Concept Of Establishing Multi-Agent Intellectual Automatically Systems In The Enterprise

Bekmuratov Tulkun, Ganiev Abdukhalil, Botirov Fayzullajon

Abstract : this article includes the development of an automated information security system at the enterprise, an overview of the enterprise security task structure, and the concept of building an automated information security system at the enterprise.

Index Terms: Enterprise security assignments, concept, information security management system, multi-agent system

1 INTRODUCTION

Creation of a unified automated information protection system requires the allocation of information protection resources according to the value of resources available in a particular segment of the enterprise. For this purpose, it is necessary to receive full information about changes in the state of protected resources, to plan the required level of protection of information, to adjust the means of protection of information. It is desirable to build automated information security systems in the form of multi-agent systems.

2 APPLICATION OF MULTI-AGENT SYSTEMS IN INFORMATION SECURITY SYSTEMS

Multi-agent systems are systems designed to organize communication with different categories of information. It has been shown that multi-agent systems can also improve system efficiency in protecting data against unauthorized access [1]. The choice of various sources of information, software and hardware for people, information systems, and automated systems for enterprise information protection determined the agents' activeness, commutability and autonomy. During the development of multi-agent systems, the functions of agents are identified according to their types [2]. The backbone of any system is the goal of the system. The purpose of the Intelligent Automated Information Protection System at the enterprise is to:

1. level of protection provided information resources is compatible with the required level of protection;
2. optimization of information protection costs.

The objectives are in some disproportions and combine two aspects of the classical task of information protection. It should be noted, the information above to provide reliable protection [3]. Price optimization plays a role in limiting the capabilities of the information protection system from above and serves as an optimal measure when working with an automated information security system.

- *Bekmuratov Tulkun Fayzievich, academic, Department of SIC ICT of TUIT named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan. E-mail: bek.tulkun@yandex.com*
- *Ganiev Abdukhalil Abdujalilovich, docent, Department of Providing information security, TUIT named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan. E-mail: a.ganiev@tuit.uz*
- *Botirov Fayzullajon Bakhtiyorovich, master, Department of Providing information security, TUIT named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan. Email: botirov_fz@mail.ru*

To achieve this goal, the automated information security system must include the following systems:

1. Security level planning system (SLPS);
2. Coordination of the participants' activities (CT);
3. Information Security Management System (ISMS);
4. System of data collection system on the condition of the object of protection (DCS).

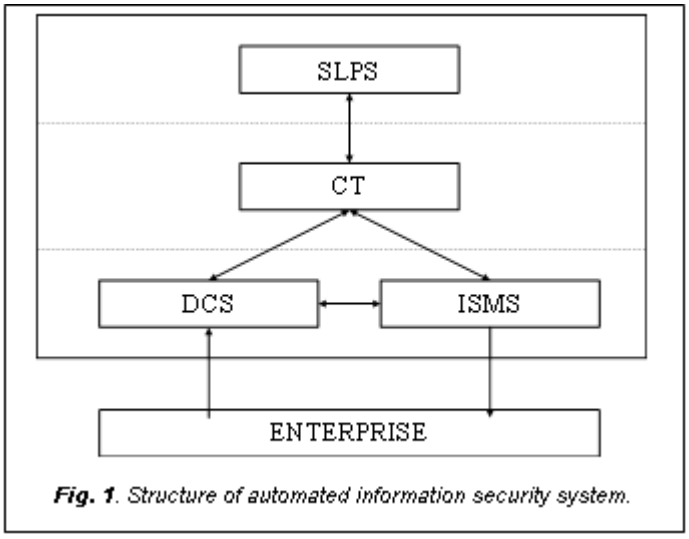

***Fig. 1**. Structure of automated information security system.*

As you can see in the picture, the system has a clear genealogy. The security system that collects information on the status of the object is the basis for the automated information protection system. It is precisely the data from that subsystem that it controls and evaluates the effectiveness of the information protection measures taken. The Gathering System also monitors user behavior, and provides an inventory of information and software resources for the intellectual information system. The object of control for an automated information protection system is not only the information protection system, but also the function of data system data processing. The development and implementation of information security threats can be prevented by F user actions and software management capabilities [4]. The required level of information protection is a key component of the planning system that can improve the effectiveness of information protection. An analysis of many information systems' work shows that the greatest impact on the level of risk for information resources is the change in the value of information resources. The distribution, volume, and cost of processing information in an enterprise information

