a mobile robotic system for audit the stability of the network infrastructure and applications to existing and future cyber threats. A variant of the functional scheme of a robotic system with a universal housing is presented and with a set of mechanical drives, depending on the characteristics of the problems to be solved. For providing high functional flexibility and speed of the robotic system it is proposed to use fuzzy neural networks. The union of two independent theories - neural networks and fuzzy logic - allowed creating neural-fuzzy systems, having a high level of intelligence and independence in decision-making. The advantage of hybrid neural-fuzzy technology of modeling and information processing is the ability to view the generated rules and giving them a meaningful linguistic interpretation. A reasonable conclusion is made, that is the main meaning of that is the main meaning of the shift of creation concepts and using of artificial intelligence - transition from individual systems to distributed information processing and the development of multi-agent intelligent systems.

1. Introduction

Cyber confrontation means new level of armed opposition. The urgent requirement of the time, taking into account the robotization of weapons and military equipment, becomes a revision of the principles of construction of automated control systems, information systems and communication networks, including from the perspective of cybersecurity. The coevolution of the system of cybersecurity should
ensure: discovery of new, previously unknown cyberthreats (cyberattacks) during monitoring (reconnaissance) of cyberspace; automatic selection of parameters of functioning information systems and communication networks under the conditions of destructive impacts without deterioration of their main characteristics (cognitive platforms of building information and telecommunication networks).

Conducting reconnaissance in cyberspace requires digital penetration in network and control systems of potential enemy and provides for the use of completely new sources, forms and methods of data and information, development of new reconnaissance tools and technologies, tactical and technical techniques.

For the reasons given above, in system of cybersecurity must be provided the opportunity of execution preemptive hardware-software impacts (preemptive attacks) and active attacks on information systems and resources of the opposing side, as well as the ability to misinformation of the opposing side about true properties and parameters of information systems and communication networks.

On the system of monitoring and reconnaissance of cyberspace must be assigned function of provision formation and database maintenance of opened (detected) different types and sources of cyberthreats (cyberattacks), that provide creating and maintaining a directory of potential threats to cyber security and signs of cyber actions to information resources, the identification of potential threats to cybersecurity, creation and maintenance of the bank of criteria for detecting cyberattacks to information systems, detection and counteraction to implemented combat software agents and counteraction them.

One of the reasons of insufficient level of efficiency of functioning an existing subsystem of cybersecurity of information systems and communication networks is that based on the network model, in which decision-making is based on the basis of indicators of network elements productivity or separate directions of communication, as well as an analysis of network resources. Control systems, which based on network models, are included in the management process at that moment, when an event, required reaction of control system, already happened, that is reactive. However, development of information systems and requirements to them dictates the need to create proactive management system, that is "acting before the situation becomes critical".

Proactive management incidents and security events must be based on automatic (intelligent) mechanisms, which use information about the" history" of analyzed network events and forecast of future events, and also on automatic adjustment of parameters of monitoring of events to the current state of the protected system.

2. Purpose
For carrying out intellectual analysis of stability of info-communication networks to destabilizing effects from cyberspace it is necessary to develop a system for detection destabilizing effects, which performs intelligent analysis of scenarios destabilizing effects that the elements and nodes of information systems, as well as the evaluation of the sustainability information systems to destabilizing effects from cyberspace. The logic of such an intelligent automated system of cybersecurity must take into account the network specifics of cyberspace, attack models, technological features of the web-environment and achievements of artificial intelligence. [1].

3. Materials and Methods
In order to solve the above problem, we offer hardware and software solutions, which based on the development of a mobile robotic system (fig.1-3). This system is used for audit (cyber reconnaissance) of sustainability of the network infrastructure and applications to existing and future cyber threats (stress load, different DDoS- attacks, malicious code in general traffic, spam, worms, attacks of type «zero day», attacks with the use of technology fuzzing, etc.), as well as for software and mathematical effects to information-management systems, for physical destruction (or incapacitation) of objects of information infrastructure of the enemy [2].
In compliance with the functional scheme, the robotic system consists of several parts:

- BeagleBoneBlack – main processor of the robotic system;
- MiniMaestro 18–ChannelUSB ServoController – driver-engine, servo drives are connected to it;
- MG996R – servodrives;
- Powersupplyunit;
- Wifiadapter.

The body is proposed to be made in the form of a metal skeleton, the size of which depends on the tasks performed, which connects and unites the necessary periphery into a single whole, at the same time, ensuring the protection and integrity of the components [3].

