Synthesis of an Expert System for Assessing the Security of Computer Networks Based on a Fuzzy Neural Network

Svitlana Kuznichenko, Sergey Shvorov, Yurii Husak, Igor Tolok, Ihor Muliar

Abstract**: *The aim of the article is to substantiate the principles of synthesis of an expert system for assessing the security of computer networks based on a fuzzy neural network, and this is an urgent scientific and technical task. Requirements for the operative security assessment of computer networks for data protection are analyzed. It was shown that data security should be provided by the network administrator or persons who need to use special decision support systems in assessing the security of computer networks. To solve this problem, factors that characterize the security of electronic systems, including computer systems, have been identified; the use of fuzzy neural networks is proposed as a mathematical apparatus for constructing an expert system; a technique for the synthesis of a fuzzy neural network for assessing the security of computer networks has been developed; an appropriate fuzzy neural network has been created and tested for adequacy; the prospects of the proposed methodology for creating an expert system for assessing the security of computer systems have been established. The scientific and practical significance of developing such a system lies in the fact that a fuzzy neural network is configured on a specific object in order to quickly determine one of the seven levels of security of computer networks that are used in the United States Department of Defense.***

***Keywords* : Fuzzy neural networks, expert systems, information security, data sample.**

I. INTRODUCTION

Problem Statement

Classically, there are two approaches to ensure the security of electronic systems, including computer networks [1-3]:

- a fragmented approach in which strictly defined threats are counteracted under certain conditions (specialized anti-virus tools, autonomous encryption tools, etc.);
- an integrated approach, providing for the creation of an information processing environment that combines various
- (legal, organizational, process - technical) measures to counter threats.

An integrated approach is typically used to protect large systems. Although often typical software tools contain built-in information protection tools, but this is not quite enough, and therefore it is necessary to ensure the implementation of:

- monitoring activities of human resources (HR), which has a high level of authority for actions in the system (by programmers, network database administrators, etc.);
- organizational and technical measures to back up important information;
- organizational measures to restore the system in case of emergency;
- organizational and technical measures for access control in the rooms in which computing equipment is located;
- organizational and technical measures for the physical protection of the rooms in which computing equipment and data carriers are located, from natural disasters, riots and etc.

Frequently, neural networks are used to create expert systems for assessing the security of computer networks [4]. However, they have several disadvantages: long learning time; the complexity of the analysis of the structure of the "trained" network, accordingly, the impossibility of its optimization; the impossibility of introducing a priori (expert) information to accelerate network learning.

Obviously, the elimination of these shortcomings would help to increase the productivity of information systems. These considerations were the basis for the creation of fuzzy neural networks, where conclusions are made on the basis of the apparatus of fuzzy logic, and the corresponding membership functions are adjusted using the learning algorithm of neural networks. These systems can not only use a priori information, but also gain new knowledge in the process functioning [5].

That is, a fuzzy neural network is a neural network with clear signals, weights, and an activation function, but t-norms, t-conorms, or other continuous operations are used to combine them.

The aim of the article is to substantiate the principles of synthesis of an expert system for assessing the security of computer networks based on a fuzzy neural network.

Revised Manuscript Received on May 30, 2020.
***** Correspondence Author

Svitlana Kuznichenko, department of Information Technologies Odessa State Environmental University Odessa, Ukraine skuznichenko@gmail.com ORCID: 0000-0001-7982- 1298

Sergey Shvorov*, Department of Automation and Robotic Systems National University of Life and Environmental Sciences of Ukraine Kyiv, Ukraine 7996445@gmail.com

Yurii Husak, Research Center, Institute of the Armed Forces of Ukraine of Kyiv, Kyiv, Ukraine. Email: y.husak1512@gmail.com

Igor. Tolok, Military Institute of Taras Shevchenko National University of Kyiv, Kyiv, Ukraine. Email: s63010566s@gmail.com

Muliar Ihor, department of Cybersecurity of Computer Systems and Networks of Khmelnytsky National University Khmelnitsky, Ukraine. Email: betsmen555@gmail.com

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

II. FUZZY NEURAL NETWORK STRUCTURE

To create a fuzzy neural network, we assess the degree of protection using, for example, as input parameters:1 – monitoring activities of human resources (HR), which has a high level of authority for actions in the system (by programmers, network database administrators, etc.); 2 – organizational and technical measures to back up important information; 3 – organizational measures to restore the system in case of emergency; 4 – organizational and technical measures for access control in the rooms in which computing equipment is located. They vary in the range [0; 1] of conventional units and are determined expertly in assessing the status of a computer network. The output of the expert system is the degree of security in the range [0; 50] of conventional units.

