National Technical University
"Kharkiv Polytechnic Institute"

MODERN PROBLEMS OF COMPUTER SCIENCE AND IT-EDUCATION

collective monograph

PREMIER
Publishing

VIENNA, AUSTRIA
2020

Authors:

ALEKSIYEV Volodymyr, BILOVA Mariia, BORYSOVA Natalia, CHEREDNICHENKO Olga, FEDORCHENKO Volodymyr, GOLOSKOKOV Alexander, GOLOSKOKOVA Anna, HARASYMCHUK Oleh, HAVRYLOVA Alla, HOLUBNYCHYI Dmytro, IVASHCHENKO Oksana, KALACHOVA Vironika, KOZULIA Mariia, KOZULIA Tatiana, LIUTENKO Irina, MELNYK Karina, MELNYK Marharyta, MILOV Oleksandr, OPIRSKYY Ivan, ROMASCHENKO Natalya, RYABUKHA Yurii, SALO Nataliia, SHMATKO Olexander, SOROKA Mykhailo, TRETIAK Viacheslav, TRYSTAN Andrii, VLASOV Andrii, VOVK Maryna, YANHOLENKO Olha, YEVSEIEV Serhii.

Modern Problems Of Computer Science And IT-Education : collective monograph / [editorial board K. Melnyk, O. Shmatko].– Vienna : Premier Publishing s.r.o., 2020.– 236 p.

ISBN 978-3-903197-19-0

The collective monograph highlights modern problems of development and using information technologies for resolving some issues in different domain areas. The proposed theoretical methodologies, models and practical approaches are considered and investigated in the context of IT-education, software engineering, artificial intelligence and cybersecurity. Every chapter describes methods, efficient algorithms and resolutions specific for the particular domain area and field of knowledge.

Authors are responsible for the content and accuracy.

Contents

CHAPTER II. CYBERSECURITY

Self-organizing organizational structures of cybersecurity systems

Oleksandr Milov
Doctor of Philosophy, Associate Professor
Department of Cyber Security and Information Technology
Simon Kuznets Kharkiv National University of Economics
ORCID: https://orcid.org/0000–0001–6135–2120

Volodymyr Aleksiyev
Doctor of Technical Sciences, Professor
Department of Cyber Security and Information Technology
Simon Kuznets Kharkiv National University of Economics
ORCID: http://orcid.org/0000–0001–6767–7524

Abstract. *The issues of self-organization of the team of agents in cybersecurity systems are discussed in this section. The approaches to the definition of self-organization, functions and structures of self-organizing systems are presented. Formed a set of mathematical models included in the model of self-organization. For the structures under consideration, such system characteristics as stability, sensitivity and flexibility are defined, and a list of tasks that ensure the assessment of the stability of the organizational structures of cybersecurity systems is defined.*

Keywords: *self-organization, stability, mathematical model, adaptability, structural and functional models*

Introduction

Cybersecurity systems (CS) undoubtedly belong to the class of complex organizational systems, the main features of which are the number of their constituent elements, the variety of links between the elements, and the limiting uncertainty (a priori or arising during operation).

The approach to solving the problem of managing such complex systems may consist in creating systems capable of self-organization, and possibly making logical decisions, i.e., making decisions in alternatives that are equally likely. When constructing the structure of such systems, the principles of self-organization are used.

Usually self-organizing systems are considered based on biological principles [1]. A characteristic feature of such systems is continuous adaptability to changing external and internal conditions and continuous improvement of functioning under constant conditions, taking into account past experience. The above properties are typical for self-organizing systems.

By self-organization we mean the development of an optimal algorithm for the functioning of a system and the choice of a learning strategy in accordance with a pledged function, or self-organization is the creation, reproduction or improvement of an organization of a complex dynamic system.

Perhaps the following definition of a self-organizing system is a set of interconnected elements (subsystems) that, independently on the basis of accumulated experience under the influence of the external environment and internal microstates, increase the degree of their organization with the aim of improving the functioning of the system and implementing the inherent functionality.

