Information security system quality assessment through the intelligent tools

E V Trapeznikov

1Omsk State Technical University, 11, Mira av., Omsk, 644050, Russia
E-mail: evtrapeznikov@yandex.ru

Abstract. The technology development has shown the automated system information security comprehensive analysis necessity. The subject area analysis indicates the study relevance. The research objective is to develop the information security system quality assessment methodology based on the intelligent tools. The basis of the methodology is the information security assessment model in the information system through the neural network. The paper presents the security assessment model, its algorithm. The methodology practical implementation results in the form of the software flow diagram are represented. The practical significance of the model being developed is noted in conclusions.

Key-words: information, intelligent tools, neural network, information system, guideline documents

1. Introduction
The technology development stage defines the concept of information as the information sphere important unit. Information processing is carried out by means of the automated systems resources including various information systems. Any automated system processing personal data in particular requires protection in accordance with the legislation. Protection is necessary for preserving three basic properties of information, namely confidentiality, integrity, accessibility.
In many studies the particular attention is paid to the intelligent tools. Currently, the most frequently used approaches are:
• genetic algorithms,
• neural networks,
• immune systems technologies,
• Bayesian network, etc.
Protection is necessary due to the increasing number of threats to data processing automated systems. At the moment, increasingly sophisticated and effective access violation detection strategies both by hardware and software are being developed and implemented. However, these systems need to be improved for preventing the illegal access. The authors of [1] propose their own solution based on the decision tree as a means of users behaviour models obtaining, neural networks as intrusion detection identifying classifiers. The paper points out that the given intelligent techniques combination makes possible to reduce the access violation risk. In [1], only user behaviour analysis for tracking unauthorized access is used.
Since network technologies are applied for information processing and storing speed increasing, at this level a large number of threats and vulnerabilities being used by the intruders occur. Network technologies form part of the automated system. The authors of [2] in their study constructed the
attacks protection and defence system theory model for network security based on the game theory. According to the model the authors developed the training algorithm on the genetic algorithm basis. These steps allow authors to evaluate human and system suspicious actions. The authors of [2] conclude with experimental data demonstrating the system effectiveness.

The automated system is a complex of components, for this reason the information security system quality is worth to be assessed in full. The adaptive system based on the neural network and intelligent agents is given in paper [3]. The developed system will make possible to implement the information security adaptive control, the system provides the timely response to threats and performs the decision-making process in real time. In paper [3] the system is said to allow attacks identifying, classifying and preventing. The adaptive system algorithm is represented in figure 1.

![Figure 1. The adaptive system of the authors [3].](image)

Some authors consider the neural networks application for creating the virus detection system. Computer viruses have become a serious threat to the information system. Due to the virus codes complexity and behavioural uncertainty, as well as the encryption emergence the traditional detection methods are becoming less effective. The viruses detecting approach application based on the artificial intelligence has become a major problem of the current antivirus researches [4, 5]. In paper [4], the approach on the basis of the dynamic and static viruses detection integration is proposed. The detection system uses the vector support mechanism as the elements classifier for dynamic virus behaviours model constructing, as well as applies the probabilistic neural network as the elements classifier for static behaviour modelling. The authors refer to the detection system effectiveness. It should be noted that most authors examine the individual aspects of information security. One of the most frequently distributed attacks is DDoS (distributed denial-of-service attack.) The network resource fails as a result of a number of requests to it sent from different points.)
In papers [6, 7] the IDS method is proposed. It is based on the neural networks delays. The method is based on the multi-tiered architecture, each host is stored in the network. Hosts are hidden in the first and second layers of the firewall. If a suspicious packet is detected, similar to the DDoS template, the system will automatically call the security module. Those packets that did not get over the security module will be isolated and then removed from the transfer.

2. Problem Statement
The various authors studies analysis shows the information security system quality assessment problem to be quite relevant under the increasing threats. The given research objective is to develop the information security system quality assessment methodology by applying the intelligent tools. One of the methodology components is the information security assessing model in the information system based on the neural network [8].