In addition, in order to deliver the robotic system to the desired location, it is planned to use 8 screws, located on its body, and for movement, both on a horizontal and vertical surface, it is planned to use 6 limbs (legs). For connect to the cable on the body there is a probe.

The mobile robotic system (swarm) will allow realizing the following characteristics: speed, mobility, absence of barriers to access; invisibility, low recognizability for enemy funds; scalability, plasticity of the robots composition, included to the swarm; high level of coordination of actions, mutual learning through the use of a single remote memory; variety of functions implemented to perform tasks.
As control channels in the robotic system is proposed to be used:
- management by radio channel (by channel of wireless broadband access), which is protected by a cryptographic algorithm AES;
- stand-alone operation [4, 10-14].

When navigating offline the robotic system must use its artificial intelligence and sensor devices (sensors of various types) for following in programmed route, also to avoid insurmountable obstacles encountered on the way, which can disable the robotic system.

Due to the dynamic nature of the tasks of management of cyber security, their high dimension, difficulties in forming a complete system of performance indicator of the management system (because of the correlation and fuzzy nature of many of them), incomplete and unreliable of checking information advisable for simultaneous provision of high functional flexibility and performance of robot technical system to use fuzzy neural networks, that use a fuzzy description of a managed process and its management system in the form of fuzzy knowledge base, as well as converting fuzzy description to command sequence, for achieve management goals [2].

The features of the proposed scheme of fuzzy system of management are consider of sequence management cycle: situation assessment, definition of management objectives, identification of the need for management, finding valid solutions and ways to achieve this goal and implementation of the selected method of achieving the goal.

4. Discussion
The union of two independent theories - neural networks and fuzzy logic - helped to create more universal intelligent technologies, called neural fuzzy systems, with traditional expert system in which knowledge is represented symbolically, successfully used in the process of decision-making in complex, many dimensional systems for processing of different kind of knowledge (fig. 1).

The technology, obtained as a result of integration, unites the ability of neural networks to self-learning and the ability of fuzzy systems to process qualitative information, as well as gives the opportunity to use all available information about the object (quantitative and qualitative). In this situation the neural network consists of special neurons, which represent particular entities of the systems with fuzzy logic. This allows presenting the system as a set of fuzzy rules and at the same time to train her as a neural network [5-9].

For high functional flexibility and speed of operation of control system cyber security it is proposed to use fuzzy neural networks, it means, that control algorithms are implemented software in a robotic system with application of technology is tribute intellectual agents (fig. 4).

Figure 4. Structure of neuro-fuzzy network.
The growth of network intelligence is provided by the use of microelectronics and application of software in each individual network device. This intelligence allows increasing flexibility, network capabilities and reliability in group application of robot technical complex even in inhomogeneous environments.

In the dynamic conditions of functioning of the mobile network can be multiple network management goals. All of them have different physical nature, as well as part of them should be maximized (bandwidth of network, capacity of the node batteries), part of them - minimized - time of delay of message transmission, \( P \) - transmission power.

In the context of decentralized management communication subsystem of typical composition of robot technical complex will implement two interrelated groups of objectives, which determine the multi-criteria management:

**Users’ goals** \( \{G_m\}, \ i=1,\ldots,k \), which determine the search of extremum or fulfilling the condition of message transmission (user optimization). For example:  
- \( G_{n1} \) – accordance to requirements of efficiency \( t_{nah} \leq t_{lad} \);  
- \( G_{n2} \) – minimum transfer time \( (min t_{nah}) \);  
- \( G_{n3} \) – the route of the specified bandwidth \( s_{nah} \geq t_{lad} \) with a condition of security provision;  
- \( G_{n4} \) – specified number of independent transmission routes \( (M_{nah} \geq M_{lad}) \); etc.; network (zonal) goals \( \{G_z\}, i=1,2,\ldots,m \), which implement the search suboptimal solutions of network or in its zone (network optimization). For example:  
- \( G_{c1} \) – minimization of service traffic \( (min V_{nah}) \);  
- \( G_{c2} \) – maximization of throughput \( (max S) \);  
- \( G_{c3} \) – minimization of the time of message transmission \( (min t_a) \);  
- \( G_{c4} \) – minimization of power of nodes transmission \( (min P) \), etc.

Operational management is presented as management with feedback and it involves the following steps \( U=\{U^c, U^p, U^n, U^p\} \):

- **\( U^c \)** - collecting information about the state of the managed network (decision about volume, frequency, depth of the collection of information);
- **\( U^n \)** - analysis of this information: identification of the situation in the network (its zone and in the node itself), check the performance of network functions and determination of the necessary control impact;
- **\( U^p \)** - identification of management goals with further detailing them to subgoals and solution development (selection of access protocol, choice of method transfer, method of information distribution);
- **\( U^p \)** - realization of decisions (sending service messages, resource reservation, setting transmission power, antenna pattern).