system depends on the stages of the product's life cycle, which determines how the product is created to support the product, the life cycle document flow. Based on these laws, it is possible to plan changes in the value of protected information resources, given the process of information obsolescence. The resulting plan is the basis of the decision to protect the information. Thus, the principle of controlling the value of the protected assets can be formulated as follows. Based on resource costing plans, the subcontracting system identifies the risks that the information system will face during the planning period. Further, it is necessary to clarify the information protection system settings to minimize the risks found. The cost of doing this should be minimal [5]. The security task is a valid reference system for the existing information security system and includes a set of functional requirements for information protection. Each information protection system, in turn, fulfills the functional requirements of protection at the level of the information protection system, in completely or in part. At the same time, each requirement of the information protection system is achieved through the synergistic operation of a particular set of information protection rather than a simple set of information protection tools. The upper level of the hierarchy is the layer of protection system. This layer corresponds to the completeness and functional requirements included in the security task. In addition, one of the requirements for a system-wide ST is that the security requirements are not exceeded. The lower layer contains security requirements that are part of the enterprise information system security task. The complete set of protection functions is a combination of protection system functions that are part of the enterprise. At the same time, the implementation of each protective function involves the interconnection of various remedies. As a result, security functions are becoming increasingly complex mechanisms of information security. Thus, the layer of protection function should not only describe the content of the function in detail, but also describe the uniqueness of the protections that implement that function. It is the security function that is opposed to potential threats, and the completeness and proper implementation of the function is the key to the success of information protection [6]. The last layer of the Enterprise Security Task hierarchy is the protective element. The level of protection measures and measures to ensure the reliable operation of the protective equipment.

3 THE CONCEPT OF BUILDING AN AUTOMATED INFORMATION SECURITY SYSTEM AT THE ENTERPRISE

Before the proposed information security concept of the hybrid system in the below regulations and principles.

1. Hierarchical structure of the IS system with multiple functions. The lower and upper levels of the system perform the overall function of interaction between the administrator and the environment, and the sub-functional layers coordinate the interaction of agents.
2. Formation of basic functional modules of hierarchical layers in the form of intelligent agents with two interconnected neural networks and expert systems
3. Multi-agency, subordination and integration of agents of different levels
4. Distribution and parallel processing of information
5. In IP dynamic flexibility of variable environmental agents
6. Accuracy, interpretability and sensitivity of the system information provided to the administrator system information
7. The openness and dynamics of the IS system structure

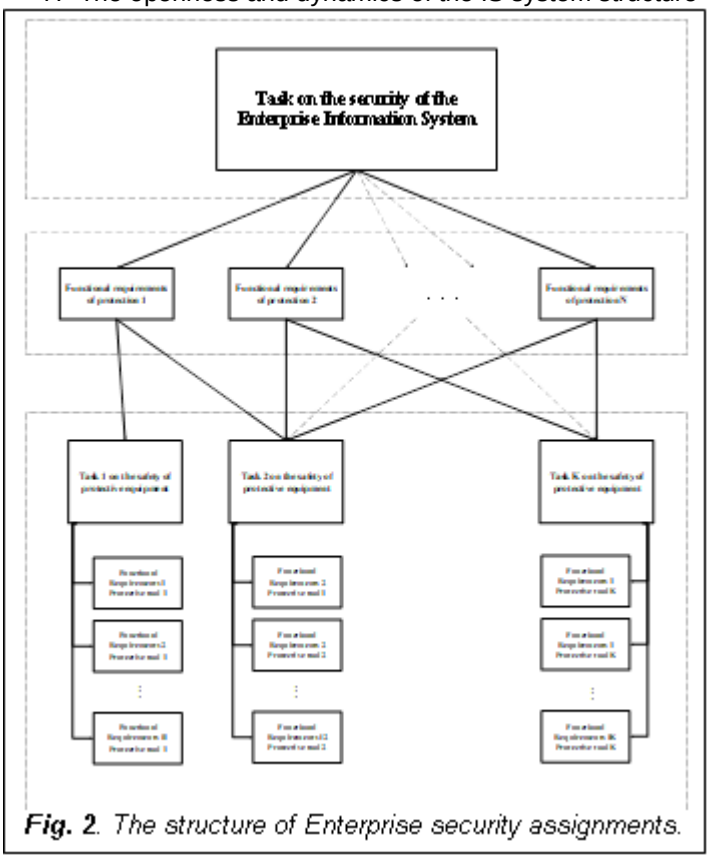

Fig. 2. The structure of Enterprise security assignments.