3. Theory
The information security system quality assessment methodology development objective by using the intelligent tools is improving the automated system protection level quality to counter the emerging threats. The methodology procedure algorithm is presented in figure 3. According to the algorithm:

Step 1. In order to properly identify the particular automated system necessary protective actions, AS class is necessary to be determined. The automated system class is identified according to the guidance document of the Federal Service for Technical and Export Control «Automated Systems. Protection against unauthorized access to information. Automated systems classification and information security requirements».

Automated systems are classified into the following categories: 3B, 3A, 2B, 2A, 1D, 1G, 1V, 1B, 1A. For class defining the following set of parameters is applied:

1. The information availability of different confidentiality level in the automated system.
2. The automated system access subject privilege to the confidential information access.
3. The automated system data processing mode: collective or individual.
Step 2. For defining the protection requirements, the guideline document on the basis of FSTEC Order of Russian Federation No. 17 of February 11, 2013, «On the Requirements Approval for the Information Protection not Constituting the State Secret and Contained in the State Information Systems» is also used. According to this order, depending on the AS class the information system security class is defined as (1):

The protection class (C) = [information relevance level; system scale]  \( (1) \)

where the information relevance level is defined as (2):
Step 3. The AS protection system current status determining questionnaires list is formed on the basis of the specified requirements for the particular automated system. For the questionnaires compiling and the survey conducting, «GOST R ISO/IEC 15408 Information technology (IT). Security features and methods. Information technologies security assessment criteria of information technology» is used.

The conducted survey results make possible to define the information security system current status, to determine its presence or absence. The questionnaires are drawn up depending on the automated system class for providing the information security necessary level.

The methodology first stage generated results are the input parameters for the information security assessment model. For identifying the possible threats and vulnerabilities, the FSTEC threat and vulnerability database is used as the model destabilizing factors [8]. The neural network training necessity is defined during the model formation process. The trained neural network allows to get the more reliable result and possible threats that may occur under the actual system state.

4. Results and discussion

The software presented in figure 5 was developed for testing the methodology.

The software makes possible downloading the data from the FSTEC database, assessing the automated system protection system status, conducting the surveys, etc.

The software provides the access rights to the software features differentiation and actions logging conducting. In operation all the information is stored in the local database. SQLite is the basis of the database.

To carry out the experiments according to the presented methodology, the automated system, a hypothetical enterprise having the existing protection system that is predetermined not to be satisfying
the regulatory requirements, was used. By using the methodology, the automated system complete analysis was carried out. Subsequently, the analytical data and destabilizing factors list were applied as input parameters of the pretrained neural network. As a consequence of the methodology complete cycle performing, the results indicating the attacks that occur in the given automated system at the protection system current level were obtained.

5. Conclusions
In the context of attacks number and their complexity increasing, the information systems protection requires the reasonable approach which would help making the decisions of possible threats and attacks on the information system in accordance with the certain characteristics. Intellectual tools make possible to create the trained system which is able to make independent decisions with a high level of confidence. The developed methodology based on the neural networks system will allow to identify and classify the possible attack or threat.

6. References

[1] Guevara C, Santos M and López V 2017 Intrusion detection with neural networks based on knowledge extraction by decision tree Int. Joint Conf. SOCO’16-CISIS’16-ICEUTE’16 (Spain: Springer International Publishing) pp 508-17
[2] Ru-jun Y 2016 Int. J. Secur. Appl. 10 317–24
[3] Mukhin V et al 2016 Adaptive security system based on intelligent agents for distributed computer systems Int. Conf. on Development and Application Systems (DAS) (Suceava) pp 320-25
[4] Zhang B et al 2014 Neurocomputing 137 C 24–33
[5] Mao W et al 2017 Computers & Security 68 C 47–68
[6] Aljumah A 2017 Int. J. Adv. Appl 4 78–83
[7] Aljumah A and Ahamad T 2016 Int. J. Comput. Sci. Netw. Secur 16 132–38
[8] Trapeznikov E V and Danilova O T 2016 The information protection analysis model on the basis of the neural network Dynamics 1 (Russia) p 302–08