Decision support system for ensuring information security of an automated process control system

A.D. Kirillova[1], V.I. Vasilyev[1], A.V. Nikonov[1], V.V. Berkholts[1]

[1]Ufa State Aviation Technical University, K. Marx str. 12, Ufa, Russia, 450008

Abstract. The problem of ensuring the information security of an automated process control system (APCS) is considered. An overview of the main regulatory documents on ensuring the safety of automated process control systems is given. For the operative solution of the tasks of ensuring information security of the automated control system of technological processes it is proposed to use an intelligent decision support system (DSS). An example of the construction and implementation of decision rules in the composition of the DSS based on the use of neuro-fuzzy models is considered.

1. Introduction

In recent years, the object of targeted attacks is increasingly becoming industrial enterprises and automated process control systems (APCS). According to the report of Kaspersky Lab, in the first half of 2018, the share of attacks on APCS in the world increased by 3.5% and amounted to 41.2%. For the current year, this figure has increased by 4.6%. According to the research [1, 2], Russia ranks 19th in the list of countries in terms of the percentage of attacks on computers for APCS. The increase in the percentage of attacks on the APCS is mainly associated with a general increase in malicious activity, while any incident of information security violations can lead to serious consequences. Until recently, the main regulatory requirements in the field of safety of APCS in the Russian Federation were:

- requirements of the guidance documents of Russia Federal Service on Technical and Export Control (FSTEC) on key systems of information infrastructure;
- Federal Law No. 256-FZ dated by 21.07.2011 “On safety of fuel and energy complex facilities” [3];
- The Order of Russia FSTEC No. 31 dated by 14.03.2014 “On approving the Requirements to protection in automated production and technological processes control systems at the critically important objects, representing the enhanced danger for the people life and health and for the environment” [4].

Since the beginning of 2018, the Federal Law “On the security of critical information infrastructure of the Russian Federation” № 187-FZ dated by 26.07.2017 came into force [5]. The notion of critical information infrastructure (CII) objects covers such groups of objects as information systems, information-telecommunication networks, automated control and management systems of the Russian Federation subjects, functioning of which is critically important for the state. In accordance with 187-FZ, the information systems of organizations operating in the fields of health, science, transport, communications, energy, banking and other areas of the financial market, fuel and energy complex, in the field of atomic energy, defense, rocket and space, mining, metallurgical and chemical industries, or

organizations that provide the interaction of these systems are subject to mandatory protection, in order to ensure their sustainable functioning when conducting against their computer attacks.
According to the law should be a categorization of CII objects, compiled a national register of significant CII objects, provides for the implementation of mandatory requirements to ensure the safety of significant CII objects, controlled by the state.
In order to concretize the requirements provided by the Federal law 187-FZ, and the conditions for their use, the FSTEC of Russia issued a sub-legal regulatory base:

- The Order of Russia FSTEC No. 235 dated by 21.12.2017 “On approval of requirements for the creation of security systems for significant objects of the critical information infrastructure of the Russian Federation and for ensuring their functioning” [6], containing requirements to structure and functioning of security systems, and also organizational and administrative documents on safety of significant CII objects;
- The Order of Russia FSTEC No. 239 dated by 25.12.2017 “On approval of requirements to providing security of significant objects of the critical information infrastructure of the Russian Federation” [7], which recommendations on safety of significant objects at various stages of their life cycle, and also lists the composition of the basic set of safety measures for significant objects of the CII of various categories of significance.

However, these changes in the legal base, currently there are no formal methods and techniques of qualitative and quantitative assessment of the level of protection and choice of effective countermeasures to ensure full compliance with regulatory requirements to ensure comprehensive information security APCS. This doesn't allow one to fully counteract the influence of a wide range of possible cyber threats on the information resources of organizations and enterprises.
Therefore, it is urgent to develop decision support algorithms, the use of which would improve the efficiency of information security APCS of a particular enterprise.
The purpose of the study in this article is to develop the structure of the decision support system (DSS), implementing the risk assessment of information security APCS.
To achieve this goal should be solved by the following tasks:

1. Development of the DSS structure applicable to the construction of a secure APCS;
2. Development of decision support algorithm in the task of assessing the requirements to ensure the protection of information in the APCS based on artificial intelligence technologies;
3. Evaluation of the possibility of using DSS by an example illustrating the features of the application of the proposed algorithm to the construction of the APCS.