Based on the above-mentioned approach, the concept of building an automated information security system in the Intelligent Information System (IIS) is proposed in accordance with the enterprise information system security task. The concept includes the following principles:

1. The principle of functional integration, which involves the creation of an integrated information security system in the enterprise;
2. The principle of hierarchical organization, which means to build an enterprise data protection system in a class of integrated hierarchical systems;
3. The principle of complex analysis of enterprise models, methods and algorithms, such as synthesis of information protection system and information security system;
4. The principle of standardization, which means that the requirements for building an information protection system are within the existing information protection standards;
5. The principle of building an open information system as the basis for building an enterprise information security system.

The system should be divided into 3 levels to develop an overview of the automated information security system. These are:

- level of planning;
- level of coordination;
- execution level

1. - Assessment of the value of information in IIS during the planned period;

$\{V_I\}$ - value of information assets in IIS;

2. - Assessment of information assets threat characteristics;

$\{A_V\}$ – The likelihood of threats occurring;

3. - assessment of vulnerabilities in the information system;

$\{R_I\}$ – Risks of information assets security breach;

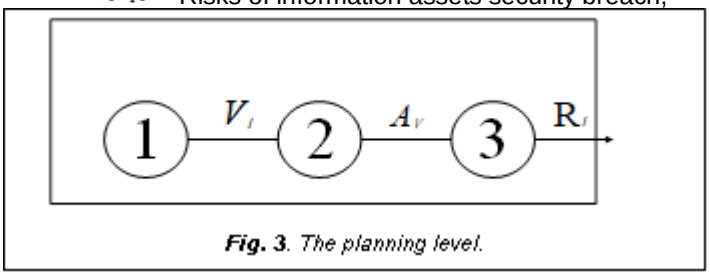

***Fig. 3**. The planning level.*

4. - formation of requirements to the information protection system;

$\{P_S\}$ - required security parameters;

5. - Generation of the required security parameters for the information protection system for the enterprise information security system;

$\{S_F\}$ - Protection function settings;

6. - selection of validated information security settings based on the data obtained;

$\{S_S\}$- Selected information security settings;

7. - send the setting to execution;

$\{S_{IS}\}$ - Information security settings;

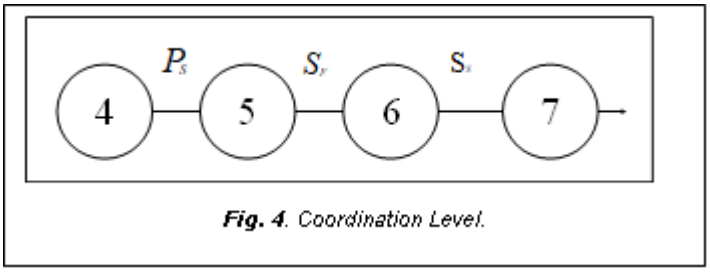

***Fig. 4**. Coordination Level.*

8. Execution Mechanism for implementing information security management systems;

IPMC - Information Protection Management Commands;

9. - object of protection;

$\{I_{OP}\}$ - Information on the condition of the object of protection;

$\{I_{SS}\}$ - information on the selected settings.

The highest level of information security management systems is the planning layer (PL). At the current level, the IIS implements the information flow model and the threats and vulnerabilities model in the IIS, which is a prerequisite for risk analysis. The value of information resources is evaluated during the planning period based on the information flow model [8-9-10].

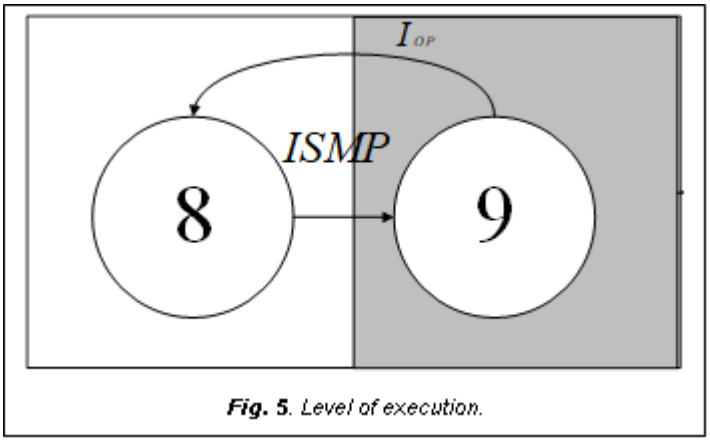

***Fig. 5**. Level of execution.*

Figure 6 shows an overview of the automated information security system of the enterprise built.

