Neuro-fuzzy models in tasks of intelligent data processing for detection and counteraction of inappropriate, dubious and harmful information

I V Kotenko[1,2]**, I B Parashchuk**[1,2] **and T K Omar**[3]

[1] Department of computer security problems, St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS), 39, 14 Liniya, St. Petersburg, 199178, Russia
[2] International Laboratory of Information Security of Cyberphysical Systems, St. Petersburg National Research University of Information Technologies, Mechanics and Optics (University ITMO), 49 Kronverksky pr., St. Petersburg, 49,197101, Russia
[3] Non-profit JSC "Almaty University of Power Engineering and Telecommunications", 26/1, Baitursynov Street, 050013 Almaty, Kazakhstan

Abstract. The paper considers methodological approaches aimed at optimizing the operation of intelligent systems of analytical processing of digital network content in order to detect and counteract inappropriate, dubious and harmful information. An approach is proposed to eliminate uncertainty, incompleteness and inconsistency of evaluation and categorization of semantic content of information objects for analyzing network content. The approach uses neuro-fuzzy models and relies on processing of incomplete, conflicting and fuzzy knowledge. At the same time, the importance of the features of inappropriate, dubious and harmful information is determined taking into account the uncertainty – ambiguity (fuzziness) and unreliability (insufficiency, incompleteness) of the original information. The results of computational experiments to determine the membership functions of unwanted information signs on the basis of the neuro-fuzzy network are presented. The use of neural-fuzzy models in tasks of intelligent data processing for detection and counteraction of inappropriate, dubious and harmful information will significantly increase the reliability and efficiency of the decisions taken to detect and counter information of this class.

1. Introduction

The rapid development of the Internet, the introduction of the global network and social networks in the political, economic, social and cultural spheres of modern society is an important and powerful stimulus for the further development of the country. At the same time, the Internet and social networks have become one of the most important threats to personal, public and state information security.

It is known that «information security» is the state of protection of the individual, society and the state from internal and external information threats.

That is why the concept of «information security of the country» has two aspects. The first aspect determines the need to protect information in computer systems, networks and objects of critical information infrastructures from internal and external threats. The second aspect determines the need to protect the individual, society and the state from information that is distributed through information and telecommunications networks and can harm the health of citizens or motivate them to illegal behavior.

From a scientific and methodological point of view, the second aspect is considered as a large set of tasks to protect against inappropriate, dubious and harmful information. Laws and other guidance and regulatory documents refer to information: that is harmful to health, moral and spiritual development of people (especially children); promotes desocialization and perpetuation of illegal and unacceptable behavior; containing public calls for terrorist and other extremist activities; promoting pornography, the cult of violence and cruelty; containing data on the methods for development, manufacture and use of drugs and suicide, as well as obscene language; containing a biased assessment of the state policy of the country; delivery of inter-ethnic and social tensions; inciting ethnic and religious hatred or enmity; undermining the sovereignty, political and social stability, territorial integrity of the country and its allies.

The solution of a complex of priority state tasks on protection against inappropriate, dubious and harmful information consists now, firstly, in development and improvement of mechanisms for blocking sites in the Internet containing prohibited information, and secondly, in the development and implementation of effective modern hardware and software tools for protection against such information.

The second task is associated with development of new models, methods and techniques based on new, fundamental, advanced and rapidly developing fields of scientific knowledge, such as data mining, big data, processing of incomplete, contradictory and fuzzy knowledge, etc.

The relevance of this topic is determined by the fact that often the problem of intelligent data processing to detect and counter inappropriate, dubious and harmful information (IDHI) has to be solved in conditions of various kinds of uncertainty.

This significantly affects the reliability of decision making, for example, at an important stage – evaluation and categorization (EaC) of the semantic content of information objects (SCIO). Elimination of uncertainty, incompleteness and inconsistency on this stage should be based on the methods of processing of incomplete, contradictory and fuzzy knowledge. The theoretical significance and the main idea of the paper are to consider new methodological and mathematical approaches aimed at reliable evaluation and classification of IDHI under uncertainty. Evaluation and categorization of these features should take into account two key types of uncertainty: ambiguity (fuzziness) and unreliability (insufficiency, incompleteness) of the original information.

2. Relevant works

The methodology and technologies of protection against inappropriate, dubious and harmful information are under close state attention all over the world [1-6].

