UNIFIED ASSESSMENT ALGORITHM IN THE INFORMATION SECURITY MONITORING SYSTEM IN THE ELECTRONIC GOVERNMENT SYSTEM

Haydarov E. D.
Head of Department of TUIT named after Muhammad al-Khwarizmi, PhD

Gafurov Sh. R.
Independent researcher of TUIT named after Muhammad al-Khwarizmi

ABSTRACT

Modern information security systems allow for the rapid detection of network attacks in the e-government system. Moreover, one of the most effective approaches to solving this type of problem is to identify the interaction between different information security systems in order to jointly process a single unified warning message within the framework of the information security monitoring system in the e-government system. This article proposes the development of a unified assessment algorithm for the monitoring system of information security in the e-government system .

Keywords: Electronic government , information security monitoring , assessment , decision-making , expert assessments , technical expertise.

INTRODUCTION

It is no secret that today, various sectors of industry are implementing e-government based on the use of computer tools and complexes to collect, process, store and present the necessary information and ensure the reliable performance of technological operations in complex systems that have become generalized as a result of providing interactive government services to customers through the e-government system. As a result of the creation of such systems, it can be seen that computerization has led to an increase in the initial complexity of systems by several hundred thousand. In these processes, it is necessary to take into account that complexity is measured not by the number of structural elements, but by the variety of variants of the functional behavior of the system, depending on the external environment. On the one hand, this provides significant advantages, on the other hand, it significantly increases the amount of data available for analysis. The complexity of the data processed in information security monitoring systems in the e-government system can further complicate the problem. As a result, the process of determining what is important becomes difficult. Difficulty in identifying relevant information can lead to incorrect decision-making or even prevent decision-making altogether. This, in turn, leads to the inability to draw a final conclusion on the timely blocking of attacks or unauthorized actions detected by the information security monitoring system in the e-government system. The large amount of information related to information security in e-government systems significantly complicates the process of detecting and preventing attacks. The use of data collection technologies can reduce the amount of information needed for decision-making by more than 85%, while at the same time identifying errors in dangerous network events in e-government systems with an indicator of less than 4%. In the e-government system, data aggregation technologies help to quickly process large amounts of data. The use of data aggregation technologies provides results that are relevant to the analytical context, that is, the location and time of data storage. According to experts, such approaches are very suitable for ensuring quick and accurate decision-making in managing e-government systems. In scientific research conducted in this area, it can be seen that it is proposed to create a meta-information security system that filters out redundant information, analyzes attacks using the correlation of security messages from each sensor, and provides a quick response to attacks. The integrated assessment method proposed in this dissertation differs from previously proposed methods in the following ways:

- Information security monitoring in the e-government system is carried out not at the level of individual devices, but at the level of the e-government system. Therefore, in the process of information security monitoring, information obtained from the entire complex of information security systems in the e-government system is processed and summarized;
- The large volumes of information related to the information security of the e-government system simplify the process of making the necessary decisions on information security management and allow for a single unified assessment, that is, the processes implemented with the help of additional modules are reduced;
- The number of information security messages in the e-government system allows for the implementation of security policies and the analysis and synthesis of heterogeneous data, such as vulnerabilities of end systems;
- The results of information security monitoring in the e-government system serve as the basis for creating proactive protection, since the generalization of heterogeneous information creates the opportunity to make general decisions on information security management [1, pp. 207-211, 2, pp. 399-404].

To obtain a unified assessment of the e-government system, it is first $F_\xi: \{I_X, I_S, I_V\} \xrightarrow{F_\xi} \xi$necessary to find a function, where $I_X, I_S, I_V$the implementation of the security policy and the vulnerability of the latter systems are considered indicators that allow estimating the number of information security messages, ξ –a unified assessment. To solve this problem, it was found that the use of the theory of primitive sets and primitive logic methods was effective. In such cases, it is advisable to use a one-dimensional assessment in the e-government system, as it allows you to assess the state of information security in the overall e-government system. The advantages of this approach are as follows:

- ease of understanding and interpretation – multi-dimensional assessment or the use of several indicators increases the complexity of understanding the results of information security monitoring. The presence of a single unified assessment makes it possible to establish a single, simple and understandable scale for assessing the security of the e-government system;
- decision -making speed - the more assessments of information security indicators are obtained as a result of the analysis, the more time it will take to make a decision, since it is necessary to compare different assessments and draw a final conclusion. Having only one consolidated estimate eliminates the need to compare different assessments when making a decision;
- Intuitiveness of use – the calculation of the aggregated assessment is based on logical methods. Thus, the aggregated assessment allows the user to create a model of approximate

thinking. As a result of reasoning, the user, as a rule, comes to a final conclusion and makes a decision on this basis. The role of such a conclusion is considered to be the aggregated assessment;

- Convenience in taking response measures at the e-government system level – the integrated assessment is not intended to indicate the cause of the information security incident. Instead, it is a key indicator of the need to begin investigating the causes of the information security incident and take rapid response measures at the e-government system level to remedy the situation.

The choice of logical methods in the e-government system is determined by its following capabilities:

- Working with irregular input data and values that change in a constant manner over time. The database of the information security monitoring system can contain a large amount of technical and non-technical information that must be taken into account in the decision-making process (for example, information on information security vulnerabilities, information on the implementation of information security, security policy, etc.);
- implementing qualitative assessment of both input data and output results: the ability to work not only with data values, but also with their level of reliability and its distribution;
- vague formalization of evaluation and comparison criteria: working with criteria such as “most”, “probably”, “mostly”, as well as the ability to process linguistically structured expert knowledge;
- Informal logic is a multi-valued logic that allows you to specify values for generally accepted values such as “yes/no”, “true/false”, “protected/unprotected” . It allows for more flexible modeling of multi-valued systems and mathematically modeling and processing on computers the intermediate values of indicators characterizing information security in the e-government system;
- fast modeling of complex dynamic systems and their comparative analysis at a given level of accuracy. Using the principles of system behavior described by natural logic methods, it is possible to reduce the time required to determine the exact values of variables and construct descriptive equations, as well as to evaluate various options for output values [3, pp. 62-66].

Based on the above, the unified assessment algorithm in the information security monitoring system in the e-government system is implemented as follows:

First stage. Getting started.

Stage 2. If expert evaluations have not been conducted, then expert evaluations will be conducted, otherwise, the process will proceed to Stage 5.

Third stage. Based on expert assessments $I_i: \alpha_k^i, k \in [1, T_i]$ A set of linguistic terms characterizing the input parameters and $r: \beta_j, j\epsilon[1, T]$output parameters is formed, where T_i- $I_i$is the number of parameter terms, T- is the number of output rparameter terms. α_k^i, $\beta_j$the following linguistic values are used as terms: “low”, “medium”, “high” and others.

Fourth stage. Based on the expert calculations, membership functions are constructed for all input parameters $I_i: \{P_{\alpha_k^i}(I_i): i\epsilon[1, N], k\epsilon[1, T_i]\}$and for the output parameter $r: \{P_{\beta_j}(r): j\epsilon[1, T]\}$, where I_i and $r$are the variable values of the input and output parameters. Membership functions determine the suitability of the uncertain sets of input and output parameters.

Based on the above collections, the following linguistic expressions are formalized, for example: “Multiple vulnerabilities”, “Number of information security messages”, and others.

Fifth stage. Based on expert assessments, a refined rule base is built in the form of a set of rules. $\prod_{i\in[1,N]}\{\alpha_k^i : k \in [1, T_i]\} \rightarrow \{\beta_i : j \in [1, T]\}$.

Sixth stage. Estimated parameter values are obtained from the database of the information security monitoring system .I_i

Seventh stage. The input parameters are refined, and the values of the membership functions corresponding to the estimates obtained in stage 2 are determined:$\widehat{P_{a_k^i}}$, $k \in [1, T_i]$ $i \in [1, N]$;

Step Eight : The truth levels for each of the rules are determined.

In the ninth step , the value of the output parameter is calculated based on the truth values of the rules r.

Tenth stage. $\xi = \widehat{P_{\beta_j}(r)}$ The output parameter is made vague and the resulting ξvalue is calculated.

Step eleven. That's it.