Enterprise security administrators - participants of the IIS, implement this function as there is no technology available today to allow such analysis and automate the complex decision-making process. The main difficulty is that the processes of valuing information assets, planning their value, creating many threats, and evaluating their hypertension are poorly formulated. The emergence and implementation of threats are caused by numerous threats. These are:

1. availability of valuable information;
2. weaknesses;
3. detection and use of vulnerabilities by the attacker.

Each one of these factors alone - the impact of information security up mode assessment of the gap, because it is impossible to measure the impacts of scales, measurement methods, data analysis, information risk allows you to calculate the exact relationship does not exist. At the same time, information security experts cite reasons for risk assessment and information security system settings. The development of the theoretical framework for information protection has led to the development of a set of risk analysis methods, each with its own disadvantages and disadvantages, but the practical methods of risk analysis are based on expert assessments. After the risk assessment is planned for the entire enterprise, the $\{R_I\}$ risk information is then entered into the information system so that it can be generated at the required level of protection $\{P_S\}$. This procedure identified risks could lower the required level of information protection products with a choice of settings related to a number of uncertainties , including read hectares, because it is a purpose for the increase in the use of artificial intelligence methods. The result of the formation of information security system settings is the setting of information security functions. Information protection functions $\{S_F\}$ are optional settings to protect the information system implementation is possible because of the lack of information and protection functions required to satisfy the settings and the current value of the minimum information to be made verified settings $\{S_F\}$ in the protection of competition is carried out in [11] . The selected setting is assigned to the execution layer to be implemented by the information protection facilities. Only enforcement mechanisms interact with security objects and information protection facilities. Protection of the information system of the selected settings using a acceptable to perform functions in addition to collecting information on the status of the object of protection of information and information to assess the

effectiveness of the measures used to protect the top layer to function assigned to it. At the expense of information on the current state of the object of protection the adequacy and completeness of information protection measures is checked, their excess is minimized. The constant updating of the required level of protection with the value of the information contained in the content and the state of the information system enables the effective use of allocated resources .

4 INFORMATION SECURITY MANAGEMENT SYSTEM

Information protection facilities work within an information protection system that provides a certain level of information protection. Therefore, information security management should be implemented throughout the system, and should implement all of the protection functions supported by that information protection tool. In turn, the information protection functions are the final set of enterprise security policies that may increase or decrease depending on the external environment and information technology. Information security management issues may vary from one organization to another. That is why we need to consider this issue in more detail. The issue of managing an information security system is about the inclusion / exclusion of such remedies from the security system. Information security tools support a variety of data security regimes. As a result, the information protection facilities will be able to switch between processes. For this reason, the security administrator should consider the possibility of switching between processes when defining the level of protection of the level of intersection, which means that it is desirable to determine the boundary risk unit [12]. In general, the organization's information security policy should include a minimum set of security functions that should support the information protection system. The maximum level of protection is determined by the structural capabilities of the information protection system. This may be the level of planned protection that cannot be achieved by the existing information protection system. In this case, the information processing plans need to be revised or strengthened by a protective system. As mentioned above, the organization's information system has a dynamic structure, meaning that the structure of information protection facilities is constantly changing. However, protection functions must be performed continuously at the system level. At the level of the security system, a level of coordination is included in the management system for complete control over the implementation of protection functions (the content of information protection facilities).