Technologies and methods of protection are defined, for example, in the laws «On protection of the children's Internet» and «On protection of children's privacy on the Internet», acting in the USA. They are actively used, aimed at detection of and counteraction against sexual and other undesirable materials posted on the Internet. They protect the privacy and safety of children on the Internet, including marketing restrictions [1, 2].

In the UK and Canada there is a «Cleanfeed» system, that blocks the Internet sites that contain prohibited and unwanted information in accordance with the «black lists» [3]. In Germany, requirements to remove and restrict access, usually to protect minors or to suppress hate speech and extremism, are imposed on the Internet service providers [4]. In Australia and Singapore, the tasks of filtering the Internet content are assigned to state regulators, as described in [5, 6].

In Russia, the detection of malicious sites and messages, the formation of «black lists» is currently carried out, as a rule, in manual mode [7, 8]. However, a single expert judgment on belonging of information to a particular category is always subjective [7], may be incomplete or erroneous.

In manual mode of the Internet content analysis, it is quite difficult to ensure compliance with the requirements for timely response to the emergence of new information objects and changes in the content of existing ones [8]. In addition, the Internet content tools have insufficiently high levels of speed, completeness and accuracy [7], and applied big data technologies are difficult for practical implementation [8].

Algorithms based on fuzzy logic continue to be the traditional tool used in the development of the methodology of intelligent analysis and detection of signs of inappropriate, dubious and harmful information under uncertainty. Their main advantage is the ability to simultaneously take into account the opinions and experience of many experts [9-11]. However, fuzzy logic systems are not capable to learn automatically [9]. The type and parameters of fuzzy set membership functions are static [10]. Fuzzy inference methods are chosen subjectively by human experts [11]. All of this can lead to inadequate results.

Models of artificial neural networks (ANN) are partially free from these shortcomings. For example, the paper [12] describes an approach based on the use of multilayer direct propagation ANN (multilayer perceptron).

However, this approach requires specifying auxiliary parameters characterizing the activation function of the sigmoid type, which is not always possible. In [13] the approach to the analysis of quality of communication networks on the basis of neural network synthesis of optimum system of quality indicators is stated. But this method is applicable to standard algorithms of the theory of complex systems estimation, which narrows the scope of application.

The paper [14] is devoted to the method that allows adaptive filtering of system states using recursive neural networks. But this approach is very difficult for mathematical specification and time-consuming.

In addition, none of the approaches is able to take into account simultaneously two key types of uncertainty: ambiguity (fuzziness) and unreliability (insufficiency, incompleteness, inconsistency) of the initial information – the analyzed signs of inappropriate, dubious and harmful information.

The papers [15] and [16] are devoted to modern neuro-fuzzy models (NFM) and neuro-fuzzy networks (NFN). They substantiate the possibility of constructing optimal algorithms to analyze controlled parameters of complex systems based on NFM. In this case, NFM combines advantages of fuzzy inference and neural network algorithms [17-19].

This approach will be considered in our paper. It is the basis to eliminate uncertainty (fuzziness, incompleteness and inconsistency).

The analysis of relevant works shows that direct application of the results obtained in these works is impossible for our task. The reason is that the real data processing, the processes of EaC SCIO occur under different types of uncertainty. This is due to a large number of different factors, including a variety of malicious content.

Therefore, the proposed unified approach to solve the problems of intelligent data processing to detect and counteract inappropriate, dubious and harmful information under uncertainty, is relevant.

3. Theoretical part

3.1. Formulation of the problem of elimination of incompleteness and inconsistency using NFM

Neuro-fuzzy models in tasks of intelligent data processing for detection and counteraction of IDHI are aimed at eliminating the incompleteness and inconsistency of EaC SCIO. NFM allows you to handle incomplete, inconsistent, and fuzzy knowledge. Neuro-fuzzy models (networks, systems) are data analysis ones that share neural network structures and fuzzy logic to analyz complex dynamic objects under uncertainty.

Sometimes they are used as expert systems and called neuro-expert models. They are a neuro-fuzzy network corresponding to a certain fuzzy inference model. Moreover, the knowledge of experts (a priori experience of the system) in the form of linguistic variables and fuzzy inference rules can be mutually and unambiguously reflected in the NFN structure.

