Chemical Technology, Control and Management

Volume 2019 | Issue 5 Article 8

12-28-2019

Development Of Structures Of Intellectual Information Protection System

Tulkun Fayzievich Bekmuratov
SIC ICT of TUIT, Address: Tashkent, Uzbekistan, Phone: +998 71 234 07 92;, bek.tulkun@yandex.com

Fayzullajon Bakhtiyorovich Botirov
TUIT named after Muhammad al-Khwarizmi, Address: Tashkent, Uzbekistan, Phone: +998 97 751 16 97, botirov_fz@mail.ru

Development Of Structures Of Intellectual Information Protection System

Cover Page Footnote

Tashkent State Technical University, SSC «UZSTROYMATERIALY», SSC «UZKIMYOSANOAT», JV «SOVPLASTITAL», Agency on Intellectual Property of the Republic of Uzbekistan

Erratum

??????

ISSN 1815-4840
CHEMICAL TECHNOLOGY. CONTROL AND MANAGEMENT
2019, №6 (90) pp.63-71
International scientific and technical journal
journal homepage: https://uzjournals.edu.uz/ijctcm/
Since 2005

UDC 004.056

DEVELOPMENT OF STRUCTURES OF INTELLECTUAL INFORMATION PROTECTION SYSTEM

Bekmuratov Tulkun Fayzievich[1], Botirov Fayzullajon Bakhtiyorovich[2]

[1]*SIC ICT of TUIT,*
Address: Tashkent, Uzbekistan,
E-mail: bek.tulkun@yandex.com, Phone: +998 71 234 07 92;
[2]*TUIT named after Muhammad al-Khwarizmi,*
Address: Tashkent, Uzbekistan,
E-mail: botirov_fz@mail.ru, Phone: +998 97 751 16 97

Abstract: *The structures of intelligent information protection systems are considered. The tree of tasks for protecting information of the information system of enterprise is presented. Information security management systems without automation of management processes and automated information security management systems are considered. The functional capabilities of multi-agent information protection systems are investigated and possible risks are analyzed. The proposed schemes of automated and automated information security management systems are described. The proposed technology for constructing a software package for an enterprise information security management system is considered, based on the concept of multi-agent systems as the basic technology for software implementation of an information security management system.*

Keywords*: intellectual information protection system, information security, protection of information, risk, control system of protection system, decision maker, multi-agent system.*

Аннотация: *Ахборотни ҳимоялашнинг интеллектуал тизимларининг структуралари кўриб чиқилган. корхона ахборот тизимларининг маълумотларини ҳимоя қилиш учун вазифалар дарахти келтирилган. Бошқариш жараёнларини ва автоматлаштирилган ахборот хавфсизлигини бошқариш тизимлари кўриб чиқилган. ахборотни ҳимоя қилишнинг кўп агентли тизимларини функционал имкониятлари ўрганилган ва мумкин бўлган хавфлар таҳлил қилинган. Автоматлаштирилган ахборот хавфсизлигини бошқариш тизимларининг схемаларини тавсифланган. Корхонанинг ахборот хавфсизлигини бошқариш тизими учун дастурий таъминот пакетини яратиш учун таклиф қилинаётган технология кўп агентли тизимлари, ахборот хавфсизлигини бошқариш тизимининг дастурий таъминотини амалга ошириш учун асосий технология сифатида тушунилади.*

Таянч сўзлар: *ахборотларни ҳимоялашнинг интеллектуал тизими, ахборот хавфсизлиги, ахборотлар ҳимояси, хатар, ҳимоя тизимининг бошқариш тизими, қарор қабул қилувчи шахс, кўп агентли тизим.*

Аннотация: *Рассмотрены структуры интеллектуальных систем защиты информации. Представлено дерево задач защиты информации информационной системы предприятия. Рассмотрены системы управления защитой информации без автоматизации процессов управления и автоматизированные системы управления защитой информации. Исследованы функциональные возможности мультиагентных систем защиты информации и проанализированы возможные риски. Описаны предлагаемые схемы неавтоматизированной и автоматизированной систем управления защитой информации. Рассмотрена предлагаемая технология построения программного комплекса системы управления защитой информации предприятия, основанная на концепции мультиагентных систем как базовой технологии программной реализации системы управления защитой информации.*