2. Analysis of existing approaches to assessing the level of security of APCS

The solution of the tasks of ensuring information security of the APCS has its own characteristics. This is primarily:

- high uncertainty of initial information and complexity of its receipt;
- the need to consider many of the requirements for information security when evaluating and choosing the best options.

The article [8] deals with the implementation of the system of requirements for ensuring the protection of information of the automated process control system, provided for by Order of Russia FSTEC No. 31. The goal is to develop a formalized methodology for the integrated assessment of compliance with the requirements for ensuring information security in an automated system using the fuzzy inference method and expert assessments. A procedure is proposed for determining the level of significance (criticality) of the information being processed based on a system of fuzzy rules (products), considering the degree of possible damage from the violation of the integrity, availability or confidentiality of information. The use of fuzzy models requires time-consuming configuration of model parameters with the participation of subject matter experts and information security specialists.
When forming the requirements for information security in the APCS by the Order of the Russia FSTEC, it is implied that it is necessary to develop a model of information security threats. It should contain a description of the APCS and current threats to information security.

As a result of analyzing the processes of ensuring information security of an APCS, the following main tasks can be identified, solved with the help of DSS:

- accumulation and systematization of information on information security of APCS;
- assistance in developing recommendations for minimizing the possible information security risks of APCS.

3. Development of the DSS structure for assessing the level of information security risk in APCS

The indicators used in the development of DSS for ensuring information security of the APCS can be both quantitative and qualitative. Therefore, there is always uncertainty in making decisions on assessing the risks of information security of the APCS. In this case, to determine the level of information security risk of the APCS, it is proposed to use data mining technologies using a modular (ensemble) neural network [9], which allows you to take into account accumulated experience in assessing the level of protection of the APCS and adjust the parameters of a fuzzy system based on specific expert assessments.

The general architecture of the DSS to ensure information security of the APCS is shown in Figure 1.

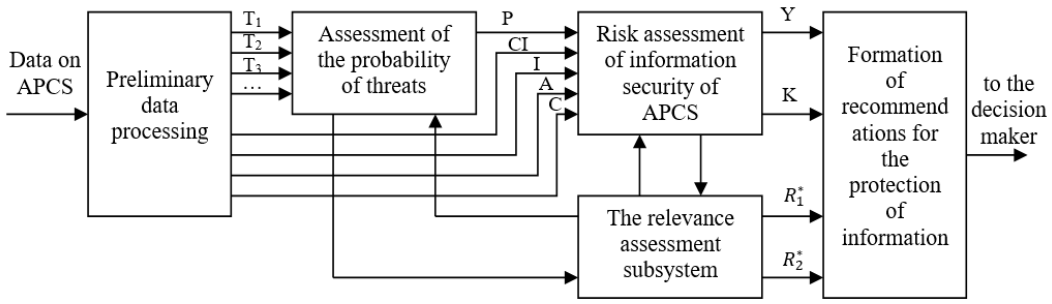

Figure 1. The general architecture of the DSS assessment of information security risk level of APCS.

The module of preliminary data processing on the APCS leads the input values of the modular neural network to a single scale. The inputs of a fuzzy neural network are given indicators of identified information security vulnerabilities of the APCS ($T_1 \div T_4$), indicators of the value of information contained in the system (*CI*), as well as the degree of possible damage in case of breach of confidentiality (*C*), integrity (*I*) or availability (*A*). The neural network determines the probability of realization of the threat P, after which, based on a set of rules, it assesses the risk Y and determines the security class (*K*) of the APCS. The output data of the rule relevance assessment subsystem are R_1^* – vector of assessments of the contribution of rules to the formation of an assessment of the probability of threats, R_2^* – vector of assessments of the contribution of rules to the formation of an information security risk assessment.

It is assumed that all rules work to some extent, i.e. have a different level of activity. However, exceeding a certain threshold value indicates a significant contribution of certain rules to the result. The selected rules can show which of the parcels are the most suitable and therefore lead to the result.

Based on the obtained security class and risk assessment Y, taking into account the contribution of decision rules to the definition of this assessment, recommendations are made in determining the composition of information protection measures.

