ПРОГРЕСИВНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

ПРОГРЕССИВНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

PROGRESSIVE INFORMATION TECHNOLOGIES

UDC 681.327.12

MODELING THE SECURITY POLICY OF THE INFORMATION SYSTEM FOR CRITICAL USE

Bisikalo O. V. – Doctor of science, Professor, Dean of the Faculty of Computer Systems and Automatics, Vinnitsa National Technical University, Vinnytsia, Ukraine.

Kovtun V. V. – PhD, Associate Professor, Assistant Professor of Computer Control Systems of Vinnitsa National Technical University, Vinnytsia, Ukraine.

Yukhimchuk M. S. – PhD, Associate Professor, Assistant Professor of Computer Control Systems of Vinnitsa National Technical University, Vinnytsia, Ukraine.

ABSTRACT

Context. Compared to universal information systems, the information system for critical use has a simplified structure of the information environment and specific requirements regarding the volumes and nature of information resources. This fact allows us to refuse excessive detail and to narrow the simulation object to the process of forming a security policy for an information system for critical use, an adequate problem description of which is achievable under the condition of a rational choice of the mathematical apparatus.

Objective. Synthesis of mathematical apparatus for the complex unified description of static and dynamic, controlled by integrity and authenticity, processes in the information system for critical use in its hierarchical representation.

Method. In the article new complex mathematical models of processes of information processing and access separation to it are obtained, which, in contrast to the existing ones, describe in the framework of the mathematical apparatus of E-networks mechanisms for protecting the environment and resources of the information system for critical use and allow to quantify the integrity of its information resources. The mathematical models of the synthesis of the policy of safe information processes interaction in the information system for critical use are developed, which allow guaranteeing the observance of local security policies on the various structural elements of the system and integrating them into the global security policy, observing a single discretionary policy everywhere in the system.

Results. The practical consequence of the obtained theoretical results is the methods of optimizing the operation of the data processing and the access separation units, which are responsible in the information system for critical use for controlling the information integrity and the authenticity of access to it, respectively. In particular, the model of security policy of a information system for critical use adapted for practical application, a method for dynamically information integrity controlling with a corresponding criterion based on the mathematical apparatus of semi-Markov networks for a comprehensive stochastic description of discrete states of the information integrity control at selected hierarchical levels of the system during the continuous discretionary access. The method allows us to select the maximum allowable values of information integrity control coefficients at the sub-levels of the OSI application level allocated in the information system for critical use based on the pre-set amount of the size of controlled information, the speed of information integrity control and the maximum period of the system is in the appropriate state. Also describes a method for controlling access to information processes that are described by superblocks on the E-network representation of the ISCU using sets of classifiers integrated into each block of the superblock that capture the fact of exceeding the corresponding thresholds by weighted degrees of identity of the attributes of the object that wants to access, which allows us to classify the identified information threat and initiate the corresponding reaction described in the system security policy. The analysis of the results of the experiments allowed to obtain optimal parameters of groups of classifiers, which, in the framework of global, local and discretionary security policies, prevent the unauthorized access to system information resources or attempts to violate their integrity.

Conclusions. The article presents for the first time the mathematical model of the information system of critical use, in which, unlike the existing ones, a single approach has been introduced to describe information processes within the global, discretionary and local security policies with an attachment to the hierarchical structure of the information system, which allows analysis and synthesis of functions services supporting user roles based on the object-relational model of organization of information resources of the

DOI 10.15588/1607-3274-2019-1-13

system, to perform their integration, induction and ensure compatibility within a single security policy, to control the information and the authenticity of static and dynamic access to it.

KEYWORDS: information system for critical use, security policy, data processing unit, access separation unit, automated speaker recognition system for critical use.

ABBREVIATIONS

ASU is an access separation unit;

DB is a database;

DMS is a database management system;

DPU is a data processing unit;

IICS is an information integrity control subsystem;

IS is an information system;

ISCU is an information system for critical use;

ISSS is an information system security subsystem;

SP is a security policy;

NOMENCLATURE

α is a type of authorization procedure;

$\varphi_b(\tau)$ is a Laplace-Stieltjes transformation of the basic probability distribution of a random variable τ;

$\Omega_i(j)$ is a result (marking) for the access points within the type of SP for the i-th structural element of the E-network;

ξ is a vector of parameters of the basic distribution law;

τ_{dm} is a random value of the duration of the process of the information integrity control during discretionary access m;

τ_i is a random value of the time of the IICS's stay in the state i;

c is a speed of the information integrity control;

D is a set of precedents;

B is a set of superblocks allocated on the E-network of the ISCU, in the formation of its SP;

B_l is a superblock of E-network order l;

$E(\tau_m)$ is a dynamic performance criterion for IICS of ISCU;

E is a formalized description of the E-network of the ISCU;

E_f is an ability of the ISCU to perform its functional duties while maintaining the data integrity;

E_s is an ability of the ISCU to maintain a given performance indicator without the information integrity controlling;

$E_{s\min}$ is a operational constant;

$F_b(\tau)$ is a function of the basic law of the probability distribution of a random variable τ;

$f_b(\tau)$ is a density of the basic law of the probability distribution of the random variable τ;

G is an E-network representation of the software and hardware component of the ISCU;

G_A is a set of arcs of the state graph of the E-network of the ISCU, which describes the actions of active users within the roles defined for them;

G_E is a set of entities-superblocks of the ISCU, described by sets of vertices of the graph of the E-network;

G_I is a function of the hierarchical structure of the ISCU;

G_M is a set of arcs of the state graph of the E-network of the ISCU, which describe the information flows between the entities of the ISCU;

G_R is a set of arcs of the state graph of the E-network of the ISCU, which describe the users roles;

$H(\tau)$ is a characteristic matrix of the semi-Markov process of information integrity controlling in the ISCU in time;

I is an index of module u and a block, in which this module is upper;

i is an iterator;

J is a sub index of the index I;

j is an iterator;

K is a number of lower modules in the block with the index I;

K_{dm} is a random variable of the coefficient of the information integrity control during discretionary access m;

K_i is a coefficient of the information integrity control when the IICS is in a state i;

$K_{\max i}$ is a maximum predicted value of the coefficient K_i;

k is an ISCU's level number;

L is a number of levels of the ISCU;

l is an ISCU's level number;

l_h is a number of the higher level of this layer of the ISCU;

l_l is a number of the lower level of this layer of the ISCU;

M_A is a set of the ISCU administrators;

M_{in} is an input marking function that determines the state of the input positions of the module with the index by the types of authorization procedures α;

M_F is a set of functions that provide the performance of defined ISCU roles;

M_{out} is an initial marking function that defines the status of the source positions of the module with the index by type of authorization procedures α;

M_R is a set of roles, each of which defines the limits of the capabilities allocated by the administrators for the corresponding classes of users;

M_U is a set of the ISCU users;

DOI 10.15588/1607-3274-2019-1-13

P is a set of positions for obtaining access to the E-network-based ISCU;

P_l is a set of positions for obtaining access to the l hierarchy level of the ISCU;

Q is a set of simple positions of the E-network of the ISCU;

Q_l is a set of simple positions of the l hierarchy level of the ISCU;

Q_z is a set of potential targets of intruders that are elements of the E-network representation of the ISCU;

r is a logical variable of the permissibility of an authorization;

S is a set of positions (layers) of E-networks of the ISCU;

S_l is a set of positions (layer) of the l hierarchy level of the ISCU;

t is a time variable;

T_i is a maximum permissible time of stay of the IICS in a state i;

U is a set of modules of the E-network of the ISCU;

U_l is a set of modules of the l hierarchy level of the ISCU;

u is an element of a set of modules of the E-network of the ISCU;

V_{dm} is an entire amount of information, the integrity of which has to be controlled;

V_i is an entire amount of information, the integrity of which has to be controlled when the IICS is in a state i;

v_i is a random amount of information, the integrity of which has to be controlled during the period of the IICS being in a state i;

v_{dm} is a random amount of information, the integrity of which has to be controlled during discretionary access m;

Z is a set of classes of information threats.

INTRODUCTION

The information system [1] is a structural and functional set of technical, software and other means created to support one or more types of information processes and provide information services. Actual IS are inherent hierarchy, decentralization, functional distribution, parallel execution of custom tasks, etc. Such systems function in conditions of active information exchange under the influence of random and negative factors with high cost of consequences of possible violations or errors in their work. The structure of such systems is formed according to the purpose of functioning and is characterized by high complexity on elemental saturation at the software and hardware levels, which is reflected in the complexity of control algorithms and mechanisms of switching elements of the system.