One of the reasons of insufficient level efficiencies functioning of self-organizing radio networks distributed groups of robots, built on the basis of the network model, it consists in the features of the adopted control system.

Here the decision - making is based on indicators efficiency of network elements or individual communication ways, as well as on analysis of network resources. In this case, this control system is reactive, not proactive. Therefore, it is included in the management process at the moment, when an event, requiring a control system reaction, has already occurred [10-13].

The main drawback of this approach is subjectivity of decision making in most cases. This provision is due to the fact that the analytical dependences between the state of the robot technical complex (specific network elements) and related network resources and consumer characteristics of the network are determined in an incomplete volume. That is, the existing network management model is impossible to use for predicting the behavior of the robot technical complex (network elements) when they operate as part of a network. This is the main drawback of the management system of communication networks and the group use of robotic systems.

Ensuring networks ability to self-organize, and also adaptation of their elements to different conditions of functioning requires the development of new management methods with the involvement of technologies for knowledge processing with integration of traditional approaches and methods of mathematical modeling with artificial intelligence models and, accordingly, development of provisions for the construction of an intelligent communication subsystem of robot technical system. Main sense
of existent change of concepts (paradigms) creation and using of artificial intelligence - moving from assumptions, which are only applicable for isolated systems of artificial intelligence, from individual systems, to distributed information processing and to creating of multi-agent intelligent systems.

The analysis of existing methods of knowledge processing (expert systems, genetic algorithms, fuzzy logic, neural networks) shows, that one of the trends in this area is an attempt to integration of different technologies in order to combine their characteristic advantages [14].

The representation of knowledge in neural networks in the form of weight matrices does not allow analyzing the results, while in systems of output based on fuzzy rules, the results are interpreted as inverse protocols of output. Neural networks are trained using a universal algorithm, in which the laborious extraction of knowledge replaced by training of sufficient volume training sample. For fuzzy systems of output knowledge extraction includes difficult processes of formalization of concepts, defining functions of membership and formation of rules of inference. At the same time fuzzy neural networks are trained as usual neural networks, and their results are explained as in systems of fuzzy inference.

In neural-fuzzy systems there is a traditional expert subsystem, in which knowledge is represented symbolically. This type is successfully used in the decision-making process in complex multi-dimensional systems for processing of difference types of information.

Technology, resulting from integration, combines ability of neural networks to self-learning and ability of fuzzy systems to process quality information, and also gives the opportunity to use all available information about the object (quantitative and qualitative). In this approach, the neural network consists of special neurons, which represents a specific entity of the system with fuzzy logic. This allows presenting the system as a set of fuzzy rules and to train it as a neural network.

The undoubted advantage of hybrid neural-fuzzy technology of modeling and processing information is the ability to view formed rules and giving them content, linguistic interpretation that allows considering the apparatus of neuro-fuzzy systems as a means of extracting knowledge from experimental bases of data.

Management process of robot technical complex is considered as a single constructively developing formal system, flow of work by automated control, which is executed by the collective of management agents and (hardware and software) agents. It is based on the basis of a flexible combination of two operation modes: automatic, in which variants of solutions are formed as a result of the work of software agents, and automated, in which variants of solutions are formed as a result of interactive agent interaction - trustees, implementing the functions of assistance and control of trustees, enforce integrity constraints, formalizing the rules of using of resources of the radio network.

It is necessary to note, that all criteria, on the basis of which in communications subsystem of robot technical system happens taking a decision, are configurable parameters of the network and can be dynamically overridden by network operator at the time of network planning or at the time of group application of robot technical system.

Dynamic nature of management tasks, their high dimension and the complexity of the formation of a complete system of performance indicator of control system (due to correlation and fuzzy nature of many of them), happens in the conditions of incomplete, and often unreliable checking information. Advisable for simultaneous high functional flexibility and performance of communication subsystem of robot technical complex to apply fuzzy neural networks, using fuzzy description of control action and control system n the form of fuzzy knowledge base, which converts a fuzzy description into a sequence of commands, for achieving management goals.

The features of the proposed scheme of fuzzy control system are accounting sequences of management cycle: situation assessment, definition of management objective, identification of the need for management, finding valid solutions and the way to achieve this goal and the implementation of the chosen method of achieving the goal[14].