The adoption of the correct and timely decision to ensure information security of APCS directly depends on the completeness and correctness of the established rules base. It contains solutions to one or another problem on information security of the APCS, based on the analysis of the subject area and the knowledge of experts. Therefore, the creation of a rules base in the design of DSS is a primary task.

Decision rules can be represented in a fuzzy rules base in the Mamdani fuzzy inference system and have the following form:

R_j: If X_1 is A_1^j and X_2 is A_2^j and … and X_n is A_n^j, then Y_j is B^j, where R_j – *j*-th rule (*j* = 1,2,…,*m*); X_i – input variable, (*i* = 1,2,…,*n*); Y_j – the result of applying the *j*-th rule A_i^j and B^j – terms (fuzzy subsets).

An important task of the study is to map the set of decision-making tasks to ensure the information security of an APCS on a set of decision-making rules.
The impact of vulnerability on the implementation of a specific threat is reflected in the rules that have the following scheme:

IF Vulnerability – HIGH, THEN the probability of threats – HIGH, etc.

According to this principle, the number of rules of the module for assessing the probability of threats implementation will depend on the number of vulnerabilities, differentiated according to the degree of danger and determining the impact of this threat.
To determine the security class, three input indicators of confidentiality (*C*), integrity (*I*) and availability (*A*) were introduced; at the output of the neural network, we obtain the security class of the APCS.
Input indicators of confidentiality (*C*), integrity (*I*) and availability (*A*) are determined by three linguistic terms, which are evaluated by an expert on a scale from 0 to 1:

L – (0; 0,3) – "Low damage";
M – [0,3; 0,7] – "Middle damage";
H – (0,7; 1] – "High damage".

The security class of the APCS (*K*), which depends on confidentiality, integrity and availability indicators, is also determined by three linguistic terms, the values of which are determined using a neural network based on the rules established by an expert:

L – [0; 0,3] – "First security class";
M – (0,3; 0,7) – "Second security class";
H – [0,7; 1] – "Third security class".

Rules that determine the security class of the APCS listed in Table 1. Since at the input we have three variables *I*, *A* and *C*, defined by three linguistic terms L, M and H, the rule table contains 3^3 =27 rules.

Table1. The system of rules for determining the security class.

No.	Input indicators			Security class, *K*
	I	*A*	*C*	
1.	L	L	L	L
2.	L	L	M	M
3.	L	L	H	H
4.	L	M	L	M
5.	L	H	L	H
…	…	…	…	…
27.	H	H	H	H

In the course of the work, the compiled system of rules was implemented in the FuzzyToboxbox package of mathematical modeling in Matlab based on the ensemble of neuro-fuzzy networks ANFIS.
The structure of the ensemble of neuro-fuzzy networks, proposed for solving the problem of information security risk assessment of APCS, is presented in Table 2 and Figure 2.

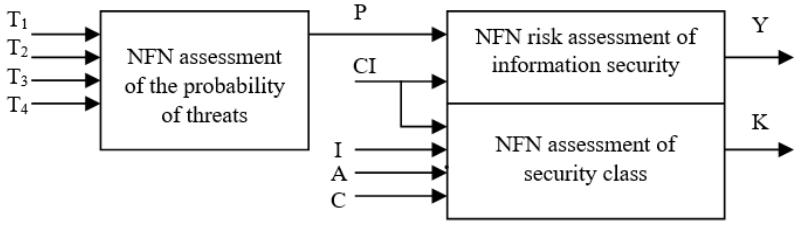

Figure 2. The structure of the ensemble of neuro-fuzzy networks in the DSS.

The training and test samples are based on the basis of expert assessments and contain options for solving the set tasks based on the analysis of the subject area. For the construction of training, sets can also be used data from systems included in the system of information security APCS.

Table 2. Parameters of the ensemble of neuro-fuzzy networks in the DSS.