Critical use of IS due to the importance of the information resources of such a system leads to the need for an integrated approach to the implementation of its security, including protectiFon of communication channels, protection of the authorization process for users (authentication) and programs, protection of remote elements of the system, holistic protection of the whole system and the creation of algorithms system behaviour when detecting information threats. Accordingly, the protection subsystem of such an IS must combine the mechanisms of protection of the components of the information environment (IS as such), mechanisms for minimizing risks for components of the information environment and information resources (data present in the IS), a set of procedural, logical and physical measures aimed at countering threats to information resources and components of the information environment. Since the security of the information resource implies the impossibility of its loss due to failures of the components of the information environment, the task of securing the information resource is decomposed into the task of ensuring the reliability of the computer database, which guarantees the continuity of the functioning of the information environment, and the problem of counteraction and prevention of threats to information resources. The requirements for ensuring the safe operation of IS are embodied in security policies [2]. The execution of the SP ensures that, in case of occurrence of foreseeable problem situations as a result of unwanted factors of different kinds, the system will be able to fulfill its target function in full.

The above information allows us to assert the impossibility of constructing an adequate mathematical model for an exhaustive description of the functioning of the IS. However, the critical use of IS narrows as characteristics of the information environment and the amount and nature of information resources that are in such an information system. This circumstance allows us to abandon excessive detail and to narrow the simulation object to the process of shaping the security policy of an information system for critical use, an adequate problematic description of which is achievable under the condition of a rational choice of the mathematical apparatus.

The object of study – the process of synthesizing an adequate SP for an ISCU.

The subject of study – the mathematical apparatus of E-networks for describing the mechanisms of security of environment and resources of ISCU in the form of SP. Mathematical apparatus of semi-Markov models for a comprehensive stochastic description of discrete states of the information integrity control at selected hierarchical levels of ISCU during continuous discretionary access.

The purpose of the work is to create an adequate mathematical model of the SP for ISCU and to generate methods for the practical application of the results of such simulation.

1 PROBLEM STATEMENT

We represent the generalized mathematical model of ISCU in the form of a tuple $\langle M_A, M_C, M_R, M_F, t \rangle$. Under security policy we will understand a complex of methods

© Bisikalo O. V., Kovtun V. V., Yukhimchuk M. S., 2019
DOI 10.15588/1607-3274-2019-1-13

that regulates the management, protection and distribution of information. Sources of danger in this case will be: the unpredictability of the result of intersection of the roles and functions of a particular user $M_R \cap M_F \forall c \in M_C$ due to the imperfection of the formal description of the system, imperfection of the users and services authentication process, the potential incompleteness or unauthorized loss of information resources. Therefore, only the adequate security policy, which is strictly formalized within the framework of the chosen mathematical apparatus, describes the permitted processes of formation and interaction of the elements of the sets from the above-mentioned tuple, controls the completeness and predictability of the results of this interaction, detects and identifies the unauthorized processes, ensures the users and services authentication processes, controls the integrity of information resources and allows us to detect deviations from the provisions of the SP and uniquely regulates the corresponding system response for such cases.

2 REVIEW OF THE LITERATURE

At the international level, the notion of information security is generally regulated by ISO/IEC 27001:2013 [3], whose annexes describe a set of measures for information security management. Directly on the issue of information security is devoted to 14 sections of Annex A of the standard: A.5 “Information Security Policies” – defines how information security policy is created, verified and managed; A.6 “Information Security Organization” – defines the list of types of users and their privileges, and also describes the organization of remote access to information, including using mobile technologies; A.7 “Safety of human assets” – fully describes the staff interaction with a controlled by IS environment; A.8 “Asset Management” – clustering information resources of IS. Identifies the peculiarities of the storage, management and information access processes at the hardware level; A.9. “Access Control” describes measures for the safe access to information resources within the framework of a defined security policy and taking into account the provisions of sections A.6-A.8 of the standard; A.10 “Cryptography” – describes the admissible technologies of information encryption and key management process; A.11 “Physical security and environment security” – describes the procedure for organizing security zones, the order of protection against identified threats, the order of security of equipment, the order of information destruction and the policy of “clean table” and “clean monitor”, etc.; A.12 “Operation Safety” – describes the process of managing the proper functioning of the entire complex of software that supports functioning of the information environment of IS; A.13 “Communication security” – defines network security measures; A.14 “Acquisition, development and maintenance of systems” – describes the steps taken to ensure the development, acquisition and maintenance of software and hardware components for functioning of IS; A.15 “Relations with suppliers” – describes a safe procedure for work with equipment, software and services suppliers; A.16 “Information Security Incident Management” – describes the procedure for writing reports of disadvantages, imperfections and vulnerabilities of IS, and procedures for responding to them; A.17 “Information Security Aspects for Ensuring Business Continuity” – describes the order of work planning for the continuous operation of IS; A.18 “Relevance” – describes the issues of compliance of information resources and the way in which the information environment of IS is organized in accordance with applicable law, in particular, on the protection of intellectual property, personal data, and the order and organization of information security checks. In general, the standard lists 114 aspects for the security of the information environment and information resources of IS, which in general describe the mechanisms of information security, mainly without guidance on the application of specific technologies, due to their rapid evolution.

According to ISO/IEC 27001:2013, protected IS have to successfully counteract the types of attacks defined during its design stage for given external operating system conditions. Usually, in order to achieve such a result, the SP of IS includes mechanisms that implement only part of the 114 aspects formulated in the standard [3]. This way of creating a SP is much faster, cheaper, and generally satisfies the standard [3], but does not guarantee the absence of vulnerabilities due to the lack of a systematic approach in its implementation.

The information search did not reveal studies where the concept of security organization of the ISCU is described at the proper level of formalization, which determines the relevance of the research presented in the article.

3 MATERIALS AND METHODS

Of course, research on the issue of the safety of ISCU should begin with its definition as a research object. ISCU is a partial case of ISs that, according to ISO/IEC 2382: 2015 [4], includes systems for the storage, retrieval and processing of information and related organizational resources that provide and distribute information.

In the broad sense, the integral components of IS are data, hardware (including communications) and software, personnel and organizational measures. ISCS, respectively, is an information system that operates so much important data that unauthorized access can lead to significant material or human losses. For the system representation of ISCU, we will use the OSI hierarchical network model [5], which, however, focuses on the communication component, while the program component is represented only by the application layer. Adapt the OSI model to describe the ISCU by breaking down its application level by sub-level, as presented in Table 1.

Further formalization of the description of the ISCU, based on the hierarchical structure presented in Table 1, is proposed to be carried out on the basis of the mathematical model of information circulation [6–9] in which, by standardizing the interfaces of the conjugation

© Bisikalo O. V., Kovtun V. V., Yukhimchuk M. S., 2019
DOI 10.15588/1607-3274-2019-1-13

Table 1 – The hierarchical structural organization of the ISCU within the application level of the OSI model

Structural element of the ISCU	The role of the structural element		Sub-level of the application level OSI, allocated within the framework of the ISCU
Administration unit	Set privilege for a set of user roles		**Administrative**
Access separation unit	Recognize the identity of the user to decide on his rights to an appropriate role in the ISCU. Supports functioning of the highest level of software of the ASU of ISCU.		**Identification**
Virtualization unit	Create a virtual working environment for an authorized user in accordance with its role		**Integration**
The ISCU resource access organization unit	Launches program manager of ISCU, which, in accordance with the role of an authorized integrator, launches system applications, utilities and access services to the ISCU resources. Supports the work of high-level software of DPU of ISCU.		**Dispatching**
Network navigation unit	Provides initiation and support of information exchange with the corresponding ISCU servers by the generated authorized program manager for the search for information		**Navigational**
Data transfer unit	Supports access to the authorized navigation tool to two types of the ISCU servers:		**Server**
	Registration server	*Unique data server*	
Object control unit	Provides support for user authentication procedures (low level of software for the ASB) and data integrity monitoring (low level of software for DPU)	Organizes the work of the authorized navigation tool with the data placed on the server according to the formulated request using the application-applied interpretations installed on the server	**Applied**
Resource management unit	Provides access for the authorized interpreter to the server resources manager. Supports the operation of the DMS kernel as the lowest level of software for DPU		**Managerial**
Data unit	Provides access to the authorized resource manager to the server databases, among which, according to the type of server, distinguish:		**Informational**
	Access authorization database, database subsystem of communication, database of information records	Database for the authentication procedure, database of profile data	

