Marek Boguslaw ALEKSANDER, Mykola KULYK, Mikołaj KARPINSKI, Yurii KHLAPONIN, Andrii MISCHENKO

INTELLIGENT TECHNOLOGIES IN INFORMATION SECURITY MANAGEMENT

Abstract

We present the analysis of the development of information and telecommunication networks of new generation. The generalized structure of the intelligent security management system is shown in the paper. Also, the structure of neural network of ITS's security assessment is shown, the principle of its operation is described.

INTRODUCTION

The development of information services requires solving problems of effective resource management while expanding the functionality of information and telecommunication networks (ITN). In the 90's of the last century it was assumed that the idea of ITN creation would be implemented using the concept of intelligent network. In 1993, the International Telecommunication Union (ITU-T) approved the first specification of Intelligent Network (IN) technology. The basic principle of building of intelligent network was a logical separation of switching and services, so appeared the opportunity to create new telecommunication services [1].

In 2014, the world leader in information and telecommunication technologies – Huawei, announced the development of a new generation of wireless networks – 5G. 5G technologies support 1000-fold increase in capacity, connection at least of 100 billion devices, and 10 Gb/s of individual user activity. It is expected that 5G-technologies would have the rapid development in the next decade [2].

Along with the development of technologies raises the question of security in information and telecommunication networks (ITN). In terms of safety the most important properties of networks are: confidentiality (of using infrastructure or part thereof); integrity (of infrastructure); accessibility (of services); control (of the use of infrastructure or part thereof); stealth (of the infrastructure using and management) [3].

In the information security the most important measures is to prevent threats to confidentiality and integrity. In ITM the major efforts should be directed at preventing threats to the accessibility of services (in ITM these attacks are easier to be implemented) and to control of the using of infrastructure (or part thereof). Access to information is realized through the formation and processing of requests to the appropriate services that operate on different servers. Therefore, the accessibility of relevant ITN services is analyzed.

So, the security in the ITN has significant differences from the security of specific information in any specified system. This requires the usage of new approaches for ITN security systems creation, including the usage of intelligent technologies.

Therefore, these studies are relevant nowadays.

1. ANALYSIS OF PUBLISHED DATA AND PROBLEM DEFINITION

Analysis of ITN operation showes that at this stage of the development of networks the ensuring of their efficient work and security is rather problematic question, considering the complexity of the structure, its multidimensionality and multilevel structure. To solve this scientific problem is proposed the application of intelligent technologies. Solutions to this problem are published in papers [4-6].

Today much attention is paid to the intelligent technologies [7,8]. Intelligent systems have recently become quite common commercial product that is widespread for users and experts in various fields of engineering, scientific and technical areas.

The creation of ITN security systems, oriented to work with incomplete or fuzzy initial information, the uncertainty of external influences and environmental performance, requires the involvement of non-traditional approaches to ITN security management, using methods and techniques of artificial intelligence. Such systems are called intelligent security systems, would form a whole new class for which not only the principles, methods of analysis and synthesis are under development, but the basic concepts and definitions need to be carefully and methodologically elaborated.

Obviously, in the presence of various kinds of uncertainties the high level of autonomy, adaptability and reliability of security management systems must be provided by increasing their intellectual capabilities, based on the processing of expertise. The formation of the concept of intelligent security management systems causes a number of fundamental issues. The first is connected with a clear definition of knowledge, not only as a form of machine presentation of information, but also as a tool for organizing of principles of security management. The most important aspect is the analysis of opportunities and peculiarities of the usage of certain information technologies for knowledge processing in tasks of intelligent management [8].

The aim of the research was to develop the scientific bases of situational security management in ITN, based on intelligent technologies.

2. THE RESULTS OF RESEARCH OF THE ITN SECURITY MANAGEMENT SYSTEM, BASED ON INTELLIGENT TECHNOLOGIES

Based on the key assumptions of the theory of situational management, for each class of threats (Fig. 1), whose appearance is considered acceptable in the operation of the network, there is a certain solution for management and counteraction such threats.

