UDC 004.056 **doi: 10.26906/SUNZ.2025.2.185-194**

Ievgen Samborskyi[1], Yevhen Peleshok[2]

[1] State University “Kyiv Aviation Institute”, Kyiv, Ukraine
[2] Research Institute of Military Intelligence, Kyiv, Ukraine

SYNTHESIS OF LOGICAL-DYNAMIC INFORMATION AND EVENT MANAGEMENT SYSTEMS FOR COMPUTER SECURITY STRUCTURES

Abstract. The article considers one of the possible approaches to solving a relevant scientific problem dedicated to the synthesis of logical-dynamic information and event management systems for the security of computer structures. An analysis of modern approaches to the creation of an integrated management system has been made, the implementation of which will allow for effective management of information arrays of security events in the conditions of changed threats to computer structures. Special attention is paid to the development of models that combine logical and dynamic aspects of management, which allow ensuring high adaptability and functional stability of computer structures in the conditions of intensification of security event activity. The implementation of such an approach will allow to automatically respond to these events, optimize the processes of detecting and eliminating the consequences of threats, as well as ensure the constant stability of the operation of computer structures. The article proposes a method for synthesizing a logical-dynamic model that synergizes not only technical, but also organizational-cybernetic aspects of the security of computer structures. The developed approaches can be recommended for use in creating more effective and secure computer tools capable of withstanding various incidents.

Keywords: control system, logical-dynamic system, information security, security event, synthesis, analysis, theory of logical-dynamic systems, computer structure, incident, array of security events.

Introduction

Statement of the problem. Modern computer structures (systems, networks), especially critical infrastructure objects, are constantly under the influence of numerous threats to the security of their functioning. This situation requires the constant creation of effective methods for managing information and security events of these computer structures. Traditional approaches to monitoring, analyzing and compensating for the destructive consequences of security events (incidents), as a rule, are often not effective enough due to the growing complexity of these information infrastructures, the high level of dynamism of threats and the need for a quick response to their unauthorized effects. A quick response to threats is possible due to the optimal adaptation of computer structures to security situations, which is possible in the case of implementing control processes of these programmable means using new approaches based on the theory of logical-dynamic systems. Control systems synthesized using this theory allow combining formal analysis methods with adaptive control algorithms, which will provide automated detection, assessment, and optimal response to security incidents. However, there are a number of unsolved problems associated with the synthesis of such systems. These problems are related to the formalization of logical-dynamic models in incident analysis, the development of algorithms for adaptive response to security events, and the flexible integration of such systems into modern computer infrastructures. Thus, the scientific and applied task of synthesizing logical-dynamic information and security event management systems arises, which requires the development of new models, methods, and algorithms to increase the level of security, interference, and functional stability of computer structures.

Analysis of recent research and publications. The analysis of the results of scientific research, which are reflected in the latest scientific publications, conducted by the authors, shows that the process of information and security event management should be organized using the theory of logical-dynamic systems. This theory allows you to model and analyze the behavior of large organizational complex systems, which are computer structures, and to take into account the features of logical and dynamic processes in these electronic computing devices. Such an approach will contribute to more effective detection and optimal response to threats in modern and promising information infrastructures.

To understand the role and place of the theory of logical-dynamic systems, let us consider a number of scientific works that outline theoretical and practical aspects of systemic approaches to organizing information security management of a computer structure, and methods for synthesizing information management systems and security events in these complex information structures.

The basic principles of systems theory and the methodology of scientific research, which are the foundations of a systems approach to information security management as a complex logical-dynamic process are set out in [1]. The scientific work considers methods of analysis and forecasting the conditions for ensuring the stability of systems, statistical data processing, mathematical models of systems, methods of nonlinear dynamics, methods of controlling the functioning of systems under conditions of unpredictability of their states, systems analysis of complex structures, as well as methods and approaches to the synthesis of control systems and the laws of functioning of these structures.

In the work [2] special emphasis is placed on the synthesis of automated and automatic information systems for managing the cyber security of complex objects. Possible approaches and principles for building these systems for organizing the security stability of information infrastructure are also formulated.

The main threats to information security that arise in modern computer structures are considered in the scientific article [3]. It pays considerable attention to the issue of optimizing information protection processes in computer

networks through the functioning of the information security management system. It is indicated that the basis of the information security management system is based on risk assessment and management of these destructive events. The process of security risk management allows you to achieve maximum management efficiency at a given level of risk. The implementation of information security risk management allows you to use effective control of their security status in distributed corporate networks by reducing the risk to the desired level.

In the work [4] the possibility of increasing the efficiency of information security management of a computer structure through the use of multi-agent technologies is investigated. The authors emphasize that information security of a computer structure is a complex problem of management organization, which requires prompt response to incidents and flexible integration of various subsystems of a computer structure to ensure information protection from possible threats. A multi-agent management system is described, which is able to detect threats, monitor and analyze information resources, and also implement mechanisms of prompt response in real time to incidents (security events).

In the works [5–7] the authors comprehensively consider the methodology for creating information security management systems. These scientific articles analyze various approaches to information security risk management and propose the implementation of this methodology in a computer model. The practical implementation of this model helps to develop and implement safe and effective information and security event management systems. It is proposed to consider the structures of information security management systems as a set of subsystems, complexes, components, and the relationships between them. This approach allowed this management system to be represented by a tree of modular units. The properties of information and the model of interaction levels of open systems during its transmission and protection in a computer network are considered by ensuring a given level of management quality. The approaches to creating a methodology for building an information security management system, initiated in works [5–7] were improved by the authors in scientific works [8] and [9]. For this purpose they used a functional analysis of information security management systems. Based on this analysis, the main approaches to the design and implementation of synthesized management systems are investigated. Special emphasis is placed on the importance of an integrated approach to risk management, as well as the role of technical, organizational and cybernetic measures in ensuring the security of information systems. A scientific publication [10] is devoted to the method of analyzing logical-dynamic processes of argument transformation in computing nodes of digital control systems. The limitations and shortcomings of formal methods used to describe data processing processes in digital control systems are identified, and a method for describing argument transformation processes using graph-analytic models is proposed. One of the possible approaches to the practical application of an information security management system is given in [11]. The authors note that the use of systemic approaches to ensuring information security allows identifying weaknesses and shortcomings in the system and eliminating them in a timely manner which will contribute to ensuring the effectiveness, optimality and cost-effectiveness of information security measures. Fundamental aspects of the synthesis of control models for complex dynamic objects taking into account their security events are given in [12]. The authors comprehensively analyze the impact of dynamic processes on the functioning of complex objects and also develop methods for flexible integration of security events into the control model to increase the reliability and stability of the system. Particular attention is paid to approaches to timely response to threats to the security of the computer structure. Along with theoretical developments the work also offers practical recommendations for the development of effective control strategies which in the future should be implemented in information infrastructures using the theory of a logical-dynamic system.