of application processes and service complexes with decomposition of the levels of access to ISCU resources, combining flexibility with each aspect of data security: confidentiality, availability and integrity. Under the flexibility of protective mechanisms in the context of confidentiality and accessibility, we will understand the rationale of the delineation of access to information, and under the inviolability – the quality of the SP model used in the ISCU. Necessary for SP modelling is the creation of its global (syntactic) model that describes the desired properties of DPU of ISCU, and sufficient – the creation of a local (semantic) SP model that describes the rules for the transition between the established states of the DPU. In the presence of a local model of SP is considered dynamic, and in its absence – static. A dynamic model of SP with a finite set of states is called a model of finite states [10]. The basic safety theorem [9] theoretically substantiates the fundamental safety of the model of the final states of the DPU of ISCU: if at the initial moment of time the global security policy is implemented and all the transitions between the DPU of ISCU satisfy the local SP model, at a later time, the global safety model will also be implemented, that is, ISCU vulnerabilities appear at the stage of its practical implementation, and not laid directly into a correctly synthesized SP model. The second indispensable component of the security of the ISCU is the ASB, which is best described in the context of the global SP by the discretionary model [11], which regulates the process of user progress towards resources of ISCU within defined roles, not taking into account the state and interconnections of DPU. However, unlike the model of finite states, the discretionary model is potentially dangerous. Secure the discretionary access processes by running each one in a dedicated, controlled, and independent process with a uniquely defined sequence of end-to-end transitions. In such a concept, the arbitrary discretionary access process, governed by global SP rules, will represent the corresponding algorithmic sequence of authorized accesses of higher-level components to the resources of the current or lower level components that are combined into a clear vertical hierarchy of ISCU, with the parameters set by the local SP rules.

In order to convey the specifics of the global and local SP organization of discretionary access to the resources of ISCU, the structure of which consists of DPU and ASU components with the above characteristics, we use the mathematical apparatus of E-networks [6–9]. Within the framework of the E-network concept, a structured process in the ISCU is presented as a basic element – a number j level l_h module, which is the result of grouping according to the meaning of the process of several neighboring levels of the ISCU with numbers $l=\overline{l_l,l_h}$ where $l_l = l_h - j + 1$. The structure of the E-network is blocked. Each module of the E-network contains a set of pairs of opposite input (simple) and output (access) positions, which differ in a unique mechanism of authorization. Number of items in the module is equal to the number of authorization mechanisms.

To identify the modules and blocks of the E-network of ISCU we will introduce a system of indices, based on the module's membership to the levels of the ISCU and the internal numbering of modules in the blocks. Define

DOI 10.15588/1607-3274-2019-1-13

the j order index as a sequence $i_1.i_2.\dots.i_j$. The level l modules are identified by the $(L-l)$ order indexes $l=\overline{1.L}$. All modules of a certain block are divided into upper and lower ones, according to their location at the levels of the ISCU. An arbitrary block of an E-network with an index I contains a single top module with an index I and $K[I]$ lower modules with numbers $j=\overline{1,K[I]}$ correspondingly, which is equivalent to the $I.j$ expression for any j module of the lower level of the I block. Accordingly, we will consider the J index as a sub-index of I index – $J\subset I\equiv I\supset J$ if $I=J.i_1.i_2.\dots.i_k$, and the case $((J\subset I)\vee(J=I))$ we will mark as $J\subseteq I\equiv I\supseteq J$. The logical variable $r=r(I,\alpha)$ describes the result of the type α authorization procedure in the module with the index I. With each idle position associated time delay procedure and conversion procedure, which is accompanied by an appropriate change in the values of the characteristic attributes of the user object. With each access point, the conditional branching operation is associated with different types of authorization procedures, the results of which are marked by the system for the user object characterized by a set of features – attributes. Each object can be moved by the positions of one authorization procedure, which is indexed in the set of authorization procedures for the transaction. Moving an object, depending on the result of the authorization procedure, can occur either from the input position of the module in to the opposite to it output or in to the input position of the same authorization procedure of the second module of the same block with the descent to one level of the hierarchy of the ISCU, or in to the input position of the same authorization procedures of the module L-level hierarchy of the ISCU. At the same time (in parallel) a lot of objects can be processed in the system, with some authorization procedure can be deferred by the time delay procedure set by the system for the corresponding module. Upon completion of the time delay procedure, the object moves with possible absorption or reproduction procedures, accompanied by corresponding transformations of the values of its attributes. Sum up the above described describing the E-network module in the form

$$u=\langle I,q,p\rangle\in U_l\,, \tag{1}$$

where $I=I(u)=i_1.i_2.i_3.\dots.i_{L-1}$, $q=q[I,\alpha]\in Q_l$, $p=p[I,\alpha]\in P_l$, $|Q_l|=|P_l|\neq 0$ – a set of modules U_l, simple positions Q_l and access point positions P_l from level l are the basis for synthesizing sets of modules U, simple positions Q, access point positions P for the entire E-network: $Q=\bigcup_{l=1}^{L}Q_l\neq\emptyset$, $|Q|<\infty$, $Q_k\cap Q_l\neq\emptyset$; $P=\bigcup_{l=1}^{L}P_l\neq\emptyset$, $|P|<\infty$, $P_k\cap P_l\neq\emptyset$; $U=\bigcup_{l=1}^{L}U_l\neq\emptyset$, $|U|<\infty$, $U_k\cap U_l\neq\emptyset$. Based on (1) the structure of the E-network itself we describe by the tuple

$$E=\langle N,K,r,M_{in},M_{out}\rangle, \tag{2}$$

where $K=K[I]$, $r=r[I,\alpha]$, $M_{in}=M_{in}[I,\alpha]$, $M_{out}=M_{out}[I,\alpha]$.

Also, we introduce the concept of the E-network positions (layers) S, $S=Q\cup P\neq\emptyset$, $Q\cap P\neq\emptyset$, $|S|<\infty$, $|Q|=|P|$, which generalizes the set of simple positions Q and access point positions P. The level $S_{l_l\dots l_h}$ layer l_h with the lower level l_l – is part of the E-network $B_0=S_{1\dots L}$ with an order $j=l_h-l_l+1$, which belongs to the layer of E-network order j level l_h and contains only modules of this layer of the E-network and connecting their arcs. For the first-order layer equality $S_{l_h\dots l_h}=U_{l_h}$ is true. E-network layers $S_{l_{li}\dots l_{hi}}$ and $S_{l_{lj}\dots l_{hj}}$ intersect if they have at least one common E-layer: $(\max(l_{li},l_{lj})\leq\min(l_{hi},l_{hj}))$, otherwise the layers do not overlap. If the layers intersect, then it is possible to define join and intersection operations for them. The join of the E-network layers $S_{l_{li}\dots l_{hi}}$ and $S_{l_{lj}\dots l_{hj}}$ there will be a layer $S_{l_l\dots l_h}=S_{l_{li}\dots l_{hi}}\cup S_{l_{lj}\dots l_{hj}}$, where $l_l=\min(l_{li},l_{lj})$, $l_h=\max(l_{hi},l_{hj})$, and the intersection of these layers will be a layer $S_{l_l\dots l_h}=S_{l_{li}\dots l_{hi}}\cap S_{l_{lj}\dots l_{hj}}$.

The foregoing allows us to introduce yet another level of generalization in the ISCU simulation on the E-network which will be called the level l_h superblock $B_{l_l\dots l_h}$ with the lower level l_l and the index I, which is part of the $B_0=B_{1\dots L}(0)$ E-network of $j=l_h-l_l+1$ order, which is inscribed in the $S_{l_l\dots l_h}$ layer whose modules indexes satisfy $J\subseteq I$. The order of the superblock shows the number of E-network levels, which contain the modules that are part of it, and the level of the superblock shows the highest E-network level in its composition. Superblock B covers a set of E-network levels, among which are the highest, lowest and intermediate levels, each of which has modules, for determination of which we introduce variables $Q_l(B)$, $P_l(B)$, $U_l(B)$, which, respectively, represent the set of simple positions, the set of access point positions and the set of modules on the levels l of the superblock. Summarizing the introduced symbols for all levels of the

DOI 10.15588/1607-3274-2019-1-13

superblock, we obtain the corresponding supersets: $Q(B)=\bigcup_{l=l_l}^{l_h} Q_l(B)$, $P(B)=\bigcup_{l=l_l}^{l_h} P_l(B)$, $U(B)=\bigcup_{l=l_l}^{l_h} U_l(B)$.

