For the modern stage of science and technology development, the problem of information protection from unauthorized access is becoming relevant. The object of research is the process of monitoring information protection objects for timely detection and securing of leakage channels. The subject of research is ensuring automatic control of monitoring means for information protection objects.

The article presents the results of the development of a method for automatic control of information protection object monitoring means by improving the control process, taking into account the peculiarities of the potential threats impact. The advantage of this study is the involvement of artificial intelligence in monitoring information protection objects in order to timely detect new threats to leakage channels. The essence of the method is to use a cybernetic approach to the development of adaptive control systems for monitoring information protection objects. The structure of the modeling method is considered, the procedure for assessing the adequacy and accuracy of determining the parameters of monitoring information protection objects. Proposals for implementing a method for controlling information protection object monitoring means based on associative control devices are substantiated. Schemes for implementing an associative control device for determining the parameters of an information protection object are presented, and the results of the practical implementation of the proposed method are also presented. A feature of the study are the developed associative control devices that provide the accumulation of knowledge in the process of learning about the threats of information leakage to the object of protection. The results of the study allow to improve the quality of detecting threats of information leakage to the object of protection and take into account possible changes in the characteristics of promising information leakage channels

Keywords: information protection, automatic control of monitoring tools, monitoring of information protection objects

UDC 004.056
DOI: 10.15587/1729-4061.2024.319058

DEVELOPMENT OF A METHOD FOR AUTOMATIC CONTROL OF MONITORING MEANS FOR INFORMATION PROTECTION OBJECTS

Serhii Herasymov
Doctor of Technical Sciences, Professor*
Serhii Yevseiev
Corresponding author
Doctor of Technical Sciences, Professor, Head of Department*
E-mail: Serhii.Yevseiev@gmail.com
Stanislav Milevskyi
PhD, Associate Professor*
Nazar Balitskyi
PhD, Head of Department
Scientific and Organizational Department
Hetman Petro Sahaidachnyi National Army Academy
Heroiv Maidanu str., 32, Lviv, Ukraine, 79026
Viktor Zaika
Doctor of Technical Sciences, Professor, Head of Department
Department of Telecommunications systems and Networks***
Serhii Povaliaiev
PhD, Associate Professor
Department of Details of Machines and the Theory of Mechanisms and Machines
Kharkiv National Automobile and Highway University
Yaroslava Mudroho str., 25, Kharkiv, Ukraine, 61002
Sergii Golovashych
PhD, Associate Professor
Department of Software Engineering and Management Intelligent Technologies**
Oleksandr Huk
PhD, Senior Lecturer
Department of Cyber Warfare
The Institute of Information and Communication Technologies and Cyber Defense
National Defence University of Ukraine
Povitryanikh Sil ave., 28, Kyiv, Ukraine, 03049
Anton Smirnov
PhD, Associate Professor
Department of Information Technology Security
Kharkiv National University of Radio Electronics
Nauky ave., 14, Kharkiv, Ukraine, 61166
Kostiantyn Rubel
PhD Student
Department of Management***
*Department of Cybersecurity**
**National Technical University "Kharkiv Polytechnic Institute"
Kyrpychova str., 2, Kharkiv, Ukraine, 61002
***Educational-Scientific Institute of Telecommunications
State University of Information and Communication Technologies
Solomyanska str., 7, Kyiv, Ukraine, 03110

Received 30.09.2024
Received in revised form 27.11.2024
Accepted date 10.12.2024
Published date 27.12.2024

How to Cite: *Herasymov, S., Yevseiev, S., Milevskyi, S., Balitskyi, N., Zaika, V., Povaliaiev, S., Golovashych, S., Huk, O., Smirnov, A., Rubel, K. (2024). Development of a method for automatic control of monitoring means for information protection objects. Eastern-European Journal of Enterprise Technologies, 6 (9 (132)), 25–38. https://doi.org/10.15587/1729-4061.2024.319058*

1. Introduction

The development of modern security tools is based on symmetric and asymmetric cryptosystems, while the emergence of a full-scale quantum computer can bring chaos to security systems and significantly reduce the level of security [1]. In addition, the introduction of an artificial intelligence (AI) system at the first stage of a targeted (mixed)

attack can significantly simplify and accelerate the detection of anomalies (deviations from normal operation) in the operation of the infrastructure. AI also allows for timely analysis of SIEM systems and similar anomaly detection and analysis systems [2]. At the same time, for any protection object, it is necessary to take into account not only the current state of information protection, but also the possibility of timely formation of preventive protection measures. When checking for the presence of information leakage channels, special technical means are used, aimed at checking certain signs of data leakage [3]. This uses a significant set of features inherent in each technical monitoring tool (verification method).

Therefore, consideration of a number of issues related to the problem of developing principles for constructing and methods for synthesizing monitoring systems for information protection objects that are capable of detecting and timely securing information leakage channels or preventing impact on them is becoming relevant [1, 3].

Control tasks in conditions of significant a priori uncertainty arise primarily when the description of the regularities of the functioning of the information protection control object cannot be formalized. Also, its formal model is so complex that the task of synthesizing optimal control in real time becomes unfeasible. Under these conditions, the only possible means of solving the problem is the accumulated control experience, that is, the accumulation of knowledge about the regularities of the formation of control influences in the form of associative pairs "stimulus-response". The generalization of this experience in "active memory" provides the superposition (generalization) of experience and the associative selection of the corresponding control when the values of the parameters of the state of the control object are supplied to the input of the stimulus.

The first known experiments on the creation of systems of this type were Rosenblatt's perceptrons, which performed image recognition; training programs, which performed recognition of oil deposits, chemical compounds, diseases, etc. [4, 5]. Modern various modifications of the approach to information processing based on knowledge accumulated in the active memory of electronic information carriers are actively developing. Systems of this kind are called expert. A feature of the modern stage of development of expert systems is an integrated approach to the development of their hardware, software and algorithmic support.

It is generally accepted that the introduction of expert systems into the practice of automatic control and decision-making leads to the creation of an automatic dispatcher, an intelligent robot, and other similar systems. Expert systems also provide a significant expansion of the areas of automatic control and an increase in the efficiency of control in conditions of insurmountable information uncertainty.

Thus, the current task is the timely detection and analysis of anomalies and/or deviations from normal operation, which, in the context of increasing computing capabilities, requires automation and efficiency.

2. Literature review and problem statement.

The analysis of work [5] showed that it is possible to use artificial intelligence systems in combination with IoT elements/systems. The proposed ICFPS creates deep learning methods, such as recurrent convolutional neural networks (RCNN) and recurrent generative adversarial neural networks (RGAN) for automatic control. However, the use of IoT elements unfortunately creates critical points of any infrastructure, so their use in protection systems must be limited. In work [6], a network monitoring index (NMI) was developed to assess the cybersecurity status of critical information infrastructure objects. The authors studied 15 existing cybersecurity indices that include a network component and identified data sources for forming NMI: network traffic analysis, vulnerability scanning results, and threat information. The proposed NMI model integrates objective data with subjective assessments of auditors, which provides a comprehensive assessment of network security. However, it should be noted that the developed approach depends on the subjectivity of assessments, the complexity of integrating heterogeneous data, and the lack of practical results for testing the model. In [7], an analytical transformation is shown to solve the problem of probabilistic limitation of transmission channel downtime. Safe maximization of energy efficiency is chosen as the objective function, and the resulting resource optimization is processed using an alternative maximization structure. However, this approach does not allow to identify indicators (criteria) of the presence of information leakage channels. In [8], four indicators based on the T-test are used to assess the resistance to side channel attacks. The results, based on the correlation coefficient, show a correlation between resistance to side channel attacks and performance. The work [9] proposes a wireless monitoring and automatic protection system for ensuring security at critical infrastructure facilities, based on wireless sensor networks (WSN). The system nodes monitor critical parameters and ensure the activation of protective devices in case of a threat. Network data processing algorithms and automated response mechanisms are used, allowing remote security control via a portable terminal. The main disadvantages of the proposed system from the point of view of cybersecurity are the dependence on the stability of the wireless network, which may be vulnerable to attacks on the network (interception of data or blocking of nodes). The proposed system also has limited reliability in conditions of external interference or threats of targeted disruption of communication. System integration requires additional measures to protect the transmitted information and ensure data confidentiality. In [10], a security authentication scheme is proposed that uses intelligent prediction mechanisms to detect spoofing attacks. However, this scheme is not adapted to an automated decision-making system for detecting information leakage channels. In [11], a manual monitoring method and an automatic active monitoring method are compared to determine the concentrations of hazardous substances. A comparison of the data obtained by the two methods demonstrated their high consistency. The automatic method provides continuous monitoring and minimizes the human factor, but requires proper protection of information transmitted over the network from possible cyber threats. To ensure effective automation, it is necessary to implement reliable mechanisms for data encryption and protection of information transmission systems, as well as to take into account the risks of interference in automated monitoring systems. In [12], two-factor authentication is used, where the authorization code is sent via a separate channel. This approach is generally recognized to be associated with significant overhead costs, both due to the use of additional channels and the need for additional processing. At the same time, no analysis of the impact of costs on in-