The purpose of the article is to develop theoretical and practical (applied) principles for creating effective information and security event management systems in a computer structure. Their implementation will ensure the efficiency, accuracy and optimality of data processing in the arrays of security events of a computer structure. For this purpose, it is planned to synthesize logical and dynamic models of automation processes for detecting and preventing information security threats.

The main goal of the article is to propose new and effective approaches to the synthesis of logical-dynamic systems that provide reliable protection of the computer structure from current existing threats and in the future, from zero-day threats.

Presentation of the main material

The organization of the process of information and security event management in a computer structure is characterized by complexity and dynamism, which require the use of fundamental theoretical research, which will become the basis for creating optimal algorithmic support for these programmable structures. The results of the analysis of the well-known theoretical developments, which are represented in scientific works [12–22] regarding the features and specifics of processes related to security events in a computer structure, indicate that it is appropriate and desirable to use the theory of logical-dynamic systems to describe them. Systems of this class are characterized by the capabilities and properties of describing hyper-complex processes in information and security event management in a computer structure (and especially those that ensure the functional stability of critical infrastructure objects) [19]. To achieve the research goal we will consider the fundamental provisions of the theory of logical-dynamic systems, their axiomatics, capabilities and specific properties. The axiomatic definition, description and formalization of these systems is as follows. A logical-dynamic system is a complex, large, organizational, hypercomplex synergistic structure. In formalized mathematical models, the components of their structure that describe the logic of processes (variations of final states) and the components that characterize the dynamics of changes in the parameters of these systems (rapid change in real time of its state) are synergistically

linked. At the same time, in logical-dynamic systems, both the rules of logic and variations of these rules or changes in the dynamic states of the system, which functionally depend on a number of external and internal factors can be interconnected. We focus on the peculiarities of the logical-dynamic system, which consists in the fact that changes are described according to clearly established logical rules. But in many situations, these rules can be dynamically (quickly) adjusted (changed) a priori by some influences, for example, such as feedback in the system or flexible adaptation to external disturbances. It follows that this dynamic system belongs to the class of controlled systems (processes in which change in real time in accordance with clearly established rules or logic), which are characterized by adaptive changes in its internal structure, associated with variations in the constituent elements of this structure. It is proposed to describe models of individual possible processes and states of such systems using classical control theory, taking into account that transitions between changes in these states occur in accordance with logical (mathematical) rules. Models of states of logical-dynamic systems are mathematical models that are used to describe and analyze the behavior of complex systems that change their state in time coordinates. In this case, logical-dynamic systems combine logical expressions of discrete mathematics with equations of system dynamics. This approach allows modeling both discrete and continuous variations of changes in the system.

Note that for modeling processes in a logical-dynamic structure, it is advisable to use the theories of:

- mathematical logic (discrete mathematics). (used for mathematical interpretation of the functioning of discrete elements of the system);
- differential equations (used to describe continuous processes that are components of the general process of system functioning);
- graphs. (interprets the structure of the system, namely: an ensemble (tuple) of elements of the logical-dynamic structure and the variation of the relationships between them);
- mathematical modeling of the functioning of finite state machines (describes discrete states of the logical-dynamic structure and transitions between them).

The results of a systematic analysis of existing approaches to the application of the main provisions of these theories confirm the feasibility and necessity of mandatory consideration of the specific features of the logical-dynamic structure. We characterize these features by a number of factors, namely:

– controllability – a feature that characterizes the ability of a logical-dynamic system to respond to external influences and promptly and adequately change its state in accordance with the synthesized control algorithm;

– system functionality – this feature takes into account the hyper-complexity of the logical-dynamic system which consists in the fact that the specified system combines structurally diverse subelements each of which clearly performs only its own specific task within the framework of the overall structure of the system;

– the presence of a general law of operation of control processes (target control function) – a logical-dynamic system that operates in accordance with established laws that determine their behavior. These laws can be either discrete (based on the implementation of logical operations), continuous (based on the application of a system of mathematical equations) or discrete-continuous (synergistically combine the properties of discreteness and continuity of processes in this system).

It should be noted that scientific works [18–22] focus special attention on the above-mentioned features of the logical-dynamic system. These features allow us to fully take into account the specifics of processes in organizing the management of information and events of computer system security. The theory of logical-dynamic systems will be used to analyze the stages of ensuring the security of a computer system when formalizing and modeling the processes of such provision. These stages include:

Intrusion detection. Logical-dynamic systems should be used to synthesize subsystems for detecting possible intrusions. These subsystems will detect abnormal conditions in the entire computer network or on its individual computers which will allow for prompt detection and optimal identification of intrusions (security incidents).

Risk analysis. At this substage, the logical-dynamic system is proposed to be used to assess the security risks of a computer structure (based on the analysis of various factors, for example, the number of vulnerabilities, the frequency of attacks and possible losses from these incidents, etc.), as well as to form strategies for minimizing them or compensating for the destructive consequences of dangerous incidents that will interfere with the normal functioning of the computer system.

Incident Management. Implementation of management processes based on algorithms synthesized using logical-dynamic systems models will allow for the automation of reliable and prompt response to computer system security incidents, for example, blocking malicious traffic or complete “isolation” of infected computers in a computer system.