We will analyze operations on superblocks, taking on analogy with the above-described operations over ISCU E-network layers. So superblocks cross over if they have at least one common module, that is, two ISCU E-networks superblocks intersect if the top module of one of them is a part of another. This assertion has a number of consequences, namely: superblocks inscribed in the same layer do not intersect; Superblocks of the same level, but of different order or not overlapping, or have a common top module and a super-block of higher order includes a superblock of the lower order; if superblocks with the same lower level intersect, then the faults have a different order and the superblock of higher order includes a superblock of lower order. In the end, the result of the intersection of superblocks will be a superblock, which includes all the shared modules of output superblocks, thus creating a new superblock: let $B_{l_l \dots l_h}(I)=B_{l_{li} \dots l_{hi}}(I_i)\cap B_{l_{lj} \dots l_{hj}}(I_j)$, $l_h=\min(l_{hi},l_{hj})$, $l_l=\max(l_{li},l_{lj})$ then, if $l_h=l_{hi}$, then $I=I_i$, or if $l_h=l_{hj}$ then $I=I_j$. Such an interpretation of operations on superblocks of the ISCU E-network is in line with the process of forming the global SP of ISCU. If the system of marking the results of discretionary access to the ISCU information resources is included in the concept of the global SP of ISCU, then its mathematical model at the level of the superblock $B=B_{l_l \dots l_h}(I_0)$ will be a subset of access point positions $\Omega_G(B)$ for the lower level of the superblock: $\Omega_G(B)\subseteq P_{l_l}(B)$. Accordingly, all access point positions for the lower level will be marked by the compliance of the global SP: $(\forall p=p[I,\alpha]\in P_{l_l}(B)\setminus\Omega_G(B))(M_{out}[I,\alpha]=0)$, which prevents unauthorized discretionary access to the lower level resources without breaking the mark: $(\exists p=p[I,\alpha]\in P_{l_l}(B)\setminus\Omega_G(B))(M_{out}[I,\alpha]=1)$.

In order to integrate the discretionary authentication model into the created model of ISCU in the context of the above-described approach to the formation of its global SP, we introduce the concept of discretionary SP of ISCU, which will determine the privileges of discretionary access of the given authorization to objects at the selected level of ISCU. By analogy with the above, we introduce a discretionary SP of level l on a superblock $B=B_{l_l \dots l_h}(I_0)$ by a subset of the access point positions $\Omega_{Dl}(B)$ for a l level of a super-block: $\Omega_{Dl}(B)\subseteq P_l(B)$, $l_l\le l\le l_h$. Performing a discretionary l-level SP $\Omega_{Dl}(B)$ on a superblock B will mean the appropriate marking of all access point positions at this level: $(\forall p=p[I,\alpha]\in P_l(B)\setminus\Omega_{Dl}(B))(M_{out}[I,\alpha]=0)$, while an attempt to violate it is marked as $(\exists p=p[I,\alpha]\in P_l(B)\setminus\Omega_{Dl}(B))(M_{out}[I,\alpha]=1)$.

Unlike the global SP, the local SP of ISCU regulates the inter-entity interaction with the projection on the concept of the hierarchical ISCU representation by applying a "control-controlled" rule for pairs of entities located at neighboring levels of ISCU. In accordance with this rule, the subjects of the current level are controllable in relation to the subjects of the higher adjacent level. The local l-level SP $\Omega_{Ll}(B)$ on the superblock $B=B_{l_l \dots l_h}(I_0)$ will be described by a set $\Omega_{Ll}(B)=\{\langle I(u),\alpha,r[I(u),\alpha]\rangle \mid u\in U_l(B),\alpha=\overline{1,N}\}$, $l_l\le l\le l_h$ and will set the attributes of the possibility of authorization in the modules of this superblock level. Accordingly, a subset of positions allowed by the local l-level SP on the superblock B will be described by a subset $\{p=p[I(u),\alpha]\in P_l(B) \mid u\in U_l(B),\alpha=\overline{1,N}$, $\langle I(u),\alpha,1\rangle\in\Omega_{ll}(B)\}$, which allows to describe situations when a local SP is executed, and when not, by expressions $(\forall p=p[I(u),\alpha]\in P_l(B) \mid u\in U_l(B),\alpha=\overline{1,N}$, $P_l(B) \mid u\in U_l(B),\alpha=\overline{1,N},\langle I(u),\alpha,0\rangle\in\Omega_{Ll}(B))\cdot$ $\cdot(M_{out}[I,\alpha]=0)$ and $(\exists p=p[I(u),\alpha]\in\langle I(u),\alpha,0\rangle$ $\in\Omega_{Ll}(B))(M_{out}[I,\alpha]=1)$ respectively. Detailing the process of forming a local SP of ISCU requires differentiation of the rules of safe inter-entity control over the controlling entities at the level of the block of the E-network. The only top module of an arbitrary block of an E-network of ISCU with an I index is associated with the controlling entity, and its lower modules (with numbers $\overline{1,K[I]}$ within the block or with numbers $\overline{I.1,I.K[I]}$ within the E-network) are associated with actual or potentially managed entities. We will develop this concept in the notion of block SP of ISCU, which establishes the attributes of permissibility of obtaining access for all modules of a block. To formalize the block SP we will describe the mechanism for reconciling the attributes permissibility of obtaining access and the corresponding sets of marked access point positions between the upper module and all the lower modules of the block. Based on the fact that the access processes for the controlling and the controlled entities are the same, it can be argued that the permissibility of obtaining access for a controlled entity requires the admissibility of a similar procedure for a controlling entity and vice versa, the inadmissibility of obtaining access to the controlling entity requires a similar for all managed entities. These conclusions allow us to formulate rules for agreeing attributes of permissibility of obtaining access in a blocked SP:

DOI 10.15588/1607-3274-2019-1-13

$$\left(\exists j \in \overline{1, K(I)}\right)\left(r[I.j, \alpha] = 1\right) \Rightarrow \left(r[I, \alpha] = 1\right), \tag{3}$$

$$\left(r[I, \alpha] = 0\right) \Rightarrow \left(\forall j \in \overline{1, K[I]}\right)\left(r[I.j, \alpha] = 0\right), \tag{4}$$

where $\alpha = \overline{1, N}$, $I = I(u)$, $u \in U \setminus U_1$.

Consider the concept of block SP in the formation of a local SP on the basis of a superblock $B = B_{l_l \ldots l_h}(I_0)$ in the form of expression

$$\Omega_L(B) = \bigcup_{l=l_l}^{l_h} \Omega_{Ll}(B) = \left\{\left\langle I(u), \alpha, r[I(u), \alpha]\right\rangle \middle| u \in U(B), \alpha = \overline{1, N}\right\}, \tag{5}$$

where all the attributes $r[I(u), \alpha]$ for all blocks are mutually agreed with the help of rules (3), (4).

We extend the application of the rules (3), (4) to the process of solving the local SP on the superblock $B = B_{l_l \ldots l_h}(I_0)$ in the form of rules

$$\left(r[I, \alpha] = 1\right) \Rightarrow \left(\forall J \subset I \middle| p[J, \alpha] \in P(B)\right)\left(r[J, \alpha] = 1\right), \quad u \in U(B) \setminus U_{l_h}(B), \tag{6}$$

$$\left(r[I, \alpha] = 0\right) \Rightarrow \left(\forall J \subset I \middle| p[J, \alpha] \in P(B)\right)\left(r[J, \alpha] = 0\right), \quad u \in U(B) \setminus U_{l_l}(B), \tag{7}$$

at $\alpha = \overline{1, N}$, $I = I(u)$.

Finally, based on the rules (3)–(7) we will formulate the process of agreeing the privileges of discretionary access for the entire SP of ISCU by combining the level of discretionary SP for all levels of ISCU with their agreement on the basis of block SP:

$$\Omega_{DP}(B) = \bigcup_{l=l_l}^{l_h} \Omega_{Dl}(B) \subseteq P(B), \tag{8}$$

where $B = B_{l_l \ldots l_h}(I_0)$, the sets $\Omega_{Dl}(B)$ are agreed according to rules (3), (4) and the processes of agreeing the marked access point positions and attributes of permissibility of obtaining access are equivalent, that is, the permitted position corresponds to the true value of the attribute of permissibility of obtaining access, while the wrong position is false.