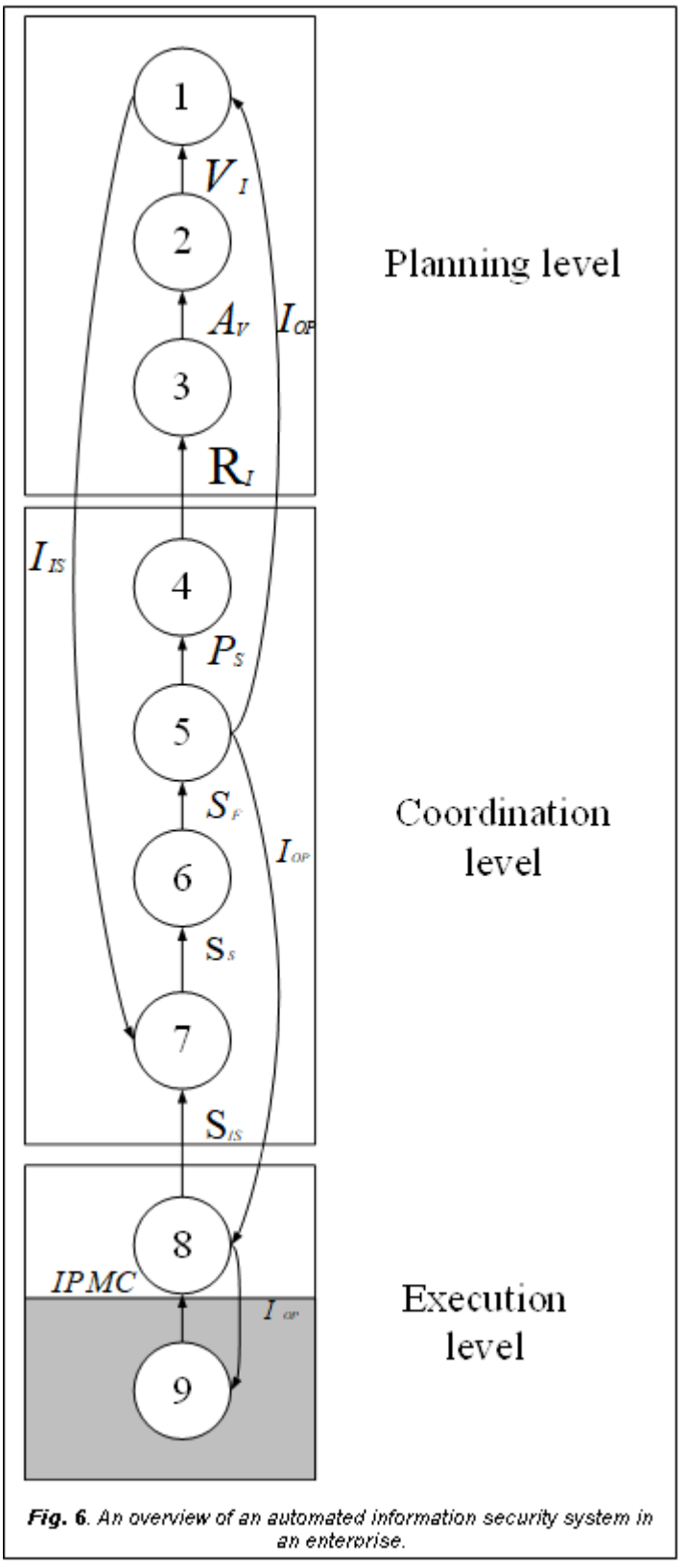

***Fig. 6**. An overview of an automated information security system in an enterprise.*

The functions of coordinating elements are:

- monitoring of protective function;
- recording the facts of the attack;
- identification;
- testing of functions;
- in the successful completion of the collection of information protection function verification.

At the planning level, control commands will be analyzed and directed to the implementation mechanisms.

At executable level, there is an executable software element (SE) that controls information services and information protection facilities. Each SE registers the state of protective devices, the interactions between protection devices and the users of the system. The SE has a built-in protection management interface and executes control effects by changing the state of the protective equipment. The state of change is simply to turn the protective device on/off. For tools with rich functionality, it is intended to set the functionality required. As individual protections also have extensive capabilities to counteract non-volatile factors, it is intended to delegate part of the SE decision-making function and enable independent change of protection status by increasing or weakening information protection. At the same time SE information protection system provides operational dispatch control. It is also envisaged to give SE a part of the rights to manage the information system functions. The modern system architecture of the software makes it impossible for users to control the movements and processes of the environment due to the limitations of the operating environment. That is, it is impossible to control the security of the network node outside the operating system. Therefore, it is necessary to place the Module of the information management system on each node of the protected system, as it is possible to control the state of the entire information system in the organization by releasing the sensors of the information security management system. The following complications arise when placing the required minimum audit tools in network nodes:

1. Audit logs should be reviewed periodically and no malicious actions are detected during the review period;

2. Logging was done through network connections, where the network fails to load, which results in costly connections in the geographically distributed network.