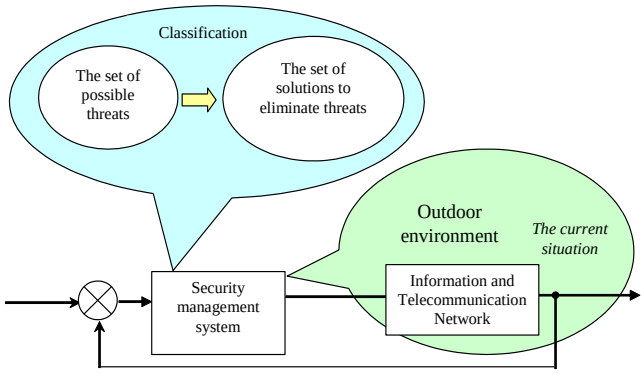

Fig. 1. *The principle of situational information security management*

Then the situation, caused by the current state of both the network and its outdoor environment, and which is identified by means of measurement and information tools of security system can be attributed to some class, to which the necessary management is considered to be known.

Thus, the implementation of the concept of situational security management, based on advanced intelligent technologies, requires a deployed base of knowledge about the purpose and principles of the system, the specific use of different algorithms, principles of the executive segment and network as a whole, as well as the current possible types of threats for information (DDos-attacks, viruses, "Trojan Horses", etc.). It is important to note that the main architectural feature, that distinguishes intelligent security management (Fig. 2) from the built in "traditional" scheme, associated with connection of mechanisms of storage and processing knowledge for realization the abilities of implementation the necessary functions in incompletely specified (or unspecified) conditions in terms of the random nature of external influences. To the effects of this kind may be refered the unforeseen change of objectives, the performance of ITN and facility management, parameters of the outdoor environment, the emergence of new types of threats and so on. In addition, the composition of the system if necessary supplemented by means of self-learning, which provide the summarize of the accumulated experience, and the replenish of knowledge.

The practical implementation of this concept involves selective use of various technologies of knowledge processing depending on the specific of problems solved, the characteristics of the controlled object, its functions, operating conditions. According to the review of numerous studies of the development of methods of knowledge processing, one of the leading trends in this area is associated with attempts to integrate various intelligent technologies to combine their advantages. For example, the high functional flexibility and performance can be achieved through the integrated use of technology expert systems and neural network structures.

High efficiency of neural information technologies in solving problems of adaptive information security management in the near future can make them indispensable in creating a new generation of security systems. The relevance of the research of artificial neural networks is evidenced by the variety of possible applications.

Since all the artificial neural networks are based on the concept of neurons, connections and transfer functions, there are similarities between different structures or architectures of neural networks. Most of the changes derived from different learning rules [9].

The structure of neural network (NN) of evaluation of the security level in the ITN, which is shown in Fig. 3 includes m-neuron ensembles (layers), which are determined by the number of classes of states of information security from a certain type of threats. Class of the protection state is equal to the neural layer, and the number of classes is determined by the depth of search of threat, that is a structural element that is designed to detect a particular class of security threats in the ITN and the number of classes is defined by