In other words, NFM are combining the capabilities of neural networks and fuzzy logic. They represent a promising approach to the organization of modern mechanisms (algorithms) of data mining of any nature. The inclusion of the concept of fuzzy logic in neural networks (NFM formation) enables such a hybrid system to deal with the process of «reasoning similar to human».

This allows to form a new knowledge base (information space, information field) of ANN taking into account the a priori experience of experts, using the fuzzy information representation, fuzzy inference system (FIS), and also allows to extract knowledge from the input data stream, intended for processing in the interests of EaC SCIO.

Methods of practical implementation of NFM for elimination of incompleteness and inconsistency of EaC SCIO, can be various [17-19]. For example, you can use a simple, so-called «joint» model. Often it is characterized as a preprocessor, where the learning mechanism of ANN determines the rules of FIS. As soon as the parameters of FIS NFM determined, the ANN operates in the normal mode, and the approximation of membership functions is carried out by a neural network based on training data.

Another method of implementation of NFM in key tasks of intelligent data processing, such as EaC SCIO, is a «parallel» model [17]. Here, the neural network helps the fuzzy system to identify, detect the signs of IDHI, especially if these signs cannot be directly measured. Learning takes place only in the neural network, and the fuzzy system remains unchanged.

In some cases, fuzzy outputs cannot be directly applied to the process of EaC SCIO. In this case, the neural network can act as a postprocessor of fuzzy outputs. In other words, a «parallel» NFM is a model in which the input data is fed to the neural network and the output from the neural network is further processed by a fuzzy system.

An important feature of the NFM is the ability to automatically generate a system of fuzzy rules, extracting hidden patterns from the data of the training sample of signs of the IDHI. The choice of NFM («joint» or «parallel») is carried out depending on the class of actually solved tasks of intelligent data processing and the tasks of elimination of incompleteness and inconsistency of EaC SCIO.

As in the tasks solved by conventional ANN, the extrapolating neural network in NFM may consist of two layers of neurons – the input layer and the output layer. In contrast to the synaptic map, used in a conventional artificial neural network, the so-called «cognitive» map is used in the extrapolating neural network of NFM for eliminate incompleteness and inconsistency.

This map is completely defined by the matrix of links between the signs of the IDHI, those subject to EaC SCIO in the framework of data mining.

A «cognitive» map is an oriented graph, whose nodes are objects or concepts (in our case these are IDHI signs), and arcs are links between them, that characterize the cause-effect relations (links). As a rule, an expert or a group of experts is involved in drawing up such cards.

The concepts of the extrapolating neural network in the HFM for eliminating the incompleteness and inconsistency of EaC SCIO can be presented, for example, by the following signs (characteristics) of the IDHI:

signs of direct calls for violence (to war, seizure of power, violent change of the foundations of the constitutional system);

signs of incitement of hatred, enmity, discord or intolerance on social (class), racial, national, linguistic or religious grounds (as a result of agitation, propaganda or other actions);

signs of pornography, a cult of violence and cruelty;

signs of propaganda of superiority, exclusiveness or inferiority of citizens in their attitude to religion or race, signs of humiliation of national dignity;

signs of orientation of the purposes (or actions) on use of information on violation of integrity of the country, on undermining of security of the state, and other signs.

The use of «cognitive» maps in the NFM for elimination of incompleteness and inconsistency of EaC SCIO allows to describe (in the interests of formation of training data of the NFM) stable cause-and-effect relationships between different signs of dangerous information, allows to naturally combine the knowledge of several experts in the issues of detection and counteraction of the IDHI.

Filling in the matrix of connections and input fuzzy vector of preferences is the starting point in the neuro-fuzzy model for intelligent systems of analytical processing of digital network content.

As a result, the output layer (the fuzzy logic inference system) of the neural network of the HFM forms the optimal set (number) of the essential, most important IDHI signs to be analyzed. The structure of the fuzzy inference system of the set (numerical quantity) values of IDHI signs is proposed in (figure 1).

The fuzzy inference system consists of five function blocks:

fuzzification block, that converts input numerical values of IDHI signs in the extent to which the linguistic variables;

rule base, containing a set of fuzzy rules of type «IF» - «THEN»;

database, which defines the membership functions of fuzzy sets used in fuzzy rules for the output of IDHI signs;

decision-making unit, performing an output operation on the basis of existing rules;

defuzzification block, that converts the output results in numerical values of IDHI signs.

