International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August 2019

Tools of the Neuro-Fuzzy Model of Information Risk Management in National Security

Alla Khomutenko, Alla Mishchenko, Artem Ripenko, Olha Frum, Zoreslava Liulchak

Roman Hrozovskyi

***Abstract*: The rapid development of information technology has strengthened the importance of the information risk management system. Integrated systems for storing and processing information, its transmission channels, as well as the information itself, are strategically essential objects of national security. The growing volumes of statistical data, as well as the traditional uncertainty and incompleteness of information on the nature of potential threats, determine the need to use new approaches for risk analysis. The neuro-fuzzy model considered in the article is based on the advantages of fuzzy logic and artificial neural networks. The proposed neuro-fuzzy network is adapted for continuous risk analysis and iterative implementation of the analysis stage. It eliminates the disadvantages of the fuzzy logical model and takes full advantage of neural networks. This system copes well with large volumes of information since there is a direct correlation between the amount of data and the speed of network learning.**

The data provided by the network at the output is expressed in understandable terms and sufficient to make a balanced and reasoned decision on information risk management.

Keywords* : *Neuro-Fuzzy Model, Risk, Information Risks, Risk Management, National Security.

I. INTRODUCTION

In modern political realities, one of the essential factors in ensuring the security of both the state as a whole and individual business entities is information security.

Now in the era of the global spread of information technology, state security is more than ever exposed to the influence of information threats. That is why the effectiveness of the information risk management system is becoming a critical national security issue [1-3].It should be immediately determined that information security will be understood as the security of information resources and information systems from accidental or deliberate influences of a natural or artificial nature, fraught with damage to both the system as a whole and its individual elements.

Within the framework of this article, it is supposed to reduce such a broad concept as information risk to two categories:- associated with the leakage, alteration or destruction of information;- associated with a malfunction in the operation of software or hardware (caused by various factors of a natural or artificial nature) [4-5].

The information risk management scheme can be simplified represented in Fig. 1.

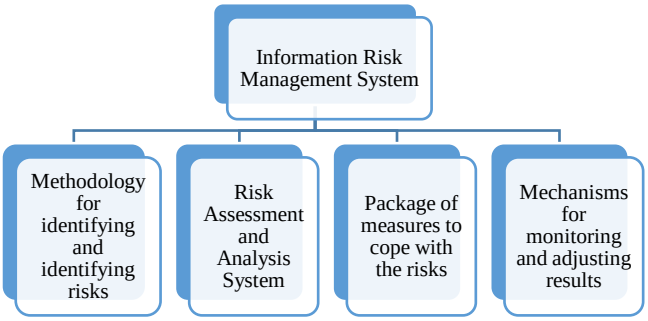

Fig. 1.Information Risk Management.

The primary stage of the risk management system is the identification and identification of risks: analysis of possible and existing vulnerabilities in the information processing and storage system, identification of potential external and internal threats, classification and verification of information of particular value to the state. The stage of risk analysis and assessment involves a qualitative and quantitative risk assessment, the result of which is information that allows you to make decisions about the necessary risk management measures. The set of steps to counter risks at the state level includes some measures aimed at reducing, adopting or counteracting, the decision on the use of which is taken at a senior level. The control and adjustment stage allows us to evaluate the effectiveness of the measures taken and, if necessary, launch the next iteration of the risk management cycle [6-7].Naturally, specialists have been dealing with these issues for more than a decade, and the mechanisms developed are quite useful. At the same time, the very nature of information risks,

Revised Manuscript Received on August 30, 2019.