Equivalently (3), (4) we have rules for coordinating the access point positions when set up a block SP on an E-network:

$$\left(\exists j \in \overline{1, K}\right)\left(p[I.j, \alpha] \in \Omega_{DP}\right) \Rightarrow \left(p[I, \alpha] \in \Omega_{DP}\right), \tag{9}$$

$$\left(p[I, \alpha] \notin \Omega_{DP}\right) \Rightarrow \left(\forall j \in \overline{1, K[I]}\right)\left(p[I.j, \alpha] \notin \Omega_{DP}\right), \tag{10}$$

at $\alpha = \overline{1, N}$, $I = I(u)$, $u \in U \setminus U_1$.

Summarizing the rules (9) and (10) formulated for different levels of ISCU, we obtain the rules for agreeing the access point positions at the discretion of a discretionary SP on a superblock $B = B_{l_l \ldots l_h}(I_0)$:

$$\left(p[I, \alpha] \in \Omega_{DP}(B)\right) \Rightarrow \left(\forall J \subset I \middle| p[J, \alpha] \in P(B)\right) \times \left(p[J, \alpha] \in \Omega_{DP}(B)\right), \quad u \in U(B) \setminus U_{l_h}(B), \tag{11}$$

$$\left(p[I, \alpha] \notin \Omega_{DP}(B)\right) \Rightarrow \left(\forall J \supset I \middle| p[J, \alpha] \in P(B)\right) \times \left(p[J, \alpha] \notin \Omega_{DP}(B)\right), \quad u \in U(B) \setminus U_{l_l}(B), \tag{12}$$

at $\alpha = \overline{1, N}$, $I = I(u)$.

Consequently, the discretionary SP of ISCU, represented by the E-network, can be set up by a set of access point positions according to the rules (11), (12), but such representation is characterized by information redundancy, which is deprived the globalized representation of the discretionary SP on the E-network:

$$\Omega_{DG}(B) \subseteq \Omega_{Dp}(B) \Rightarrow \left(p[I, \alpha] \in \Omega_{DG}(B)\right) \Leftrightarrow \left(p[I, \alpha] \in \Omega_{Dp}(B)\right) \wedge \wedge \left(\left(\forall J \supset I \middle| p[J, \alpha] \in P(B)\right)\left(p[J, \alpha] \notin \Omega_{Dp}(B)\right)\right), \tag{13}$$

where $\alpha = \overline{1, N}$, $I = I(u)$, $u \in U(B)$. There is a reverse possibility – to represent $\Omega_{DP}(B)$ having a set of $\Omega_{DG}(B)$:

$$\left(p[I, \alpha] \in \Omega_{DP}(B)\right) \Leftrightarrow \left(\left(\exists J \supseteq I \middle| p[J, \alpha] \in P(B)\right)\left(p[J, \alpha] \in \Omega_{DG}(B)\right)\right). \tag{14}$$

As a result, the index of one of the two access point positions p' and p'' from the globalized set of allowed access point positions $\Omega_{DG}(B)$ for a same authorization can't be a subindex of another:

$$\left(p' = p[I', \alpha] \in \Omega_{DG}(B) \wedge p'' = p[I'', \alpha] \in \Omega_{DG}(B)\right) \Rightarrow \Rightarrow \left(I' \not\subset I'' \wedge I'' \not\subset I'\right). \tag{15}$$

Lets get a set $\Omega_{Dp}(B)$ of this same SP on the basis of (14), taking into account (15), which will include in to $\Omega_{Dp}(B)$ each element of $\Omega_{DG}(B)$ and all access point positions whose indexes are its subexpectives:

$$\left(\forall p = p[I, \alpha] \in P(B) \setminus \Omega_{Dp}(B)\right)\left(M_{out}[I, \alpha] = 0\right), \tag{16}$$

which makes all access point positions that are not marked by this SP unavailable, and an attempt to initiate them will take into account with the help of the expression:

© Bisikalo O. V., Kovtun V. V., Yukhimchuk M. S., 2019
DOI 10.15588/1607-3274-2019-1-13

$$\left(\exists p = p[I,\alpha] \in P(B) \setminus \Omega_{Dp}(B)\right)\left(M_{out}[I,\alpha]=1\right). \quad (17)$$

The implementation of the discretionary SP at the DPU level is guaranteed by an execution of the local SP $\Omega_L(B)$, defined in (5), the discretionary SP $\Omega_{Dp}(B)$, defined in (8), and expression $\left(\forall p = p[I,\alpha] \in P(B)\right) \cdot \cdot \left(\left(p \in \Omega_{Dp}(B)\right) \Leftrightarrow \left(r[I,\alpha]=1\right)\right)$ on the superblock B of E-network. Accordingly, if at a certain time a discrete SP is executed on a certain superblock of the E-network of ISCU, and all objects moving in this superblock satisfy the inductive superblock of the local SP, then at any later time the discretionary SP on the superblock will also be executed. Perform marking of the positions allowed by the selected local SP on a superblock $B = B_{l_l \ldots l_h}(I_0)$ of the E-network like:

$$\begin{gathered}\left(\forall p = p[I,\alpha] \in P_{l_h}(B)\right)\left(\left(M_{in}[I,\alpha]=1\right) \wedge \left(M_{out}[I,\alpha]=0\right)\right) \wedge \\ \wedge \left(\forall p = p[I,\alpha] \in P(B) \setminus P_{l_h}(B)\right)\left(M_{in}[I,\alpha] = M_{out}[I,\alpha]=0\right).\end{gathered} \quad (18)$$

We will call marking (18) basic. On its basis we get the induced by discretionary SP marking

$$\begin{gathered}\left(\forall p = p[I,\alpha] \in \Omega_{DG}(B)\right)\left(\left(M_{in}[I,\alpha]=0\right) \wedge \left(M_{out}[I,\alpha]=1\right)\right) \wedge \\ \wedge \left(\forall p = p[I,\alpha] \in P(B) \setminus \Omega_{DG}(B)\right)\left(M_{in}[I,\alpha] = M_{out}[I,\alpha]=0\right).\end{gathered} \quad (19)$$

Expression (19) describes the discretionary access to the resources of the lower level of the ISCU hierarchy with the privileges that are maximally permissible within the framework of the discretionary SP specified on the superblock. In the framework of expressions (18), (19) we formulate the notion of global SP $\Omega_G(B)$ on a superblock B, as induced by a discrete SP provided on the same superblock $\Omega_{GD}(B)$, if $\Omega_G(B) = \Omega_{GD}(B)$. A subset $\Omega_G(B) \subset P(B)$ satisfies (15) since all its elements belong to the lower level of the ISCU hierarchy, therefore, on any arbitrary superblock, any global SP is induced by a single discretionary SP, which, in turn, is induced by a local SP. Thus, for an arbitrary global SP, which is given by (15) on the superblock of an E-network, it is possible to define the access operations (11) and the transformation operations (12) on this superblock so the induced by the given global SP marking of the superblock (19) may be derived from the basic marking (18) within the local SP, which induced by this global SP.

The above expressions mathematically correctly and holistically describe the interaction of all levels of SP in a hierarchical ISCU with DPU and ASU, but, given the complex nature of the ISCU, the question of agreeing of SPs of superblocks on the scale of whole ISCU is relevant. To study this issue, we will define the concept of weak and strong compatibility (incompatibility) of SP. Weak compatibility (incompatibility) of SP Ω_i and Ω_j we consider like the absence (existence) of direct contradictions between them and denote $\Omega_i \sim \Omega_j$ ($\Omega_i \nsim \Omega_j$). Strong compatibility (incompatibility) of SP Ω_i and Ω_j we consider like the absence (existence) of contradictions in the distribution of their SP to the entire E-network and denote $\Omega_i \approx \Omega_j$ ($\Omega_i \not\approx \Omega_j$). We also consider that two arbitrary SPs are the same type if they relate to one level of the E-network representation of ICU (both global, both local, etc.), or different types in opposite cases.