Deploying SE can be divided into:

- analysis of current events;

- the ability to independently make independent decisions on resource protection, that is, the ability to perform operational control over the protection of individual data sets, which significantly increases the load on the computing power;

- protected resource threats decrease in reaction time;

- In the context of the organization's temporary node information required to maintain the level of protection given to receive.

The need to extend the functionality of SE decision-making algorithms is related to the unofficial distributed information system, which does not guarantee constant contact with the decision-making hierarchy. Deployed from a host management system (generally considered to be a state of affairs), the SE can detect the destructive actions and attacks, independently support the protected node, make decisions about and respond to threats. It is desirable to deploy a management system SE that records all potentially significant events for protection in each network node [13]. To do this, you must give the SE the necessary rights. Computing techniques can be multi-functional or multi-user tools with multiple SEs. The functions of the security management subsystem should be assigned to the management mechanisms that provide the SE with all the protection management interfaces on the same network node, which allows:

1. use of information protection devices as control system sensors;

2. automate the process of re-configuring information protection devices in accordance with the required level of protection.

The main purpose of the management system is to ensure the required level of organization's information resources protection while minimizing the cost of information protection. The main functions of information security system management are:

- Collection of information on the condition of the object of protection;

- Information processing and object of protection on the basis of information on the status of plans for the required level of security and risk planning;

- Selection of information security system settings;

- Improve information security settings;

Control over current indicators of the object of protection and appropriate plans.

5 CONCLUSION

In summary, the following work has been done in this article. These are:

1. developed system of automated information security system at the enterprise;

2. developed an enterprise security task structure;

3. the concept of building an automated information security system at the enterprise was proposed;

4. developed an overview of the automated IIS of the enterprise

REFERENCES

[1] Bekmuratov T.F., Botirov F.B., “Multi-agent system of protection from unauthorized access”, 2019 International Conference on International Scientific and Practical Conference "Innovative ideas of modern youth in science and education", USA, p.4-7.

[2] Bekmuratov TF, Botirov FB, Application of multicenter systems in information security systems // Problemy information and energy. 2018. No. 5. S. 78–83.

[3] Legkov K.E. Methods of automation of information systems of automated system of up -to-date objects object specification // T-Comm: Telecommunications and transport. 2018. Volume 12. No. 5. S. 31-40

[4] I Formatless bezopasnost и язык программирования CS. Malkov M.A. Intelligent system. Theory and Applications. 2016. T. 20. No. 3. S. 209–213.

[5] Jidko E. A., Razinkov S. N. The model of the system and the information on the system and the uptake of the data object // System Upgrade, the thread and the bezopasnosti. 2018. No. 1. S. 122–135. URL: http://sccs.intelgr.com/archive/2018-01/06-Zhidko.pdf

[6] Zhidko EA, Razinkov SN Model of security and information protection subsystem of a communication and control system of a critical object. Control Systems, Communic ation and Security, 2018, pp. 122–135. Available at: URL: http://sccs.intelgr.com/archive/2018-01/06-Zhidko.pdf (in Russian).

[7] Bekmuratov T.F., Concepts and post-modern intellectual systems of information and information technologies // Problems of information security and cyber security in information technologies and communications: Republican scientific and technical conference. Tashkent - 2018., pp. 4-8.

[8] Jidko E. A. Nauchno-obosnovanniy podxod k Classification ugroz information information technology // Information systems and technology. 2015. No. 1 (87). S. 132–139.
[9] Sazonova S. A. Otsenka nadejnosti raboti setevix obyektov // Vestnik Voronezhskogo Institute of Technology. 2016. No. 1 (16). S. 40-42
[10] Gavrilov V. E., Zakarinniy A. A. Informatsionniye sistemi i informatsionniye materiali voprosi obespecheniya zashite informatsii v avtomatizatsiya informatsionnix sistemax na oblachnix texnologiy s ispolstvovaniyem sistemov iskusstvennoy Intel // Sistemi i sredstva informatsiY. - 20 16. - T. 26. - No. 4. - S. 38-50.
[11] M Models and methods podderjki prinyatiya resheniy PO Obespechenie informatsionnoy Safety informatsionno upravlyayushchix System. Zegjda PD, Anisimov VG, Suprun AF, Anisimov EG, Saurenko TN Problems of informational design. Computer System. 2018. No. 1. S. 43-47.
[12] Bekmuratov T.F., Botirov F.B,, Problems of information security management // Problems of information security in information technologies and communications: Republican scientific and technical conference. Tashkent - 2019., pp . 151-155.