creasing security and availability during information transmission is performed. In [13], an automatic method for collecting and monitoring fault codes in industrial processes controlled by microcontrollers using Industry 4.0 technologies is proposed. Examples are Big Data, industrial networks, manufacturing execution systems (MES) and cloud computing. The method includes 12 steps adapted to microcontrollers, which allows real-time error codes to be monitored on a production line of five interconnected processes. Due to this, the system allows to accurately determine the causes of downtime and improve resource allocation to reduce time loss due to failures. The implementation of the method in real conditions has shown its effectiveness in identifying problem areas and increasing productivity. Regarding information security methods, the main focus is on protecting data collected in real time through industrial networks and cloud platforms. A system based on automatic data collection must have an appropriate level of protection against unauthorized access and manipulation of information. However, despite the effectiveness of using such technologies, the disadvantages are the risks associated with the security of information networks that process sensitive data on the state of industrial processes. Taking these aspects into account is important for preventing cyberattacks and ensuring data security within the framework of Industry 4.0. In [14], the security of information transmission is considered physically as an additional level of security that ensures the confidentiality of radio communication. Typical characteristics of a wireless channel (noise, interference) can be used to preserve the confidentiality of the message from potential interceptors. Coordinated planning of channel switching between different cells that use the same radio resources is proposed, based on the use of spatial information. However, the issue of ensuring the reliability of information transmission is not investigated in the work. In [15], the implementation and testing of a scalable EHR control system based on blockchain is proposed. The disadvantage of this work is the two-channel transmission of information, which does not provide the necessary reliability of information transmission. The paper [16] presents a new method for fast and accurate detection of multiple moving objects in images, which is important for security. The method combines source feature extraction (center of gravity, shape, flow) and a neural network to improve detection accuracy, even with complex backgrounds and different object motion modes. However, the method relies on pre-extraction of features and depends on the efficiency of the neural network for classification, which may be limited by lighting conditions or incomplete training data. The paper does not address the stability of the method in noisy or very low-light conditions, which may affect detection accuracy. The papers [17, 18] investigated the decision-making process associated with managing digital communities in the ecosystem of digital social channels, especially in the context of antagonistic digital communication and the spread of malicious content. The proposed method is based on the analysis of the information situation in managing digital communities under conditions of complete uncertainty, antagonistic behavior, and partial uncertainty. However, there are no results of research into the possible impact of unreliable transmission channels (broken channels) on decision-making. The work [19] proposes an integrated method for automatic retrieval in BIM, focusing on geometric and attribute information of "secondary" building objects for effective management during the operation and maintenance (FM) phase. However, from the point of view of information security, especially in the context of critical infrastructure objects, this approach raises several concerns. Automatic retrieval through segmented point clouds and the use of machine learning for data processing can be vulnerable to attacks such as data manipulation or unauthorized interference in processing processes. Potential vulnerabilities can be associated with unreliable authentication of devices on the network or unsecured data transmission channels, which in critical infrastructures can lead to serious consequences. In addition, the scalability of this system in conditions of high sensitivity of information about building components and their attributes requires a special approach to data encryption and protection against leaks. The work [20] considers the important problem of personal data protection in the context of algorithmic monitoring, which is relevant in the era of big data. However, the work does not consider specific threats associated with the use of such technologies at critical infrastructure facilities, where data leaks or misuse can lead to serious security breaches, including cyberattacks or sabotage. The work [21] considers methods for maintaining the security of information systems, the degree of vulnerability of which is partially observed. In each period, the decision-maker must make one of three decisions: do nothing, check and implement (remove the vulnerability), if necessary, and implement directly. The disadvantage of the study is the lack of calculation of indicators that would help make a particular decision (no threat ranking). The work [22] is devoted to the use of GNSS-RTK technology for automatic monitoring of the technical condition of port structures, in particular for detecting structural displacements and damages. Since traditional monitoring methods require constant human intervention, the authors propose a new solution for automatic warning of port safety risks. They propose the use of warning signals (whistles, lights or messages) for a quick response to possible structural displacements. GNSS-RTK technology allows obtaining accurate monitoring data that can be used to predict future changes and damages to structures. This solution is aimed at ensuring the safety, stability and efficient operation of port facilities in the conditions of the technological revolution 4.0. However, the effectiveness of automatic systems in real conditions is critically important, which requires additional research and improvements in the field of information security, especially in the context of protecting monitoring data from malicious influences. The paper [23] describes the development of a real-time object detection and monitoring system for security, using deep learning and filtering algorithms to improve the accuracy of object tracking in complex environments. Although the system demonstrates high performance on the MOT15, MOT16, and MOT17 datasets, the paper does not pay enough attention to information security issues, in particular, the protection of personal data and the integrity of information in real time. The use of such technologies in critical infrastructures without proper protection can create vulnerabilities, which is a serious risk to data privacy and security. In [24], the authors propose the use of chaotic encryption to ensure the security of data transmission over communication channels. Through a comprehensive analysis, it evaluates the performance of chaotic encryption algorithms in terms of encryption strength, computational efficiency, and resistance to attacks. In addition, the study studies the integration of chaotic encryption with conventional cryptographic proto-

cols to create hybrid encryption schemes capable of providing multi-level protection. However, the authors do not take into account the need to ensure the speed and reliability of data transmission, as well as the possibility of building multi-circuit security systems.

Thus, the current unsolved problem is the lack of effective methods for timely detection of new threats to the object of information protection and securing of leakage channels. Existing manual (expert) methods of threat monitoring do not allow for prompt detection and securing of information leakage channels. The study is aimed at improving the quality of detection of threats to the object of information leakage, including by taking into account possible changes in the characteristics of new information leakage channels.

3. The aim and objectives of the study

The aim of the study is to develop a method for automatic control of monitoring means for information protection objects, which, based on artificial intelligence systems, will ensure timely detection and analysis of anomalies and/or deviations from normal operation, which, in the context of increasing computing capabilities, requires automation and efficiency.

To achieve the aim of the study, it is necessary to solve the following tasks:

– to develop a functional scheme for automatic control of monitoring of protected objects;

– to develop a simulation model of automatic control of monitoring of protected objects;

– to determine the structure of the method of automatic control of monitoring means of information protection objects and the algorithm of its application.

4. Research materials and methods

The object of the study is the means of monitoring information protection objects. The main hypothesis of the study is the assumption that with optimal control organization, the means of monitoring information protection objects are able to detect and secure information leakage channels in a timely manner. The simplifications adopted in the study consist in determining the probability of detecting the threat of information leakage to the object of protection by monitoring means equal to one. When developing a method for automatic control of the means for monitoring information protection objects, the following research methods were used:

– theoretical – methods of operational analysis, control theory;

– experimental (when building a simulation model) – statistical decision theory, principles of systems analysis and modeling.

The use of the mentioned theoretical research methods will allow to develop a functional scheme of automatic control of monitoring of information protection objects. The use of the above experimental research methods will allow to develop a simulation model of automatic control of monitoring of information protection objects. The use of a set of the above theoretical and experimental research methods will allow to develop a method of automatic control of monitoring means of information protection objects.

An important trend of modern times is the creation of a new generation of automatic control computing devices, in which the computing block has the form of a homogeneous system composed of identical elements. By the nature of their action, they differ from each other only by the influence of another level, that is, the control circuit, which regulates the functioning of the device for calculating the required parameters. The prerequisite for the creation of such automatic control systems was the development of microelectronics.

When solving this type of problem, in many cases it is necessary to limit oneself to using a computing device to assess the state of the system and to determine alternative options for influencing the system, that is, to the participation of the computing device in the role of a kind of advisor.

The introduction of such a form of control by means of monitoring information protection objects means a big step forward. However, the next stage should be prepared – direct control of the organization of a complex of many elements, which is carried out by a computing device. If the ultimate goal of automatic control of the organization is to regulate the structure, that is, the configuration, then the schematic diagram can be presented as follows (Fig. 1). In Fig. 1, let's denote: K – a complex consisting of many elements; F – a certain block, the so-called formator (i.e., a block that forms the organization of the complex K).

This block has a computing device that evaluates the data S obtained from the measurement results, relating to the variables of the internal state of the information protection object, i.e. the state of the internal structure. This data is obtained at different points inside the complex and is compared with the required values provided by the command variables R. Based on this comparison and taking into account the disturbing variables P acting on the complex. And also based on other variables V at its own output, the formator calculates the correction variables A, which detect the impact on the system and provide its control.