Ключевые слова: *интеллектуальная система защиты информации, информационная безопасность, защита информации, риск, система управления системой защиты, лицо, принимающее решение, мультиагентная система.*

Introduction

Management is a targeted effect on a managed system, aimed at ensuring its required behavior. In the field of information security, management refers to activities to maintain the information system in a safe condition. Safe is the state of security of information processed by computer technology or an automated system from internal or external threats. There are many regulatory documents, monographs, articles that affect the task of managing information security systems. The tasks to be solved in the process of controlling the protection of information (PI) and system functions are described in sufficient detail PI management. However, today there are no approaches to automation of information security management, automation of PI processes in Intellectual Information System (IIS) of enterprise. The chapter discusses the task of automating information protection processes, the need for software control of PI systems in IIS of enterprise. The concept of building an intelligent automated information protection system based on a multi - agent approach is proposed. The advantages of this approach are formulated.

The application of multi-agent systems in information security systems is now much more efficient. Because in one system, in which different agents performing different tasks are summarized, that is, the functional capabilities of the multi agent system increase [1].

Research Methods and the Received Results

Having determined the general concept of the PI management system, it is necessary to dwell in more detail on the goals of the PI management system, the structure and tasks of each of its components, and how the combination of these goals will contribute to the achievement of the general goal of the management system. In Figure 1 shows the tree of objectives of the PI system in a virtual enterprise.

Currently, the most optimal tool for preventing cybercriminals from getting protection from cybercriminals would be to develop intellectualism of cybercriminals management [2]. As an effective means of protecting against cybercrime is the development of intellectual property of cybercrime management, it means that in the case of Information Protection resulting from the construction of a multi-agent intellectual automated property system, it is necessary to formulate two interconnected neural network and expert systems components, the basic functionality of hierarchical levels in the form of intellectual agents [3-6]. So it can be seen from this that the construction of an intelligent automated system of Information Protection is called purposeful implementation in hierarchical form.

The goal is the end result achievable with in a certain time interval. The main goal of the control systems of the airspace PI of enterprise (C0) is to maintain the correspondence between the required (planned) and actual security levels. Wood goals represents a directed graph $\{G = < A, E >\}$, where $\{A_{ijks}\}$- the set of goals and let keep secure IP of enterprise. Many ribs {E} represent the interconnections between goals and sub goals. The goal tree has a hierarchical structure and is divided into three branches: the branch of the planning level (C1 - management at the IIS level), the branch of the coordination level (C2 - management at the IP level of an individual enterprise), and the branch of the executive level (C3 - management at the level of information resource). At the top level, there is only one goal - the common goal of the system C0.

Branch C1 includes the following objectives:

1. C11 - Planning the value of information assets on the basis of complex technical product life cycle;
2. C12 – Risk analysis;
3. C121 - Formation of many threats;
4. C122 - Assessment of threat characteristics;
5. C13 - Transfer of risks to the level of coordination.

Risk analysis is necessary for an adequate assessment of information protection measures, the implementation of which will minimize the damage from the impact of information threats in the planning period. Risk analysis includes the formation of many threats (C121) and the assessment of

threat characteristics (C122) based on assessments of the value of information that will be processed in the forecast period and estimates of the frequency of threats, In order to achieve these goals, the security administrator of IIS and others should be directly involved persons whose responsibilities include ensuring the safe and reliable functioning of the airspace [7].

The risk analysis should take into account not only the generalized information assets of the enterprises participating in the enterprise, but also the mutual influence of information systems combined together. Since such a combination can lead to the formation of new threats and vulnerabilities, means of protection against which are not provided in the IIS. The results of the risk analysis should be transferred to the coordination level.