Predicting possible threats. Using logical-dynamic systems models to predict based on the analysis of accumulated a posteriori data in security event arrays about specific features of incidents in a computer system will ensure optimal identification of future incidents.

System analysis of the proposed stages shows that the implementation of logical-dynamic systems models will ensure the management of information and security events of a computer system. The use of logical-dynamic systems will also allow to realize a number of significant advantages over the known traditional methods of managing information and security events of a computer system, namely: flexibility, accuracy, automation of management and forecasting of the development of processes in these tools. A methodology for organizing the management of security events of a computer system has been developed which is based on the use of the theory of logical-dynamic systems and is given in Table 1.

The dominant component of the proposed methodology is the synthesis of a system for managing information and security events of a computer system. Let us consider, as an example, one of the components of this management system in more detail, namely: a subsystem for detecting unauthorized intrusions into the software environment of a computer system.

Table 1 – **Methodology for organizing information and event management of computer security structures**

Stages of the methodology	Algorithms for implementing the stages of the methodology
Formalization of the description of the system and its subsystems	Description of the computer structure model (network with servers and workstations), its structure and specifics of functioning
Identification of possible (probable) security incidents and events	Formation of a list of security events that taking into account the probability of their occurrence will occur in the system: • login of an unauthorized user; • attempt to gain access to confidential information; • appearance of various viruses; • attack on the server to further create a denial of service to users; • attack on the server for unauthorized removal, distortion or destruction of information; • appearance of new events (zero-day events).
Development of the logical component of the model	The logical component of the computer structure model is synthesized which describes the structural relationships between the logical elements (states) of the system: • login to the system by an unauthorized user – logical transition: attempt to gain unauthorized access to confidential information; • detection of a virus on a computer – logical transition: attack on other computers in the system (network).
Development of a dynamic component model	The dynamic component of the model is synthesized. Its structure consists of equations that describe the temporal variations of incidents (security events), namely: • the time required for guaranteed detection of intrusions into the system; • the speed of virus propagation in the system; • the duration of the attack on the system.
Control system synthesis	A security information and event management system is synthesized, the structural components of which are: • a subsystem for detecting unauthorized intrusions into the software environment; • a subsystem for analyzing possible risks; • a subsystem for predicting situations of possible threats; • a subsystem for managing incidents (security events).
Testing and tuning	• the information and security event management system is tested on a real or virtual model (digital twin) of the computer structure; • the information and security event management system is configured in accordance with the requirements for the given security level of the computer structure.

Applying the theory of logical-dynamic systems to form an algorithm of functioning we will consider the following functional elements:

Data collection. Collects data about all current computer system states and events that occurred on the network, such as changes in IP addresses, MAC addresses, port states, use of management protocols, etc.

Data analysis and optimal processing. Analyzes data collected in security event arrays and optimally processes it to further identify anomalies in network behavior that indicate an intrusion into a computer system.

Intrusion detection and identification. Detects anomalies according to the intrusion identification template, generates notifications (if necessary) and forms control actions to compensate for the destructive consequences of these incidents.

Intrusion response. Implementation of control actions for automatic control of the process of optimal and prompt response to unauthorized intrusions (for example, forms effective control actions for emergency blocking of the attacker's IP address or for complete and reliable isolation of an infected computer).

To implement the methodology for organizing the management of information and events of computer system security using the theory of logical-dynamic class systems, we will consider specific aspects of its axiomatics. In the future, we will use the obtained theoretical results in the synthesis of control systems for ensuring the security of computer systems.

It should be noted that the modeling of information and security event management processes of a computer system using the theory of logical-dynamic systems differs significantly in essence and content from classical approaches to the organization of management using the theory of automatic control systems, for example, in the management of pulse systems, systems with modal control or multi-connected control systems, etc. Considering that the control object - a security event of a computer system is described, as a rule, by models of complex systems that combine two fundamental classes of automatic systems, namely logical and dynamic. We will use a number of new categories and concepts of a mathematical nature, and we will conduct their further interpretation and adaptation for the synthesis of a system for managing information and security events of a computer system. To do this, we will consider a possible approach to the mathematical description of a logical-dynamic system, which will be the basis for creating a methodology for the synthesis of complex hypercomplex control structures [24], [25]. Under a dynamic system, we will consider a system that is generally described axiomatically by a mathematical model represented by an ordered set (tuple):

$$SD = \left(T, X, U, \Omega, Y, \Gamma, \varphi, Z\right). \quad (1)$$

Applying a number of necessary additional definitions in model (1) and using the appropriate interpretation for describing processes in complex large

organizational systems, we will describe the models of the component subsystems of the dynamic system SD, namely:

а) finite dynamic subsystem

$$SD_{[0,1]} = (\Omega, Y, Q, \lambda, \delta), \quad (2)$$

б) диференціальної динамічної субсистеми

$$SD_{[0,\infty]} = (T, U, X, Y, \varphi, \eta),$$

в) symbiotic (synergistic) combination of mathematical expressions (1) and (2) will describe a model of a logical-dynamic system

$$\begin{cases} SD_{[0,1]} = (\Omega, Y, Q, \lambda, \delta), \\ SD_{[0,\infty]} = (T, U, X, Y, \varphi, \eta), \\ \Omega_{[0,1]} = (T, Y, U, Z). \end{cases} \quad (4)$$

Components of a tuple (1) which are included in (2), (3), (4) describe the variable logical and dynamic states of the system logical-dynamic system. We will describe these components in more detail below.

Note that the set of time instants T is considered in (4) as an ordered subset of the set of real numbers. For finite dynamical systems this set of time instants is T will be plural Z which corresponds to an ordered abelian group of integers. Multiple input influences Ω not empty. Therefore, we can specify a set of instantaneous values of input influences U and instantaneous values of the output quantities Y.

Write the system state transition function, namely:

$$\varphi : T \times T \times T \times X \times \Omega \to X. \quad (5)$$

The values of this function describe its following possible states:

$$x(t) = \varphi(t, \tau, x, \omega) \in X. \quad (6)$$

The given function (6) has the properties of directed time, consistency of the mapping (4), causality, and also semigroup properties

$$\varphi(t_3, t_1, x, \omega) = \varphi(t_3, t_2, \varphi(t_2, t_1, x, \omega), \omega), \quad (7)$$

for any values $t_1 < t_2 < t_3$ and $x \in \Omega$, $t_1 < t_2 < t_3$.