If the ultimate goal of automatic control of means is to regulate the structure, i.e. configuration, then the schematic diagram can be presented as follows. Creating a closed control loop of monitoring information protection objects means and thus consistently and completely applying the principle of feedback is one of the pillars on which Norbert Wiener put forward the concept of cybernetics [4, 11].

Thus, decentralization of control leads to a decrease in uncertainty associated with the collection and processing of information. However, in turn, it serves as a source of new uncertainty. Indeed, as soon as a subsystem receives the right to make decisions, it turns into a kind of independent organism, and, therefore, inevitably acquires its own interest, in general not identical to the interests of the upper levels. The difference of these interests is determined by many factors – the system of relations, penalties, incentives, etc.

Thus, the main reason for the uncertainty that arises in conjunction with the formation of a hierarchical structure in the control system is the inevitability of contradictions between the whole and its parts, which is manifested in the non-identity of the interests of the entire system and its individual links. Therefore, it is possible to assert only about the optimal degree of decentralization, about the optimal distribution of decision-making functions between the central body and the links of the system. Such a system of views on the causes of the emergence of a hierarchical structure in control systems opens up the possibility of wide use of operational analysis methods for research.

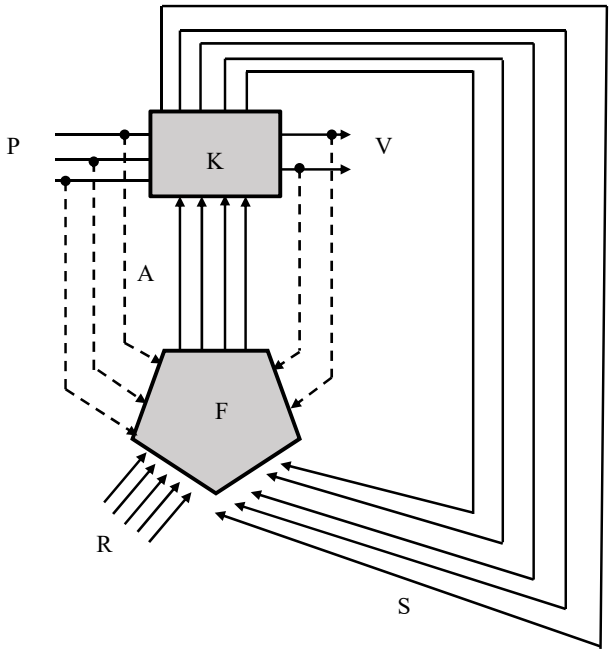

Fig. 1. The basic scheme of automatic control of monitoring means for information protection objects

5. The results of the development of an improved method of automatic control of the monitoring protection means

5. 1. Development of a functional scheme for automatic control of protection objects monitoring

Control is understood as the process of organizing such a purposeful action on some part of the environment, which is called the object of control, as a result of which the needs of the subject interacting with this object are satisfied. The analysis of control distinguishes triad – environment, object, subject (Fig. 2).

The subject is influenced by the state of the environment X and the state of the object Y. If the state of the environment X cannot be changed, then the state of the object can be controlled by the corresponding organized action U from the space R ($U \in R$), which determines the control procedure. The state of the object Y affects the state of the subject's needs. Let $A(\alpha_1, \alpha_2,..., \alpha_k)$ be the subject's needs, where αi is the state of the subject's i-th need (k is the subject's total resource base). The subject builds its behavior in such a way as to minimize needs, that is, let's come to the problem of multi-criteria optimization $\alpha_i(X,Y) \to \min_{U \in R}(\overline{i,k})$.

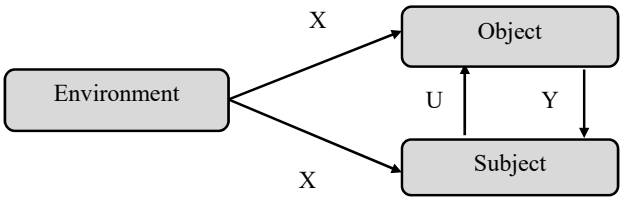

Fig. 2. Schematic representation of the monitoring tools control process for information protection objects

This dependence characterizes the unknown, but existing connection of needs with the state X of the environment and the behavior U of the subject. A moderate approach to the control process allows to decompose the control algorithm and introduce into consideration the intermediate stage of study – the formulation of the control goal, and the solution should be carried out at an intuitive level $Z^*=\varphi_1(A, X)$, where φ_1 – algorithm for synthesizing a goal based on needs A and the state of the environment X. The value Z^* more precisely can be characterized as a model of the state necessary to achieve the ultimate goal, that is, it is such a state Y_X^*, which will satisfy the needs of the subject at a fixed state of the environment X and the needs A. Formulating the goal Z^* with the help of an algorithm φ_1 the subject thereby translates it`s needs into the language of the object's states: $Z^* := Y \to Y_X^*$,which allows to transfer the procedure of synthesis and implementation of control to another subject or automated complex.

In the second stage, control U_X^* is determined, the implementation of which ensures the achievement of the goal Z^*, that is $U_X^* = \phi_2(Z^*, X)$, , where φ_2 – control algorithm. This algorithm should be built using the principles of cybernetics.

It is quite clear that different functions of the control process are performed by different structural elements: the first function (φ_1) is performed by the subject, and the second (φ_2) – by control (controlling) device (CD). Fig. 3 shows a control system that represents an object in combination with a control device.

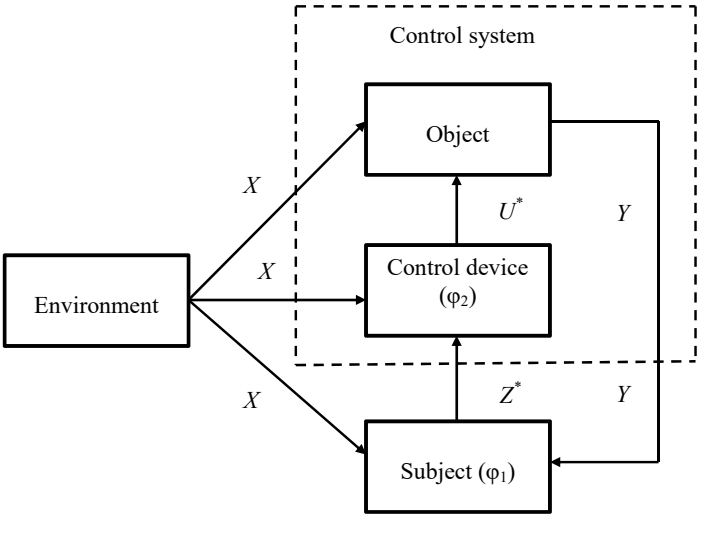

Fig. 3. Functional diagram of the control process

The central link in the method of monitoring means control for information protection objects is a simulation model – a formalized process diagram, i.e. a formal description of the procedure for the functioning of a complex object in the system under study (Fig. 4). Other models in this diagram constitute the external mathematical support for the simulation process.

Input models provide the specification of certain values of input factors. Deterministic input models are arrays of values of constants, or functions $\alpha(t)$ depending on time t. Random input models are random number sensors (RNS) that simulate the specification of random influences. Due to the fact that the result of a single simulation cannot characterize the process as a whole, there is a need to analyze the results of multiple simulations, because due to the law of large numbers, statistical estimates of unknown parameters acquire statistical stability. The output model provides accumulation, processing and analysis

of a set of random results. For this purpose, multiple recalculation of the values of the output characteristic is organized at constant values of α and x (controlled variables) and different values of random factors y – "cycle by variable y". In this regard, the output model includes programs for planning the experiment, and in addition solves the problem of processing random values of the output characteristic, that is, reduces the problem to a deterministic one using the "averaging by result" method. The optimality criterion E_k is introduced into the proposed optimization model (Fig. 4) to find the optimal algorithm for controlling monitoring means of information protection objects. The optimality criterion for modeling can be the minimum expenditure of time or material resources (financial costs, energy consumption, etc.) when implementing automatic control of monitoring means of information protection objects.

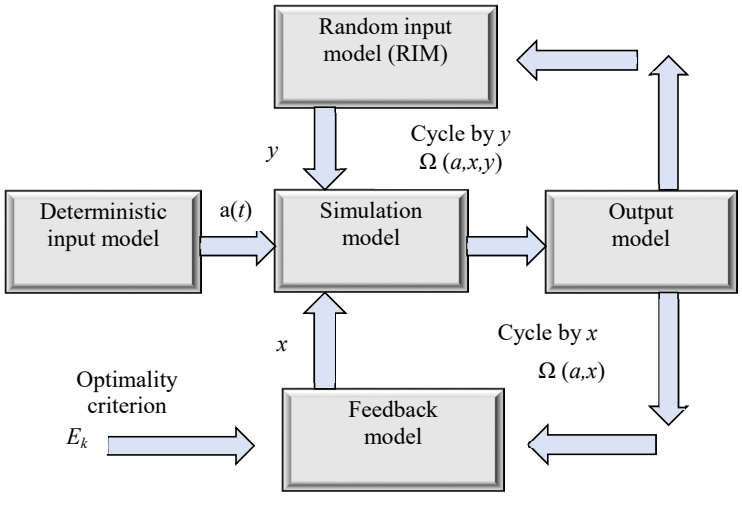

Fig. 4. Structure of the algorithm for modeling the functional diagram of the control process for an optimization model with random factors

The feedback model allows, based on the analysis of the obtained simulation results, to change the values of the controlled variables, implementing the strategic planning function of the simulation experiment. The operation of the feedback model depends on the selected optimality criterion E_k, since the function of implementing the strategic planning of the simulation experiment depends on it.