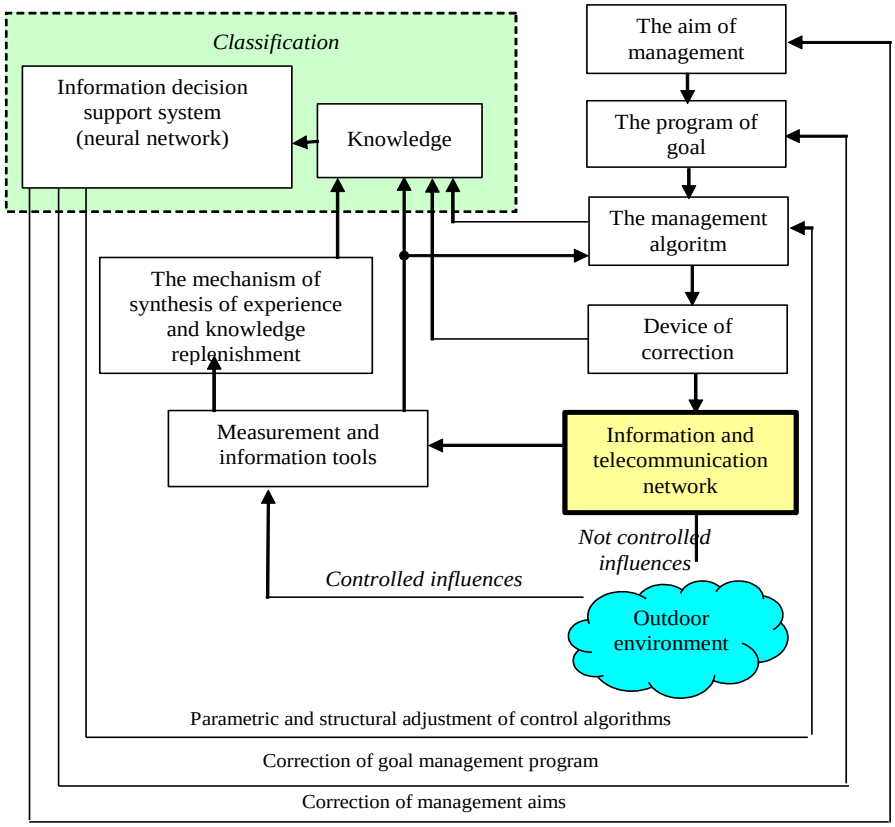

Fig. 2. *Generalized structure of intelligent security management*

parameters, which are detected by the measurement and information tools of security system to determine the status of information security in ITN.

The number of neural elements (neurons) in the layer is deter-

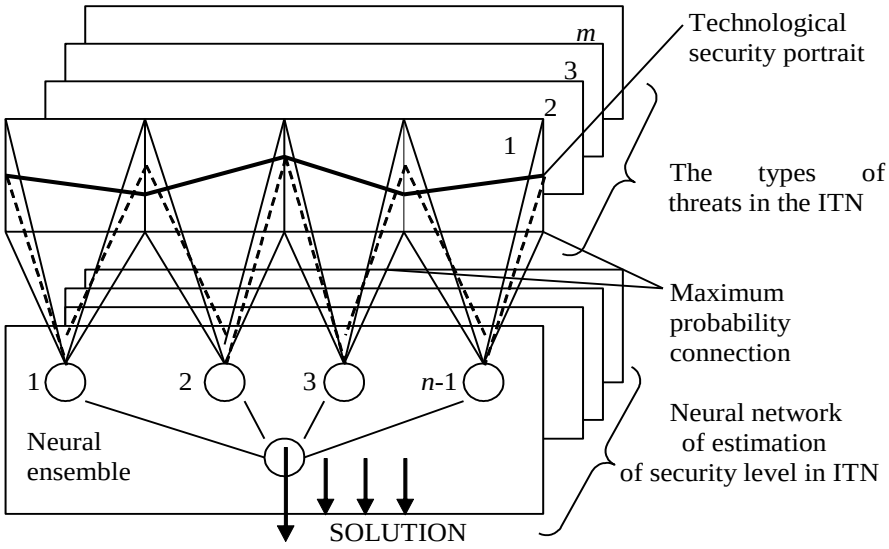

Fig. 3. *The structure of the neural network of evaluation of the security level in ITN*

mined by the amount of statistical samples. Herewith the large statistical samples increase the dimension of the space of security states, presented by the technological security portrait (set of symptoms), and small do not allow conclusively link the symptoms with the diagnoses. The best is a portrait that allows you to get the required amount of information about the security of ITN from the specific set of threats at a certain time. The volume of statistical sample will be determined by the number of applied threat detection systems (antivirus, intrusion detection systems, firewall, etc.). The combination of neural ensembles (layers) is a neural network (NN). Such neural network is a simplified Markov model. However, they have associative properties that resemble the properties of biological systems [10]. The initial structuring of the neural network should be made with formal synthesis methods by which the optimal structure is determined, including the number of neural layers and neural ensembles, the number of neural elements in each layer, the presence of deterministic relations between them and the initial weights.