Thus, the application of neural-fuzzy systems will allow optimizing the process of managing the communication subsystem of robot technical complex by taking into account the current situation in the network (level of load in the nodes, quality of the transmission paths, residual capacity of the node batteries, distances between subscribers, speed of their movement, etc), as well as the requirements for the transmission of certain types of traffic in the group application of robotic systems.
5. Conclusion
Taking into account the above mentioned aspects, the presented communication subsystem of robot technical complex has developed intellectual capabilities on the analysis and recognition of the situation, the making of a strategy appropriate behavior, planning the sequence of actions, as well as the synthesis of control actions. This will optimize the management process of communication subsystem of robotic system by taking into account the current situation in the network (level of load in the nodes, quality of the transmission paths, residual capacity of the node batteries, distance between the subscribers, their movement speed, etc.), as well as the requirements for the transmission of certain types of traffic by the group application of robotic systems [7].

To protect the control channel it is proposed to implement in the robot technical system cryptographic chip, which will support the cryptographic protocol AES and will allow encrypting open control protocols [7].

Autonomous operating mode we offer to implement on the basis means of artificial intelligence by implementing a hybrid neural-fuzzy technology of modeling and information processing.

The proposed robot technical system allows:
- network security analysis;
- network security audit;
- identifying the vulnerabilities of networks;
- analysis of the structure of networks;
- reconnaissance;
- active opposition to the enemy;
- the bypass protection;
- testing of wireless networks to penetration;
- stress - testing of networks.

References
[1] Ivanov Yu 2014 Robot technical tools, complexes and systems of military destination. Fundamentals. Classification Methodical manual (Moscow: Main research-and-development test center of robotics).
[2] BaranovVV, MaksimovaEA, LautaOS 2019 Analysis of models of information support for processes and systems in the implementation of multi-agent intellectual interaction Instrumentation and systems. Control, testing, diagnostics 4 32-41
[3] Baranov V, IvanovD, KotsinyakM, MoskovchenkovV, Nechepurenko A 2017 Application of the method of topological transformation of stochastic network for modelling the impact system In Proc. of Interuniversity scientific-practical conference on Actual problems of ensuring information security of work (St. Petersburg, pp. 38-43).
[4] IvanovD, KotsinyakM, LautaO, Nechepurenko A 2017 Model of distribution of factors of information influence on elements of information and telecommunication network In Proc. of VI International scientific-technical and scientific-methodical conference (St. Petersburg, pp. 420-425).
[5] Parashchuk I, IvanovYu, RomanenkoP 2010 Neural network methods in tasks of modeling and analysis of the effectiveness of communication networks HAC 104-110.
[6] KotsinyakM, IvanovD, LautaO, Nechepurenko A 2017 Methods of assessing the security of information and telecommunications network in the information counteraction In Proc. of XXIII International scientific-technical conference (St. Petersburg, pp. 83-89).
[7] KotsinyakM, IvanovD, LautaO, A Nechepurenko A 2017 Model of targeted cyber-attack In Proc. of XXIII International scientific-technical conference (St. Petersburg, pp. 90-98).
[8] SaenkoI, LautaO, KotenkoI 2016 Application of the method of transformation of stochastic networks for modeling mobile banking attacks Bulletin of higher educational institutions. Instrument making 59 (11) 928-933.
[9] KotsinyakM, LautaO, NechepurenkoA, ShterenbergI 2016 Methods of assessment of stability of information and telecommunication network in the conditions of information impact Works of educational institutions of communication 2 (4) 82-87.

[10] KotsinyakM, KarganovV, LautaO, NechepurenkoA 2016 Methods of substantiation of measures of counteraction to radar reconnaissance of high-precision weapons Defence technology issues. Series 16: Technical means of countering terrorism 99-100 54-57.

[11] BaranovV, KotsinyakM, LautaO, MoskovchenkoV 2016 Method of assessment of stability of information and telecommunication network in the conditions of information impact Journal of Volgograd state University. Series 10: Innovative activity 11 (2) 11-15.

[12] KotsinyakM, LautaO, DrachevV, KlinshovI 2016 Cybersecurity. Analysis of legal documents of the Russian Federation, which regulate political and military activities in cyberspace InProc. Conference SCRI "National development" (St. Petersburg, pp. 109-117).

[13] LautaO, NikitinV, KlinshovI, LautaA 2016 Legal documents of the United States, the regulatory political and military activities in cyberspace in Proc. of Conference SCRI "National development" (St. Petersburg, pp. 118-125).

[14] BaranovV, GudkovM, KribeI, LautaO, NechepurenkoA 2017 Protection of the control channel of robotic systems Actual problems of information security 32-37.