Let's describe the concept of compatibility (incompatibility) of the same type of SP with such expressions

$$\begin{gathered}\left(\Omega_G(B_i) \sim \Omega_G(B_j)\right) \Leftrightarrow \left(\Omega_G(B_i) \cap P_N(B_j) = \Omega_G(B_j) \cap P_N(B_i)\right), \\ \left(\Omega_G(B_i) \nsim \Omega_G(B_j)\right) \Leftrightarrow \left(\Omega_G(B_i) \cap P_N(B_j) \neq \Omega_G(B_j) \cap P_N(B_i)\right).\end{gathered} \quad (20)$$

$$\begin{gathered}\left(\Omega_{Dl}(B_i) \sim \Omega_{Dl}(B_j)\right) \Leftrightarrow \left(\Omega_{Dl}(B_i) \cap P_N(B_j) = \Omega_{Dl}(B_j) \cap P_N(B_i)\right), \\ \left(\Omega_{Dl}(B_i) \nsim \Omega_{Dl}(B_j)\right) \Leftrightarrow \left(\Omega_{Dl}(B_i) \cap P_N(B_j) \neq \Omega_{Dl}(B_j) \cap P_N(B_i)\right).\end{gathered} \quad (21)$$

$$\begin{gathered}\left(\Omega_{Ll}(B_i) \sim \Omega_{Ll}(B_j)\right) \Leftrightarrow \left(\left|\Omega_{Ll}(B_i) \cap \Omega_{Ll}(B_j)\right| = N\left|U_l(B_i) \cap U_l(B_j)\right|\right), \\ \left(\Omega_{Ll}(B_i) \nsim \Omega_{Ll}(B_j)\right) \Leftrightarrow \left(\left|\Omega_{Ll}(B_i) \cap \Omega_{Ll}(B_j)\right| < N\left|U_l(B_i) \cap U_l(B_j)\right|\right).\end{gathered} \quad (22)$$

$$\begin{gathered}\left(\Omega_L(B_i) \sim \Omega_L(B_j)\right) \Leftrightarrow \left(\left|\Omega_L(B_i) \cap \Omega_L(B_j)\right| = N\left|U_l(B_i) \cap U(B_j)\right|\right), \\ \left(\Omega_{Ll}(B_i) \nsim \Omega_{Ll}(B_j)\right) \Leftrightarrow \left(\left|\Omega_L(B_i) \cap \Omega_L(B_j)\right| < N\left|U(B_i) \cap U(B_j)\right|\right).\end{gathered} \quad (23)$$

$$\begin{gathered}\left(\Omega_{Dp}(B_i) \sim \Omega_{Dp}(B_j)\right) \Leftrightarrow \left(\Omega_{Dp}(B_i) \cap P(B_j) = \Omega_{Dp}(B_j) \cap P(B_i)\right), \\ \left(\Omega_{Dp}(B_i) \nsim \Omega_{Dp}(B_j)\right) \Leftrightarrow \left(\Omega_{Dp}(B_i) \cap P(B_j) \neq \Omega_{Dp}(B_j) \cap P(B_i)\right).\end{gathered} \quad (24)$$

From (20)–(24) it is evident that the weak compatibility (incompatibility) of the same type of SPs on the same superblock is interpreted as their equality (inequality):

$$\begin{gathered}\left(\left(\Omega(B_i) \sim \Omega(B_j)\right) \wedge \left(B_i = B_j\right)\right) \Leftrightarrow \left(\Omega(B_i) = \Omega(B_j)\right), \\ \left(\left(\Omega(B_i) \nsim \Omega(B_j)\right) \vee \left(B_i \neq B_j\right)\right) \Leftrightarrow \left(\Omega(B_i) \neq \Omega(B_j)\right).\end{gathered} \quad (25)$$

Strong compatibility of the same types of SPs $\Omega(B_i)$ and $\Omega(B_j)$ on the superblocks B_i and B_j accordingly will be interpreted as their simultaneous weak compatibility with a certain single SP of the whole E-network B_0 of the same type:

$$\begin{gathered}\left(\Omega(B_i) \approx \Omega(B_j)\right) \Leftrightarrow \left(\left(\exists \Omega(B_0)\right)\left(\left(\Omega(B_i) \sim \Omega(B_0)\right) \wedge \left(\Omega(B_j) \sim \Omega(B_0)\right)\right)\right), \\ \left(\Omega(B_i) \not\approx \Omega(B_j)\right) \Leftrightarrow \left(\left(\forall \Omega(B_0)\right)\left(\left(\Omega(B_i) \nsim \Omega(B_0)\right) \vee \left(\Omega(B_j) \nsim \Omega(B_0)\right)\right)\right).\end{gathered} \quad (26)$$

From (26) it is seen that the strong compatibility (incompatibility) of the same type of SPs on the same superblock is interpreted as their equality (inequality):

$$\begin{gathered}\left(\left(\Omega(B_i) \sim \Omega(B_j)\right) \wedge \left(B_i = B_j\right)\right) \Leftrightarrow \left(\left(\Omega(B_i) \approx \Omega(B_j)\right) \wedge \left(B_i = B_j\right)\right) \Leftrightarrow \\ \Leftrightarrow \left(\Omega(B_i) = \Omega(B_j)\right),\end{gathered} \quad (27)$$

© Bisikalo O. V., Kovtun V. V., Yukhimchuk M. S., 2019
DOI 10.15588/1607-3274-2019-1-13

$$\left(\left(\Omega(B_i) \nsim \Omega(B_j)\right) \vee (B_i = B_j)\right) \Leftrightarrow \left(\left(\Omega(B_i) \napprox \Omega(B_j)\right) \vee (B_i = B_j)\right) \Leftrightarrow$$
$$\Leftrightarrow \left(\Omega(B_i) \neq \Omega(B_j)\right).$$

On the basis of already formulated, we will analytically describe the concept of compatibility (incompatibility) of different types of SPs. We describe the weak compatibility (incompatibility) of the l-level discretionary SP $\Omega_{Dl}(B_i)$ on a superblock B_i with a discrete SP with a permissive representation $\Omega_{Dp}(B_j)$ on the superblock B_j witch an expressions:

$$\begin{aligned}&\left(\Omega_{Dl}(B_i) \sim \Omega_{Dp}(B_j)\right) \Leftrightarrow \left(\Omega_{Dl}(B_i) \cap P(B_j) = \Omega_{Dp}(B_j) \cap P_l(B_i)\right),\\ &\left(\Omega_{Dl}(B_i) \nsim \Omega_{Dp}(B_j)\right) \Leftrightarrow \left(\Omega_{Dl}(B_i) \cap P(B_j) \neq \Omega_{Dp}(B_j) \cap P_l(B_i)\right).\end{aligned} \quad (28)$$

Weak compatibility (incompatibility) of the level discretionary SPs of different levels will be considered as weak compatibility (incompatibility) of certain discretionary SPs with which these level discretionary SPs are weakly compatible (incompatible):

$$\begin{aligned}&\left(\Omega_{Dl_i}(B_i) \sim \Omega_{Dl_j}(B_j)\right) \Leftrightarrow \left(\left(\exists \Omega_{Dp}(B_i) \middle| \Omega_{Dl_i}(B_i) \sim \Omega_{Dp}(B_i)\right) \times\right.\\ &\left.\times \left(\exists \Omega_{Dp}(B_j) \middle| \Omega_{Dl_j}(B_j) \sim \Omega_{Dp}(B_j)\right)\left(\Omega_{Dp}(B_i) \sim \Omega_{Dp}(B_j)\right)\right),\\ &\left(\Omega_{Dl_i}(B_i) \nsim \Omega_{Dl_j}(B_j)\right) \Leftrightarrow \left(\left(\forall \Omega_{Dp}(B_i) \middle| \Omega_{Dl_i}(B_i) \sim \Omega_{Dp}(B_i)\right) \times\right.\\ &\left.\times \left(\forall \Omega_{Dp}(B_j) \middle| \Omega_{Dl_j}(B_j) \sim \Omega_{Dp}(B_j)\right)\left(\Omega_{Dp}(B_i) \nsim \Omega_{Dp}(B_j)\right)\right).\end{aligned} \quad (29)$$