New approaches to the definition of "self-organization" offer synergetics. One of the properties of self-organizing systems is its purposeful (expedient) behavior. Under expediency is understood as a general characteristic of the behavior of complex dynamic systems, aimed at achieving a specific end result. The concept of expediency means that an act or behavior can be considered directed towards achieving a "goal", that is, a final condition in which the system establishes a certain temporal or spatial relationship with another system. Then the term "expediency" is used as a synonym for a goal controlled by feedback.

Analysis and synthesis of cybersecurity systems with the properties of self-organizing systems should be performed using a systematic approach, i.e. from different sides and at different levels. Within the framework of a unified system approach, an extensive network of mathematical models of systems can be built, taking into account different generalities, different types (classes) of organization and a different subject area.

A cyber security system as a self-organizing system is characterized by a set of functions performed by it. The functional description consists in defining the functions of the system, given in accordance with the spatial or structural feature. System functions are defined through interconnections with other systems.

Analysis of self-organizing structures of cybersecurity systems

Structural description is reduced to the description of the structure based on functional characteristics. The structural approach is otherwise called morphological. It focuses on the analysis of the elements of the structure and their organization. Each element is considered as a system, the functions of which are realized with the help of connections of this element with others. There are informational, structural and financial ties. The informational description of a system determines the dependence of its structural and functional properties on external and internal information.

The mathematical model of a self-organizing system is constructed in accordance with its definition and properties [2–4]. The basis for building the model is a structural-functional approach. From the point of view of this approach, the self-organizing SS system can be viewed as a set:

$$SS = \langle \Sigma, \Phi, R_w, G, A, P, \Theta \rangle,$$

where Σ is the structure of the system;

Φ – system function;

R_w –is the emergence ratio;

G – many goals;

A – the relation of adaptability;

P – a set of memory elements;

Θ – set of time moments.

System structure. One of the most important characteristics of a self-organizing system is its structure. The concept of structure reflects the orderliness, organization of the system. The definition of the concept "structure" is reduced to the statement that this is a way of organizing – interconnection – of separate parts or elements. The structure of the system will be understood as a set of elements and relations between them, which are determined on the basis of the distribution of functions and goals set for the system. Moreover, the structure Σ is considered as a multigraph with certain nodes:

$$\Sigma = \langle S, C, R, R_i \rangle$$

where S is the set of elements of the system (the nodes of the multigraph);

C – the set of parameters of elements (the set of statements regarding the properties of the nodes of a multigraph);

R – the set of connections between the elements (arcs of a multigraph);

R_i – the incidence relation that assigns a pair of nodes to each arc.

The structure of self-organizing systems is characterized by integrity, adaptability and development.

The integrity of the structure of the system is determined by the set of elements and the branched connections between them. Depending on the purpose of the study, there are several criteria for distinguishing a system, forming a system of parameters. The integrity of the system is manifested in two laws:

- the whole is not reduced to the simple sum of the parts;
- a change in one part causes a change in the other parts and in the system as a whole.

The adaptability of the structure of the system, its response to changes in the environment emphasize its dynamic properties – its variability in functioning. The property of adaptability determines the internal transformations of the structure, which are implemented by the elements, do not go beyond its borders and are aimed at maintaining and improving functioning.

The extreme form of system variability is the development of its structure, which is understood as the complication of the system, its accumulation of information, the transition to a more ordered state.

System function It is, in contrast to the structure, an external manifestation of its properties when interacting with the encompassing environment (the market).

The function of the system is a way to act when the goal is achieved and for a self-organizing system is determined by its goal.

Set the system function as

$$\Phi = \langle \Pi, F \rangle ,$$

where Π – the set of variables that determine the function of the system;

$X \subseteq \Pi = W \times M$;

X – is the set of input actions that interact with the information inputs W;

F – the set of functions on variables that, for each element, determine the dependence of the output variables on the input variables.

A state is a set of essential properties that the system possesses at a given time. The state of the system is determined by the set of states of its elements.

The functions implemented by the self-organizing system can be conditionally divided into three groups: target, basic (basic), auxiliary (additional).

The objective function corresponds to the main functional purpose of the system and is set solely by the purpose of its operation.

The main functions reflect the orientation of the system and are a combination of the macrofunctions implemented by it, necessary for the most optimal achievement of the goal, and are determined by the objective function and the system quality criteria.