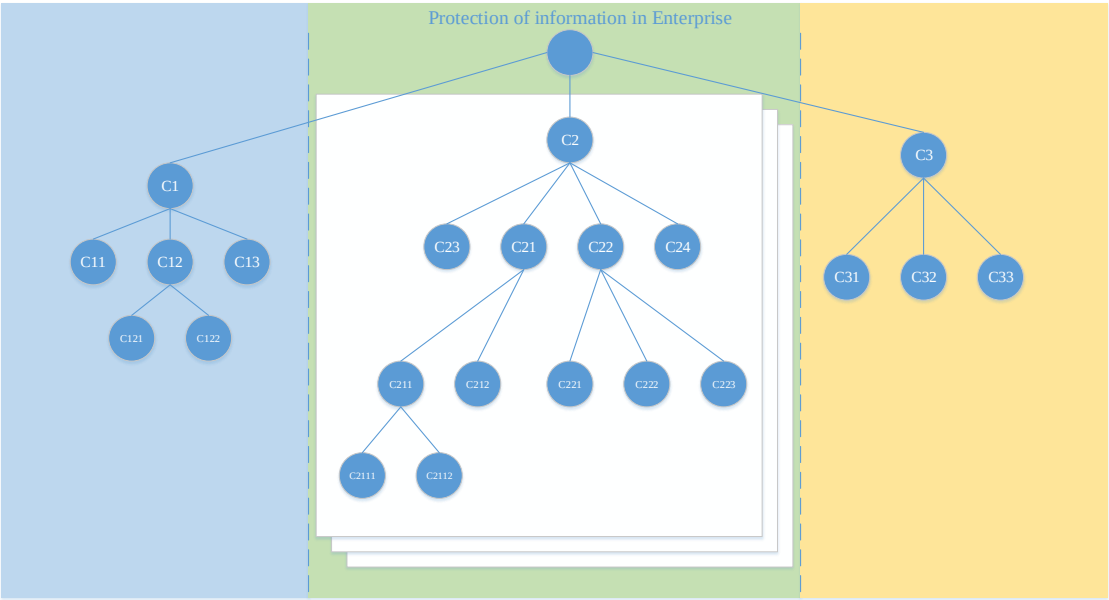

Fig. 1 - ***The goal tree of the PI enterprise control system.***

In turn, the level of coordination solves the problems associated with the achievement of the following goals:

1. C21 - Assessment of the current state of IP enterprise;
2. C22 - Calculation of the current values of security indicators and comparing them with the required indicators;
3. C23 - Monitoring the state of the PI system;
4. C24 - Formation of configurations of PI facilities based on requirements;
5. C211 - Analysis of the status of resources and processes;
6. C212 - Collection of data on the state of the system;
7. C2111 - Identification of anomalies;
8. C2112 - Identification of distributed attacks;
9. C221 - Identification of increased risks;
10. C222 - Identification of increased security;
11. C223 - Formation of recommendations to eliminate inconsistencies between the required and current levels of security.

Based on the results of the risk analysis, the configuration of the PI system (C24) is selected, which should be implemented by the PI tools and subsystems to ensure the security of the enterprise information assets. The PI system configuration contains a set of functional requirements, the implementation of which will allow maintaining residual risks at a level not exceeding the permissible value of risks in the planning period [8]. The selected configuration is implemented through the execution level. Assessment of the current state of IP is necessary to identify manifestations of destabilizing factors, the impact of which can harm IP. For this, data on the status of the system

(C212) is selected from the database of security events. A lot of the selected data is analyzed (C211) in search of anomalies (C2111) and the identification of distributed attacks (C2112).

Based on the selected data, current security indicators are calculated, which are compared with the planned indicators. The identification of increased risks (C221) and the identification of increased protection measures (C222). Given the fact that the safety functions are determined by the configuration of the PI system discovered facts of discrepancies between the actual and required security indicators are sent for consideration to the security administrator or other person making decisions on information security. Also on the approval, the proposed protection measures aimed at addressing the identified discrepancies security indicators in the event that the identified discrepancies sufficient to change the communication system operating configuration selected and implemented a new communications system configuration for all elements of the IS of enterprise, which allows it to move to a new state, equally safe around the entire perimeter of the IP of enterprise. The executive level implements the following goals:

1. C31 - Formation of management teams;
2. C32 - Analysis of operational data;
3. C33 - Collection of data on events PI.

The executive level collects and primary analyzes data on the state of protected assets (CPL) and generates and implements management teams (C31). Collects data on the state of protected assets allows you to control all changes in IP and the environment that could potentially affect the security of the protected object. ” Such an analysis is possible only in the case when each asset, each channel of unauthorized access, each vulnerability will be monitored by means of the control system PI. Data collection is carried out by intercepting events occurring in the protected node: user actions and processes, calls to and from external networks. Each intercepted event is analyzed (C32) for belonging to a variety of destabilizing factors. Based on the results of the analysis, an event can be:

1. discarded as unrelated to PI;
2. processed as a prerequisite for a destabilizing factor, which should be notified to the person responsible for the security of the protected asset;
3. Processed as a clear sign of the threat to protected assets, and therefore emergency measures can be taken to prevent the spread of destabilizing effects to other elements of the IS of enterprise.

These are the main goals of the automated system for controlling the PI of enterprise.

The complexity of the information system of the enterprise does not allow achieving all the goals of managing the efforts of security administrators. A large number of potentially dangerous events, large volumes of document flows and services lead to the fact that the person responsible for information security cannot process such a volume of data. In the case of the distribution of management functions between several administrators, a mismatch in their actions may occur because each of them has only part of the information necessary for making decisions to protect information. Undetected vulnerabilities, uncontrolled threats arise, and potential risks grow. To successfully achieve management objectives, it is necessary to automate part of the functions of security administrators. This will allow security administrators to concentrate on analyzing the situation and making strategic decisions to protect information, while ensuring timely collection of data on the state of the system, initial analysis of information, preparation of possible solutions, and accurate implementation of instructions [9].

Let us evaluate the possible degree of automation to which the functions of managing information security at the enterprise can be subjected. To do this, we will use the constructed tree of the PI control target on the enterprise (Fig. 1). First, we will analyze the group of planning goals for the required level of IS at the airspace. The planning of the value of information resources can be automated by developing and implementing models of information processes, evaluating changes in the value of information at various stages of the system life cycle, determining the numerical values of the parameters of the aging functions of various types of information on the

enterprise, and identifying the dynamics of document flows. All this allows us to solve the problem of planning the value of information resources. The formation of many threats and assessment of their danger at this stage of automation is almost impossible, since these procedures are not formalized and are implemented only by expert methods. In addition, the accuracy of planning the level of threat exposure largely depends on the completeness of the list of threats and the correctness of their hazard assessment. The solution to the planning problem involves the use of heuristic methods; therefore, it can be algorithmzed and implemented in the form of software only in the part related to the calculation and presentation of the results. The formation of many threats, the initial assessment of various parameters of threats remains the prerogative of man - an information security expert.

It is known to us that with the help of multi-agent intellectual systems, system efficiency can be increased even when protecting data from unauthorized access from the enterprise network [10]. For this reason, the effectiveness and functional capabilities of the protection mechanism created if it is developed on the basis of multi-agent intellectual systems in the development of the intellectual method of information Protection in the organization will be further increased [11].

The choice of the optimal configuration of the protection system for the planned level of protection is a difficult to solve exhaustive task, the approach to solving which is the use of artificial intelligence methods - fuzzy logic. The group of goals for solving the tasks of monitoring the implementation of protection plans for information resources of an IP includes assessing the current level of security of the information system, identifying discrepancies between the planned and actual security indicators, and monitoring the status of the PI control system. Assessment of the current state of the information system consists in analyzing security events, in analyzing changes in the structure of the information system, in searching for vulnerabilities and detecting attacks, in checking the basic functions that determine the level of protection.