* Correspondence Author

Alla Khomutenko*, Finance Department of Odessa National Economic University, Odessa, Ukraine

Alla Mishchenko, Department of International Relations, Faculty of Journalism and International Relations, Kyiv National University of Culture and Arts, Kyiv, Ukraine

Artem Ripenko, Odessa Forensic Research Institute of Ministry of Justice of Ukraine, Odessa, Ukraine

Olha Frum, Department of Industrial Economics, Odessa National Academy of Food Technologies, Odessa, Ukraine

Zoreslava Liulchak, Department of Marketing and Logistics Lviv Polytechnic National University, Lviv, Ukraine

Roman Hrozovskyi, Research Laboratory of the Department of Application of Information Technologies and Information Fight of the National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine

and the areas in which they arise suggests the need for constant re-evaluation and modernization of existing methods. As the key elements of the system, it is possible to single out the stages of analysis and risk assessment; it is for these points that it is proposed to test the tools of the neuro-fuzzy model.

The effectiveness of protecting national interests in the field of information security depends both on the approach to its organization and on the correct choice of methods for calculating information security risks [8-9].

At present, probabilistic methods based on the calculation of statistical assessments of the possibility of occurrence of adverse events are most widely used for risk assessment. At the same time, the use of these methods in the framework of the national security program may be limited due to the difficulty of accumulating a statistical sample of the volume, sufficient to confirm the specific law of the distribution of a random variable. The information risk management scheme can be simplified to imagine how.

II. METHODOLOGY

A. Fuzzy logic as the basis of a risk analysis methodology.

The advantage of fuzzy-logical methods is most fully manifested in cases of high complexity and non-linearity of the studied objects, as well as in situations of insufficient or inaccurate information. Indeed, in its essence, fuzzy logic is designed to describe complex concepts in terms close to natural human language.That is why its use in such an area as an information risk management system looks so attractive because it is no secret that analysts and risk managers have to deal with large volumes of not always complete or accurate information when analyzing risks and threats.The methodology of neuro-fuzzy modelling is based on two principles - fuzzy logic and artificial neural networks. The basics of these technologies separately originated in the 20th century, but their effectiveness was most fully revealed after synergy and using modern computing power. Let us consider each of them in more detail.The basis of the fuzzy-logical model is the concept of a fuzzy set, which is a combination of ordered pairs of elements x of the universal set X and functions $\mu_A(x)$:

$$A = \{(x, \mu_A(x)) | x \in X\} \quad (1)$$

Moreover, $\mu_A(x)$ is a membership function showing the degree to which the element x belongs to the fuzzy set A and takes values in the range [0,1], it can be seen that in contrast to the Boolean set, where the values can be only 0 or 1, in fuzzy sets, they can take any value from the range.

Other important elements of the fuzzy-logical model are the concept of a linguistic variable, for the description of which a set of values and rules is used:

$$\{x, T(x), X, G, M\} \quad (1)$$

In this case, x is the name of the variable, for example, "probability of a risk event" or "degree of risk". The values that a linguistic variable can take are called terms, and their peculiarity is that they can be expressed in simple lexical forms, in our example regarding the degree of risk, it can be "high", "medium", "low". The set of values of terms is determined by $T(x)$; each term is essentially a fuzzy variable on the set X.The set of terms $T(x)$ is minimal, and new terms can be defined on the basis of the rules G and M, where G is a syntax rule for the formation of new names of terms, for example, “very” and “not very”, which allows creating variables of the form “very high, ”and M is a semantic procedure that converts a new name into a fuzzy variable (set the type of membership function).

Despite the universality and effectiveness of the fuzzy-logical model, it has some drawbacks, in particular, a set of fuzzy rules is set by a person and, accordingly, it may be incomplete, in addition, the parameters and type of membership function are also chosen by an expert based on subjective experience, and therefore they may not fully correspond to the real environment.

The elimination of these shortcomings is possible with the synergy of fuzzy logic with artificial neural networks. It is characteristic that neural networks themselves also have a number of disadvantages.

B. Artificial neural networks as a basis for building a hybrid network

An artificial neural network is a structure based on the principles of organization of biological neural networks and consists of connected and interacting artificial neurons. The simplest neural network consists of three layers of neurons: an input layer - collecting information for further processing, a hidden layer - processing all incoming information and an output layer - representing the result of processing. The interconnection between neurons is based on the so-called synapses, which have such a characteristic as weight. The main work is done on a hidden layer, where all incoming information from the previous layer is normalized using the activation function and transferred to the output layer. In fig. Fig. 2 shows the structure of the neural network without feedback; the line connecting neurons are synapses, whose designation and weights are omitted for clarity.