CONCLUSIONS

It is proved that security in the ITN has significant differences from the security in any specified system.

The structure of ITN intelligent security management system is shown.

The structure of neural system of evaluation of the security level in ITN is shown.

For the first time the term of technological security portraits as a combination of states of protection that meet the identified threats in ITN at a certain time, is mentioned.

REFERENCES

1. Pinnes E, Operations and Management for Next Generation Network / Presentation in ASTRAP IP-based Network Management & Internet Charging Semiran Bangkok. – February 22-24, 2001.
2. http://consumer.huawei.com/ua/news/ show_one/27.
3. Khlaponin Y.I. General, characteristics of threats in cyberspace / Y.I. Khlaponin, V.V. Ovsyannikov, N.A. Palamarchuk, Priority areas of telecommunication systems and networks of special purpose: VI scien.- pract. sem. Military Institute of Telecommunications and Information "KPI", 20 October 2011 .: Theses. - K., 2011. - P. 157 .
4. Artemenko M.Y., Berkman L.N., Tolyupa S.V., Neural networks and their applications in telecommunication systems. Radio: All-Ukrainian. scien.- Engineering. Coll. 2007 - Vol. 134.- C. 45-53.
5. Baklanov I.G., NGN: Principles of building and organization. - M .: Eco-Trendz, 2008 - 468 p.
6. Gerasimov B.N., Tarasov V.A., Tokarev I.V. Man- machine system solutions with Adoption element artificial intelligence. - K .: Naukova Dumka, 1993. - 168 p.
7. Makarov I.M., Intelligent automatic control system. - M .: Fyzmatpyt, 2005. - 573 p.
8. Pospelov D.A., Artificial Intelligence in foreign studies / Pospelov D.A, Stefanyuk V.P. // Clearing materials. Science. - M .: Ynformprybor. -1986. - №3. - P. 3-25.
9. Khlaponin Y.I., Arrangement for learning images recognition, Patent on inventions from 16.05.91 № 4944920/24.
10. L. Kleinrock, Theory of mass of service. - M .: Mashinostroenie, 1979. - 342 p.

Authors:
ALEKSANDER Marek Boguslaw - State Higher Vocational School in Nowy Sacz, 1 Staszica St, Nowy Sącz, 33-300 Poland, aleksmar@pwsz-ns.edu.pl, http://www.pwsz-ns.edu.pl/

KULYK Mykola - National Aviation University in Kyiv, 1 Kosmonavta Komarova Ave, Kyiv, 03058 Ukraine, Rector, http://nau.edu.ua
KARPINSKI Mikolaj - University of Bielsko-Biała, 2 Willowa St, Bielsko-Biala, 43-309 Poland and State Higher Vocational School in Nowy Sacz, 1 Staszica St, Nowy Sącz, 33-300 Poland, mkarpinski@ath.bielsko.pl, http://www.eng.ath.bielsko.pl/, http://www.pwsz-ns.edu.pl/
KHLAPONIN Yurii - National Aviation University, 1 Kosmonavta Komarova Ave, Kyiv, 03058 Ukraine yfcnz0408@ukr.net, http://nau.edu.ua
MISCHENKO Andrii - National Aviation University, 1 Kosmonavta Komarova Ave, Kyiv, 03058 Ukraine partpravo@i.ua, http://nau.edu.ua