The registration of information system events is amenable to automation, since existing operating systems, database management systems, and many application programs have built-in audit tools for user and process actions. There are also application programming interfaces that can be used to programmatically access audit records; it is possible to create and implement additional functions that intercept and record additional events not provided for by audit tools built into software products. Analysis of changes in the structure of IIS enterprise is possible by scanning networks, compiling their topologies, and describing the functional purpose of nodes. There are many vulnerability search and attack detection systems. Based on the results of a multilateral analysis, automated calculations of real protection indicators are possible, comparing them with planned ones and identifying discrepancies. Based on the discrepancies identified, the source of the increase or the reason for the risk reduction is determined. Further, the resulting vector of discrepancies can be sent to the person responsible for security for further analysis and decision-making on eliminating the identified discrepancies or taking the identified risks. Moreover, using the knowledge bases about precedents in the field of information protection and measures to protect against them, a set of measures can be prepared to minimize the revealed deviations. The selected protection measures can be sent to the security administrator along with the vector of the mismatch of the security indicators. The administrator will be able to approve the proposed measures and send them for implementation. Automation of these processes is possible by the methods of fuzzy logic, artificial intelligence, data mining methods. Monitoring the status of the control system of the air conditioner control system consists in checking the operability and correctness of the performance of its functions by all components of the air conditioner system and the air conditioner control system. For this purpose, it is possible to create procedures for verifying the state of various elements of the PI system, which consist in comparing a certain set of parameters of each element of the system of the airspace with the standard. In case of discrepancies in the values of the perimeters of the element and the standard, the element is destroyed and replaced with a copy of the standard. Also necessary are the procedures for the distribution of the elements of the SCPI enterprise in the new segments connected to the IS of enterprise.

The adjustment of the state of the PI system consists in comparing the required level of PI with some configuration of the PI system and reconfiguring the PI system in accordance with this configuration. Now, there is no formalized algorithm for the transition from the requirements for PI to the configuration of the PI system. In essence, this is a task from exposing a finite set of values of security indicators $P' = \{p_W\}$ to a finite set of states of the protection system $\{P_S\}$ where $s = 1,2,3, \dots x$. This process can be automated using knowledge bases and fuzzy logic methods. The initial data for these methods $P_S = F\{p_W\}$ can be expert assessments of the conformity of the PI system configuration to the protection level. It should be noted that these methods can be implemented in software. However, these methods are not formal and potentially contain an error, or they may not take into account the hidden patterns of the processes described by them and depend on the qualifications of the experts setting up the system. In this connection, the participation of security administrators at this stage of management is necessary. This participation boils down to a review of the safety facts, proposed management decisions, and an assessment of their adequacy and appropriateness. In this case, the security administrator acts as the decision maker (DM) - Only after the approval of the DM, the control actions can be directed to implementation. Distribution of accepted changes is possible to carry out automatically. To this end, security equipment and application software that has built-in security functions are provided with an application program interface (Application Programming Interface - API). In fig. 2 and fig. 3 presents the control of the PI system in the classic version and with the use of an automated PI control system.

Using feedback, the PI control system receives the Y -set of data characterizing the change in the state of the control object under the influence of a variety of external and internal Q factors, based on which the IIS IP security audit is performed and a decision is made on whether the current state of the IIS IP matches or does not match the required level of security.

Many catalogs of developed and verified security tasks for IIS enterprise are used as standards in the comparison process. The set E of discrepancies revealed during the security audit between the current and required levels of security of the IIS enterprise is the basis for the formation of the IS IP in a safe state. The control actions prepared by the system controlling protection of information (SCPI) are sent for approval C' to the person making the security decision, who, ultimately, assumes responsibility for the changes being implemented and the transfer of the IIS enterprise to a safe state. Approved control actions C are directed to the implementation of the executive mechanisms of the PI control system.

Based on all the foregoing, we can conclude that most of the functions of the control system of the PI are potentially possible to automate and implement programmatically. Functions of the security administrator - making decisions and adjusting the functioning algorithms of the SCPI enterprise.

Within the framework of the information system of the airspace, it is obvious that the best approach to automating the management functions of the PI is to create a software package for the control system.

In this paper, it is proposed to use the technology for constructing a software SCPI enterprise based on multi - agent systems as the basic technology for software implementation of a control system. It is necessary to dwell in more detail on the reasons for choosing multi-agent technology as a basis for designing a control system for PI. The development goal is a distributed dynamic object management system: protection means, information flows, information services. On the enterprise scale, the creation of a single control center (DC) and decision making, which has a global vision of problems and tasks, leads to a significant increase in information flows from controls to the control center and vice versa, which leads to a significant time delay in decision-making due to the need for centralized processing of the entire amount of information received in HQ about each incident on the GI. In the event of a loss of network connection with the control center, the network node remains without control and management capabilities. In case of failure of the control system, the control system of the enterprise PI stops, which attackers when planning attacks on information assets of the enterprise can use.