For the synthesis of a fuzzy neural network, the graphic interface of hybrid neural networks is used, which is implemented in the application package ANFIS Editor (Fuzzy Logic Toolbox) of the MatLAB system [5] (Fig. 1).

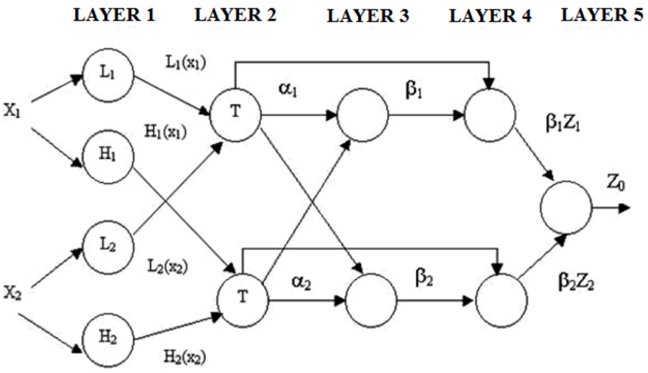


Fig. 1. Fuzzy neural network structure (ANFIS architecture)

Generalized this network can be described as follows.

LAYER 1. The outputs of the neurons of this layer are the values of the membership function at specific (given) input values.

LAYER 2. The outputs of the neurons of this layer is the degree of truth of the premises of each rule of the knowledge base of the system, calculated by the formulas:

$$\alpha_1 = L_1(x_1) \wedge L_2(x_2) \qquad (1)$$

$$\alpha_2 = H_1(x_1) \wedge H_2(x_2) \qquad (2)$$

The letter T, which means their functionality to implement an arbitrary t-norm for modeling the operation "AND", denotes all neurons of the layer.

LAYER 3. The neurons of this layer calculate the values:

$$\beta_1 = \frac{\alpha_1}{\alpha_1 + \alpha_2}, \; \beta_2 = \frac{\alpha_2}{\alpha_1 + \alpha_2}. \qquad (3)$$

LAYER 4. Neurons of this layer perform operations:

$$\beta_1 Z_1 = \beta_1 D^{-1}(\alpha_1), \; \beta_2 Z_2 = \beta_2 M^{-1}(\alpha_2) \qquad (4)$$

Moreover, the coefficients *N* and *M* are established from the relations:

$$D^{-1}(\alpha_1) = c_4 + c_5 + \frac{1}{b_4} ln \frac{1-\alpha_1}{\alpha_1} \qquad (5)$$

$$M^{-1}(\alpha_2) = c_4 + \frac{1}{b_4} ln \frac{1-\alpha_2}{\alpha_2} \qquad (6)$$

LAYER 5. The neuron in this layer calculates the output of the network:

$$Z_0 = \beta_1 Z_1 + \beta_2 Z_2 \qquad (7)$$

Correction of network parameters for membership functions *N* and *M* occurs in accordance with the selected algorithm (in this case, the back propagation of errors is used) according to the formulas:

$$b_4 = b_4' - \frac{\eta}{b_4^{2\prime}} \cdot \delta_k \cdot \frac{\alpha_1 + \alpha_2 - \alpha_3}{\alpha_1 + \alpha_2 + \alpha_3} \qquad (8)$$

$$c_4 = c_4' + \eta \delta_k \qquad (9)$$

$$c_5 = c_5' + \eta \delta_k \frac{\alpha_1}{\alpha_1 + \alpha_2 + \alpha_3} \qquad (10)$$