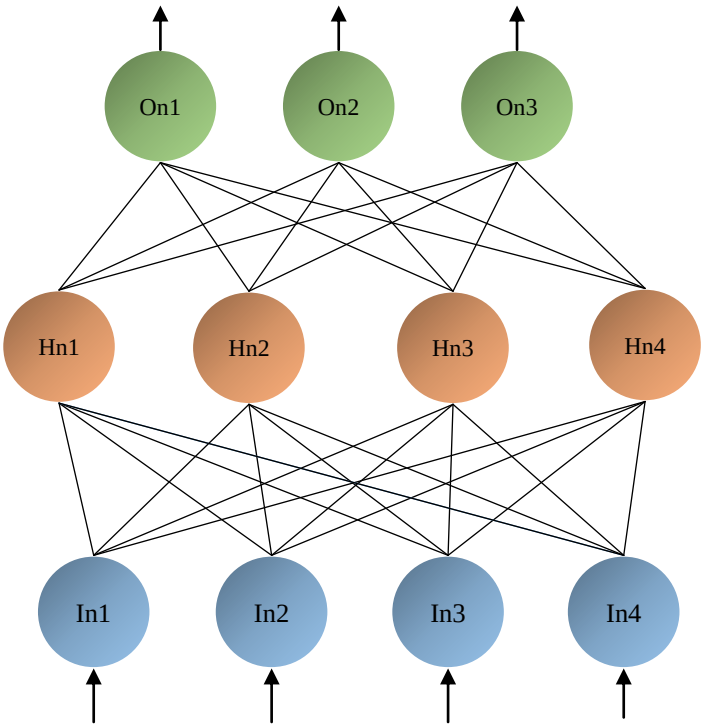

Fig. 2.Neural network structure

In order to illustrate the process of processing information by a neural network, we take a section of the network consisting of two input neurons and one hidden neuron. In the diagram, the incoming information flows indicated by xi are received by the input level neurons In1 and In2, then through the synapses wi the data are transmitted to the neuron of the hidden level Hn1. The process of interaction of information with synapses is described by the formula:

$$p_i = x_i \cdot w_i \quad (3)$$

All information coming to the Hn1 neuron is summed up forming input data:

$$Hn1_{input} = p_1 + p_2 = (x_1 \cdot w_1 \cdot) + (x_2 \cdot w_2) \quad (4)$$

Information processing by the Hn1 neuron consists of normalizing data using an activation function, in particular, a linear function, a sigmoid type or hyperbolic tangent, in a general form:

$$y = f_{activation}(Hn1_{input}) \quad (5)$$

A key feature of the neural network is that despite the simplicity of each neuron individually, connected together into a sufficiently large network, they are able to perform fairly complex tasks (Fig. 3). Unlike traditional algorithms, a neural network is not programmed but trained on the basis of a selection of source data. In the learning process, the neural network reveals the relationship between input and output data and is able to give the right result even according to data that were not in the initial sample.

Disadvantages of neural networks, this is the flip side of the coin of their merits, the work of the hidden layer is essentially a “black box”, which leads to the complexity of analyzing the work of a trained network, besides it is impossible to enter a priori information from experts on a neural network.

The synergy of both systems results in neuro-fuzzy models that combine the advantages of both approaches and eliminate their drawbacks. The main advantages of such hybrid neural systems are the interpretability and accuracy of the simulation.

A fuzzy-neural network is based on the structure of a normal neural network, and it has clear weights, signals and an activation formula, while the combination of information flows x_i with the weights of synapses w_i is carried out using the t-norm and t-conorm. Moreover, weights, input and output data are in the range [0,1].