Parameter	NFN assessment of security class	NFN assessment of the probability of threats	NFN risk assessment of information security
Number of inputs (input linguistic variables)	4	4	5
Number of terms of each linguistic variable	1	3	2
Number of generated rules	27	81	16
Fuzzy Inference algorithm	Sugeno	Sugeno	Sugeno
Learning iterations	1000	1000	1000
Training sample size	75	75	75
Test sample size	25	25	25
Error on test sample	1e-3	1e-3	1e-3

The detailed structure of the network that determines the probability of threats is shown in Figure 3.
The first layer is the terms of the input variables T1÷T4. Input data in this layer is converted to fuzzy. At the output of the layer, we obtain the degree of belonging to the input variable value to a certain term.
The second layer is the antecedents of fuzzy rules. Each node of this layer corresponds to one fuzzy rule. In this case, to determine the probability of threats to be realized, the inference system has 81 rules. The output node of the layer is the degree of execution of the rule $\mu_i(T)$.
The third layer is the conclusion of the rules. The nodes calculate the contribution of the corresponding rule to the network output.
The fourth layer is the combination of the result obtained according to different rules. The node of this layer summarizes the contributions of all the rules.
One of the drawbacks of fuzzy models is the effect of "retraining". The model gives a minimal error on the elements of the training set with a large error on the elements of the testing set. To overcome this drawback, the initial sample is divided into two subsets: training and test.
Increasing the dimension of the input vector of linguistic variables exponentially increases the number of elements of layer 2 of the ANFIS model, as well as the number of adjustable weight coefficients. This makes it difficult to train the model and increases the requirements for the training sample [10].

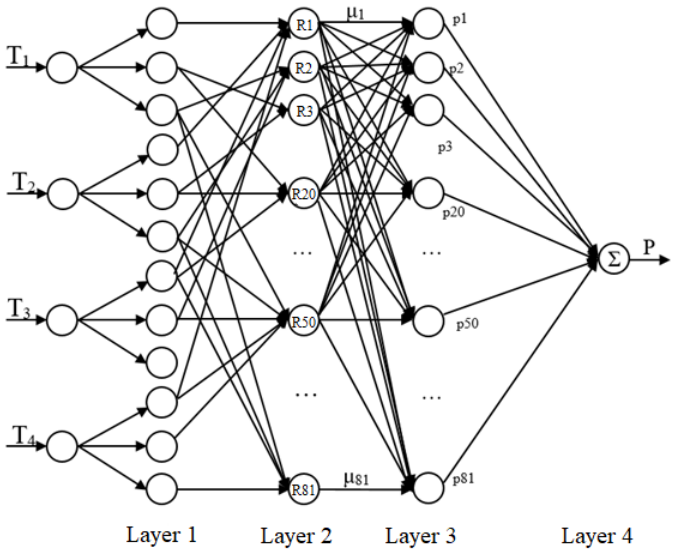

Figure 3. The structure of fuzzy neural network for threat probability assessment.

This paper uses the generation of a fuzzy model using fuzzy clustering (FCM) to reduce the dimension of the second layer of the neuro-fuzzy model ANFIS. When using FCM clustering, it is possible to control the sample size (the number of observations in the sample, the number of input variables) used to build the model, and the type of model (Sugano / Mamdani) [10, 11, 12].
In order to formulate recommendations for reducing the level of information security risk in an APCS, all the rules in this case work to varying degrees. But exceeding the threshold value allows you to select the rules with the most significant contribution to the result. An analysis of the parts of the antecedents of the ranked list of rules makes it possible to identify linguistic variables and their meanings that lead to the current result.
As a result of the research, a DSS was built, which allows to assess the level of information security risk of the APCS and issue recommendations for its minimization.

4. Evaluation of the possibility of using DSS

The example of using the developed DSS is illustrated by the example of the APCS, the physical architecture of which is shown in Figure 4. DSS helps to assess the practical implementation of the requirements of information security standards and to ensure the necessary level of security for APCS.
The input data for the DSS are the results of the information security audit conducted at the security facility, which includes security analysis to search for vulnerabilities, analysis of the documentation, structure and configuration of the system. The initial data for the audit are including the results of using network security scanners and the accumulated data of intrusion detection systems [13].
Suppose that according to the results of the audit, the APCS has the following vulnerabilities:
T_1 – Lack of identification and authentication of subjects and objects of access; T_2 – Incorrect Default Permissions; T_3 – No perimeter protection of APCS, connection with corporate networks and the Internet; T_4 – Lack of protection against denial of service attacks. The input parameters of the neural network are defined as follows: $T_1 = 0.3$ (M); $T_2 = 0.1$ (L); $T_3 = 0.6$ (M); $T_4 = 0.95$ (H).
At the same time, the value of information processed and circulated in data transmission networks of the APCS is defined as $CI = 0.6$.