By additional functions, we will mean functions aimed at maintaining or improving the quality of the system's functioning within certain limits.

The set of functions of the self-organizing system, as well as the structure, is determined by unity, adaptability and development. Since it has integrity, the first condition for its existence should be the unity of its functioning. The function is the defining side of the system and represents the unity of its composite properties, internal processes, relationships. The unity of the functioning of the system is the subordination of the behavior of the system of a single goal. The adaptability of the functions of the system is manifested in their change depending on changes in the external and internal environment. The development of the system in functional terms is expressed in the expansion of its functional capabilities.

Emergence. The emergence relationship R_w reflects the unity of the structure and function of the system, the relationship between them. It is a parameter forming a system: from the two previous objects – structures and functions – it forms a system. Neither structure nor function form a system. The emergence in some way connects the elements of the structure with functions, maps Φ into Σ: $R_w = |\Phi| \times |\Sigma|$, where | … | means a set of elements of Φ or Σ; × – the sign of the Cartesian product of two sets.

Set of goals. The set G corresponds to the set of goals facing the system; G is a multi-grid, i.e., a distributive grid endowed with join, intersection, and composition operations. If $\alpha_1 \le \alpha_2$, then $\alpha_1 \circ \alpha \le \alpha_2 \circ \alpha$ and $\alpha \circ \alpha_1 \le \alpha \circ \alpha_2$ $\forall \alpha, \alpha_1, \alpha_2 \in G$. The order relation on G is interpreted as follows: if $\alpha_1, ..., \alpha_n \in G$ and $\alpha_1 \le \alpha_2$, then the solution of the α_2 problem provides for the solution of the α_1 problem; $\alpha_1 \cup \alpha_2$

interpreted as a task consisting in solving problems α_1 and α_2; $\alpha_1 \cap \alpha_2$ – as the largest of those problems whose solution is obtained simultaneously with the solution of problems α_1 and α_2. The operation of composition on G is interpreted as a strictly sequential solution of problems, and the closure of G with respect to composition means that an arbitrary development of a set of targets in time is provided in the system. The sets Σ and G are connected as follows. Let $H(\Sigma)$ be the set of mappings that preserve the order of a partially ordered set Σ into itself. Then $H(\Sigma)$ is a multigrid with operations $\cup$, $\cap$, and $\circ$, and there is a homomorphism $\gamma : G \to H(\Sigma)$.

The assignment of a mapping $\gamma : G \to H(\Sigma)$ reflecting the restructuring of the system under the influence of the goal *α* can be taken as a comparison of the goal $\alpha \in G$ and the structure $\sigma \in \Sigma$ of some new structure $\sigma' = \gamma(\alpha)\sigma$.

Adaptability. The relationship of adaptability links the behavior and structure of the system with changes in the effects of the external environment and with internal states. Adaptability in some way reflects the effects of the external environment X and the state M on the structure Σ and the function Φ. This ratio falls into two: A_1 and A_2. $A_1 < A_2$ and. Here

$$A_1 = |\Xi| \times |\Sigma|; \quad A_2 = |\Xi| \times |\Phi|$$

where $\Xi = W \times M, X \subseteq \Xi$.

Time. Θ is a directed set of moments of time, that is, a set with an operation ≤. In a self-organizing system, a specific situation ς is put in correspondence with each moment of time, that is, there is a map $\beta : \Theta \to \Omega$, where Ω is a set of situations.

Memory. In order to use previous experience, the cyber security system must be able to accumulate and store information, that is, have a memory. Memory is a set $P = \{z_\beta\}_{\beta \in I}$ of various elements representing a distribution grid with join $\cup$ and intersection $\cap$ operations. The operation of intersection of the elements z1 and z2 is interpreted as the allocation of a common memory area for situations ς1 and ς2, which have similar parts, and the join operation – as the allocation of a part of memory for dissimilar situations ς1 and ς2. The closedness of the set P with respect to the operations of union and intersection extends the number of possible states of memory.