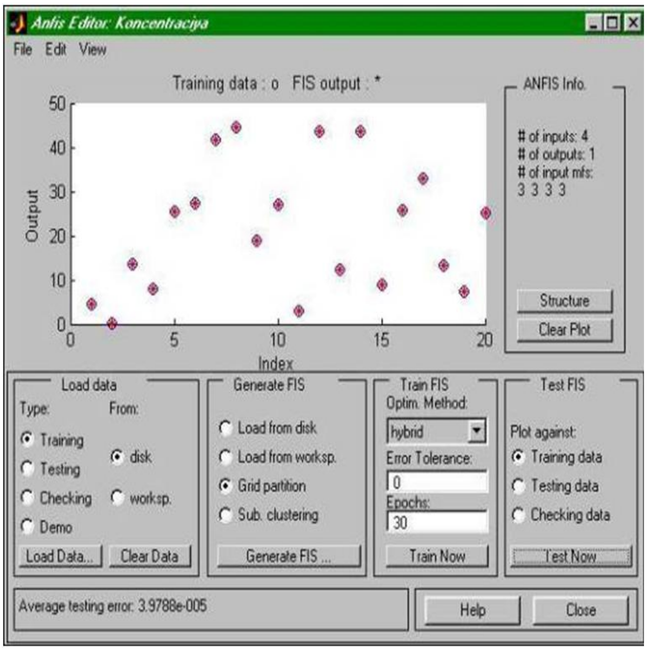
$$\delta_k = y^k - o^k, \; k = 1...N \qquad (11)$$

where η is given neural network learning rate; y^k is reference output of a neural network; o^k is the actual output of the neural network; b_4', c_4', c_5' are the value of these same coefficients in the previous step iterative learning of a neural network; *N* is the number of model sets of input (training) data.

III. SELF-TUNING OF ANFIS TO THE TRAINING SET OF EXPERIMENTAL DATA

For effective neural network modeling, we take three blocks of 20 sets of expert data: training data, testing data, checking data. The presence of three blocks is not mandatory, sometimes just a training and a control one is enough, however the test block improves the quality of further work, since it makes sure that the so-called "retraining" of the network has not occurred.

When training an expert system we selected the default settings, set 30 epochs for self-tuning. An acceptable standard error was obtained, which was 3.9788e-005 mg / l (Fig. 2).



ANFIS Info.
# of inputs: 4
# of outputs: 1
# of input mfs:
3 3 3 3

Load data
Type: ● Training ○ Testing ○ Checking ○ Demo
From: ● disk ○ worksp.

Generate FIS
○ Load from disk
○ Load from worksp.
● Grid partition
○ Sub. clustering

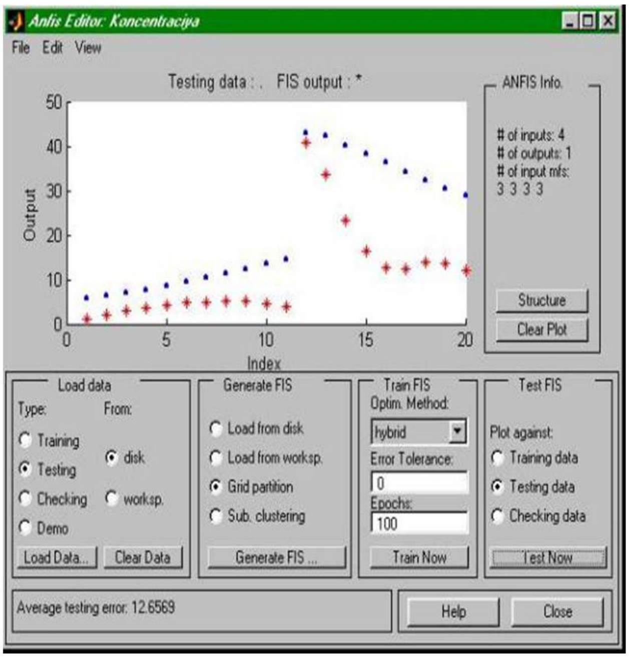
Train FIS
Optim. Method: hybrid
Error Tolerance: 0
Epochs: 30

Test FIS
Plot against: ● Training data ○ Testing data ○ Checking data

Average testing error: 3.9788e-005

Fig.2. Self-tuning of ANFIS to the training set of experimental data when setting the system parameters by default

Then, we entered the value of the testing data. The results obtained at the default settings were unsatisfactory - the standard error was 12.6569 mg/l (Fig. 3).