Let's write down the values $\eta : T \times X \to Y(t)$. This expression defines the output values $y(t) = \eta(t)$ by the values of the state transition function, namely: $y(t) = \eta(t, x(t))$.

Let us make some clarifications to adapt the mathematical models (5), (6), (7) to the applied terminology of real systems. Then (τ, x) where $\tau \in T$, $x \in X$ is called a "system event". In this case the phase space of events will be the set $T \times X$. System state transition function φ is interpreted as its trajectory (variations of the system) in the form of a solution to an ordinary differential equation. Control (inputs to the system) ω or transforms a state describing system events x into a state that is described as $\varphi(t, \tau, x, \omega)$. We emphasize that considering variations of the system SD in the context of the logical-dynamic approach we mean solutions φ along a certain path of controlled discrete transitions on a finite set of states – the system outputs. These states adequately describe the current events in the system. In this case let us assume that for models of logical-dynamic systems $Q = Y$.

A dynamic differential system is defined in such a way (3) that its models have the properties of smoothness, reversibility and completeness [1]. Thanks to these properties we can formalize the concepts of reachability, controllability and observability, on the basis of which it is intended to consider the problem of optimal control of the state or events in the specified system. When synthesizing complex control systems which include the system of information and event management of the security of a computer structure we propose to apply the theory of dynamic differential systems to solve a narrow range of control problems within the framework of individual aspects of the functioning of these systems. But this theory is a convenient mathematical apparatus, the use of which allows formalizing models of control processes in a simplified formulation. The specified axiomatics is characteristic of the stage of system synthesis, the purpose of which is, firstly, to build the structure of the system, and secondly, to create a general law of the functioning of the control system and individual laws of the functioning of its subsystems. It is also advisable to carry out the synthesis of the information and event management system of the security of a computer structure using the theory of finite automata [23]. We will perform it based on the given law of the functioning of the discrete (logical) part of this control system. For this purpose we will use the applied apparatus of Boolean algebra which contains means of analyzing finite dynamic systems that are of an iterable nature, in connection with which taking into account all the volumes of information processing is one of the main difficulties in solving the applied problems of this synthesis. We will also take into account other difficulties in the synthesis of modern systems for managing security events of a computer structure, which are associated with a number of the following manifestations in the processes of its functioning. Let us consider these manifestations in more detail. The intensification of the processes of functioning of modern computer structures generates incompatibility of restrictions that act as contradictory requirements between the provisions of the normative theory and the limiting physical constants. This is what incompatibility of constraints on elements means $u(t)$, $x(t)$ plurals U and X where $u(t) \in U$, $x(t) \in X$. The unification of automation tools for managing information processing processes in a computer structure, as a rule, establishes a finite class of functions, limiting physical constants (for example, the volumes of the computing environment of these structures and the volumes of information processed, etc.), generates on the set X type restriction system

$$x_i(t) \le x_{0\max}(t), \quad (8)$$

Within the framework of one model, these requirements (8) are incompatible. This is due to the fact that the equation

$$x_i(t) = f_i(x,u,t),\ i = 1,2,...,n \qquad (9)$$

for $u(t) \in U$ and $x_i(t) \le x_{0\max}(t)$ are valid only on a finite subinterval $[t_0, t_1]$.

To implement the necessary process of system functioning on the entire set of values *T* the parameters of the object itself must also be controllable. This requirement is expressed in the discretely varying functions in equation (7). From this requirement it follows that the automatic information and event management system of the security of a computer structure is synthesized as a coordinate-parametric control system [24]. Sets of constraints on sets *U* and *X* have the volumes ("power") of finite sets. This in turn means that a discrete controlled process on a set of functions $f_{il,}\ i = 1,2,...,n$ (by index $l = 1,2,...,s$) makes sense in processes controlled by finite state machines. The functioning of this object occurs in a wide range of various heterogeneous states (different phases, system state, different nature of interaction in the information environment, etc.). Let us take into account that complex objects, as a rule, have a multi-purpose nature of functioning. This implies the need to implement a controlled change in the structure of interacting subsystems. In the process of achieving a goal or some planned sequence of sub-goals the control object undergoes structural variations in unidentified and critical situations. As a result the set of these conditions requires the analysis and synthesis of a system with coordinate-structural control. The structure of the system must be controllable $SD_{[0,\infty]} = (T, U, X, Y, \varphi, \eta)$ which implies a variation in the original mathematical model $F_k \in F$ functions $f_{(il)k} \in F_k,\ k = 1,2,...,K$.

In all considered cases, which assume the presence of a controllable system structure, we will use the following categories of sets, namely:

- finite sets of threshold and other constraints on the phase coordinates of the system state;
- finite sets of normalized (unified) functions and quantities;
- finite set of subgoals and their relative ordering;
- finite set of homogeneous operating conditions, information environments and their relative ordering;
- finite set of system structures generated by abnormal situations (events) controlled by processes and operations.

We will define the elements of these finite sets formally. They are mathematical objects that model discrete transitions on finite sets of coordinate functions $u(t) \in U$, parameters $f_{il} \in F_k$ and structures $F_k \in F$ in the laws of functioning of complex systems with coordinate-structural control. To formalize the law of control of the functioning of a complex system, it is necessary, in addition to determining the elements of finite sets U, F_k and F, interpreted as discrete states of the system, we will also describe the probable paths of transitions on these sets. The proposed approach models, together with the transition conditions the order of changes in the states of the system or the law of functioning of a finite dynamic system. Transition conditions on finite sets are attributed to the class of deterministic conditions – two-valued predicates. The domain of definition of the subject variables of such predicates is vector spaces with a scalar or probability measure, countable sets of time cycles and other heterogeneous sets of events. The domain of values of the specified predicates is described by the two-element set {0,1}. Then the calculation of two-valued inhomogeneous predicates transfers the synthesis of the model of functioning of complex coordinate-structural control systems into the domain of finite analysis. This analysis is based on Boolean algebra which will allow identifying the logical part of the laws of functioning of such systems by finite state machines. Based on the considered approach, a mathematical description of systems of the logical-dynamic class as models of functioning with structural and parametric control is obtained [25]. This approach to the organization of control in systems of the specified class is successfully algorithmized, since the functions of predicates are optimally implemented in the computing environment of the computer structure. In the established methodology for the synthesis of information and event management systems for computer structure security which is based on the theory of a logical-dynamic system described by a mathematical model (3) we distinguish the following stages:

Systemic. At this stage, the architectures (structures) of the system are synthesized and the laws of its functioning are formed.