Let $K(Q,U)$ be the set of maps of a Cartesian product $\Omega \times \Omega = \Omega^2$ into the set of solutions U: $K(\Omega,U) = \{\varphi \mid \varphi : \Omega^2 \to U\}$. The set $K(Q,U)$ will also be a distributive grid. For the memory operation, it is necessary that the grid $K(Q,U)$ be mapped homomorphically to the grid P, that is, that a homomorphism $\xi : K(\Omega,U) \to P$ exists.

The structural-functional approach includes two stages.

Structural analysis. One of the most important characteristics of the system is its structure. The structures of self-organizing systems are distinguished by a large number and variety of elements and connections between them, which are derived from the distribution of system functions and the goals set for it.

The goal of structural analysis is to build a visual model that displays the existing system of relations of elements both with the external environment and with each other.

When building models of self-organizing systems, their structure should be considered at the level of organization, functioning and implementation. When analyzing the system at the organization level, the following is done:

- a description of its composition and construction of the structural scheme;
- definition of subsystem functions and drawing up their functional diagram;
- description of connections between subsystems and between elements.

When analyzing at a functional level:

- functions of the system, subsystems and elements are studied;
- their relationships are determined;
- a generalized functional structure of the tasks of the self-organizing system is compiled.

When analyzing at the implementation level:

- identifies the main elements necessary for the implementation of a self-organizing system;
- a structural model of the system is compiled, taking into account the topology of the location of the elements and their interaction with each other and with the external environment.

Functional analysis. Functional analysis is based on the study of the functioning of the system in time, its interaction with the external environment, expressed in its perception of input signals and disturbing influences and in its response in the form of output signals. The functioning of the system in time is determined by its transition from state to state and the change in output signals. We define the concept of functional analysis.

Model of operation – predicts a change in state over time.

The set of moments of time Θ is a directed set of real non-negative numbers. The set Θ can be continuous, discrete, or discrete-continuous. The functioning of the system in time is considered as the transition of the system from state to state.

The state of a self-organizing system is defined as a set of states of its elements:

$$\vec{m} = \left(m_1, m_2, \ldots, m_i, \ldots m_n\right), \vec{m} \in M,$$

where $\vec{m}$ is the state of the system; m_i is the state of the i-th element;

M is the state space, which is defined as the Cartesian product:

$$M = M_1 \times M_2 \times \ldots \times M_i \times \ldots \times M_n,$$

where M_i – set of states of the i-th element.

Input signals $\vec{w} \in W$ of the self-organizing system. Here W is the input signal space, which is a vector $\vec{w}(\tau) = \left(w_1(\tau), w_2(\tau), \ldots, w_i(\tau), \ldots, w_n(\tau)\right)$, where $w_i(\tau)$ is the input signal at the i-th input of the system at the time τ.

The input signal space W is called the direct product $W = W_1 \times W_2 \times \ldots \times W_i \times \ldots \times W_n$, where W_i is the set of signals of the i-th input.

The output signals of the system $v \in V$ are defined in the same way as the input signals: $\vec{v}(\tau)=(v_1(\tau),v_2(\tau),...,v_i(\tau),...,v_m(\tau))$, where vi($\tau$) is the signal of the i-th output at the time τ.

The output signal space $V = V_1 \times V_2 \times ... \times V_i \times ... \times V_m$, where V_i is the set of signals of the i-th output.

The study of the dynamics of self-organizing systems is complicated by the fact that they are systems with aftereffect. The future of its behavior depends on the prehistory of its states, i.e. the state $\vec{m}(\tau)$ of the system at a time $\tau > \tau_0$ is determined by how it came to a state $\vec{m}(\tau_0)$. The difficulty also lies in the fact that these systems belong to the class of indeterministic. To trace the causal relationships in them is impossible. The dependence of the output signals on the input and on their states is ambiguous.

Structural and functional model. Although biological self-organizing systems may be distributed, it seems appropriate to select in them the blocks corresponding to the functions performed. Taking into account the above presentation of the self-organizing system, the structural-functional model shown in (Fig. 1) is proposed. Here are the following designations:

– S is a self-organizing network;
– BSP – block the source program;
– the BSS is a block of structural self-organization;
– BFS – block of functional self-organization;
– BPS – block parametric self-organization;
– BG – block of the goals;
– BCC – block of criteria calculation;
– BM – block of memory block;
– BC – control block.