In the process of developing an intellectual method of Information Protection at the enterprise, it is necessary to take into account the issue of management of the Information Protection System. Because, in the issue of management of Information Protection System, the information security policy shows the minimal bottleneck of the protection functions that the information protection system should support, and the maximum level of protection is determined by the structural capabilities of the Information Protection System [12-15].

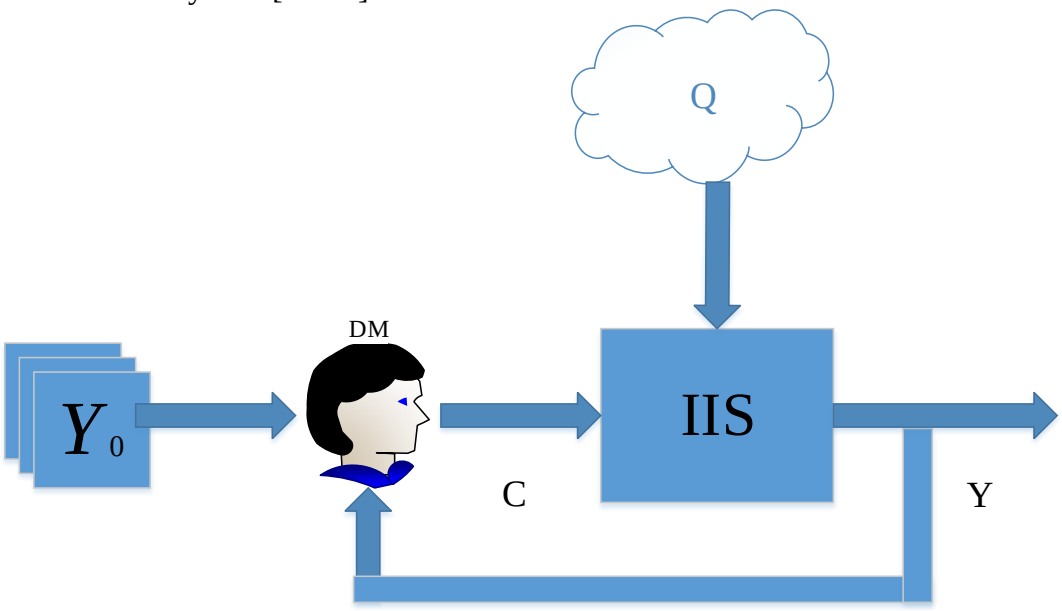

Fig. 2 - ***Scheme management system PI without automation of control processes.***