Structural-logical. This stage involves the formation of a structure for algorithmic support of computer structure management processes.

Software-technical. At this stage, the creation of separate functional blocks of the software for the information and event management system for computer structure security and their implementation in these information structures is envisaged.

It should be noted that each of the above stages is accordingly based on independent and inherent mathematical models and approaches to system analysis and optimization of management processes, as well as on corresponding algorithmic procedures.

The results of theoretical studies show that the complication of the laws of system functioning can lead to the fact that it will be problematic to describe the synthesis object as a single (indivisible) whole by the models of the system stage. As a result, it is difficult to perform the operation of quantitative comparison of alternatives or to interpret the synthesis object and its functioning processes by numerical indicators of modeling. The synthesis process itself using models of the system, structural-logical and software-technical stages is problematic to combine functionally. The problem of the complexity of a single structural procedure arises, since the results of the synthesis of control laws obtained at the system stage require

flexible adaptation to the model of the software-technical stage. We will take this problem into account in the future when ensuring the quality of management.

The criteria of quality of management, the main of which are the speed of working out of controlling influences and the minimum time spent on the implementation of management will be represented by elements of models in sets of vector spaces. But the peculiarity of these spaces is that they are almost completely "opened up" as a single system of assessments in the categories of models of the structural-logical and program-technical stages. This indicates that the criteria of quality of management are constructive within the models and are invariant with respect to the criteria of the efficiency of the functioning of the system being synthesized. Therefore, we will take into account this feature that the synthesis process as a decisive procedure is mathematically open-ended. Closure involves the representation of the main estimates and algorithmic and programmatic components of the object by categories of models of the system stage, which will be supplemented at the next stages of the implementation of the models. The above allows us to conclude that the step-by-step solution of synthesis tasks from the point of view of mathematical correctness is consistent. At the same time the ability of the logical-dynamic system to model complex, dynamic environments and include both logical rules and dynamic behavior makes them suitable for solving current problems of information management and security events in modern and promising computer structures. The results of solving these problems are proposed to be implemented in algorithms the structure of which is presented in Table 2.

Table 2 – **Structure of algorithms for managing information and security events of a computer structure**

Algorithm components	**Algorithm substeps**	**Functions that are implemented using the theory of logical-dynamic systems**
Adaptive security management	Real-time threat detection	• models the dynamic nature of incidents, adapting to variations in new security events and vulnerabilities of the computer structure; • detects anomalies and potential violations in real time (thanks to logical security policy rules and dynamic models that describe the behavior of the computer structure).
	Responding to security incidents and events	• promptly generates the necessary control actions to ensure security based on predefined rules and results of analysis of the current state of the system; • initiates automated (automatic) countermeasures, such as isolating affected systems or blocking malicious traffic.
Risk assessment and minimization	Vulnerability analysis	• models the relationships between different components in a computer structure; • models approaches to identifying potential vulnerabilities in a computer structure; • models possible attack scenarios to assess the risks associated with variations in vulnerabilities; • models the hierarchy of priorities for efforts to mitigate or compensate for the consequences of incidents.
	Dynamic risk management	• constantly monitors the security status of the system; • promptly adjusts security event management in accordance with the current risk level; • automatically increases the level of security monitoring in the event of a significant increase in the flow of incidents; • implements if necessary more stringent access control to the software environment of the computer structure.
Ensuring compliance with security policies	Formal modeling of security policies	• modeling security policies for use in a computer structure; • forming logical rules that interpret access control policies; • adjusting information array protection rules in accordance with current security requirements.
	Maintaining compliance with security policies	• checking the system configuration for compliance with defined security policies; • identifying abnormal deviations in the system configuration from the reference (defined, specified) security policies; • ensuring (guaranteeing) the system's compliance with established security standards and rules.
Intrusion detection and prevention	Anomaly detection	• evaluates the behavior of the system for compliance with established norms (rules); • promptly detects deviations that indicate unauthorized intrusion; • synergizes logical rules that determine the given behavior of the system for compliance with its dynamic models of functioning; • detects non-specific (unconventional, unknown) anomalies.
	Responding to an intrusion	• automatically responds to detected intrusions; • automatically blocks malicious information transmission traffic; • blocks suspicious processes in the information environment and promptly generates danger alerts.

To create a methodology for organizing information and security event management in a computer structure (Table 2), we adapt through specification and necessary additional definitions the theory of logical-dynamic systems and the mathematical model (3) for the further implementation of process management in order to significantly mitigate or compensate for the consequences of computer incidents. When synthesizing the processes of information and event management of computer security in the mathematical model, a number of formalization descriptions of its constituent (structural) components were used. The proposed approach provides the possibility, through decomposition (3), to present the model of a logical-dynamic system in the form of:

$$S = (X, Y, Z, f, g', L, h). \quad (10)$$

Taking into account the axiomatics of the logical-dynamic system we will further define the mathematical expressions (1)–(9) which makes it possible to formalize its components in (10).

Let us consider the components of the set structure (10) in detail.

1) $X = \{x_1, x_2, \ldots, x_n\}$ – a set that describes the current states of a computer structure. These states are formalized by the following indicators:

- use of computer structure resources (processor, RAM, data storage devices, etc.);
- the number of network traffic patterns used to ensure information security at the physical level;
- the number of processes involved for secure information processing;
- indicators of the status of security software (firewalls, antiviruses, etc.);
- system vulnerability status indicator, etc.