5. 2. Development of a simulation model for automatic control of protected objects monitoring

The simulation model reflects the sequence of elementary processes along the "modeling" time axis t^M, therefore, the process of functioning of an object over a time interval of duration T can be represented as a random sequence of discrete time moments t_i^M. At each of these moments, the states of the object elements change, and in the intervals between the moments of time t_i^M – not.

The implementation of the basic principles of system analysis and modeling makes it possible to formulate the basic provisions for constructing modeling algorithms.

Temporal modeling with a deterministic step (Δt principle), consisting of a set of repeatedly repeated actions:

– at the i-th step at time t_i^M; all elements are viewed and those that are changing their state at this moment are determined;

– all state changes occurring at a given time are modeled t_i^M;

– there is a transition to the (i+1)-th step, which is executed at time $t_{i+1}^M = t_i^M + \Delta t$.

This principle is the most universal, but uneconomical in terms of using computer time.

The accuracy of implementing a mathematical model on a computer through the prism of a set of different types of errors:

– modeling errors resulting from lack of awareness or inaccurate input data specification;

– modeling errors that arise when simplifying the initial mathematical model;

– errors in calculating the characteristics at the system output due to the discrete implementation of the mathematical model on a computer, including rounding errors;

– modeling errors due to the limitations of statistics during selective processing of statistical information or the limited number of random tests of the model in the computing device (simulation) environment.

Thus, an improved method of controlling monitoring means for information protection objects using elements of artificial intelligence systems is built on the implementation of:

– functional diagram of the control process (Fig. 3), where a control device is additionally introduced;

– structural diagram of the modeling algorithm (Fig. 4) for the optimization model with random factors.

The proposed method allows to form a control system for monitoring information protection objects, capable of automatically updating and expanding the existing database on the presence of characteristics of the impact on the protection object.

With some generalizations, the scheme shown in Fig. 1 may also be of interest for some interesting cases of automatic control of the organization of systems. It can also be successfully used in some cybernetic systems that automatically improve themselves in the process of their work.

Thus, it is proposed to develop in a direction that allows systems to better perform their functions, which is why they are called automatically self-learning systems, which are a very progressive form of cybernetic systems. Let's consider two examples:

1. Control scheme with a regulating device in the form of a self-learning system (Fig. 5).

In Fig. 5 it is indicated: CS – controlled system; x – regulated variable; SCS – self-improving cybernetic system, which consists of two blocks – K and F. The main block of the SCS – block K – a computing device that works as a regulating device. Block F – a regulation block that determines the parameters of the main block K. The SCS block can be considered a system with "artificial intelligence", since this block contains "learning" procedures to respond to new threats (channel characteristics) of information leakage.

Block F consists of two parts:

a) control block N, which receives information from a higher level: about the control variable w; about the deviation x_w of the controlled variable; about the correcting variable of the control block y; about the state variables of the digital control block K.

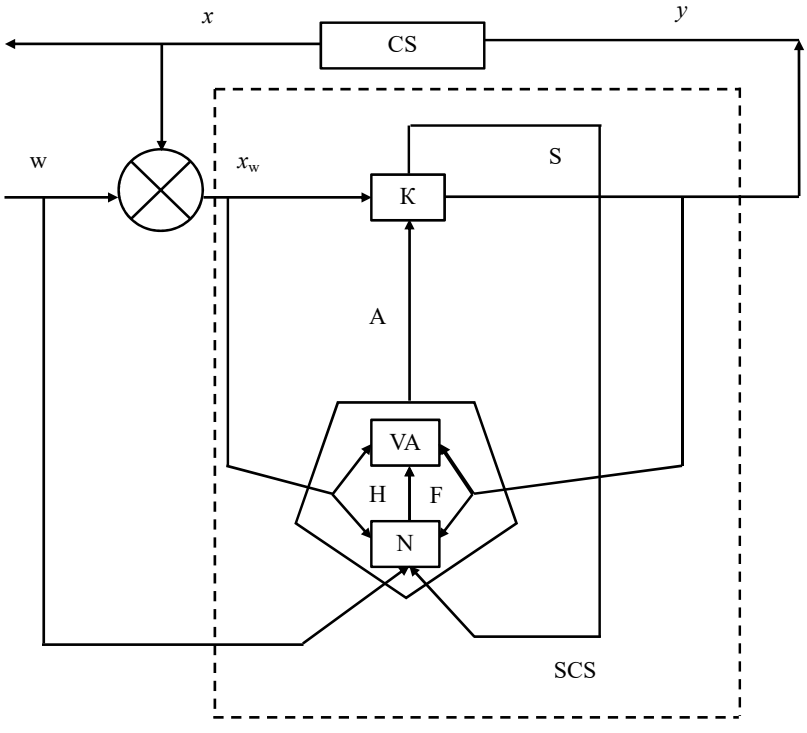

Fig. 5. Control scheme with a regulating device in the form of a self-learning system

Guided by the evaluation of this data, block N gives command H to block VA;

b) the task of the VA block is to select the most adequate one from the available algorithms for control. Based on the variables (x_w and y) entered into it and the command (direction, guiding command) H, this block selects the algorithm A, according to which the control block K – a digital computer – should operate. This scheme is interesting in that it contains a higher-level control block N, which evaluates the quality of the functioning of the block K.

It is assumed that the cybernetic system SCS operates cyclically. For example, the control block K operates according to a certain algorithm A_1. If its operation does not meet the requirements of the evaluation in the block N, then the corresponding command H is given, and the block VA selects another algorithm for the control block K in the next cycle. The results of using the algorithm A_2 are also evaluated by the block N, and depending on the result of this block, a new command H is generated and given. As a certain number of cycles are completed (after the completion of the self-learning stage), the digital control block K will probably work satisfactorily, and the block VA will no longer change its algorithm of operation. When conditions change, for example, when the command variable w changes over time, or when the parameters of the control system CS change, the block F again intervenes in the work, changing the algorithm A of the operation of the control block K.

2. The case (Fig. 6) when a self-improving cybernetic system, the organization of which is automatically regulated, is connected in parallel with the control block RU during the self-improvement period, but its parameters are not quantitatively determined. The control system (the CS control system and the control block RU) is here ready to be connected to the SCS system.

When the toggle switches are set to position 1, the control system operates normally. During this period, based on information about x_w and y_{RU}, as well as w, the development of the organization of the main block K, which was not organized properly at the beginning and is gradually improving, adapting to the performance of its functions in the future, is controlled by the regulating block F.

After switching the toggle switches to position 2, the functions of the control block RU are transferred to the main block and the control block is thus switched off. The main block K is not further improved, and the block F can be switched off. However, it is possible that the block K will continue to improve itself if it continues to be influenced by the block F, and then a situation similar to the previous case is created.

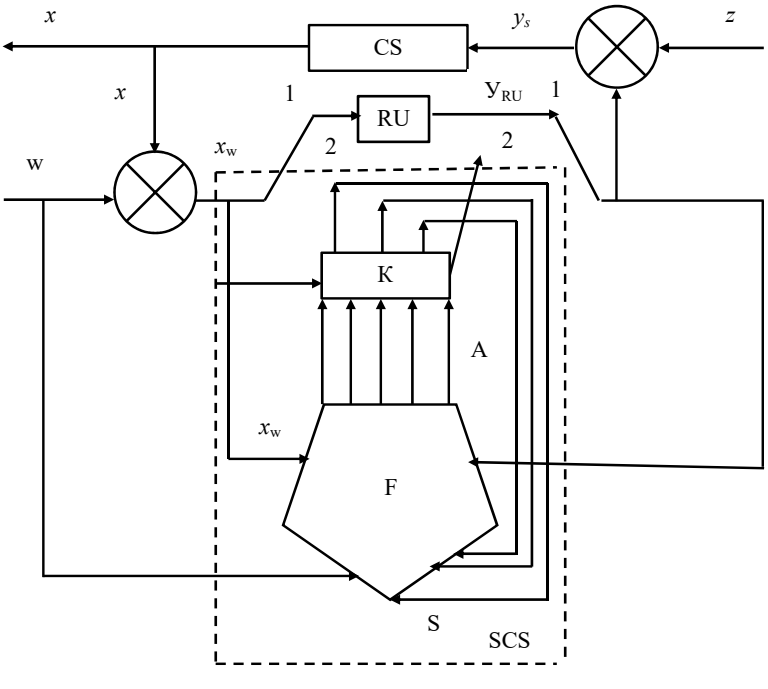

Fig. 6. Connection diagram of a self-improving cybernetic system in parallel with a regulating block

However, there is a significant difference here – the development of the block K is carried out during the preparatory period without including it in the control scheme, which facilitates the commissioning of the control system. The block K is included in the control scheme as a regulating device not earlier than the required basic parameters are achieved. This case has the advantage that in this way a copy of a well-organized and functioning device is created, without the need to study its dynamic characteristics in detail.