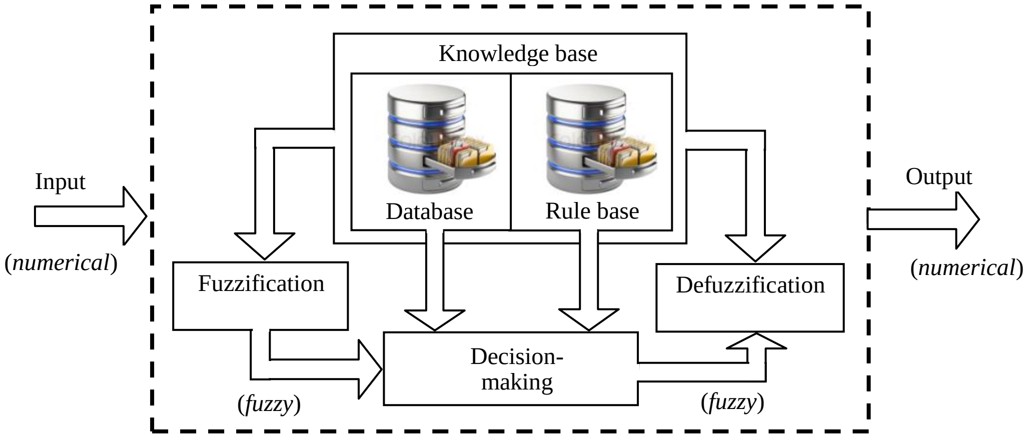

Figure 1. Fuzzy inference system in NFM for obtaining numerical values of IDHI signs.

Thus, from the point of view of the task of elimination of incompleteness and inconsistency of EaC SCIO, theoretical aspects of neuro-fuzzy networks are used.

They combine neural networks and fuzzy logic, collect the best properties of both methods and at the same time free from their problems.

On the one hand, such structures include computing power and the ability to train neural networks, and on the other hand, the intelligent capabilities of neural networks are enhanced by the inherent «human» way of thinking fuzzy rules of decision-making.

In addition, the NFM is able to take into account simultaneously two key types of uncertainty: ambiguity (fuzziness) and unreliability (insufficiency, incompleteness, inconsistency) of the initial information – the analyzed signs of unwanted, questionable and malicious information.

In the NFM, the output is based on fuzzy logic, and the parameters of the membership functions are configured using neural network learning algorithms. The module of fuzzy EaC SCIO is represented in the form of a multilayer network. In this network, layers act as elements of the fuzzy inference system.

3.2. Formation of the structure and formulation of functions of the levels of the NFN to eliminate incompleteness and inconsistency of EaC SCIO

The fuzzy inference system in NFM is implemented on the basis of the structure of ANFIS (*Adaptive-Network-Based Fuzzy Inference System).* This five-layer neural network of direct propagation of the signal, including adaptive fuzzy inference network.

A variant of the NFN with ANFIS-type structure for solving the tasks of elimination of incompleteness and inconsistency of EaC SCIO is presented in figure 2.

The first (input) layer L_1 implements membership functions for each term of each input variable – the values of IDHI signs.

The first input of the layer receives input signals that characterize a specific sign X_1 of the IDHI, the second – opinion of experts X_2 about this sign. At the output of the layer, we obtain the value of the membership function μ_{X_1} and μ_{X_2} for these signals.

This is a procedure of fuzzification – conversion of numerical input variables (values of IDHI signs) into a fuzzy form.

The parameters of the membership functions become the weights of the connections to neurons in the first layer of the network, and they will be modified in the learning process.