Anfis Editor: Koncentracija

Testing data : . FIS output : *

ANFIS Info.
# of inputs: 4
# of outputs: 1
# of input mfs:
3 3 3 3

Load data — Type: ◉ Testing; From: ◉ disk

Generate FIS: ◉ Grid partition

Train FIS — Optim. Method: hybrid; Error Tolerance: 0; Epochs: 100

Test FIS — Plot against: ◉ Testing data

Average testing error: 12.6569

Fig.3. Self-tuning of ANFIS to a control set of experimental data with default settings of the system

During the learning, the number of neurons in each layer was reduced by one in the structure of the fuzzy neural network (Fig. 4), membership functions varied. As a result of 64 stages of iterative learning (Fig. 5), we obtained an average deviation of 0.28268 mg/l. This value, taking into the aspects of assessing the degree of security, suits us. The quality of the hybrid neural network has been assessed by inputting checking data.The standard error was 0.34339 mg / l (Fig. 5). So ANFIS is "trained".

The expert system synthesized in this way is quite easy to integrate into working software, increasing the ability of information protection systems to adequately and adaptively assess the degree of security of real computer systems. At the same time, it is advisable to periodically “re-learning” such a fuzzy neural network model - supplementing the knowledge base with new data collections [6-10].

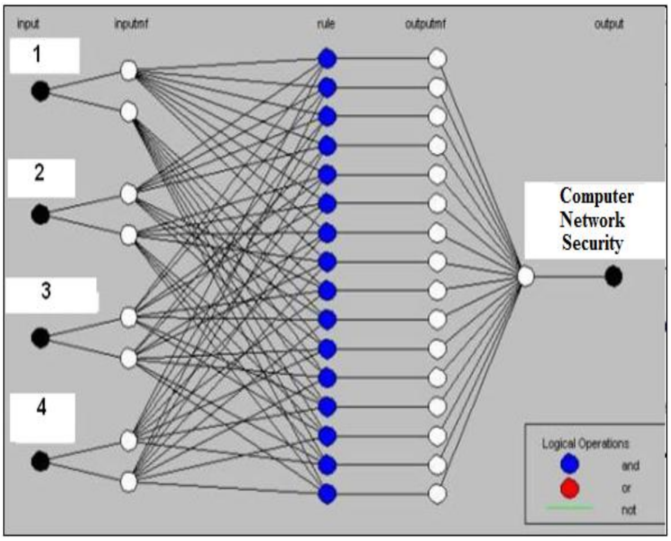


Fig.4. The structure of a "trained" fuzzy neural network

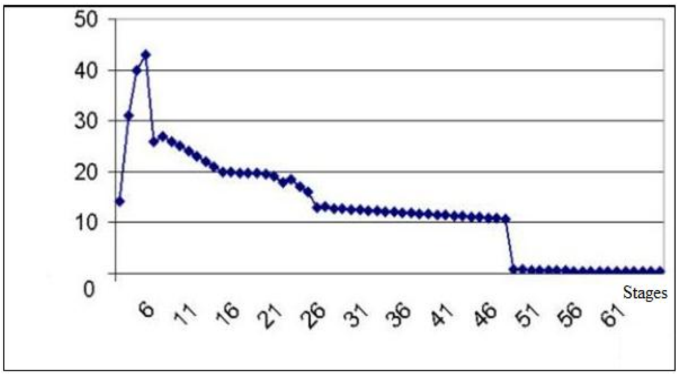


Fig. 5. Step-by-step reduction in standard error for ANFIS expert training

IV. ANALYZING AND EVALUATING THE SECURITY OF COMPUTER NETWORKS

One of the main tasks of the expert system is to promptly assess the security of computer networks in data protection since the advantage of the network is access to shared data and devices, which makes it possible to gain unauthorized access to this data. By data security we mean protecting network resources from destruction and protecting data from accidental or intentional disclosure, as well as from illegitimate changes.

