The information protection level assessment system implementation

E V Trapeznikov¹

¹Omsk State Technical University, 11, Mira av., Omsk, 644050, Russia

E-mail: evtrapeznikov@yandex.ru

Abstract. Currently, the threat of various attacks increases significantly as automated systems become more widespread. On the basis of the conducted analysis the information protection level assessment system establishing objective was identified. The paper presents the information protection level assessment software implementation in the information system by applying the programming language C#. In conclusions the software features are identified and experimental results are represented.

Key words: information security, neural network, development environment, legislation

1. Introduction

Modern automated systems are a set of various software and hardware technologies. Due to the abundance of technologies being used both at the time of establishing and during the operation of automated systems, threats and vulnerabilities can occur absolutely at any time.

Any automated system malfunction can lead to the irreversible consequences. A demonstration of this is the statistics of Kaspersky Lab ICS CERT for the first half of 2017. According to the mentioned statistics the number of automated control systems unique computers attacked by encrypting Trojans has increased that is shown in figure 1.

![Figure 1. The statistics by the number of attacked computers.](image_url)
In the given type of attack there is a disfunction of two information properties at once, namely integrity and accessibility. The information is no longer available to its owner. The chance to return the information becomes minimal. According to the same statistical data, the most vulnerable data transmission channel is the Internet and removable media. The detection and prevention of these attacks has become an important part of the security. The number of attacks that use the sophisticated methods has recently increased. The main purpose of these attacks is to filter to the destination and remain unnoticed. The intrusion detection system is one of the important ways of computer networks high security ensuring and is used for various attacks preventing [1, 2, 3, 4].

Most threats also occur due to the user errors [3, 4]. Paper [3] states that the attacker often applies real user accounts and standard administration tools to hide the stay inside the system. According to the authors, the most detection systems use only signature-based analysis and cannot identify malicious activities. In addition, it is impossible to analyze user actions manually owing to the task complexity. In the study the authors apply neural networks for detecting the user suspicious behavior. Besides, the authors draw the conclusions showing the qualitative improvement in detecting the suspicious users with an accuracy of 98%.

The authors [6] suggest the network packets analysis and certain attributes collection for neural network training material creating. The created classifier based on the neural network provides the fake packets identifying performance of 96%.

One of the topical problems common to the modern systems is the «hardware Trojans» emergence [7, 8, 9]. The authors of the presented papers use neural networks in their studies for analyzing the various features obtained from the equipment to determine the information extracting attempt fact.

It should be noted that most authors do not consider the comprehensive approach for assessing the information protection quality. However, this approach is be prioritized. The comprehensive approach should provide the complete assessment of the whole protection system from all alleged threats. The complete preliminary analysis of the protection system will ensure the correct assessment in accordance with the legislation.

2. The problem statement
To increase the vulnerabilities detection level most authors use various smart tools. One of the most frequently used are neural networks. Neural networks can be used for different problems solving. In recent years neural networks have been applied to provide security for the problems as attacks classification, prevention, detection. The general concept of neural networks is that neurons are able to correct weights in such a way as to predict the results correctly. Neural network different parameters are corrected at the training stage and subsequently the studied model is applied to the test data for assessment. The research objective is the information protection system quality assessment methodology implementation in accordance with the information security assessment model in the information system based on the neural network [10, 11].

3. Theory
For implementing the software, the programming language C # and development environment Microsoft Visual Studio 2015 were used. The local program database is formed by using SQLite, it is the embedded cross-platform database supporting the sufficiently complete SQL command set. The general flow diagram of the software is shown in figure 2.
Figure 2. The program flow diagram.
To achieve the objective the object-oriented programming method was applied.

For the software development, the MVC architecture (a scheme for application data, user interface and control logic partitioning into three separate components, namely the model, view and controller) is used in a manner that each component can be modified independently. The program interface is shown in figure 3.