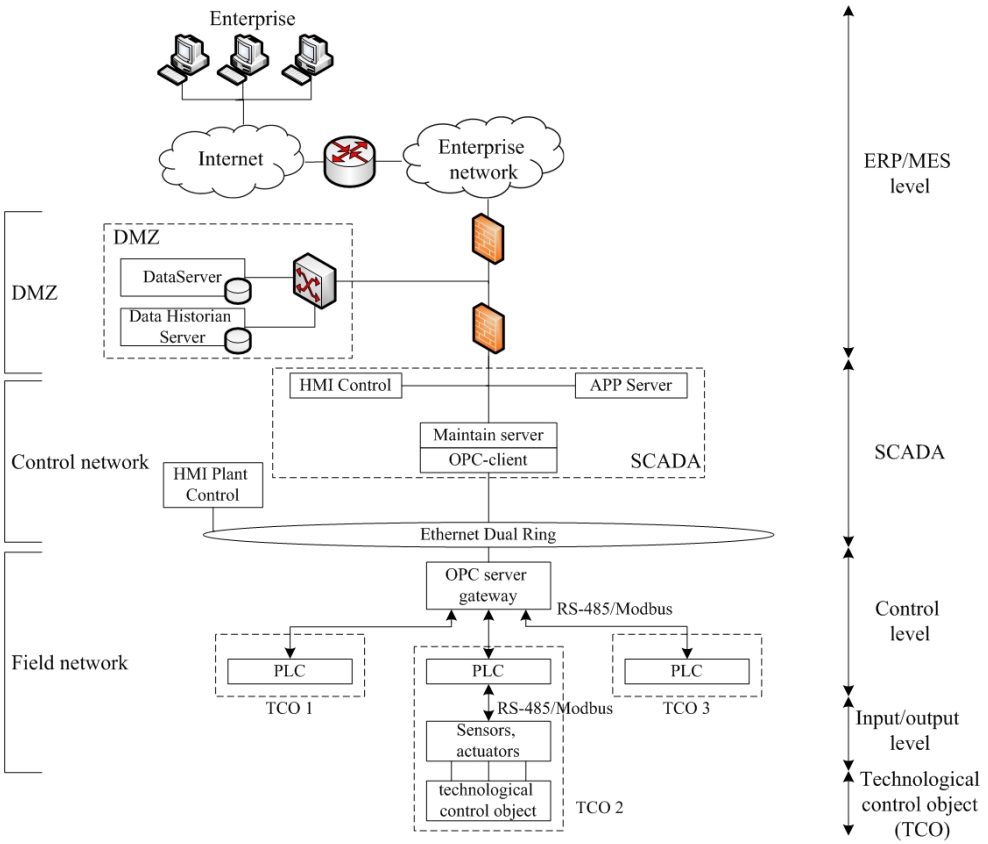

Figure 4. Physical architecture of APCS.

At the output of the neural network, we obtain the values of the probability of the threat realization (*P*), the information security risk assessment of the APCS (*Y*), and the vector of assessments of the contribution of rules to the formation of the probability of the threat (R_1^*) and the risk estimate (R_2^*).
As the calculations showed, the probability value of the threat realization is 0.727. This suggests that the probability of a threat acting through these vulnerabilities is above average. In turn, the inputs of a fuzzy neural network to determine the level of information security risk of the APCS are given the values $P = 0.727$ and $CI = 0.6$. With such input indicators at the output of the network, we obtain the value of the risk level equal to 0.537, that is, the risk level is also above average.
Formation of recommendations for reducing the level of information security risk of the APCS is as follows. All the rules in this case work in various degrees but exceeding the threshold value (in this case it is equal to 0.95) allows you to select the rules with the most significant contribution to the final result. These selected rules allow us to show why such an assessment of probability and risk was obtained, and to identify weak points. Based on knowledge of weak points, appropriate measures are taken to protect information from the APCS.
The DSS ultimately issues an information security risk assessment for the APCS, and recommendations for ensuring a given level of information security with instructions on what should be paid priority attention.