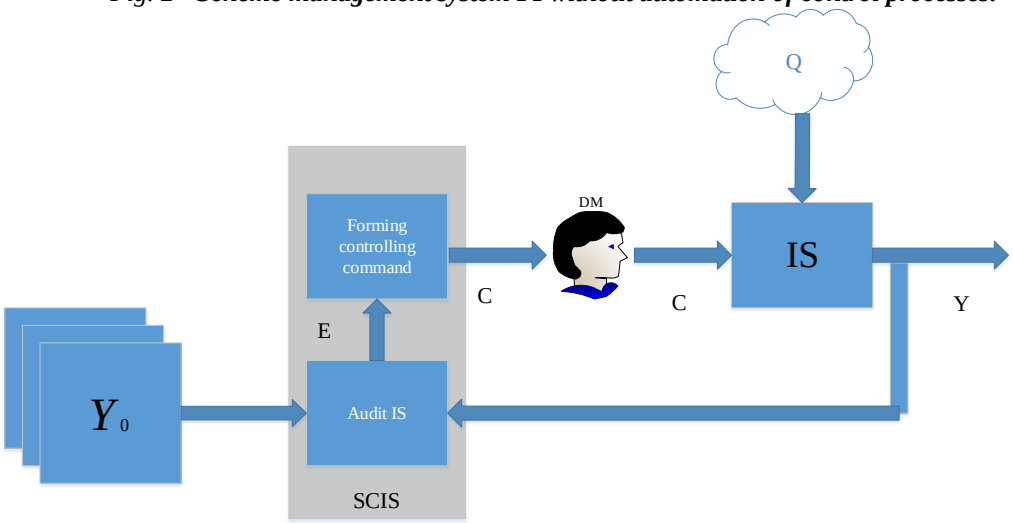

Fig. 3 - ***Scheme of automated control system PI.***

Using a multi - agent approach, from our point of view, will allow us to avoid the difficulties described above. The organization of the government system in the form of a multi - agent system allows you to:

1. Distribute decision-making functions throughout the information system. Each agent, possessing only a part of the data about the system, providing management of the information resources entrusted to it, contributes to the achievement of the common goal of the management system.
2. The interaction between agents in the process of functioning allows you to control the entire information system, coordinate actions, and adjust the goals of agents.
3. Removing part of the agents from the system will not lead to tangible consequences for the system.

4. Autonomy, as a property of agents, allows them to function independently, guided by their local protection goals, when they are disconnected from the information system.

5. The agent is able to perceive the environment (the operating system of the node) directly or through sensors - other programs. The agent contains algorithms for interpreting the information received, forming response actions and implementing these actions both independently and through other performers.

6. The multi - agent system has an open architecture, which allows the control system to remain operational in case of changes in the structure and purpose of the information system. Therefore, a multi - agent approach is preferable when organizing a distributed object control system , which is IP of enterprise

Security administrators determine the protection policy for the entire IIS enterprise and manage the PI system based on data Y_k received from the coordinators and based on information about the stage of the life cycle of complex technical product (CTP) [16-17].

Conclusion

The results of the work of security administrators are sent to the coordinators for execution, $\{AK_l\}$- agents - coordinators of the SCPI at various enterprises participating in the enterprise, as well as the console of local security administrators. Agents - coordinators control the correctness of the implementation of the functions of PI. At the same time, the coordinators carry out the formation of PI systems configurations specific for each enterprise of the enterprise participant. Many management commands determine the states in which agents - executors must transfer funds PI. Information about the state of the object of the PI is collected and sent to the coordinators for further processing. Many agents - the executor is distributed throughout the IP of enterprise and interacts with the coordinating agents in accordance with the logical topology of the segments of the enterprise computer network. It is agents - performers who interact with the means of protection and the object of protection. It should be noted that the proposed structure assumes the presence of only vertical connections between agents in the intelligent control system of PI at the airspace. The proposed structure corresponds to the concept of managing information security at the airspace and allows you to successfully automate most of the management tasks. At the same time , it should be noted that the placement of control agents in each node of the distributed information system and their functioning will lead to additional consumption of computing resources by the protection system, in the drawback of the proposed structure. However, the damage associated with non-productive consumption of computing resources seems to be significantly less than the savings in resources allocated to information due to the functioning of the control system [18-20].

A promising area of intellectualization of software agents of multi-agent information protection systems is the use of technologies of deep learning, deep neural networks and Neural Turing Machines [21].

References:

1. Bekmuratov T.F., Botirov F.B., Multi-agentli tizimlarni axborot xavfsizligi tizimlarida qo‘llanilishi//Problemi informatiki i energetiki. 2018. № 5. S. 78-83.
2. Bekmuratov T.F., Botirov F.B., Kiberhimoya boshqaruvining intellektual mexanizmlari//Axborot texnologiyalari va kommunikatsiyalari sohasida axborot xavfsizligi va kiberxavfsizlik muammolari: Respublika miqyosidagi ilmiy-texnik konferensiY. Toshkent - 2018, b. 108-112.
3. 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.
4. Bekmuratov T.F. Mul'tiagentnaya gibridnaya nechetko-neyronnaya e`kspertnaya sistema informacionnoy bezopasnosti. Problemy' informatiki i e`nergetiki. -2013.- Vy'p. 3-4. S.3-14.
5. Bekmuratov T.F. Nechetko-neyronnaya e`kspertnaya sistema informacionnoy bezopasnosti: harakteristiki, koncepciya i zadachi postroeniya. DAN RUz. - Tashkent, 2013, vy'p. 6. S. 16-20.