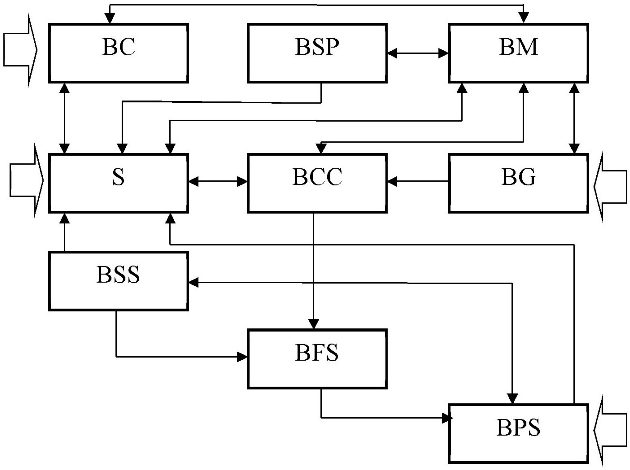

Figure 1. – Structural and functional model of self-organizing system

External environment. The external environment will be understood as a set of elements that are not included in the system, but a change in their state causes a change in its state. Since the system is connected to the environment with its informational and control inputs and outputs, we will assume that the environment affects the system through its inputs. The medium may include any source of information. Sometimes, for the purpose of simplification, the environment is considered as a source of successive signals, selected from a finite alphabet. In the case of a cybersecurity system, the external environment is a multitude of sources of threats.

Self-organizing network. It is the network S of the self-organizing system that represents the indeterministic part of the system. With the help of other blocks, an object model is built on the network, a sequence of heuristics and self-organization algorithms are implemented.

We define a sequence of heuristics as a sequential construction of a statement in discrete time, when at the initial moment a certain system of statements is specified, and at each next moment a system of statements is obtained according to certain rules (programs) from those available at the previous time. These rules may change during the evolution of a sequence of heuristics.

The sequence of heuristics is characterized by the ambiguity of intermediate results. The ambiguity is determined, on the one hand, by its nature as a search procedure, on the other, by the position of each of the rules applied in their general list, as well as accumulated constraints and heuristics. By fixing the sequences of states of the self-organizing system, as well as the laws and heuristics that led to the achievement of the goal, one can obtain various implementations of the heuristics sequence.

The sequence of operations given in a certain self-organizing system when it reaches its goal, obtained when implementing a certain specific set of conditions, is called the implementation of a sequence of heuristics.

A network consists of a set of elements determined by the complexity of the task, with a changing function of the element and a multitude of adjustable connections. The parameters of links and elements, their functions change depending on the class of the tasks being solved, their specific conditions and environmental conditions when solving the problem. Network rebuilding is carried out depending on the state of other units of the system.

Source program BIL makes a selection of the types of elements used in solving a particular class of problems. Specifies a preliminary structure of the system, a preliminary set of functions of the elements that will be used during self-organization, a preliminary set of parameters. In addition, it sets restrictions on the structure of the system, types of functions of elements, parameters. The source program may include an extension of the class of tasks solved by the system.

Structural self-organization. The BSS changes the network structure by increasing or decreasing the number of elements in the network, changing the pattern, number and nature of connections. This unit controls the highest level of system adaptability.

Functional self-organization. The BFS adapts the type of functions of network elements according to and controls the start of structural self-organization when the resources of functional self-organization are exhausted and the target is not achieved.

Parametric self-organization. BPS adjusts the system parameters by one of the methods described above. If the target is not reached within a certain time, it starts the block of functional self-organization.

The goals of the self-organizing system. BC manages the development of criteria for self-organizing system. The goals of the system in this case are set from the outside and are predefined for the system.

Calculation of the criteria. The selection and calculation of criteria is carried out by BVK. The selection of criteria is determined by the goal and is made from the set of permissible criteria that are heuristic and is laid in IOO during the design of the system.

The accumulation and storage of information is made in the BP, which is associated with almost all the blocks of the self-organizing system. It stores information about the past behavior of the system, about the situations that led to the achievement of the goal.