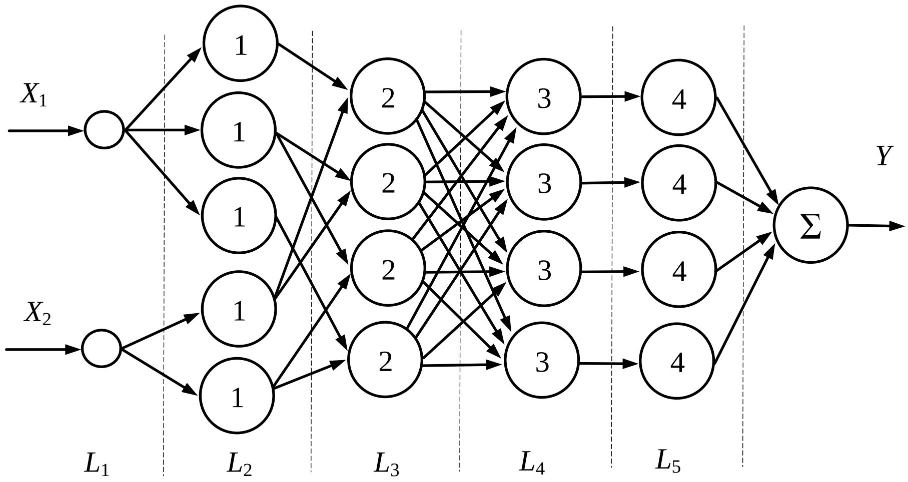

Figure 2. Variant of the NFN with ANFIS-type structure for solving the tasks of elimination of incompleteness and inconsistency of EaC SCIO.

As membership functions of input and output variables (IDHI signs), the Gauss function is used in the form of

$$\mu_A = \exp\left[\frac{1}{2}\left(\frac{X_n - a_i}{b_j}\right)^2\right],$$

where a_i, b_j – parameters of the membership function that require adjustment in the learning process of the NFN, X_n – a sign of the IDHI entering the input of the NFN.

The configuration of the second layer links corresponds to the structure of the rules of fuzzy inference in NFM for eliminate incompleteness and inconsistency of EaC SCIO.

Rule R_1: if X_1 is $\tilde{A}_1$ and X_2 is B_1;

Rule R_2: if X_1 is $\tilde{A}_2$ and X_2 is B_2;

Rule R_n: if X_1 is $\tilde{A}_n$ and X_2 is B_n, where $(\tilde{A}_1, \tilde{A}_2, ..., \tilde{A}_n)$ – fuzzy sets.

Then the rule $(R_1, R_2, ..., R_n)$ can be represented in the form of fuzzy implication (the conjunction of two statements in one)

$$R_k : \tilde{A}_k \to \tilde{B}_k, \ \ k = 1,...,N.$$

The second layer L_2 implements a logical output block. The number of neurons in a layer is equal to the number of rules.

Each node of the layer is connected to the previous layer in such a way that the node of the layer L_2 corresponding to the k-th rule is connected to all neurons of the layer L_1 corresponding to the fuzzy sets of conditions of this rule. The output value of the second layer L_2 will be the weight of the rule α:

$$\alpha_1 = \tilde{A}_1(X_1)\,\tilde{B}_1(X_2);$$
$$\alpha_2 = \tilde{A}_2(X_1)\,\tilde{B}_2(X_2).$$

Elements of the third layer L_3 is carried out the normalization of the degree of compliance with the rules and calculate the normalized values of importance (preference) β of the particular sign of the IDHI:

$$\beta_1 = \alpha_1 / \alpha_1 + \alpha_2;$$
$$\beta_2 = \alpha_2 / \alpha_1 + \alpha_2.$$

A clear value of importance (significance, preference) β of a particular sign of the IDHI, which determines the conclusion of each rule, in the fourth layer L_4 is considered as a fuzzy set with a Gaussian membership function.

Adaptive nodes of the fourth layer L_4 calculate the contribution of each fuzzy rule to the network output by the formula

$$Y = \sum_{i=1}^{n} \beta_i (X_1 + X_2),$$

where Y – the numerical value of the importance (significance, preference) of a particular sign of the IDHI.

This value, through the use of the NFM, takes into account both types of uncertainty: ambiguity (fuzziness) and unreliability (insufficiency, incompleteness) of the original information.

Thus, the fifth layer L_5 is an implementation of the defuzzification block – the transformation of fuzzy output variables (values of signs of the IDHI) into a numerical form.

At the output of the layer L_5 , in the summator, a clear total value of Y importance (significance, preference) of a particular sign of unwanted, questionable and malicious information is formed.

4. Experimental part

Let the vector of characterizing the sign of direct appeals to violence (for example, to war) goes to the first entrance of the NFN $X_1 = \{Pr_{\text{war}}(k)\}$, and the opinions $X_2 = \{Pr_{\text{war}}^{\text{exp}}(k)\}$ of experts on this sign of the IDHI – on the second.