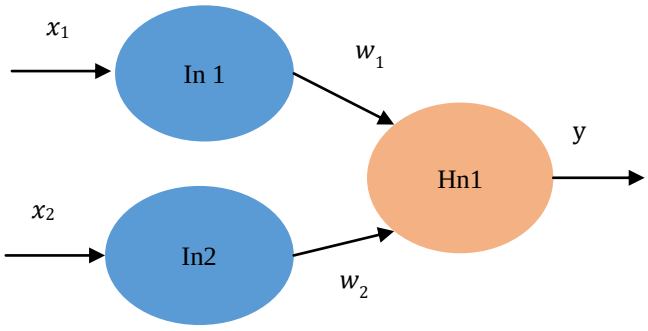

Fig. 3.Artificial neuron.

In the framework of the neuro-fuzzy model, new concepts are introduced - fuzzy neurons.

The fuzzy neuron "AND" whose input data are combined using the triangular conorm $p_i = S(w_i, x_i)$, and the output is formed using the triangular norm

$$y = AND(p_1, p_2) = T(p_{z1}, p_2) = T(S(w_1, w_2), S(w_s, x_s)) \quad (5)$$

The fuzzy "OR" neuron whose input is combined using the triangular norm $p_i = T(w_i, x_i)$, and the output is formed using the triangular conorm:

$$y = OR(p_1, p_2) = S(p_{z1}, p_2) = S(T(w_1, w_2), T(w_s, x_s)) \quad (6)$$

To use hybrid networks in expert risk assessment, fuzzy conclusions mechanisms are provided. The system of fuzzy conclusions is based on a set of fuzzy related rules formed by experts and having the form:

$$Rule_1: IF\ x\ is\ A_1\ THEN\ y\ is\ B_1 \quad (7)$$

$$Rule_2: IF\ x\ is\ A_2\ THEN\ y\ is\ B_2 \quad (8)$$

Although the fuzzy rules are set by the expert, and therefore are based on his subjective opinion, the use of neural networks can increase the objectivity of the model by extracting knowledge from the recorded input-output data and approximating the original dependencies by the network.

III. RESULT AND DISCUSSION

Let's consider the capabilities of neuro-fuzzy networks using a practical example; for this, we use the test database of statistical data on possible risks.

To begin with, we define the risk value as a function R function of the potential damage (cost of information, resource or asset) A, information security threat T and information system vulnerability V:

$$R = f(A, T, V) \quad (9)$$

Now we have input factors for the neural network, and we will define three linguistic variables: "Security threat", "Damage to assets", "System vulnerability". The basic term set for these variables will be identical: "Very Low", "Low", "Medium", "High", "Very High". The graphs of the membership function for each of the terms are presented in the diagram in Figure 4.