2) $Y = \{y_1, y_2, \ldots, y_m\}$ – a set that comprehensively describes security events in a computer structure, namely:

- unauthorized intrusion attempts;
- presence of malicious software;
- denial of service attacks;
- leakage of confidential information;
- system errors in information processing, etc.

3) $Z = \{z_1, z_2, \ldots, z_k\}$ – a set of actions for implementing security measures (security management). This set describes the following actions:

- blocking IP addresses;
- implementation of quarantine dossiers;
- emergency (safe) completion of information processing processes;
- correction (adjustment) of the consequences of vulnerabilities;
- prompt notification of computer security personnel.

4) $f: X \times Y \to X$ – a function that formally describes changes in system states. This function characterizes changes in the system state depending on the destructive effects of security events. Taking into account the metric of the current system state $x \in X$ and security events $y \in Y$, function $f(x, y) = x' \in X$ where x' – a new state of the system that characterizes variations in system dynamics depending on incidents.

5) $g: X \times Y \to Z$ – a function of selecting security management approaches based on the current state of the system and security events that have occurred in the computer structure. It determines what actions must be taken promptly in response to a security event to ensure the functional stability of the computer structure. Current state is set $x \in X$ and security event $y \in Y$, $g(x, y) = z \in Z$. This function reflects the security policy or decision-making process for significantly mitigating the destructive consequences of incidents or fully compensating for them.

6) $L = \{l_1, l_2, \ldots, l_p\}$ – a set of logical conditions for ensuring the safe state of the system. These conditions can be used to refine approaches to choosing an action in the case of:

- CPU load over 80%;
- the firewall is disabled;
- the number of unsuccessful login attempts is more than three, etc.

7) $h: X \to \{True, False\}_p$ – a function that is described by a set of logical conditions of the states of a computer structure (which are true or false) $h(x) = \{h_1(x), h_2(x), \ldots, h_p(x)\}$, where $h_i(x)$ – truth value of a logical condition l_i in possible states x.

8) $g': X \times Y \times \{True, False\}_p \to Z$ – an extended action selection function that takes into account not only the system state and event, but also the truth value of logical conditions $g'(x, y, h(x)) = z \in Z$. Its application allows for the implementation of more complex and context-dependent security responses in the computer structure. We will present the developed dynamics of incident compensation in the form of a formalized model that implements the phased steps of this compensation and display it in the form of an algorithm:

Step 1: /Initial state/ *The system is (starting) in the initial state* $x_0 \in X$.

Step 2: /Occurrence of an event – the occurrence of a security incident/ *A security event is occurring.* $y \in Y$.

Step 3: /Change (transition) of states/ *Change (transition) of states* y_i *transitions to a new state* $x_i' = f(x_i, y_i)$.

Step 4: /Condition assessment/ *Logical conditions L are displayed with the new status:* $h(x') = (b_1, b_2, \ldots, b_p)$, where $b_i \in \{True, False\}$.

Step 5: /Formation of management actions (influences)/ *Based on the new state* x_i' *and security events* y_i' *an action is being formed to manage security information and events* $z_i = g(x_i', y_i, h(x'))$.

Step 6: /Implementation of management actions/ *Selected action* z_i *is processed by the system and affects the change in its state.*

Step 7: /Repetition/ *When new (subsequent) incidents (security events) occur, the process from step 2 to step 6 is repeated cyclically.*

Present the implementation of the application of model (9) taking into account the proposed step-by-step stages. In this example, if the system is in a secure state and an attempt is made to log in to the system, the system remains in a secure state, and the security management action consists in blocking access. If a security event (incident) is detected, the system enters a vulnerable state, and the security management action involves compensating for the destructive consequences

of the security event. The formalization of the specified approach is presented in the form of a variation of the states of the computer structure:

X = {safe, vulnerable} – system states.

Y={login attempt, incident detected} – security events.

Z={block access, compensate for the consequences of the incident} – safety management actions.

State transition function *f* is defined as follows:

f(secure, login attempt) = safe.

f(safe, security event detected) = impressionable.

f(vulnerable, login attempt) = impressionable.

f(вразливий, виявлено вірус) = impressionable.

Action selection function g introduce it like this:

g(secure, login attempt)= block access.

g(safe, incident detected)= compensate for the consequences of the incident.

g(vulnerable, login attempt)= block access.

g(vulnerable, incident detected)= compensate for the consequences of the incident.

Taking into account this formalization, the incident detection algorithm can be presented in a simplified form as follows:

X ={*Normal, high, attacked*}.

Y ={*LoginFailure, MalwareDetected*}.

Z ={*BlockIP, QuarantineFile, LogAlert*}.

L ={FailedLoginAttempts > 3}.

Transitions and actions:

f (*Normal, malware detected*) = attacked.

f (*Normal, LoginFailure)=HighCPU*) (if there were many failed logins).

g'(*HighCPU, LoginFailure, True)*=BlockIP (if *FailedLoginAttempts > 3* true).

g'(*Attacked, MalwareDetected) = QuarantineFile* (regardless of other conditions).

Conclusions

Thus, the paper proposes an approach to the synthesis of a logical-dynamic system for managing information and security events of a computer structure. It is noted that by synergistically integrating logical and dynamic components of the processes of functioning of a computer structure into models, it is possible to synthesize systems that will not only detect and respond to security threats, but also predict and prevent potential vulnerabilities. The synthesized systems have increased adaptability and functional resistance to security threats. The implementation of logical rules provides accurate correlation and analysis of events, and dynamic modeling facilitates the prediction of system behavior and operational compensation of destructive factors. Further scientific research is proposed to be carried out with an emphasis on the practical implementation and evaluation of the results obtained in real systems for managing information and security events of a computer structure, as well as on improving dynamic models and automating the adaptation of logical rules.