Control block. Recording and retrieval of information from the memory, depending on the signals at the control output of the network, is controlled by the BC.

Sustainability, sensitivity and flexibility of organizational structures of Cyber Security

In the theory of automatic control of systems, the stability of a system is understood as its ability to return to its original state when external influences are eliminated. This definition, when applied to cybersecurity structures, would mean that the technological and organizational structures are capable of self-healing (or self-organization) when restoring the previous state of the functioning environment. However, firstly, this situation does not take place in cyber threats, since they are in continuous development under the influence of various factors, such as changes in the general nature of threats, the emergence of hybrid threats, general economic trends, scientific and technological progress and other factors. Therefore, it cannot be considered possible to return to the initial state, i.e. complete removal of external influences. Secondly, the technological and organizational structures can undergo changes only as a result of the decision made on its reconstruction, modernization, replacement, etc. Although at some stage in the development of the security system it may be advisable to return to the structure that has already been used, the decision to do so is made in a specific situation and is a consequence of responding to external threats.

Thus, the concept of sustainability, as it exists in the literature, does not apply to the structures of cybersecurity systems.

Another concept of sustainability is formulated by J. Casti [5]. Considering the structures described by oriented graphs, we introduce the concept of stability, connecting the effect of changes in the value of the function $v_i(t)$, describing the state of a vertex of the graph u_j to the initial changes of $p_j(t)$ to another u_j depending on the intensity of the influence $f(u_i, u_j)$ (propagation of disturbances in the graph). A node u_i is called stable if an infinite sequence of values of the function $v_i(t)$ is bounded. And the whole graph is stable if all its vertices are stable.

The structure of cybersecurity systems that ensure the sustainable implementation of various business processes operating in virtual environments created by Internet technologies is, as a rule, a hierarchical structure that can be described as a tree type graph, where each of the vertices is in turn described by a graph primarily of information flows. Within the framework of the strategic management structure, the cybersecurity system structure is a subgraph, some of its vertices are adjacent to the vertices of another graph, representing the structure of both cyber attacks and means of countering them. The complexity of using the concept of sustainability lies, firstly, in determining a single function that characterizes all the vertices of the structure, and secondly, in determining the intensity of influence of some structures on others, and finally, this concept of sustainability does not take into account the possibility of changing the composition of the vertices of the structure graph, which is precisely the most important in the study of the structures of cybersecurity systems.

Thus, it is necessary to develop such a concept of sustainability, which would [6]:

- took into account the continuity of changes in the structure of multiple cyber attacks of the security system;
- did not contradict the specifics of changes in the technological and organizational structure of the cyber security system associated with decision making;
- took into account the possibility of changes in the composition of the elements of the structure;
- had an interpretation in both information technology and economic categories and would allow to construct quantitative assessments of all components of the structure of strategic, tactical and operational management.

From the point of view of assessing the quality of the structure in relation to the environment of the formation of cyber attacks, the tasks of assessing sustainability are the most important. They are designed to clarify the conditions for maintaining the structure. If the concept of structure flexibility can be viewed from the standpoint of the flexibility of hardware and software, then the concepts of stability and sensitivity are not considered at all. To introduce these concepts, it is necessary to consider the structure as a dynamic object with the property of adaptability. The following construction is not limited to the framework of a certain structure that constitutes a structure, first of all, of strategic management, but is in a sense universal and proceeds from the general principles of sustainability.

In the future, if the structure that is part of the overall cybersecurity strategic management structure is considered in its relationship with others, it will be called a substructure. If the structure is considered independently, then it will be called simply a structure.

Consider the external environment of any substructure. It includes both the external environment of the entire security system and other substructures. Over time, the external environment of functioning undergoes certain changes. Let the external environment be described at each moment of time t by the vector of parameters ξ_t from the space of possible states of the external environment Ξ. Fixing some time point t_0, we follow the change of the vector t_0 during the time interval $[t_0, t_1]$. During the time $D_t = t_1 - t_0$ in the space of possible states of the external environment Ξ, the trajectory of the environment will be formed, consisting of the sets ξ_t, $t \in [t_0, t_1]$. Denote the time interval $[t_0, t_1] = T$. If the laws of environmental change are known, and it is possible to unambiguously determine its behavior on the interval T, then in all subsequent constructions the concept of a trajectory can be used. For the purposes of determining sustainability, it is not so much the change in the state of the environment of the formation of cyber threats in the past observed periods as the prediction of its state and the predicted trajectory. The laws of changing the state of the environment of a security system cannot be considered absolutely known due to its great variability and insufficient knowledge. Therefore, we can only talk about the predictive set of environmental conditions. This set is determined by the factors taken into account, forecast accuracy, initial conditions, etc.