At the output of the layer L_1 we get the value of the membership function μ_{A_1} and μ_{A_2}

$$\mu_{A_1} = \exp\left[\frac{1}{2}\left(\frac{Pr_{\text{war}}(k) - a_i}{b_j}\right)^2\right];$$

$$\mu_{A_2} = \exp\left[\frac{1}{2}\left(\frac{Pr_{\text{war}}^{\text{exp}}(k) - a_i}{b_j}\right)^2\right].$$

The configuration of the links of the second layer L_2 corresponds to the structure of the rules.

Rule R_1: if $Pr_{\text{war}}(k)$ is A_1 and $Pr_{\text{war}}^{\text{exp}}(k)$ is B_1.

Then: the Rule R_k can be represented as a fuzzy implication

$$R_k : \tilde{P}r_{\text{war}}(k) \to \tilde{P}r_{\text{war}}^{\text{exp}}(k);$$

$$R_{k+1} : \tilde{P}r_{\text{war}}(k+1) \to \tilde{P}r_{\text{war}}^{\text{exp}}(k+1).$$

At the output of the second layer L_2, we obtain the values that will be the weights of the rules for the neuro-fuzzy EaC SCIO:

$$\alpha_1 = Pr_{\text{war}}(k)\, \tilde{P}r_{\text{war}}(k)\, Pr_{\text{war}}^{\text{exp}}(k)\, \tilde{P}r_{\text{war}}^{\text{exp}}(k);$$

$$\alpha_2 = Pr_{\text{war}}(k)\, \tilde{P}r_{\text{war}}(k+1)\, Pr_{\text{war}}^{\text{exp}}(k)\, \tilde{P}r_{\text{war}}^{\text{exp}}(k+1).$$

Elements of the third layer L_3 fulfill the normalization of the degree of compliance with the rules and calculate the normalized values of particular sign of the IDHI.

Next is the exception of incorrect rules.

If some element of the layer L_2 is connected to different elements of the layer L_3, then no more than one connection with the greatest weight is selected, and the rest are excluded.

Thus, only one conclusion is made in accordance with the specific condition of the rule.

In the case where the weights of all links are negligible, they are all excluded and it is assumed that this rule has no significant effect on the output variable.

The third layer L_3 normalizes the degree of compliance with the rules and calculates the normalized values of the importance (preference) of such a sign of the IDHI as the presence of direct calls for violence (war) – $\{Pr_{\text{war}}(k)\}$:

$$\tilde{\beta}_1 = \frac{Pr_{\text{war}}(k)\,\tilde{P}r_{\text{war}}(k)\,Pr_{\text{war}}^{\text{exp}}(k)\,\tilde{P}r_{\text{war}}^{\text{exp}}(k)}{(Pr_{\text{war}}(k)\,\tilde{P}r_{\text{war}}(k)\,Pr_{\text{war}}^{\text{exp}}(k)\,\tilde{P}r_{\text{war}}^{\text{exp}}(k)) + (Pr_{\text{war}}(k)\,\tilde{P}r_{\text{war}}(k+1)\,Pr_{\text{war}}^{\text{exp}}(k)\,\tilde{P}r_{\text{war}}^{\text{exp}}(k+1))}$$

Adaptive nodes of the fourth layer calculate the contribution of each fuzzy rule to the network output by the formula

$$Y = \sum_{i=1}^{n} \tilde{\beta}_i (Pr_{\text{war}}(k) + Pr_{\text{war}}^{\text{exp}}(k)).$$

The fifth layer is the implementation of the defuzzification block. At the output of the L_5 layer, a clear value of the importance (preference) of such a sign of the IDHI as the presence of direct calls for violence (war) $\{Pr_{\text{war}}(k)\}$.

We introduce a «boundary», threshold value of the membership function, describing the importance (preference) a sign of the IDHI at the k-th step of the EaC, for example, at the level of $\mu^{\text{th}}(k)$=0,65.

Then the graph of convergence of the values of the membership function describing the importance (preference) of such a sign of the IDHI as the presence of direct calls for violence (war) has the form depicted in figure 3.