Working with the program is carried out on the basis of authentication data, namely the login and password. For ensuring the data storage security, the user password is stored in the encrypted form. The authentication is performed via the entered password encryption and comparison with the database password by the specified login.

To continue working with the software, it is necessary to initialize the project opening, or creation. The project is given its name and date. All the information about projects is stored in the database corresponding table (ProjectStructure).

![Figure 3. The program interface.](image)

The automated system class identifying is necessary for information protection requirements compiling. The system class shows the processed information access level in the system, the users access, etc. The class definition is performed according to the guideline 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».

The questionnaire conducting will make possible to define the information security system current level, to determine whether the information is present. The questionnaire is carried out by using the State Standard. The questionnaire results are the neural network input data set.

In addition to the questionnaire, the input parameters are FSTEC databank threats and vulnerabilities. Loading is performed in the corresponding local database tables, namely FstecThreatsTable and FstecVulnerabilityTable. The data source are Excel files with threats and vulnerabilities. The program performs the transformation for the further work. After determining all the parameters, the neural network is run for calculations. A separate stage is neural network training according to the "with the teacher" method, in which the initial data decision is predetermined and neural network changes the weighting factors for achieving the solution. The final stage is all the results output for the user.
4. Results and discussion

For the experiments conducting the hypothetical enterprise was determined. At the given enterprise there is the automated system in which the data to be protected are processed. The automated system class was defined as 2A: users have the same access rights (authority) to all AS information processed and (or) stored on various confidentiality level media.

Further, for determining the protection system current state, the survey was conducted by using GOST R ISO/IEC 15408 Information technology (IT). Security methods and tools. Information technologies security assessing criteria.

The results revealed the protection system actual state data. These data are the part of the neural network input data. In addition, the input data used the threats and vulnerabilities FSTEC bank data.

The neural network calculations found out the results about possible threats, for example, IST threat 030 «The threat of using default identifying /authentication information» was typical for the system as the most common passwords were used to authenticate the users.

However, for improving the neural network performance, it is necessary to conduct its training additionally by using data on real enterprises.

5. Conclusion

The studied researches demonstrate the software development relevance for the automated systems protection level assessment. Each study focuses on the identification and elimination of a certain type of threats, as well as the comprehensive approach.

The developed software makes possible:

- To differentiate the access rights to the program features according to the identification data.
- To create, edit users for working with the software
- To log all users actions.
- To create and save the current projects.
- To download the information from the FSTEC data bank
- To classify the investigated automated system.
- To conduct the automated system survey for determining the protection system current state.
- To form the list of possible threats based on the survey results and the destabilizing factors list by using the neural network.

References

[1] Akashdeep, Manzoor I and Kumar N 2017 Expert Syst Appl C 88 249–57
[2] Saied R Overill E and Radzik T 2016 Neurocomputing 172 385–93
[3] Ussath M et al 2017 Identifying Suspicious User Behavior with Neural Networks IEEE CScCloud (New York) p 255–63
[4] Banik D and Chowdhury R R 2016 Offline signature authentication: A back propagation-neural network approach Sixth ISED (Patna) pp 334–39
[5] Amruta M and Talhar N 2016 Effective denial of service attack detection using artificial neural network for wired lan SCOPES p 229–34
[6] Hasegawa K, Yanagisawa M and Togawa N A 2017 IEICE T Fund Electr E 100 1427–38
[7] Ni L. et al 2016 A method of noise optimization for Hardware Trojans detection based on BP neural network 2nd IEEE ICCC (China: Chengdu) p 2800–04
[8] Li J. et al 2016 A novel hardware Trojan detection based on BP neural network 2nd IEEE ICCC (China: Chengdu) p 2790–94
[9] Danilova O T and Trapeznikov E V 2015 Information Counteraction to the Terrorism Threats 24 24–9
[10] Trapeznikov E V 2017 Proceedings of the Tula State University. Technical sciences 2 312–18