The value obtained as a result of the algorithm is called the unified estimate of the scope of work and is used in the process of ensuring information security in the e-government system. For this, the procedure for calculating the value of the output parameter when using the algorithm is of great importance, since a logical conclusion is drawn. As a result of the seventh stage, the calculated truth values of each rule are applied to the conclusions of each rule.

The proposed algorithmic methodology has the following characteristics:

- The initial set of proposed rules may be drawn up by a specialist and may be incomplete and contradictory from the user's point of view;
- The type and parameters of the membership functions describing the input and output parameters of the system are chosen subjectively and may not accurately reflect the real state of the system, but they accurately reflect the state of the system's failure;
- The information security monitoring system in the e-government system allows decision-making in cases where there are a large number of heterogeneous information security indicators in the database and the decision-making process for managing the information security process is not clear [4, pp. 165-169].

Based on the above , the input data is adequate, therefore, at the initial stage of the methodology, it is very important to correctly conduct expert assessments, build linguistic variables, as well as membership functions and normalization rules. The advantages of the methodology for obtaining a summary assessment of the results of information security monitoring in the e-government system are as follows:

- technically very flexible, as it can be used to perform quantitative and qualitative assessments of input data and output results, and allows the user to work not only with data values, but also with their level of confidence and their distribution;
- can be used for various technical and non-technical indicators, i.e., it allows you to take into account the human factor, which is a characteristic of many technically similar systems. Since most systems rely on technical indicators, more than 55% of threats are not technological, but are implemented using the human factor;
- Technically, it can be used for a wide range of indicators and is easy to understand and use.

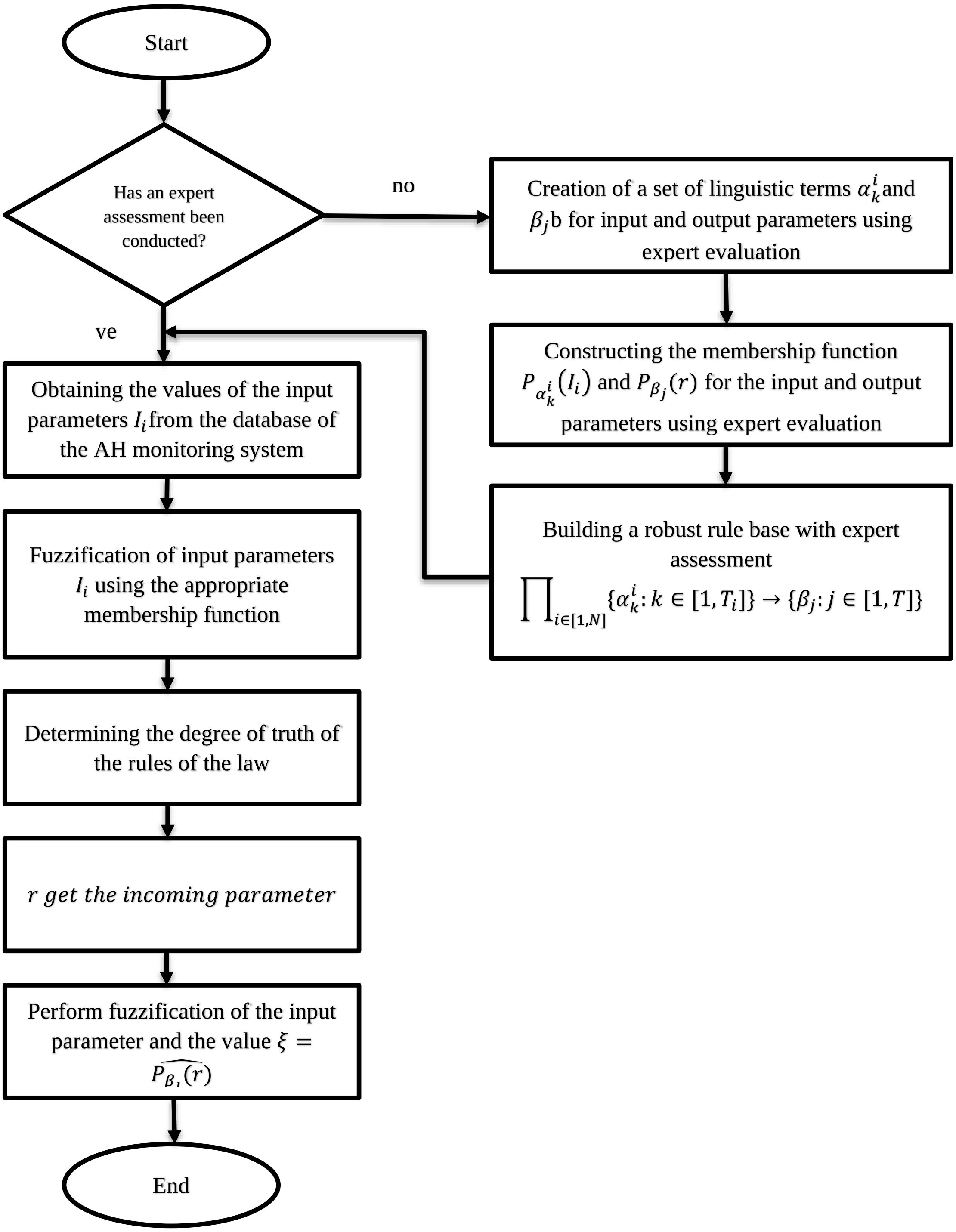
Start
Has an expert assessment been conducted?
no
ve
Creation of a set of linguistic terms $\alpha_k^i$and β_jb for input and output parameters using expert evaluation
Constructing the membership function $P_{\alpha_k^i}(I_i)$ and $P_{\beta_j}(r)$ for the input and output parameters using expert evaluation
Building a robust rule base with expert assessment $\prod_{i\in[1,N]}\{\alpha_k^i: k \in [1,T_i]\} \to \{\beta_j: j \in [1,T]\}$
Obtaining the values of the input parameters $I_i$from the database of the AH monitoring system
Fuzzification of input parameters I_i using the appropriate membership function
Determining the degree of truth of the rules of the law
r get the incoming parameter
Perform fuzzification of the input parameter and the value $\xi = \widehat{P_{\beta,}(r)}$
End