REFERENCES

1. Hrytsiuk P. M., Dzhoshi O. I. ta Hladka O. M. (2021) Osnovy teorii system i upravlinnia. NUVHP, Rivne. 272 s.
2. Yashchuk V.I. Proektuvannia avtomatyzovanykh informatsiinykh system upravlinnia kibernetychnoiu bezpekoiu obiektiv krytychnoi infrastruktury Ukrainy, Aktualni problemy upravlinnia informatsiinoiu bezpekoiu derzhavy: zb. tez nauk. dop. nauk.-prakt. konf. (Kyiv, 26 bereznia 2021 r.). [Elektronne vydannia]. – Kyiv : NA SBU, 2021. C. 233–235.
3. Hrebeniuk A.M. Osnovy upravlinnia informatsiinoiu bezpekoiu: navch. posib. / A.M. Hrebeniuk, L.V. Rybalchenko. – Dnipro: DDUVS, 2020. – 144 s. http://er.dduvs.edu.ua/handle/123456789/5717.
4. Hnusov Yu. V., Mozhaiev O. O. Rozrobka multyahentnoi systemy upravlinnia informatsiinoiu bezpekoiu. Pravo i bezpeka. 2022. No 4 (87). S. 171–183. https:/ /doi. org/10.32631/pb.2022.4.14.
5. Mokhor V., Tsurkan V. (2021). Kompiuterna model rozrobky system upravlinnia informatsiinoiu bezpekoiu. Zbirnyk "Informatsiini tekhnolohii ta bezpeka", 9 (1), C. 80–90. https://doi.org/10.20535/2411-1031.2021.9.1.249814.
6. Tsurkan V. Metod syntezu struktury systemy upravlinnia informatsiinoiu bezpekoiu // Ukrainskyi naukovyi zhurnal informatsiinoi bezpeky, 2020, tom 26, vypusk 2, C. 116–122. DOI: 10.18372/2225-5036.26.14926.
7. Tsurkan V., Shapoval O. (2022). Analiz metodiv otsinky ryzykiv bezpeky kompiuternoi merezhi. Zbirnyk "Informatsiini tekhnolohii ta bezpeka", 10 (2), C. 204–215. https://doi.org/10.20535/2411-1031.2022.10.2.270437.
8. Volodymyr Mokhor, Vasyl Tsurkan Metodolohiia pobudovy system upravlinnia informatsiinoiu bezpekoiu zakhyst informatsii, tom 23, № 4, zhovten-hruden 2021, C. 200-212. DOI: 10.18372/2410-7840.23.16766.
9. Tsurkan V. (2020). Metod funktsionalnoho analizuvannia system upravlinnia informatsiinoiu bezpekoiu. Elektronne fakhove naukove vydannia "Kiberbezpeka: osvita, nauka, tekhnika", 4(8), C. 192–201. https://doi.org/10.28925/2663-4023.2020.8.192201.
10. Ushkarenko O.O. Metod analizu protsesiv peretvorennia danykh v obchysliuvalnykh vuzlakh tsyfrovykh system upravlinnia Vcheni zapysky Tavriiskoho NU imeni V.I. Vernadskoho. Seriia: Tekhnichni nauky Tom 32 (71) № 4 2021, stor. 162…168, https://doi.org/10.32838/2663-5941/2021.4/25
11. Skitsko Oleksii, Shyrshov Roman. Systema upravlinnia informatsiinoi bezpeky yak instrument pidvyshchennia zakhyshchenosti ta efektyvnosti obiektiv krytychnoi infrastruktury. International Science Journal of Engineering & Agriculture. Vol. 2, No. 6, 2023, pp. 12-22. doi: 10.46299/j.isjea.20230206.02
12. I. Samborskyi, Ie. Samborskyi, V. Hol , Y. Peleshok, S. Sholokhov .,(2024) Synthesis of the model of management of complex dynamic objects taking into account the events of their security. Information Technology and Security. January-June 2024. Vol. 12. Iss. 1 (22) P. 4-16. https://doi.org/10.20535/2411-1031.2024.12.1
13. Sholokhov S.M., Pavlenko P.M., Nikolaienko B.A., Samborsky I.I., Samborsky E.I.,(2023/2024) The method of optimizing the distribution of radio suppression means and destructive software influence on computer networks. Radio Electronics, Computer Science, Control. 2023/2024. № 4 (67). P. 16-29. URL: https://doi.org/10.15588/1607-3274-2023-4-2
14. Ye. Samborskyi, I. Samborskyi, Osoblyvosti obrobky masyviv podii bezpeky dlia upravlinnia zakhystom elektronnykh komunikatsiinykh system. Materialy II Mizhnarodnoi naukovo-praktychnoi konferentsii "Kiberbezpeka derzhavnykh instytutsii ta podolannia kryzovykh staniv" : v 2 t. Kyiv : ISZZI KPI im. Ihoria Sikorskoho, 2023. T. 1.s. 293–294.