We call the set of predicted states of the external environment on the interval T the variety of the external environment Ξ_T. The volume of this variety, $- V_\Xi -$, will be determined by the variability of the external environment, the parameters describing it, and the accuracy of the forecast. The specific form of this quantity depends on the structure under consideration and needs special construction.

Let S be the space of various structures of one purpose (for example, structures of information security systems). The concept of quality includes, as an integral part, the degree of compliance of the security system structure with a multitude of potential cyber threats in such a way that the structure should as far as possible meet the requirements of the external conditions at each point in time. Consequently, each point ξ_t of the trajectory of the environment in the space Ξ will correspond to some structure S_t from the space S. The combination of these structures constitutes the trajectory of the structure during the time interval T.

Considering the predictive set of states of the environment, we obtain the set of all structures corresponding to the elements of the variety of the environment. We call this set the variety of structures S_T. Thus, if $a()$ is a mapping that allows the structure S to be constructed from the current state of the external environment (multiple attacks) ξ, then we have:

$$0 : \Xi \to S, \tag{1}$$

$$a(\Xi_T) = S_T. \tag{2}$$

The main characteristic of the diversity of S_T structures is its volume $- V_S$. The essence of the V_S volume is a reflection of the degree of diversity of structures that need to be built to ensure that the structure corresponds to the set of potential cyber threats from the environment of operation at each time point from interval T.

The concepts introduced allow us to come to the following definition of stability.

Definition 1. The stability of the structure – the ability of the structure to ensure the invariability of the results of the functioning of the cybersecurity system with a constant strategy of its behavior under the conditions of hybrid threats (the ability of the structure to correspond to the greatest possible diversity of the external environment).

The structure S_0 corresponding to the initial state of the external environment ξ_0 is called stable in correspondent to the variety Ξ_T, if the condition

$$V_S(S_T) << \delta V_\Xi(\Xi_T), \tag{3}$$

where the variety Ξ_T is obtained by the prediction on the initial state ξ_0;
the variety S_T is obtained according to (2).

The concept of sustainability thus defined is closest to the sustainability of adaptive systems.

The concept of sensitivity of a structure is closely related to the concept of stability. They can be considered as reciprocal. Depending on the situation in which the structure is studied, and the objectives of the study, either both concepts can be used, or each of them separately.

Definition 2. Let us call the sensitivity of a structure the ability of a system to change its state and the result of functioning when changing a multitude of cyber threats from the external environment. The measure of sensitivity is the ratio of the volume of necessary changes that must be made in the structure to the volume of changes in the state of the environment from the point of view of multiple cyber threats during the period of time T:

$$d(S_0,T) = \frac{V_S(S_T)}{V_\Xi(\Xi_T)}. \tag{4}$$

The measure of sensitivity and stability are among the many criteria for the quality of a structure. The importance of the criteria is determined by the current situation and the purpose of the functioning of the security system as a whole. As was noted, in different situations of functioning of cybersecurity systems, the criteria may have different interpretations and, moreover, the very concept of quality includes a different set of criteria, the role of a particular criterion as positive or negative also depends on the situation of solving problems. In particular, under the conditions of a constructed and functioning structure, the addition of the concept of stability is stability with correspondence to transformation.

Let some resources be allocated to ensure compliance of the structure with the current state of the environment, for example, the amount of funds that can be spent on the transformation of the cybersecurity system (or the allowable amount of losses from non-compliance with many cyber threats) – C^* and the maximum time T^*. Then, if the original structure S_0 is to be transformed into S_t, then the transformation process must satisfy the following conditions:

$$C(S_0,S_t)'' \ C^* \tag{5}$$

$$t(S_0,S_t)'' \ T^* \tag{6}$$

where $C(,)$ – transformation cost;

$t(,)$ – time to transform.