Figure 1. Block diagram of the integrated assessment algorithm in the information security monitoring system in the e-government system.

The above proposed algorithm allows the introduction of the following improved modules into information security monitoring systems in the e-government system:

- integration of the adaptive configuration block of information security systems in the e-government system into the information security monitoring system;
- creating a multi-level system for storing information security messages in the e-government system;

- implementation of correlation analysis of information security messages of the electronic government system [5, p. 45-48].

CONCLUSION

Based on the above, the system implementing information security monitoring in the e-government system should be integrated with other information systems in the e-government system , and the information security monitoring system should be able to make a final decision on the protection mechanism through a unified assessment of the information collected based on the operating mode of the information security monitoring system together with other information security systems, and the information security systems should be able to It is possible to reduce additional loads. In addition, due to the high adaptive characteristics of security software tools used to ensure information security, it is proposed to control the mechanism of operation of the adaptive configuration block of information security monitoring in the electronic government system.

REFERENCES

1. Z. An, J. Chen, K. Song and R. Xu, "Research on Computer Information Security Protection System Based on Big Data Background," 2023 3rd Asia-Pacific Conference on Communications Technology and Computer Science (ACCTCS) , Shenyang, China, 2023, pp. 207-211.
2. Y. Sun and Y. Kou, "Design of Campus Network Security Intelligent Monitoring System Based on BP Algorithm," 2023 IEEE 15th International Conference on Computational Intelligence and Communication Networks (CICN) , Bangkok, Thailand, 2023, pp. 399-404.
3. Botirov FB, Gafurov Sh.R. Automation of information protection processes in the enterprise's information system, Ict in education: Challenges and solutions, International conference, Tashkent, May 20, 2021–P. 62-66.
4. L. Fang, X. Shi, S. Liu and P. Li, "Research on Evaluation and Design of Safety Instrumented Systems Security," 2023 IEEE 3rd International Conference on Electronic Technology, Communication and Information (ICETCI) , Changchun, China, 2023, pp. 165-169 .
5. Z A. Heza, M. Stankova and G. Ivanova, "Spheres of Information Security and Information Protection in Ukraine," 2023 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo) , Kyiv, Ukraine, 2023, pp. 45-48.