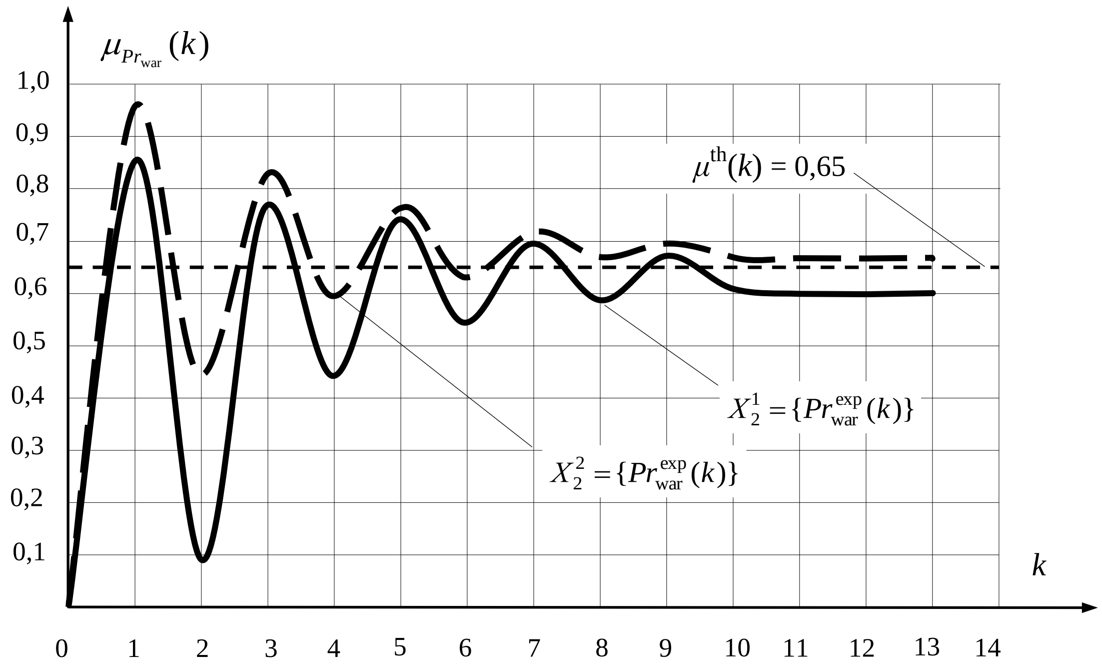

Figure 3. Chart observations of importance (preference) of the sign of the IDHI $\{Pr_{\text{war}}(k)\}$ in the operation of NFN.

The results of the experimental calculation show that the NFN in order to eliminate the uncertainty of the EaC SCIO has stabilized after the tenth step. The state of the network can be interpreted as a prediction of the guaranteed importance (preference) of IDHI sign $\{Pr_{\text{war}}(k)\}$ to detect and counteract unwanted, questionable, and malicious information.

This condition is characterized by a decrease in the importance (preference) of IDHI sign $\{Pr_{\text{war}}(k)\}$ for one variant of the initial expert opinions on this sign $X_2^1 = \{Pr_{\text{war}}^{\text{exp}}(k)\}$ and an increase in the importance (preference) of IDHI sign for another variant of the initial expert opinions $X_2^2 = \{Pr_{\text{war}}^{\text{exp}}(k)\}$.

In other words, for the different values of experts' opinions on this IDHI sign, the final values of the importance (preference) of this sign will be different and may take values above and below the threshold. This characterizes the weight (influence, importance, preference of accounting) of a particular sign of the IDHI in the EaC SCIO tasks.

As a result of the consistent implementation of the EaC SCIO stages, taking into account the uncertainty, a number of important, essential signs of the IDHI can be obtained. According to experts, it is desirable to include these signs of the IDHI in the control procedures. This will improve the objectivity (accuracy, informativeness) of content monitoring and management of detection and counteraction of unwanted, questionable and malicious information.

5. Conclusion

From the point of view of practice, the presented approach allows, in our opinion, to build a decision support system for the EaC SCIO, able to assess the importance of signs of malicious information quickly and with high accuracy, taking into account the uncertainty of the description and observation of these signs, the requirements and conditions of the functioning of the intelligent system of analytical processing of digital network content.

The advantage of the proposed approach is the possibility of using a decision support system based on the neuro-fuzzy model not only for content analysis, but also for synthesis – for the selection of the most important features of unwanted information in the control loop of detection and counteraction of such information in conditions of incompleteness, fuzziness and unreliability of the source data.

At the same time, through the use of NFN, evaluation and categorization of the signs of the IDHI takes into account both key types of uncertainty: ambiguity (fuzziness) and unreliability (insufficiency, incompleteness) of the source information.

Thus, the use of the proposed neuro-fuzzy models in the tasks of intelligent data processing to detect and counter inappropriate, dubious and harmful information will significantly increase the reliability and efficiency of the evaluation and categorization of the semantic content of information objects, as well as increase the objectivity of decisions to detect and counteract dangerous information.