The restriction (5) reflects the availability of funds for the transformation, and the restriction (6) means that the transformation must not only be carried out, but also within a certain period. A longer time deprives of its expediency, since the forecast of the state of the environment cannot be reliable for a longer period due to its large variability.

Definition 3. We call a structure flexible with correspondent to resources if the changes that need to be carried out in it during time T satisfy the constraints (5) – (6).

If, along with the variety of structures of S_T, the variety of S_R can be obtained – all sorts of transformations of the original structure within the constraints, then the concept of sustainability receives the following extension.

Definition 4. We call a structure stable in resources with correspondent to the variety $\Xi_{''}$ if $S_R \supseteq S_T = a(\Xi_T)$.

Those, the structure has the ability to comply with the state of the external environment (the set of potential cyber threats) for a given period of time with given restrictions on resources.

From consideration of the concepts introduced, it follows that the process of assessing the stability of a structure breaks down into a number of subtasks:

Determine the set of parameters describing the set of cyber threats from the external environment – ξ.

Determine the current state of multiple cyber threats from the external environment – ξ_0.

Predict the state of the multitude of threats for a given period of time T and build a diversity of the external environment $\Xi_{''}$.

Design a mapping $0()$, allowing to construct the structure under study.

Construct the structure S_0, corresponding to the initial state ξ_0 and the variety S_T, corresponding to the variety $\Xi_{''}$.

Determine the stability and sensitivity of the structure S_0 with respect to the variety $\Xi_{''}$.

To determine the flexibility of the structure, it is necessary to solve additional problems.

Determine the amount of resources allocated for the transformation of the cybersecurity system (C^*,T^*).

Identify the many possible transformations – S_R.

Determine the flexibility of the structure with respect to resources.

Conclusion

In the modern environment of the Internet virtual space, there is an invariable threat of cyber-attacks. It should also be considered the different nature of these cyber threats and the appropriate environment or distribution space, for example, data transmission channels, data processing systems or computing systems, as well as data warehouses. In most cases, cyber threat is not only one type of attack, intrusion or data compromise, but a series of certain way planned or relatively random incidents that can provoke a synergistic effect of their influence and lead to extremely undesirable consequences. Consequently, a special approach is needed to ensure the reliability of cyber defense, considering the hybrid nature of the threats and the actual open space of the Internet, including other (heterogeneous) conditions for transmission and communication in the digital environment.

It is proposed to consider the cyber defense system as a self-organizing organizational structure, which is constructed like the functioning, development and adaptation of biological organisms. This should contribute to the creation of systems that provide an adequate level of protection when the conditions for self-organization and adaptation to external threats are realized, as well as the desire to obtain a synergistic effect on the cyber defense systems. For the construction of such systems described mathematical tools. In turn, the direction of development of self-organizing organizational structures of cybersecurity systems should satisfy the conditions of stability, sensitivity and flexibility of organizational structures.

References:

1. Camazine Scott. Self-organization in Biological Systems / Scott Camazine, Jean-Louis Deneubourg, Nigel R. Franks, James Sneyd, Eric Bonabeau, Guy Theraula. Princeton University Press, 2003.– 538 p.
2. Gershenson Carlos. Design and Control of Self-organizing Systems. Mexico City Boston Vicosa Madrid Cuernavaca Beijing CopIt ArXives, 2007.– 188 p.
3. Gershenson C. A General Methodology for Designing Self-Organizing Systems. ECCO working paper 2006. 2005–05.
4. Fernando Rosas, Pedro A. M. Mediano, Martín Ugarte, and Henrik J. Jensen. An Information-Theoretic Approach to Self-Organization: Emergence of Complex Interdependencies in Coupled Dynamical Systems. Entropy 2018. 20, 793.
5. Castie John. Large systems. Connectivity, complexity and disaster.– M.: Mir, 1982.– 216 p.
6. Milov A. V., Polyakova O. Yu. Modeling the system characteristics of the economy. Lecture notes.– Kharkov: Publishing House INZHEEK, 2004.(Russian).