5. Conclusion

The proposed structure of the DSS to ensure information security of automated process control systems.
The algorithm for decision support based on data mining technology using a modular (ensemble) neural network has been developed, which allows solving the problem of risk assessment and compliance of requirements for ensuring information security of an APCS and identifying current threats to a specific protection object.
Risk assessment of information security of APCS is necessary to develop recommendations for reducing the risk level and choice of effective countermeasures that ensure full compliance with the regulatory requirements for ensuring comprehensive information security of the APCS.
The use of the proposed fuzzy neural network in assessment information risks of the APCS makes it possible to adequately use the qualitative and quantitative evaluations obtained from the experts as input data and will also improve the level of enterprise security by maintaining the information protection system of the APCS up to date.

6. References

[1] Cybersecurity of industrial automation systems in 2018 [Electronic resource]. – Access mode: https://ics.kaspersky.ru/media/2018-Kaspersky-ICS-Whitepaper-ru.pdf (13.11.2018).
[2] Threat landscape for industrial automation systems: H1 2018 [Electronic resource]. – Access mode: https://ics-cert.kaspersky.com/reports/2018/09/06/threat-landscape-for-industrial-automation-systems-h1-2018/ (13.11.2018).
[3] On safety of fuel and energy complex facilities / Federal Law No. 256-FZ dated by 21.07.2011 [Electronic resource]. – Access mode: http://www.consultant.ru/document/cons_doc_LAW_64872/ (13.11.2018).
[4] On approval of requirements to provision of information security in automated systems of production and technological processes control at critically important objects, potentially dangerous objects, and the objects representing higher danger to the human life and health and environment / Order of FSTEC of Russia No. 31 dated of 14.03.2014 [Electronic resource]. – Access mode: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot (13.11.2018).
[5] On the security of critical information infrastructure of the Russian Federation / Federal Law No. 187-FZ dated of 26.07.2017 [Electronic resource]. – Access mode: https://www.consultant.ru/document/cons_doc_LAW_220885/ (13.11.2018)
[6] On approval of requirements for the creation of security systems for significant objects of the critical information infrastructure of the Russian Federation and for ensuring their functioning /

Order of Russia FSTEC No. 235 dated by 21.12.2017 [Electronic resource]. – Access mode: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1589-prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-236 (13.11.2018).
[7] On approval of Requirements to providing security of significant objects of critical information infrastructure of the Russian Federation / Order of FSTEC of Russia No. 239 dated of 23.12.2017 [Electronic resource]. – Access mode: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot (13.11.2018).
[8] Vasilyev, V.I. Integrated assessment of information security requirements implementation in automated control systems intended for production and technological processes / V.I. Vasilyev, V.E. Gvozdev, M.B. Guzairov, A.D. Kirillova // Information and Security. – 2017. – Vol. 20. – P. 618-623.
[9] Vasilyev, V.I. System of decision making support on information security maintenance of automated technologic processes systems / V.I. Vasilyev, A.M. Vulfin, M.B. Guzairov, A.D. Kirillova // Infocommunication technology. – 2017. – Vol. 15(4). – P. 319-325.
[10] Jang J.-S.R. ANFIS: adaptive-network-based fuzzy inference system // IEEE Transactions on Systems, Man and Cybernetics. – 1993. – Vol. 23(3).
[11] Takagi, T. Fuzzy Identification of Systems and its Applications in Modeling and Control / T. Takagi, M. Sugeno // IEEE Trans. System, Man, Cybern. – 1985. – Vol. 15(1). – P. 116-132.
[12] Takagi, T. Stability Analysis and Design of Fuzzy Control Systems / T. Takagi, M. Sugeno // Fuzzy Sets and Systems, North-Holland. – 1992. – Vol. 45. – P. 135-156.
[13] Shanmugavadivu, R. Network intrusion detection system using fuzzy logic / R. Shanmugavadivu, N. Nagarajan // Indian Journal of Computer Science and Engineering (IJCSE). – 2011. – Vol. 2(1). – P. 101-111.

Acknowledgments
This work is partially supported by the Russian Science Foundation under grants №17-48-020095.