In general, a network administrator or a security officer must guarantee data security. In order to guarantee data security, a multilevel security system is developed: built-in remedies - system software tools (passwords, access rights); physical remedies - locks, doors, security, alarms, etc.; administrative control - organizational measures, orders of the administration; legislation and social environment - copyright and property rights laws, intolerance to computer piracy.

In this case, there is a need to assess the level of protection of the information system with the help of the proposed expert system. For this purpose, a fuzzy neural network is configured to a specific object in order to promptly determine one of the 7 levels of security for computer systems used by the US Department of Defense. The neural network is configured in accordance with the world-wide classification of the level of the system security, which is defined in the Orange book "The Trusted Computer System Evaluation Criteria". Thus, using the proposed expert system for a specific object, one of 7 levels of security of computer and network systems is determined according to the following security levels [11]:

D - Minimal Protection level. Reserved for systems that do not guarantee the required level of security at other levels;

C1- Discretionary Security Protection level. Allows users to apply access restrictions to protect private information;

C2 - Controlled Access Protection level. Contains C1 level requirements, as well as protection of the registration process in the system, accounting of security events, isolation of resources of different processes;

B1 - Labeled Security Protection level. The ability to protect individual files, records in files, other objects of the system with special security tags stored with these objects is added to the requirements of level C2. It is believed that a well-prepared hacker can cope with such protection, but an average user cannot do this;

B2 - Structured Protection level. The complete protection of all system resources directly or indirectly accessible to the user is added to the requirements of level B2. It is believed that hackers will not be able to penetrate the system with such level of protection;

B3 - Security Domains level. The explicit specification of users, who are denied access to certain resources, and more complete logging of potentially dangerous events are in addition to the requirements of level B2. It is believed that even experienced programmers are not able to overcome the system with this level of security;

A1 - Verified Design level. Full protection of information with specified and verified protection mechanisms is used. It is believed that no one (even special services experts) can penetrate the system with this level of protection without permission.

V. CONCLUSION

1. The article shows that data security in complex network computer systems must be guaranteed by its administrator (special person) using the decision support system for the operational assessment of computer network security. Based on the solutions proposed by the described expert decision support system, the administrator must quickly implement a specific, specified and verified mechanism for protecting computer networks. Thus, the substantiation of the principles of synthesis of an expert system for assessing the security of computer networks based on a fuzzy neural network is an urgent scientific and technical task.
2. To solve this problem, factors that characterize the security of complex computer networks have been identified and the use of fuzzy neural networks as the mathematical apparatus for building an expert system has been proposed. An analysis of the existing sources showed that expert systems based on neural networks are now being used. They have a number of disadvantages: a long training time, the complexity of analyzing the structure of a trained network, the impossibility of its optimization; the impossibility of introducing unconditional (expert) information to accelerate network learning.
3. In order to eliminate significant shortcomings, a method for synthesizing a fuzzy neural network for assessing the security of computer networks was developed, an appropriate neural network was created, and tested for adequacy. For the synthesis of a fuzzy neural network, a graphical interface of hybrid neural networks was used, implemented in the application package ANFIS Editor (Fuzzy Logic Toolbox) of the MatLAB system. As input parameters, we used data about: organizational measures to control personnel who have a high level of authority for actions in the system; organizational and technical measures for the backup (duplication) of critical information; organizational measures to restore the system in case of emergency; organizational and technical measures for managing access in the premises in which computing equipment is located. They varied in the range [0; 1] arbitrary units and were determined expertly in assessing the state of a computer network. The output of the expert system is the level of security in the range [0; 50] arbitrary units. When training an expert system, the default settings were selected from the training set and 30 cycles (Epoch) of self-tuning were set. An acceptable standard error of 3.9788e-005 was obtained, which is sufficient for training artificial neural networks for such systems. Thus, the prospects of the proposed methodology for creating an expert system for assessing the security of computer networks have been established.
4. The scientific and practical significance of developing such a system lies in the fact that a fuzzy neural network is configured on a specific object to quickly determine the level of security of computer networks, which is necessary for the administrator of computer systems. Based on this, the proposed work solves the urgent task of substantiating the principles of the synthesis of an expert system for assessing the security of computer networks based on a fuzzy neural network, this is promising because it provides an operational definition of one of the seven levels of computer network security that are used in the US Department of Defense.