6. References

[1] Baykan E, Henzinger M, Marian L and Beber I 2009 Purely URL-based topic classification *Proceedings of the 18th international conference on World wide web (WWW '09)* ACM, New York, NY, USA pp 1109-1110.

[2] Calado P, Cristo M, Moura E, Ziviani N, Ribeiro-Neto B and Goncalves M A 2003 Combining link-based and content-based methods for web document classification *Proceedings of the 12th International Conference on Information and Knowledge Management* (CIKM'03) New York, NY, ACM Press pp 394-401.

[3] Dumais S and Chen H 2000 Hierarchical classification of web content *Proceedings of the 23rd annual international ACM SIGIR conference on Research and development in information retrieval (SIGIR '00)* ACM, New York, NY, USA pp 256-263.

[4] Joachims T 1998 Text categorization with support vector machines: learning with many relevant features *Proceedings of ECML-98, 10th European Conference on Machine Learning* Chemnitz, Germany pp 137-142

[5] Kan M Y 2004 Web page classification without the web page *Proceedings of the 13th International World Wide Web conference (WWW Alt.'04)* ACM, New York, NY, USA pp 262-263

[6] Kan M Y and Thi H O N 2005 Fast web page classification using url features *Proceedings of the 14th ACM international conference on Information and knowledge management (CIKM'05)* ACM, New York, NY, USA pp 325-326

[7] Kotenko I, Chechulin A and Komashinsky D 2015 Evaluation of Text Classification Techniques for Inappropriate Web Content Blocking *Proceedings of the IEEE 8th International Conference on «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (IDAACS'2015)* Warsaw, Poland pp 412-417

[8] Kotenko I, Chechulin A and Komashinsky D 2017 Categorisation of web pages for protection against inappropriate content in the internet *International Journal of Internet Protocol Technology* (IJIPT) **10** 1 pp 61-71

[9] Rodriguez-Lopez R 2008 Monotone method for fuzzy differential equations *J. Fuzzy Set Systems* pp 2047–2076
[10] Crespo F and Weber R 2005 A methodology for dynamic data mining based on fuzzy clustering *J. Fuzzy Set Systems* pp 267-284
[11] Kotenko I, Saenko I, Ageev S and Kopchak Y 2015 Abnormal Traffic Detection in networks of the Internet of things based on fuzzy logical inference *Proceedings of the XVIII International Conference on Soft Computing and Measurements (SCM'2015)* IEEE Xplore 5-8
[12] Rojas R 1995 Neural Networks Springer-Verlag, Berlin p 453
[13] Parashchuk I B 2002 System Formation Algorithm of Communication Network Quality Factors using Artificial Neural Networks *Proceedings of the 1st IEEE International Conference on Circuits and System for Communications (ICCSC'02)* St.PGU, St. Petersburg, Russia pp 263-266
[14] Parlos A G, Menon S K and Atiya A F 2001 An algorithmic approach to adaptive state filtering using recurrent neural networks *Proceedings of the IEEE Trans. Neural Networks* **12** 6 pp 1411-1432
[15] Nesteruk G Ph and Kupriyanov M S 2003 Neural-fuzzy systems with fuzzy links *Proceedings of the VI-th Int. Conference SCM'2003* St.Pb StPSETU «LETI» **1** pp 341-344
[16] Polschykov K O 2013 Synthesis of neuro-fuzzy systems of data flows intensity control in mobile ad-hoc network *Proceedings of the 23rd International Crimean Conference Microwave and Telecommunication Technology* (*CriMiCo*) pp 517- 518
[17] Takagi T and Sugeno M 1985 Fuzzy identification of systems and its applications to modeling and control *IEEE Transactions on Systems, Man and Cybernetics* SMC-**15** 1 pp 116-132
[18] Buldakova T I and Dzalolov A Sh 2012 Analysis of Data Processes and Choices of Data-processing and Security Technologies in Situation Centers *Scientific and Technical Information Processing* **39** pp 127-132
[19] Ajith A 2005 Adaptation of Fuzzy Inference System Using Neural Learning *Computer Science Department* Oklahoma State University, USA pp 130-134

Acknowledgments
This research was supported by the Russian Science Foundation under grant number 18-11-00302 in SPIIRAS.