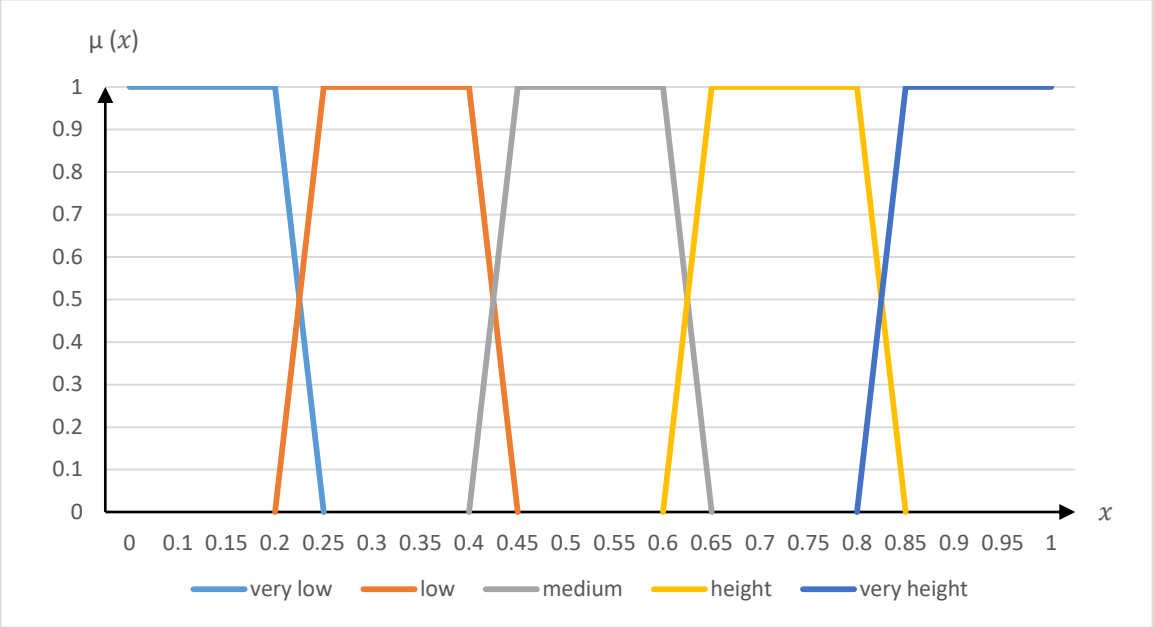

Fig. 4. Membership function graphs

The output of the network will be determined by the linguistic variable "Risk Level" and the basic term-set: "Negligible", "Low", "Below Average", "Medium", "High", "Critical".Thus, membership functions for input and output linguistic variables are defined. It remains to determine a set of fuzzy rules, in a real environment, they are set by an expert, and in this case, they will be similar:

IF (Security risk is Very low) AND (Damage to assets is Low) AND (System vulnerability is Low) THEN (Risk level is Low)

IF (Security risk is Very high) AND (Damage to assets is High) AND (System vulnerability is High) THEN (Risk level is Critical)

In this example, for three input linguistic variables, and five terms, 125 fuzzy rules are needed.

A generalized scheme of a neuro-fuzzy network that will process data is presented in Figure 5.