15. P. Pavlenko, Ye. Samborskyi, Modeli obrobky podii bezpeky dlia upravlinnia zakhystom kompiuternykh system. Materialy KhVI mizhnarodnoi naukovo-tekhnichnoi konferentsii “AVIA-2023”. – K.: NAU, 2023 C. 13.8–13.11
16. Ye. I. Samborskyi, Rozrobka modeli upravlinnia podiiamy bezpeky kompiuternykh system, Materialy X Mizhnarodnoi naukovo-tekhnichnoi Internet-konferentsii “Suchasni metody, informatsiine, prohramne ta tekhnichne zabezpechennia system keruvannia orhanizatsiino-tekhnichnymy ta tekhnolohichnymy kompleksamy”, 24 lystopada 2023 [Elektronnyi resurs]. – K: NUKhT, 2023. – 224 s. – Rezhym dostupu: https://nuft.edu.ua/naukova-diyalnist/naukovi-konferencii., s. 213.
17. Ye. Samborskyi, I. Samborskyi, Model otsinky ta upravlinnia podiiamy bezpeky kompiuternykh system, Materialy VI Naukovo-praktychna konferentsiia kursantiv (studentiv), aspirantiv, doktorantiv ta molodykh uchenykh “Aktualni pytannia zastosuvannia spetsialnykh informatsiino komunikatsiinykh system”, Kyiv : ISZZI KPI im. Ihoria Sikorskoho, 2023, s. 38–39.
18. Sholokhov S.M., Peleshok Ye.V., Samborskyi Ye.I. Syntez synerhetychnoi modeli optymalnoho upravlinnia protsesamy zabezpechennia informatsiinoi bezpeky kompiuternykh system. Perspektyvy rozvytku ozbroiennia ta viiskovoi tekhniky Sukhoputnykh viis: Zbirnyk tez dopovidei Mizhnarodnoi naukovo-tekhnichnoi konferentsii (Lviv, 15-16 travnia 2024 roku), Lviv, NASV, 2024, C. 283–284.
19. Pavlenko P.M., Samborskyi Ye. I. Syntez systemy upravlinnia podiiamy bezpeky dlia zabezpechennia zakhystu informatsiinoho seredovyshcha infrastruktury krytychnykh obiektiv, // Materialy KhI Vsesvitnoho konhresu “Aviatsiia v XXI stolitti” – “Bezpeka v aviatsiino-kosmichnykh tekhnolohiiakh”, 25–27 veresnia 2024, Kyiv: NAU, 2024, stor.11.16–11.19.
20. Ye. Samborskyi, I. Samborskyi, Osoblyvosti zastosuvannia tsyfrovykh dviinykiv dlia upravlinnia podiiamy bezpeky kompiuternykh system krytychnykh infrastruktur, // Materialy III Mizhnarodnoi naukovo-praktychnoi konferentsii “Kiberbezpeka derzhavnykh instytutsii ta podolannia kryzovykh staniv”, 14 veresnia 2024, Kyiv : ISZZI KPI im. Ihoria Sikorskoho, 2024. 294 c.
21. Samborskyi Ye. I., Zastosuvannia tsyfrovykh dviinykiv dlia optymizatsii upravlinnia podiiamy bezpeky kompiuternykh system, 22 lystopada 2024 roku. Materialy II Mizhnarodnoi naukovo-praktychnoi Internet-konferentsii “Innovatsii ta perspektyvni shliakhy rozvytku informatsiinykh tekhnolohii” (IPShRIT-2024), m. Cherkasy, 2024. C. 105–106.
22. Pavlenko P.M., Samborskyi Ye.I. Model upravlinnia podiiamy bezpeky kompiuternykh system krytychnoi informatsiinoi infrastruktury na osnovi tsyfrovykh dviinykiv, Materialy II mizhnarodnoi naukovo-praktychnoi konferentsii “Suchasni aspekty didzhytalizatsii ta informatyzatsii v prohramnii ta kompiuternii inzhenerii”, 19–21 hrudnia 2024 roku., m. Kyiv, Derzhavnyi universytet informatsiino-komunikatsiinykh tekhnolohii , 2024, C. 181–184.
23. Krychevets O.M., Zastosuvannia elementiv teorii kintsevykh avtomativ dlia doslidzhen dynamichnykh vlastyvostei obchysliuvalnykh komponentiv vymiriuvalnykh system. Vymiriuvalna tekhnika ta metrolohiia 77 (2016): C. 121–126.
24. Rabchun D. I, Lohiko-dynamichna model protsesu upravlinnia resursamy zakhystu v umovakh informatsiinoho protystoiannia. Suchasnyi zakhyst informatsii, №3, 2016, s.62–67.
25. Zhuk K. D. Pytannia aksiomatychnoho pidkhodu do pobudovy teorii lohiko-dynamichnykh system keruvannia, Avtomatyka, № 3-6, 1971, s. 62–74.

Received (Надійшла) 21.02.2025
Accepted for publication (Прийнята до друку) 16.04.2025

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Самборський Євген Іванович – аспірант кафедри організації авіаційних перевезень Національного університету “Київський авіаційний інститут”, Київ, Україна;
Ievgen Samborskyi – Postgraduate student, Department of Air Transportation Organization, National University “Kyiv Aviation Institute”, Kyiv, Ukraine.
e-mail: seinauedu@gmail.com; ORCID Author ID: https://orcid.org/0000-0003-4441-1947.

Пелешок Євген Володимирович – кандидат технічних наук, старший науковий співробітник Науково-дослідного інституту воєнної розвідки, Київ, Україна;
Yevhen Peleshok – Candidate of Technical Sciences (PhD), Senior Researcher, Research Institute of Military Intelligence, Kyiv, Ukraine.
e-mail: pel85@ukr.net; ORCID Author ID: https://orcid.org/0000-0003-0033-1160;
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57209822977.

Синтез логіко-динамічних систем управління інформацією та подіями безпеки комп'ютерних структур

Є. І. Самборський, Є. В. Пелешок

Анотація. У статті розглядається один з можливих підходів до вирішення актуального наукового завдання, присвяченого синтезу логіко-динамічних систем управління інформацією та подіями безпеки комп'ютерних структур. Зроблено аналіз сучасних підходів до створення інтегрованої системи управління, реалізація якої дозволить ефективно керувати інформаційними масивами подій безпеки в умовах змінених загроз комп’ютерним структурам. Окремо увага приділяється розвитку моделей, які об’єднують логічні та динамічні аспекти управління, що дозволяють забезпечити високу адаптивність і функціональну стійкість комп’ютерних структур в умовах інтенсифікації активності подій безпеки. Реалізація такого підходу дозволить автоматично реагувати на ці події, оптимізувати процеси виявлення та усунення наслідків загроз, а також забезпечити постійну стабільність роботи комп'ютерних структур. У статті пропонується метод синтезу логіко-динамічної моделі, яка синергетизує не лише технічні, але й організаційно-кібернетичні аспекти безпеки комп’ютерних структур. Розроблені підходи можуть бути рекомендовані для використання при створення більш ефективних та безпечних комп’ютерних засобів, здатних протистояти різноманітним інцидентам.

Ключові слова: система управління, логіко-динамічна система, інформаційна безпека, подія безпеки, синтез, аналіз, теорія логіко-динамічних систем, комп’ютерна структура, інцидент, масив подій безпеки.