The basic scheme (Fig. 1) can also be used to explain other classical cybernetic systems, examples of which are the homeostat, the Farley and Clark system, the perceptron, etc. [1, 24, 25]. It can also be used to illustrate the connections in a new type of systems developed for automatic control of monitoring facilities for information protection [1, 24, 25].

Associative control devices (ACDs) implement the AI function of the developed model. The AI function consists in recognizing potential threats that can affect information protection objects. In the ACD, the AI function is presented as a set of technological tools and algorithms that provide information (forecasts, recommendations and possible solutions) on the existence of information leakage channels or channels of influence of potential threats on the protection object. The characteristics of potential threats to the information protection object for the purpose of establishing leakage channels are considered in more detail in the works [3, 25]. The ACD block that needs to be trained provides the selection of a control signal based on associations accumulated during the training process. The structural diagram of the ACD is shown in Fig. 7, where:

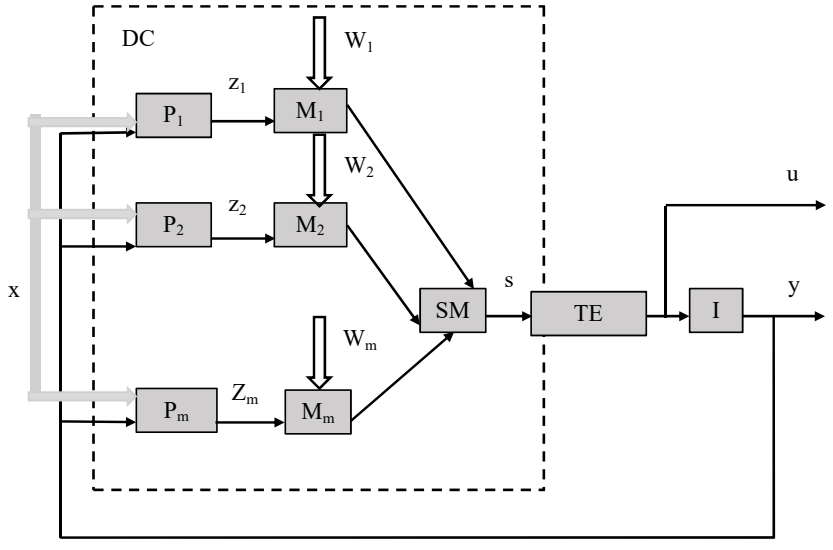

Fig. 7. Scheme of associative control of information protection object monitoring tools

– DC – dichotomous classifier, which divides the space of input signals belonging to different classes;

– P_1, P_2,..., P_m – preprocessors that map the extended inverse feedback signal y of the observed situation vector X into the rectification space Z;

– M1, M2,..., M_m – multiplication chains that multiply the components of the directed space vector z_i by the components of the normal vector to the separating hyperplane W_i;

– SM – adder;

– TE – threshold element, which corresponds to the negative value of the variable s the output signal with the level "–1", and to the positive value – "+1";

– I – integrator, which ensures the change in the value of the control signal *y* according to the results of the remote control operation;

– *X* – vector of input signals that encodes the state of the control situation;

– y – control signal;

– u – binary control signal;

– s – a signal that characterizes the direction and magnitude of the deviation of an image point in Euclidean space from the separating hyperplane.

The basis of the ACD is a dichotomous classifier that assigns the observed image vector to one of two classes. It performs this task according to the rule:

$$x \in \begin{cases} X_1, \psi(x) > 0, \\ X_2, \psi(x) < 0, \end{cases} \quad (1)$$

where X_1, X_2 – half-spaces of feature space *X*, containing vectors of observed features of the first and second classes, respectively (1); $\psi(x)$ – solving rule (parting surface).

The task of learning ACP is reduced to determining the solution rule $\psi(x)$ on a sample intended for training, the elements of which are image vectors x_j, for which there is a priori information about their belonging to a particular class.

Almost all known learning algorithms are based on the principle [12] that the solution rule can be represented as a finite number of terms of the expansion of the separating function in a series according to a system of orthogonal functions:

$$\psi(x) = W\phi(x), \quad (2)$$

where *W* – vector of weight coefficients; $\psi(x)$ – vector of a system of orthogonal functions.

Such important characteristics of a classifier as recognition ability, convergence speed, reliability and predictive ability [2] are determined by the choice of a system of orthogonal functions. Thus, in the case of $\psi(x)=x$ it is possible to obtain a linear classifier (or linear threshold element), in the case of choosing the function parameterization $\psi(x)$ using piecewise linear approximation, it is possible to obtain a piecewise linear classifier of the perceptron type, in the case of direct use of the system of orthogonal functions, there is a learning Φ-machine [2, 24], which has the greatest capabilities for qualitative image classification.

For further study, it is convenient to present the dichotomous classifier as composed of two serially connected parts: a preprocessor and a threshold logic element (TLE). The processor performs calculations according to the formula:

$$z_i = \phi_i(x), \quad (3)$$

where z_i – components of the image vector in the rectifiable space *Z*.

The threshold logic element performs the separation of images in the directed space *Z* according to the rule:

$$z \in \begin{cases} x_1, W \cdot z > 0, \\ x_2, W \cdot z < 0, \end{cases} \quad (4)$$

where $W{\cdot}z$ – separating hyperplane; *W* – normal vector to the dividing hyperplane.

Thus, training a classifier to divide observed images into two classes (4) based on a training sample reduces to solving two problems:

1) defining functions $\varphi_i(x)$, implemented by the preprocessor;

2) definition of the normal vector W, implemented by TLE.

To solve the first problem, various approaches can be used: stochastic approximation, Bayesian learning, potential function methods, nearest neighbors, generalized portrait, etc. [7, 12, 15, 18].

The second problem should be solved using the error-correction learning method, which is discussed in almost all publications that consider the process of pattern recognition [11, 17]. This method ensures the convergence of the learning process for an arbitrary linearly separable data set. The idea of the method is to provide a mapping of the separating hyperplane from the incorrectly classified point [4]. From dependence (3) it follows that the algebraic sign of the scalar product of the weight vector W by the image vector in the directed space Z:

$$W \cdot z = s, \tag{5}$$

indicates on which side of the solution hyperplane the point representing the image is located.

In the first step of the learning process, the normal vector is taken $W=K$, where K is obtained as a result of solving the problem of determining $\varphi_i(x)$. Next, the sequential review of the elements of the training sample begins. When at the k-th step the image x^k, entered by TLE not in the class to which it belongs, mining $W \times z^k$ has an algebraic sign opposite to the desired one. Therefore, it is necessary to adjust the weight vector according to the requirements of the training sample. Such a corrected vector is denoted by W'. The requirement for such a vector is that its product with the image vector $W \cdot z = \varpi\,(\varpi = -\varpi)$ acquired the opposite sign compared to the sign of the misclassification. To increase the convergence of the learning process, the new weight vector is calculated by the formula:

$$W' = W + \Delta W. \tag{6}$$

Combining dependencies (5) and (6), the equation is calculated:

$$(W + \Delta W) z^k = -\varpi, \tag{7}$$

which solution is the correction to the vector W:

$$\Delta W = -\frac{2\varpi}{z^k \cdot z^k} z^k. \tag{8}$$

The method for solving the first problem is as follows: defining functions $\varphi_i(x)$ mapping of image vectors x into the rectification space Z, is based on the following considerations. Let, at the request of the input signal (image vector) $x \in X$ it is necessary to decide what sign the output signal ϖ should have. Otherwise, it is necessary to divide the image space X into two regions X_1 and X_2 so that in the case $x \in X_1$, then the signal $\varpi > 0$, if $x \in X_2$, then the signal $\varpi < 0$. So, as in the previous case, the problem is reduced to dividing the space X into two subspaces X_1 and X_2. Only in this case, not a dividing hyperplane is obtained, but a dividing hypersurface, which must then be refined using a draining sample (at the same time performing the functions of controlling the learning of the ACD).

The solution to the problem can be obtained using methods of statistical decision theory [4]. These methods are reduced to the following two main ones:

1. The conditional probability densities of the type $p(x|\omega_1)$ i $p(x|\omega_2)$ are estimated from the sample, which are then used to estimate the probability that the signal x belongs to a particular subspace of the space X.