6. Bekmuratov T.F., Botirov. F.B. Kiberhimoya boshqaruvning intellectual mexanizmlari. Materialy' Respublikanskoy nauchno-prakticheskoy konferencii «Problemy' informacionnoy bezopasnosti i kiberbezopasnosti v sfere informacionno-kommunikacionnoy tehnologii», Tashkent,22-23 noyabr', 2018g. S.106-108.
7. Legkov K.YE. Metodicheskiye osnovi upravleniya informatsionnimi podsistemami avtomatizirovannix sistem upravleniya slojnimi obyektami spetsialnogo naznacheniya // T-Comm: Telekommunikatsii i transport. 2018. Tom 12. №5. S. 31-40
8. Informatsionnaya bezopasnost i yazik programmirovaniya CS . Malkov M.A. Intellektualniye sistemi. Teoriya i prilojeniY. 2016. T. 20. № 3. S. 209-213.
9. Jidko YE. A., Razinkov S. N. Model podsistemi bezopasnosti i zashiti informatsii sistemi svyazi i upravleniya kriticheski vajnogo obyekta // Sistemi upravleniya, svyazi i bezopasnosti. 2018. № 1. S. 122-135. URL: http://sccs.intelgr.com/archive/2018-01/06-Zhidko.pdf
10. T.F.Bekmuratov, F.B.Botirov. Multi-agent system of protecting information from unauthorized access, Shemical technology. control and management, 2019, №1(85), p. 72-77.
11. Bekmuratov T.F., Botirov F.B., Nabiyev M.M. Mashinali o‘qitish va chuqur o‘qitishning vazifalari va kiberxavfsizlik, “Muhammad al- Xorazmiy avlodlari” ilmiy amaliy va axborot tahliliy jurnali, 3(9)/2019, s. 3-7.
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.
13. Jidko YE. A. Nauchno-obosnovanniy podxod k klassifikatsii ugroz informatsionnoy bezopasnosti//Informatsionniye sistemi i texnologii. 2015. № 1 (87). S. 132-139.
14. Sazonova S. A. Otsenka nadejnosti raboti setevix obyektov // Vestnik Voronejskogo instituta visokix texnologiy. 2016. № 1 (16). S. 40-42.
15. Gavrilov V. YE., Zatsarinniy A. A. Nekotoriye sistemotexnicheskiye i normativno-metodicheskiye voprosi obespecheniya zashiti informatsii v avtomatizirovannix informatsionnix sistemax na oblachnix texnologiyax s ispolzovaniyem metodov iskusstvennogo intellekta // Sistemi i sredstva informatiki. - 2016. - T. 26. - № 4. - S. 38-50.
16. Ghalechyan, A. (2016). Information Struggle in the military field (Teghekatvakan payqary’ r’azmakan olortum, in Armenian). Yerevan: Noravank SEF.
17. Harutyunyan, E. A. (2002). The Problem of Combination of Civilization and Human Qualities (Qaghaqakrt’ut’yan u mardkayin orakneri hamateghman himnaharcy’, in Armenian) Transitional Society/Socio-Cultural Transformations, 52-68.
18. Partyka, T. L., & Polov, I. I. (2002). Information Security (Informatsionnaya bezopasnost’, in Russian). Moscow: Infra – M.
19. Melyukhin, I. S. (1999). Informatsionnoe obshchestvo (Informational Socienty, in Russian). Moscow: MSU.
20. Mokrousov SN «Security issues in the development of oil and gas resources on the continental shelf and on land of the Russian Federation» / / Journal-directory Transport security and technology. - 2006. - № 1.
21. Ian Goodfellow, Yoshua Bengio, Aaron Courville - Deep Learning The MIT Press Cambridge, Massachusetts London, England. ISBN 978-1-491-93799-0 (анг.) © 2017 Massachusetts Institute of Technology.