Similarly, we define the weak compatibility (incompatibility) of the l-level single local SP $\Omega_{Ll}(B_i)$ on the superblock B_i witch the local SP $\Omega_L(B_j)$ on the superblock B_j:

$$\begin{aligned}&\left(\Omega_{Ll}(B_i) \sim \Omega_L(B_j)\right) \Leftrightarrow \left(\left|\Omega_{Ll}(B_i) \cap \Omega_L(B_j)\right| = N\left|U_l(B_i) \cap U(B_j)\right|\right),\\ &\left(\Omega_{Ll}(B_i) \nsim \Omega_L(B_j)\right) \Leftrightarrow \left(\left|\Omega_{Ll}(B_i) \cap \Omega_L(B_j)\right| < N\left|U_l(B_i) \cap U(B_j)\right|\right).\end{aligned} \quad (30)$$

Weak compatibility (incompatibility) of the level local SPs of different levels will be considered as weak compatibility (incompatibility) of certain local SPs, with which these level local SPs are weakly compatible (incompatible):

$$\begin{aligned}&\left(\Omega_{Ll_i}(B_i) \sim \Omega_{Ll_j}(B_j)\right) \Leftrightarrow \left(\left(\exists \Omega_L(B_i) \middle| \Omega_{Ll_i}(B_i) \sim \Omega_L(B_i)\right) \times\right.\\ &\left.\times \left(\exists \Omega_L(B_j) \middle| \Omega_{Ll_j}(B_j) \sim \Omega_L(B_j)\right)\left(\Omega_L(B_i) \sim \Omega_L(B_j)\right)\right),\\ &\left(\Omega_{Ll_i}(B_i) \nsim \Omega_{Ll_j}(B_j)\right) \Leftrightarrow \left(\left(\forall \Omega_L(B_i) \middle| \Omega_{Ll_i}(B_i) \sim \Omega_L(B_i)\right) \times\right.\\ &\left.\times \left(\forall \Omega_L(B_j) \middle| \Omega_{Ll_j}(B_j) \sim \Omega_L(B_j)\right)\left(\Omega_L(B_i) \nsim \Omega_L(B_j)\right)\right).\end{aligned} \quad (31)$$

The mutual weak compatibility (incompatibility) of the local, discretionary and global SPs on the same superblock will be considered as induction of given local SP by the discretionary SP and, in turn, by the global SP:

$$\begin{aligned}&\left(\Omega_L(B_i) \sim \Omega_{Dp}(B_j)\right) \Leftrightarrow \left(\left(\exists \Omega_{Dp}(B_i) \middle| \Omega_L(B_i) \sim \Omega_{Dp}(B_i)\right) \times\right.\\ &\left.\times \left(\Omega_{Dp}(B_i) \sim \Omega_{Dp}(B_j)\right)\right),\\ &\left(\Omega_L(B_i) \nsim \Omega_{Dp}(B_j)\right) \Leftrightarrow \left(\left(\forall \Omega_{Dp}(B_i) \middle| \Omega_L(B_i) \sim \Omega_{Dp}(B_i)\right) \times\right.\\ &\left.\times \left(\Omega_{Dp}(B_i) \nsim \Omega_{Dp}(B_j)\right)\right).\end{aligned} \quad (32)$$

$$\begin{aligned}&\left(\Omega_L(B_i) \sim \Omega_G(B_j)\right) \Leftrightarrow \left(\left(\exists \Omega_G(B_i) \middle| \Omega_L(B_i) \sim \Omega_G(B_i)\right) \times\right.\\ &\left.\times \left(\Omega_G(B_i) \sim \Omega_G(B_j)\right)\right),\\ &\left(\Omega_L(B_i) \nsim \Omega_G(B_j)\right) \Leftrightarrow \left(\left(\forall \Omega_G(B_i) \middle| \Omega_L(B_i) \sim \Omega_G(B_i)\right) \times\right.\\ &\left.\times \left(\Omega_G(B_i) \nsim \Omega_G(B_j)\right)\right).\end{aligned} \quad (33)$$

$$\begin{aligned}&\left(\Omega_{Dp}(B_i) \sim \Omega_G(B_j)\right) \Leftrightarrow \left(\left(\exists \Omega_G(B_i) \middle| \Omega_{Dp}(B_i) \sim \Omega_G(B_i)\right) \times\right.\\ &\left.\times \left(\Omega_G(B_i) \sim \Omega_G(B_j)\right)\right),\\ &\left(\Omega_{Dp}(B_i) \nsim \Omega_G(B_j)\right) \Leftrightarrow \left(\left(\forall \Omega_G(B_i) \middle| \Omega_{Dp}(B_i) \sim \Omega_G(B_i)\right) \times\right.\\ &\left.\times \left(\Omega_G(B_i) \nsim \Omega_G(B_j)\right)\right).\end{aligned} \quad (34)$$

Weak compatibility (incompatibility) of the level local SP witch level discretionary SP will be considered as weak compatibility (incompatibility) of a certain local SP with a certain level discretionary SP, with which output SPs are weakly compatible (incompatible):

$$\begin{aligned}&\left(\Omega_{Ll_i}(B_i) \sim \Omega_{Dl_j}(B_j)\right) \Leftrightarrow \left(\left(\exists \Omega_L(B_i) \middle| \Omega_{Ll_i}(B_i) \sim \Omega_L(B_i)\right) \cdot\right.\\ &\left.\cdot \left(\exists \Omega_{Dp}(B_j) \middle| \Omega_{Dl_j}(B_j) \sim \Omega_{Dp}(B_j)\right)\left(\Omega_L(B_i) \sim \Omega_{Dp}(B_j)\right)\right),\\ &\left(\Omega_{Ll_i}(B_i) \nsim \Omega_{Dl_j}(B_j)\right) \Leftrightarrow \left(\left(\forall \Omega_L(B_i) \middle| \Omega_{Ll_i}(B_i) \sim \Omega_L(B_i)\right) \cdot\right.\\ &\left.\cdot \left(\forall \Omega_{Dp}(B_j) \middle| \Omega_{Dl_j}(B_j) \sim \Omega_{Dp}(B_j)\right)\left(\Omega_L(B_i) \nsim \Omega_{Dp}(B_j)\right)\right).\end{aligned} \quad (35)$$

Weak compatibility (incompatibility) of the level local SP witch the discretionary SP will be considered as weak compatibility (incompatibility) of given discrete SP with a certain local SP, with which the source level local SP is weakly compatible (incompatible):

$$\begin{aligned}&\left(\Omega_{Ll}(B_i) \sim \Omega_{Dp}(B_j)\right) \Leftrightarrow \left(\left(\exists \Omega_L(B_i) \middle| \Omega_{Ll}(B_i) \sim \Omega_L(B_i)\right) \times\right.\\ &\left.\times \left[\left(\Omega_L(B_i) \sim \Omega_{Dp}(B_j)\right)\right),\right.\\ &\left(\Omega_{Ll}(B_i) \nsim \Omega_{Dp}(B_j)\right) \Leftrightarrow \left(\left(\forall \Omega_L(B_i) \middle| \Omega_{Ll}(B_i) \sim \Omega_L(B_i)\right) \times\right.\\ &\left.\times \left(\Omega_L(B_i) \nsim \Omega_{Dp}(B_j)\right)\right).\end{aligned} \quad (36)$$

Similarly, the weak compatibility (incompatibility) of the level local SP witch a global SP will be considered as weak compatibility (incompatibility) of given global SP with a certain local SP, with which the source level local SP is weakly compatible (incompatible):

$$\begin{aligned}&\left(\Omega_{Ll}(B_i) \sim \Omega_G(B_j)\right) \Leftrightarrow \left(\left(\exists \Omega_L(B_i) \middle| \Omega_{Ll}(B_i) \sim \Omega_L(B_i)\right) \times\right.\\ &\left.\times \left(\Omega_L(B_i) \sim \Omega_G(B_j)\right)\right),\end{aligned} \quad (37)$$

© Bisikalo O. V., Kovtun V. V., Yukhimchuk M. S., 2019
DOI 10.15588/1607-3274-2019-1-13

$$\left(\Omega_{Ll}(B_i) \nsim \Omega_G(B_j)\right) \Leftrightarrow \left(\left(\forall \Omega_L(B_i) \middle| \Omega_{Ll}(B_i) \sim \Omega_L(B_i)\right) \times \right.$$
$$\left. \times \left(\Omega_L(B_i) \nsim \Omega_G(B_j)\right)\right).$$