REFERENCES

1. Yu.P. Zaichenko Computer Networking: A Tutorial, Kyiv “Slovo”, 2003, p. 286. (in Ukrainian)
2. G.M. Lozikova Computer networks. Kyiv, Center for Educational Literature, 2004, p.128. (in Ukrainian)
3. T. Voletskaya Computer networks. Hardware. Kyiv, Center for Educational Literature, 2004, p.208 p. (in Ukrainian)
4. Poznyak A.S. Dynamic neural networks for nonlinear control: Identification state estimation and trajectory tracking / A.S. Poznyak, E.N. Sanchez // World Scientific. 2001. London. pp.102-120.
5. El-Din A.G., Smith D.W. Neural networks model to predict the wastewater inflow incorporating rainfall events / El-Din A.G., Smith D.W. // Water Res. 2002, V. 36, pp.1115-1126.
6. V.M. Shtepa, N.A. Zayets, O.V. Lenkov, A.S. Shvorov. Methodical principles of using neural networks for determining the importance of incoming electronic documents. Modern Special Technique. 2013. № 3 (34), pp. 58-63. (in Ukrainian)
7. Osypenko V. About some design principles of information-retrieval system and processing of electronic documents in Internet. Bulletin of Lviv Polytechnic National University. 2014. № 80, pp. 10–15.
8. V. Lysenko, Y. Gunchenko, S. Shvorov, S. Lenkov, S. Kuznichenko, E. Lenkov. Methodological Bases of Construction of Intensive Training Flight Simulators of Aircrews // Proceedings 5th International Conference “Methods and Systems of Navigation and Motion Control”. ISBN: 978-153865870-3 – Kyiv, 2018. – pp. 198 – 203.
9. Shvorov, S.A., Pasichnyk, N.A., Kuznichenko, S.D., Tolok I., Lienkov, S.V., Komarova, L.A. Using UAV during Planned Harvesting by Unmanned Combines // IEEE 5th International Conference Actual Problems of Unmanned Aerial Vehicles Developments, APUAVD 2019 ISBN: 978-172812592-3. – Proceedings 8943842, pp. 252-257.
10. Y. A. Gunchenko, P. S. Emelyanov, S. A. Shvorov and E. S. Lenkov, "Theoretical basis development of the intelligent training systems for the intensive training of air traffic controllers," 2016 4th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC), Kiev, 2016, pp. 134-137. doi: 10.1109/MSNMC.2016.7783125
11. Yurii Gunchenko, Serhii Lienkov, Yurii Husak, Sergey Shvorov, Dmytro Zaitsev. Model of Functioning Data-Transfer Systems Special Purposes Taking into Account the Influence of Cyber Attack// International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9, Issue-6, March 2020. P 2248-2252. DOI: 10.35940/ijitee. E3050.049620.

AUTHORS PROFILE

Svitlana Kuznichenko, Candidate of Geographical Sciences, Associate Professor, department of Information Technologies Odessa State Environmental University Odessa, Ukraine. Email: skuznichenko@gmail.com ORCID: 0000-0001-7982- 1298

Sergey Shvorov, Doctor of Technical Sciences, Professor, Department of Automation and Robotic Systems National University of Life and Environmental Sciences of Ukraine Kyiv, Ukraine Email: 7996445@gmail.com

Yurii Husak Doctor of Military Sciences, Senior Researcher, Research Center, Institute of the Armed Forces of Ukraine of Kyiv, Kyiv, Email: y.husak1512@gmail.com
http://orcid.org/0000-0002-3423-2112

Igor. Tolok, Candidate of Pedagogical Sciences, Associate Professor, Honored Worker of Education of Ukraine,Military Institute of Taras Shevchenko National University of Kyiv, Kyiv, Ukraine. Email: s63010566s@gmail.com.
http://orcsid.org/0000-0001-6309-9608

Muliar Ihor PhD, assistant professor of Cybersecurity of Computer Systems and Networks of Khmelnytsky National University,Khmelnitsky, Ukraine. betsmen555@gmail.com.
http://orcid.org/0000-0002-6659-605X