2. An assumption is made about the shape and parameters of the boundaries of the solution domains, then the parameters are adjusted according to the gradient of the quality criterion in order to achieve its extremum.

The first method is more versatile. According to the theory of statistical decisions, it is recommended to assign signal x to class ω_1, if the posterior probability for this class is maximum: $p(x|\omega_1) \geq p(x|\omega_2)$. This rule ensures a minimum probability of incorrect division of space X into two subspaces X_1 and X_2.

Since the posterior probabilities are unknown a priori, Bayes' formula is applicable to their calculation [19, 24]:

$$P(\omega_i|x) = \frac{P(\omega_i)\, p(x|\omega_i)}{p(x)},$$

where $p(\omega_i)$ – a priori probability of presenting an image belonging to the class w; $p(x|\omega_i)$, $p(x)$ – conditional and unconditional density distribution of a value x.

Values $p(\omega_i)$, $p(x|\omega_i)$, $p(x)$ are calculated from training samples:

$$x_{ik(i)} = \left\{ x_{ik(i)} : i = 1,2; k(i) = 1,2,..,k_i \right\}.$$

Thus, the classification rule will look like this – if:

$$\frac{P(\omega_1)\, p(x|\omega_1)}{p(x)} > \frac{P(\omega_2)\, p(x|\omega_2)}{p(x)},$$

then the observed object $x \in X_1$.

If the occurrence of an arbitrary class $[p(\omega_1)=p(\omega_2)]$ is equally likely, then the classification rule is written more simply: $p(x|\omega_1) \geq p(x|\omega_2)$.

Therefore, to implement the solving rule, it is necessary to determine the conditional probability densities $p(x|\omega_i)$ from the training samples.

Since $p(x|\omega_i)$ are unknown a priori, then the only way to solve the problem is to approximate these densities by certain densities with simple sufficient statistics. For this purpose, the approximation is used $p(x|\omega_i)$ by the sum of Gaussian densities.

This approximation performs the division of areas X_1 and X_2 of the space X into regions x_{1i} and x_{2i}, that are characterized by the fact that within them the distribution of a random vector x is a multivariate normal distribution. This process has much in common with the partitioning of the feature space into clusters when synthesizing piecewise linear classifier algorithms, as well as with the Lagrange interpolation polynomial [4].

Significant analogies are seen with the method of potential functions [2], when an exponential function of the form is chosen as the system of orthogonal functions $e^{-\alpha R^2}$.

To simplify the computational procedures, it is assumed that multidimensional Gaussian densities have independent random variables, and the variances of all random variables are equal to each other. Taking into account these assumptions:

$$p(x|\omega_i) = Q \sum_{a=1}^{A} K_{ia}\, p_{ia}(x),$$

where:

$$p_{ia}(x) = \frac{1}{\left(\sqrt{2\pi}\sigma\right)^L} e^{\frac{1}{2\sigma^2}(x - M_{ia})^T (x - M_{ia})}, \tag{9}$$

M_{ia} – mathematical expectation of the a-th component of the Gaussian density of the class ω_i; L – measure of distribution; Q – normalizing factor.

Used in the formula sufficient statistics K_{ia} and M_{ia} are determined from the training sample using a stepwise adaptive procedure, which, although it does not give optimal values, is practically suitable and expedient. Since it provides a satisfactory approximation by simple means under the condition of a small volume of the training sample.

The procedure boils down to the following four steps in sequence:

1. The first element of the training sample is introduced. Let it belong to the class ω_1. Let's create the first subclass of the class ω_1 with conditional distribution density

$$2.\ p\left(x\left|\omega_1\right.\right)=K_{11}p_{11}=\frac{K_{11}}{\left(\sqrt{2\pi}\sigma\right)^L}e^{\frac{1}{2\sigma^2}\left(x-M_{11}\right)^T\left(x-M_{11}\right)},$$

where $M_{11}^1=x_{11}$; $K_{11}^1=1$.

3. Let's introduce the second element of the training sample, which also belongs to the class ω_1. Checking the condition $\left|x_{12}-M_{11}^1\right|\le T$.

4. If the condition of the second point is met, then the parameters of the first subclass ω_1 are specified by formulas:

$$M_{11}^2=\frac{x_{12}+1\cdot M_{11}^1}{2},\ \ K_{11}^2=K_{11}^1+1.$$

If the condition of point 2 is not fulfilled, then the second subclass of the first class is formed:

$$p\left(x\left|\omega_2\right.\right)=K_{12}p_{12}=\frac{K_{12}}{\left(\sqrt{2\pi}\sigma\right)^L}e^{\frac{1}{2\sigma^2}\left(x-M_{12}\right)^T\left(x-M_{12}\right)},$$

where $M_{12}^1=x_{12}$; $K_{12}^1=1$.

Thus, the sequential refinement of the Gaussian distribution parameters of each subclass is performed based on the training sample according to the formulas:

$$M_{ia}^{\nu}=\frac{x_{ia}+\left(\nu-1\right)\cdot M_{ia}^{\nu-1}}{2},\qquad(10)$$

$$K_{ia}^{\nu}=K_{ia}^{\nu-1}+1.\qquad(11)$$

From the above it follows that the output signal of the dichotomous ACD classifier must function in accordance with the algorithm:

$$u=\operatorname{sign}\left[\begin{array}{l}\frac{1}{N_1}\sum_{a=1}^{A}K_{1a}\phi_{1a}\left(x,M_{1a}\right)-\\-\frac{1}{N_2}\sum_{a=1}^{A}K_{2b}\phi_{2b}\left(x,M_{2b}\right)\end{array}\right],\qquad(12)$$

where:

$$\phi_{1a}\left(x,M_{1a}\right)=e^{\frac{1}{2\sigma^2}}\sum_{j=1}^{A}\left(x_j-Mj_{1a}\right)^2;$$

$$\phi_{2b}\left(x,M_{2b}\right)=e^{\frac{1}{2\sigma^2}}\sum_{j=1}^{B}\left(x_j-Mj_{2b}\right)^2.$$

According to algorithm (12), the input image will be assigned by the classifier to the first class when the variable u=+1, and to the second, when the variable u=–1. The functions implemented by the preprocessor are completely defined by expression (9) and the parameters M_{1a} and M_{1b}, calculated from the training samples according to formula (10). The initial value of the normal vector of the separating hypersurface (5) is calculated from the training sample according to formula (11).

The proposed algorithm (12), when implemented as a complex of universal subroutines, can be reduced to a dichotomous automatic classification of recognition patterns of potential threats to the information protection object.

Let's limit ourselves to considering a control object, the mathematical model of which has the form of a system of time-invariant differential equations:

$$\dot{x}_1=x_2,\dot{x}_2=u,\qquad(13)$$

where $\left|u\left(t\right)\le1\right|,t_0\le t\le T$.

Thus, the proposed model can be used in the method of controlling monitoring means for information protection objects.

5. 3. Definition of the structure of the method of automatic control of information protection object monitoring means and the algorithm of its application

Modern control objects have quite complex mathematical models, characterized by the presence of many variables, cross-connections, nonlinearities, variability and uncertainty of parameters. It is known that for such systems, methods for constructing optimal control systems in most practically important cases allow obtaining only open-loop controls. In real systems, systems with inverse feedback are preferred. Therefore, the current task is to develop such methods that allow, based on a finite number of trajectories of optimal system behavior and the corresponding optimal controls, to create an algorithm for the functioning of a closed system. Therefore, it is proposed to consider one of the possible variants of such a technique, based on a two-stage procedure. At the first stage, optimal open controls are calculated and based on them, a training and control sequence of data pairs "observed state of the system - corresponding optimal control" is compiled. At the second stage, a control sequence is obtained for use in an automatic classifier of existing threats to information protection objects with the separation of the entire space of states of the monitoring system, each corresponding to its own optimal level of the control signal.

This method is used in the control of monitoring facilities for information protection objects. The algorithm for applying the optimal control synthesis method is as follows:

1. Select a subset of the initial conditions of the initial and control sample trajectories from the full set of initial conditions.

2. Calculate optimal controls for an open system and their corresponding optimal trajectories for each element of the subset.

3. Quantize the area of state space of interest and identify the control with hypercubes through which the computed trajectories pass; create a training and control sequence.

4. Train an automatic classifier using training and control sequences.

The application of the specified stages for the synthesis of a closed-loop control system with optimal speed is considered. This example reveals the possibilities of the control method and the problems that still need to be solved.

In this case, the restrictions apply to the control object, the mathematical model of which has the form of a system of time-invariant differential equations (13).

The control law is obtained, which translates the control system (13) from the initial one $x(0)$ to the final state $x(T)$ in minimum time.

For this purpose, a program for modeling the dichotomous classifier of an associative control device and the process of training this device has been developed. The program consists of two subroutines AUU (AV, AK, X, UM, L, M, D, U) and LEARN (X, Y, L, N, AK, AM, J).