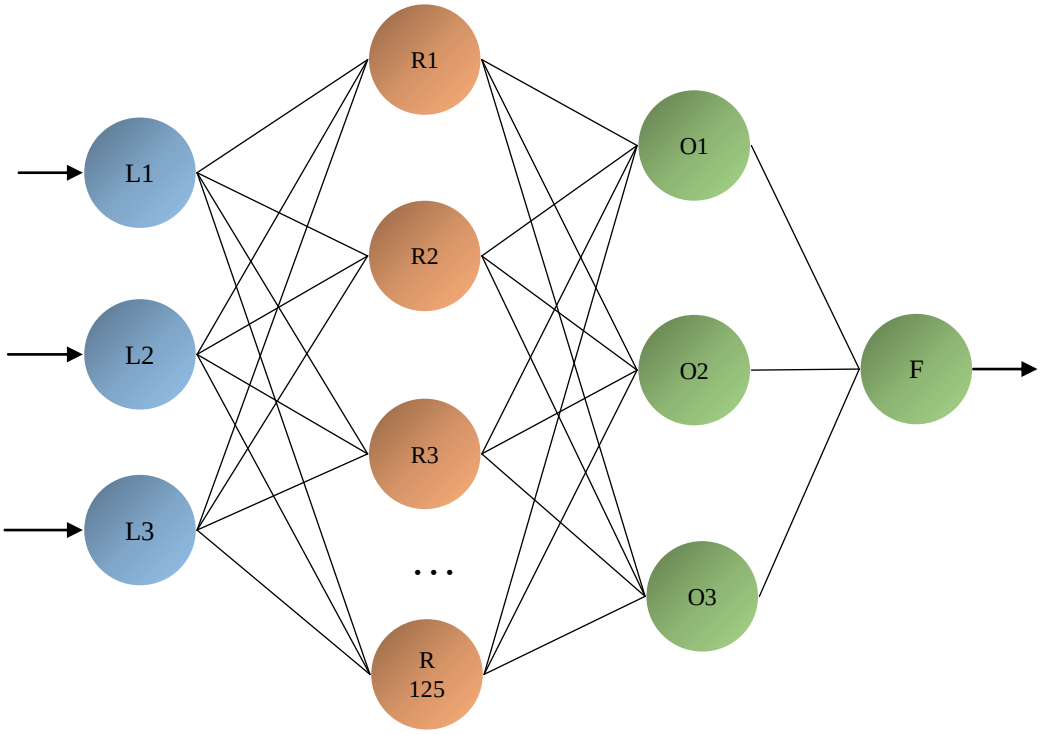

Fig. 5.Generalized scheme of a neuro-fuzzy network

The neurons of the L_i layer are ordinary input neurons; their task is to set the membership function of the input data to five terms.

The neurons of the R_i layer are fuzzy neurons of the "I" type, created one for each of the 125 fuzzy rules defined in this example, their task is to determine the truth of the premises of the given rules.

The neurons of the O_i layer are sets of fuzzy neurons that determine the membership function for the output

The only neuron of layer F - calculates the output of results for the output linguistic variable "Risk Level".

The training of a neuro-fuzzy network is carried out on the basis of a sample of data that can be collected statistically, by a survey method or by any other. The quality of network training, and as a result, the accuracy of the results obtained is proportional to the volume of the training sample.

IV. CONCLUSION

The number of training eras depends on the desired level of the permissible error of the output operations, for given parameters: 3 input variables with five terms, one output variable with five terms, 125 fuzzy rules, a network of a given structure learns for 25-30 eras. The considered neuro-fuzzy network is adapted for continuous risk analysis and iterative execution of the analysis stage. It eliminates the disadvantages of the fuzzy logical model and takes full advantage of neural networks. This system copes well with large volumes of information since there is a direct correlation between the amount of data and the speed of network learning.The data provided by the network at the output is expressed in understandable terms and is sufficient to make a balanced and reasoned decision on information risk management.

REFERENCES

1. Gary Stoneburner, Alice Goguen, and Alexis Feringa. Risk Management Guide for Information Technology Systems // National Institute of Standards and Technology NIST Special Publication 800-30, 2002. 95 c.
2. O. Goncharenko, O. Holiuk, I. Liganenko, O. Frum et al. Improving Staff Stimulation Systems: Causal-Consequence Approach, International Journal of Engineering and Advanced Technology, Volume-8 Issue-5, June 2019, pp. 891-894
3. S. Bondarenko, V. Lagodienko, I. Sedikova and O.Kalaman, Application of Project Analysis Software in Project Management in the Pre-Investment Phase, Journal of Mechanical Engineering and Technology, 9(13), 2018, pp. 676-684
4. O. Prokopenko, V. Omelyanenko, T. Ponomarenko, O. Olshanska Innovation networks effects simulation models, Periodicals of Engineering and Natural Sciences., 2019, Vol. 7, No. 2, August, pp. 752-762
5. Minimum Security Requirements for Federal Information and Information Systems, National Institute of Standards and Technology, Federal information processing standards publication, 2006, P. 17
6. V. Lagodiienko, M. Malanchuk, I. Gayvoronska and D. Sedikov. Selection of criteria for key performance indicators by the matrix method, International Journal of Mechanical Engineering and Technology, 10(1), 2019, pp. 1303-1311
7. S. Lekar, D. Shumeiko, V.Lagodiienko, V. Nemchenko, O. Nikoliuk, O. Martynyuk, The Use of Bayesian Networks in Public Administration of the Economy, International Journal of Engineering and Advanced Technology, Volume-8 Issue-5, 2019, pp. 1419-1421
8. O. Salnikova et al. Matrix approach to risk management in the national security system, highlighting the criteria for choosing the optimal strategy for decision making, International Journal of Engineering and Advanced Technology, Volume-8 Issue-5, June 2019, pp. 2407-2411
9. L. Rodchenko st al. Modelling the Risk Management of Financial Investments by the Fisher Criterion in Public Administration, International Journal of Innovative Technology and Exploring Engineering, Volume-8 Issue-9, July 2019, pp. 66-69