The LEARN subroutine uses a multi-step adaptive procedure for approximating the posterior conditional density by the sum of Gaussian densities. During the program operation, calculations are performed using formulas (10), (11) and logical analysis of the training sample entered into the subroutine from the main program. The output parameters of the subroutine are an array of average values of Gaussian densities (potential functions) of subclasses AM(I,J): an array of weight coefficients AK(J) and the number of subclasses J formed during the training process. The subroutine uses as input parameters an array of elements of the training sequence X(I,K), where I is the element number in the state vector x, K is the element number in the training sample; an array indicating the belonging of the elements of the training sequence to a particular class Y (the variable Y can take two values "+1" or "–1"); indications about the dimension of the state vector x are given by the constant L; the number of elements contained in the training sample is represented by the integer constant N; the standard deviation of the Gaussian conditional density variables is given by the variable D. The following intermediate variables are used in the calculations: Q – variance of the elementary Gaussian distribution; R – square of the distance of the training sample element from the average subclass; P – subclass number; $N1$ – number of training sample elements belonging to the first class; $N2$ – number of training sample elements belonging to the second class; M – number of subclasses prepared as a result of training on the sample. The text of the LEARN subroutine is implemented in the FORTRAN engineering computing language environment.

The AUU subroutine calculates the control influence according to formula (12). The output parameter of the subroutine is the control signal U. As input parameters, the program uses: an array of average values of potential functions of subclasses (Gaussian components of the posterior conditional density distribution) AM(I,J); an array of weight coefficients of potential functions of subclasses (initial values of the vector W) AK(J); the current state vector of the automatic control system X(I); the maximum value of the control influence UM; the dimension of the state vector L; the number of subclasses formed in the learning process M; the standard deviation of the Gaussian conditional densities is given by the variable D. The following intermediate variables are used in the calculations: I – running number of the element in vector X of the array AM; J – running number of the subclass; ARG – square of the difference between vectors X and AM; $POT1$ – potential of the first class; $POT2$ – potential of the second class; $N1$ – running number of subclasses in the first class; $N2$ – running number of subclasses in the second class.

The procedure for refining the components of the vector of weight coefficients of potential functions operates in the case of the need to train the TLE using the software described in [26].

The optimal speed-optimized feedback controller is represented in the state space by a surface that divides the state space into two regions according to the control mode. This surface is determined by synthesis and implemented by the control system's computer. In most cases, obtaining such a dividing surface analytically or geometrically is impossible. In the described approach, such a surface is implicitly given by the sequence being learned.

The size of the training sequence and the subsequent accuracy of the training depends on the number of quantization levels along each coordinate axis. However, the complexity of the training process also depends on this.

In the conditions of such a contradiction, a compromise solution is calculated. At present, the theory of learning does not give any recommendations. Perhaps, further research in this area will allow to find such a solution to the problem, when determining the number of quantization levels will be one of the components of the general learning problem.

For example, a dense urban area in the form of a square of four to five apartment buildings (entrances to the building) is considered. The total number of apartments in this case is 20. Similarly, a corresponding area of twenty offices around can be considered for an office center building. According to the modeling conditions, it is assumed that each of the rooms contains a GSM receiver/transmitter for wireless information transmission (mobile phone). In the center of the area under consideration (in the form of a square), there is an information protection object (Wi-Fi router), the information transmission process of which is influenced by the wireless channels of GSM receivers/transmitters (in all rooms). The influence of wireless channels of GSM receivers/transmitters on the object of information protection is considered as a potential threat in the modeling. The main parameters of wireless data transmission systems and their possible influence on the object of information protection are given in [27]. To illustrate the example, the quantization is performed quite arbitrarily: the region of the state space of interest is divided along each of the coordinate axes into ten levels to the right and left of the origin. These ten levels characterize the signal power levels of wireless channels of GSM receivers/transmitters - potential threats to the object of information protection. Then, according to the quantization of the state space, the full set of initial conditions is 400 (20 rooms of 10 levels each to the right and left of the information protection object). Calculating such a large number of optimal trajectories is a complex and cumbersome task. Obtaining a training sequence will be even more difficult. Based on the recommendations obtained for pattern recognition systems, a subset of initial states was taken, which consists of twenty elements (GSM receivers/transmitters), which are arbitrarily selected points inside the square (Wi-Fi router).

To calculate the optimal controls and trajectories of an open system, it is proposed to use various methods specified in [2]. To solve the problem, the method of iteration of control devices is used.

The convenience of this method is that the solution of the boundary value problem is reduced to the solution of two single-point boundary value problems. This allows to reduce the sensitivity of the solution of the optimization

problem to the non-idealities of the computational process. One of the main difficulties in solving the problem is the choice of weight coefficients when determining the variation of the control influence. When modeling, the value of the weight coefficients is calculated using analytical relations for the coefficients of information and internal availability of the wireless radio channel, which were obtained in [27].

After determining the optimal controls and trajectories, a training sequence is formed. The coordinates of the centers of the squares formed as a result of quantization of the state space and the corresponding optimal controls are selected as the elements of the sequence. From the entire set of elements suitable for forming the training sequence, 10 squares with control +1 and 10 squares with control – 1 are selected. The selection is made randomly. Thus, the number of elements of the initial sequence is 5 % of the number of elements of the entire set of admissible states.

6. Discussion of the results of developing a method for automatic control of monitoring means for information protection objects

The research proposes the results of the development of a method for automatic control of information protection object monitoring means. The developed method is based on the proposed functional diagram of the control process (Fig. 3) and the structural diagram of the modeling algorithm (Fig. 4) for the optimization model with random factors and formula (12). Formula (12) allows to determine the algorithm of operation of the associative control device by means of monitoring information protection object monitoring.

A feature of the proposed method is the developed simulation model – a formalized scheme of the process of controlling the means of monitoring information protection objects (Fig. 4). In this case, the use of associative control devices that need to be trained is proposed. Such devices provide sampling of the control signal according to the associations that accumulate during the training process (Fig. 7). That is, the advantage of this study is the involvement of artificial intelligence in monitoring information protection objects in order to timely detect new threats to leakage channels. Compared with previous studies, where a method for synthesizing an automated decision support system for information leakage [3] was proposed, this study allows to determine the procedure for controlling threat monitoring tools for such a system. That is, this study is a development of previous studies, the results of which are reflected in [1, 3]. for making a well-founded decision. The advantage of this study compared to the work [6], where 15 existing cybersecurity indices were studied, is the development of associative control devices that provide knowledge accumulation in the process of learning about the threats of information leakage to the object of protection. The advantage of this study compared to the work [11], which considered the manual monitoring method and the automatic active monitoring method of hazard determination, is the use of artificial intelligence for threat monitoring. This allows to improve the quality of detection of threats of information leakage to the object of protection and to take into account possible changes in the characteristics of new (promising) channels of information leakage.

The limitations of this study are the set of statistical data on the characteristics of threats that cause a possible information leak of protected objects. To form an adequate set of such data, it is necessary to analyze the array of statistical samples of possible threats [25]. At the same time, the study proposed a step-by-step adaptive procedure that does not give optimal values, but provides a satisfactory approximation under the condition of a small volume of the training sample regarding possible threats of information leakage of protected objects.

The disadvantages of this study are the assumption made about the technical serviceability of the information protection object and its components in terms of preventing data leakage. At the same time, the study assumes that the probability of detecting the threat of information leakage to the protection object by monitoring means is equal to one, which should also be attributed to the disadvantages of the presented study.

The development of this research consists in developing algorithms for the operation of an artificial intelligence system for learning to predict the emergence of new (promising) threats to information leakage to the object of protection. However, such research may encounter the problem of collecting statistical data on the threats of information leakage channels to verify the adequacy of the proposed algorithms.

7. Conclusions

1. A functional scheme for automatic control of monitoring of protected objects has been developed. A feature of the proposed scheme is a moderate approach to the control process, which allows decomposing the control algorithm and introducing into consideration an intermediate stage of study (monitoring) – formulation of the control goal. Formulating the control goal of monitoring means (timely detection of information leakage channels) using the algorithm, the system translates its needs into the language of the states of the information protection object. This allows the monitoring means control system to transfer the procedure for synthesis and implementation of control decisions regarding the detection of information leakage channels. At the second stage, a control solution is determined that ensures the achievement of the goal of the monitoring means control system – securing the information leakage channels. It is proposed to introduce the principles of cybernetics (mathematical algorithms of the artificial intelligence procedure) into the operation of the control device of the automatic control scheme for monitoring protection objects. This allows to train the system to respond to new threats.

2. A simulation model of automatic control of monitoring of protected objects has been developed. A feature of the proposed model is the algorithm for functioning and training of associative control devices, developed using the method of solving the inverse problem of restoring functional dependencies from empirical data. The algorithm is presented in the form of a set of universal subroutines suitable for use in solving a wide class of

control, monitoring and decision-making tasks, which can be reduced to dichotomous automatic classification of recognition patterns.

3. The structure of the method of automatic control of means of monitoring information protection objects and the algorithm of its application are determined. The control is based on the compilation of a training (initial) sequence. The elements of such a sequence allow to choose the appropriate optimal controls of means of monitoring threats to information protection objects for prompt (timely) and reliable detection of possible channels of information leakage and their securing.

Conflict of interest

The authors declare that they have no conflict of interest regarding this study, including financial, personal, authorship, or other, that could influence the study and its results presented in this article.

Financing

The study was conducted without financial support.

Data availability

The manuscript has no associated data.

Use of artificial intelligence

The authors confirm that they did not use artificial intelligence technologies when creating the presented work.

References

1. Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M., Hrytsyk, V., Milov, O. et al.; Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M. (Eds.) (2022). Modeling of security systems for critical infrastructure facilities. Kharkiv: PC TECHNOLOGY CENTER, 196. https://doi.org/10.15587/978-617-7319-57-2
2. Balitskyi, N., Ivanyk, E., Bolkot, P., Ilkiv, I., Smychok, V., Vankevych, P. (2022). Adaptation of extreme planning methodology to optimize the functioning of training simulators for personnel of the army land divisions. The scientific heritage, 1 (83 (83)), 29–32. https://doi.org/10.33577/2312-4458.23.2020.79-85
3. Shmatko, O., Herasymov, S., Lysetskyi, Y., Yevseiev, S., Sievierinov, O., Voitko, T. et al. (2023). Development of the automated decision-making system synthesis method in the management of information security channels. Eastern-European Journal of Enterprise Technologies, 6 (9 (126)), 39–49. https://doi.org/10.15587/1729-4061.2023.293511
4. Koshevoy, N. D., Kostenko, E. M., Pavlyk, A. V., Koshevaya, I. I., Rozhnova, T. G. (2019). Research of multiple plans in multi-factor experiments with a minimum number of transitions of levels of factors. Radio Electronics, Computer Science, Control, 2, 53–59. https://doi.org/10.15588/1607-3274-2019-2-6
5. Prabu, A. V., Kumar, G. S., Rajasoundaran, S., Malla, P. P., Routray, S., Mukherjee, A. (2021). Internet of things-based deeply proficient monitoring and protection system for crop field. Expert Systems, 39 (5). https://doi.org/10.1111/exsy.12876
6. Khudyntsev, M., Lebid, O., Bychenok, M., Zhylin, A., Davydiuk, A. (2023). Network Monitoring Index in the Information Security Management System of Critical Information Infrastructure Objects. Information and Communication Technologies and Sustainable Development, 270–290. https://doi.org/10.1007/978-3-031-46880-3_17
7. Li, Z., Lin, Q., Wu, Y.-C., Ng, D. W. K., Nallanathan, A. (2024). Enhancing Physical Layer Security With RIS Under Multi-Antenna Eavesdroppers and Spatially Correlated Channel Uncertainties. IEEE Transactions on Communications, 72 (3), 1532–1547. https://doi.org/10.1109/tcomm.2023.3333919
8. Mizuno, T., Nishikawa, H., Kong, X., Tomiyama, H. (2023). Empirical analysis of power side-channel leakage of high-level synthesis designed AES circuits. International Journal of Reconfigurable and Embedded Systems (IJRES), 12 (3), 305. https://doi.org/10.11591/ijres.v12.i3.pp305-319
9. Sun, Q., Liu, X., Sun, Y., Wang, M., Han, X., Chen, X. (2021). A Security Wireless Monitoring and Automatic Protection System for CCEL. Wireless Communications and Mobile Computing, 2021 (1). https://doi.org/10.1155/2021/6652246
10. Qiu, X., Yu, J., Zhuang, W., Li, G., Sun, X. (2023). Channel Prediction-Based Security Authentication for Artificial Intelligence of Things. Sensors, 23 (15), 6711. https://doi.org/10.3390/s23156711
11. Marumoto, K., Suzuki, N., Shibata, Y., Takeuchi, A., Takami, A., Yamakawa, A. et al. (2024). Comparison between a manual monitoring method based on active sampling and an automatic active monitoring method at urban and rural sites: Toward the accumulation of comparable data for effectiveness evaluation of the Minamata Convention. Environmental Monitoring and Contaminants Research, 4, 55–68. https://doi.org/10.5985/emcr.20230015
12. Culbreth, S., Graham, S. (2023). Demonstrating Redundancy Advantages of a Three-Channel Communication Protocol. International Conference on Cyber Warfare and Security, 18 (1), 513–522. https://doi.org/10.34190/iccws.18.1.964
13. Ramos Luna, J. P., Ibarra Villegas, F. J., Pérez Wences, C. (2024). Automatic method for collecting and monitoring fault codes in industrial processes guided by PLCs. Revista de Ciencias Tecnológicas, 7 (3), e361. https://doi.org/10.37636/recit.v7n3e361
14. Marabissi, D., Abrardo, A., Mucchi, L. (2023). A new framework for Physical Layer Security in HetNets based on Radio Resource Allocation and Reinforcement Learning. Mobile Networks and Applications, 28 (4), 1473–1481. https://doi.org/10.1007/s11036-023-02149-z

15. Díaz, Á., Kaschel, H. (2023). Scalable Electronic Health Record Management System Using a Dual-Channel Blockchain Hyperledger Fabric. Systems, 11 (7), 346. https://doi.org/10.3390/systems11070346
16. Wang, L., Zhang, X., Bai, C., Xie, H., Li, J., Ge, J. et al. (2024). Rapid automatic multiple moving objects detection method based on feature extraction from images with non-sidereal tracking. Monthly Notices of the Royal Astronomical Society, 534 (1), 385–399. https://doi.org/10.1093/mnras/stae2073
17. Fedushko, S., Molodetska, K., Syerov, Y. (2023). Analytical method to improve the decision-making criteria approach in managing digital social channels. Heliyon, 9 (6), e16828. https://doi.org/10.1016/j.heliyon.2023.e16828
18. Herasymov, S., Tkachov, A., Bazarnyi, S. (2024). Complex method of determining the location of social network agents in the interests of information operations. Advanced Information Systems, 8 (1), 31–36. https://doi.org/10.20998/2522-9052.2024.1.04
19. Wen, Y., Wang, M., Wang, G., Ariyachandra, M., Brilakis, I., Xiao, L. (2024). An Integrated Solution for Automatic 3D Object-based Information Retrieval. Apollo - University of Cambridge Repository. https://doi.org/10.17863/CAM.107961
20. Huang, R. (2024). Protection of Personal Information of Workers under Algorithmic Monitoring. Communications in Humanities Research, 33 (1), 198–204. https://doi.org/10.54254/2753-7064/33/20240094
21. Mookerjee, R., Samuel, J. (2023). Managing the security of information systems with partially observable vulnerability. Production and Operations Management, 32 (9), 2902–2920. https://doi.org/10.1111/poms.14015
22. Nguyen, T. B. D., Le, V. H., Tran, D. C. (2023). Safety Warnings for Technical Status of Port Structure by Automatic Monitoring in Vietnam. Proceedings of the 4th International Conference on Sustainability in Civil Engineering, 665–672. https://doi.org/10.1007/978-981-99-2345-8_68
23. Abba, S., Bizi, A. M., Lee, J.-A., Bakouri, S., Crespo, M. L. (2024). Real-time object detection, tracking, and monitoring framework for security surveillance systems. Heliyon, 10 (15), e34922. https://doi.org/10.1016/j.heliyon.2024.e34922
24. Yevseiev, S., Kuznietsov, O., Herasimov, S., Horielyshev, S., Karlov, A., Kovalov, I. et al. (2021). Development of an optimization method for measuring the Doppler frequency of a packet taking into account the fluctuations of the initial phases of its radio pulses. Eastern-European Journal of Enterprise Technologies, 2 (9 (110)), 6–15. https://doi.org/10.15587/1729-4061.2021.229221
25. Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O., Korol, O., Milevskyi, S. et al.; Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O. (Eds.) (2021). Synergy of building cybersecurity systems. Kharkiv: PC TECHNOLOGY CENTER, 188. https://doi.org/10.15587/978-617-7319-31-2
26. Derevickiy, D. P., Fradkov, A. L. (1981). Prikladnaya teoriya diskretnyh adaptivnyh sistem upravleniya. Moscow: Nauka, 215.
27. Yevseiev, S., Milevskyi, S., Sokol, V., Yemanov, V., Volobuiev, A., Dakova, L. et al. (2024). Development of functionality principles for the automated data transmission system through wireless communication channels to ensure information protection. Information and Controlling System, 4 (9 (130)), 18–33. https://doi.org/10.15587/1729-4061.2024.310547