Weak compatibility (incompatibility) of the level discretionary SP witch a local SP will be considered as weak compatibility (incompatibility) of a given local SP witch a certain discretionary SP, with which the output level discretionary SP is weakly compatible (incompatible):

$$\begin{aligned}&\left(\Omega_{Dl}(B_i) \sim \Omega_L(B_j)\right) \Leftrightarrow \left(\left(\exists \Omega_{Dp}(B_i) \middle| \Omega_{Dl}(B_i) \sim \Omega_{Dp}(B_i)\right) \times \right.\\ &\left. \times \left(\Omega_{Dp}(B_i) \sim \Omega_L(B_j)\right)\right),\\ &\left(\Omega_{Dl}(B_i) \nsim \Omega_L(B_j)\right) \Leftrightarrow \left(\left(\forall \Omega_{Dp}(B_i) \middle| \Omega_{Dl}(B_i) \sim \Omega_{Dp}(B_i)\right) \times \right.\\ &\left. \times \left(\Omega_{Dp}(B_i) \nsim \Omega_L(B_j)\right)\right).\end{aligned} \tag{38}$$

Similarly, the weak compatibility (incompatibility) of the level discretionary SP and global SP will be considered as weak compatibility (incompatibility) of given global SP with a certain discretionary SP, with which the output level of the discretionary SP is weakly compatible (incompatible):

$$\begin{aligned}&\left(\Omega_{Dl}(B_i) \sim \Omega_G(B_j)\right) \Leftrightarrow \left(\left(\exists \Omega_{Dp}(B_i) \middle| \Omega_{Dl}(B_i) \sim \Omega_{Dp}(B_i)\right) \times \right.\\ &\left. \times \left(\Omega_{Dp}(B_i) \sim \Omega_G(B_j)\right)\right),\\ &\left(\Omega_{Dl}(B_i) \nsim \Omega_G(B_j)\right) \Leftrightarrow \left(\left(\forall \Omega_{Dp}(B_i) \middle| \Omega_{Dl}(B_i) \sim \Omega_{Dp}(B_i)\right) \times \right.\\ &\left. \times \left(\Omega_{Dp}(B_i) \nsim \Omega_G(B_j)\right)\right).\end{aligned} \tag{39}$$

On the strong compatibility (incompatibility) of different types of SPs on superblocks, we will understand the weak compatibility (incompatibility) of some of the same type SPs across the whole E-networks of ISCU, which are weakly compatible (incompatible) with the corresponding output SPs on superblocks (situation (26) is a partial case of the newly described):

$$\begin{aligned}&\left(\Omega_i(B_i) \approx \Omega_j(B_j)\right) \Leftrightarrow \left(\left(\exists \Omega_i(B_0) \middle| \Omega_i(B_i) \sim \Omega_i(B_0)\right) \times \right.\\ &\left. \times \left(\exists \Omega_j(B_0) \middle| \Omega_j(B_j) \sim \Omega_j(B_0)\right)\left(\Omega_i(B_0) \sim \Omega_j(B_j)\right)\right),\\ &\left(\Omega_i(B_i) \not\approx \Omega_j(B_j)\right) \Leftrightarrow \left(\left(\forall \Omega_i(B_0) \middle| \Omega_i(B_i) \sim \Omega_i(B_0)\right) \cdot \right.\\ &\left. \cdot \left(\forall \Omega_j(B_0) \middle| \Omega_j(B_j) \sim \Omega_j(B_0)\right)\left(\Omega_i(B_0) \nsim \Omega_j(B_j)\right)\right).\end{aligned} \tag{40}$$

Let us generalize the formalization of the concept of weak and strong compatibility of SPs on the superblocks for the case when we have two different types of SP Ω_i and Ω_j on the superblocks B_i and B_j with the corresponding indexes $I_i = I(B_i)$ and $I_j = I(B_j)$. If these superblocks intersect, then the weak and strong compatibility of their SPs is equivalent: $\left(\Omega_i(B_i) \sim \Omega_j(B_j)\right) \Leftrightarrow \left(\Omega_i(B_i) \approx \Omega_j(B_j)\right)$, but if these superblocks also coincide ($B_i = B_j = B$ and SPs are of the same type), then the weak and strong compatibility of their SPs is equivalent to: $\left(\Omega_i(B) \sim \Omega_j(B)\right) \Leftrightarrow \left(\Omega_i(B) \approx \Omega_j(B)\right) \Leftrightarrow \left(\Omega_i(B) = \Omega_j(B)\right)$. If superblocks do not overlap, but the index of one of them is a subindex of another: $I_j \subset I_i$, then their SPs are necessarily weakly compatible, but not necessarily strongly compatible. If the index of any of the superblocks is not a subindex of another $\left(I_i \not\subset I_j\right) \wedge \left(I_j \not\subset I_i\right)$, then their SPs are necessarily strongly compatible and, accordingly, weakly compatible. The obtained expressions are presented in Table 2 for ensuring weak and strong compatibility (incompatibility) of different types of SPs on the superblocks of the ISCU E-network for convenience of use.

To sum it up, we suppose that a complex of SP $\Omega(B) = \left\langle \Omega_G(B), \Omega_{Dp}(B), \Omega_{Dg}(B), \Omega_L(B)\right\rangle$ is defined on the superblock B of the ISCU E-network if of all types of SPs on the superblock has defined and they are at least weakly compatible ($\Omega_G(B)$, $\Omega_L(B)$ are a global and a local SP respectively for which DPU meets the requirements, and $\Omega_{Dp}(B)$ and $\Omega_{Dg}(B)$ are an authentication and a globalized representation of the discretionary SP for which ASU meets the requirements). In this representation, the discretionary SP is induced by the local SP, and the global one SP is induced by a local and discretionary SPs respectively. Taking into account that the ISCU E-network is a composition of superblocks, it is possible to extend the above formulated concept of SP setting on the superblock to the scale of the entire ISCU while preserving the correctness and compatibility of mathematical representations and the possibility of the formal synthesis of a protected hierarchical ISCU with any complexity level in accordance with the ISO/IEC 27001:2013 standard.

Table 2 – Expressions to provide weak and strong compatibility (incompatibility) different types of SPs on the superblocks of the ISCU E-network

Type of SP	Global SP	Level discretionary SP	Level local SP	Local SP	Discretionary SP
Global SP	(20), (26)	(39), (40)	(37), (40)	(33), (40)	(34), (40)
Level discretionary SP		(21), (29), (26), (40)	(35), (40)	(38), (40)	(28), (40)
Level local SP			(22), (31), (26), (40)	(30), (40)	(36), (40)
Local SP				(23), (26)	(32), (40)
Discretionary SP					(24), (26)

© Bisikalo O. V., Kovtun V. V., Yukhimchuk M. S., 2019
DOI 10.15588/1607-3274-2019-1-13

Consequently, new flexible mathematical models of reliable information processing are described which, in contrast to the existing ones, comprehensively describes mechanisms for providing authenticationly access to information resources of ISCU within the framework of the chosen mathematical apparatus which allows to quantify the integrity of information processes in the system. The mathematical models of the synthesis of the policy of secure interaction of information processes in the ISCU are developed, which allow to separately considering SPs on various structural components of the ISCU represented by the E-network with the possibility of their further integration. In particular, mathematical models of SPs for ISCU with object-relational model of an informational environment organization are developed and mechanisms of SPs integration, induction and compatibility within the hierarchical representation of the ISCU are proposed.

4 EXPERIMENTS

The correspondence of the selected model of SP to the proposed in the Table 1 hierarchical structure of the ISCU is ensured by the operation of DPU and ASU. Empirical investigations of those units will verify the adequacy of the above mathematical models. Let’s make an experimental statement to evaluate the work of these units. The DPU implements an efficient information processing in the ISCU according to actions of users witch segregated by roles. The information security of these processes is provided by the work of the IICS, which is hosted on the registration server, and structurally attributed to the application level of the system hierarchy. As the integrity of information we will understand the qualitative state of the software and information components of the ISCU. Accordingly, information integrity controlling involves the regulated functioning of the services of its definition, preservation and restoration. However, controlling the information integrity, like any process, requires resources that will increase with the system operation time. Given the critical use of the described IS, it is necessary to create a mechanism for controlling the integrity of its information, which will function efficiently by giving priority to the use of resources for the functional purpose of ISCU in real time, while guaranteeing a given level of information security. Taking into account the above, we will determine the optimal scenario of the IICS operation $a \in A$ as the result of solving the mathematical programming task with the target function $E_f(a) \to \max$ and the limit $E_s(a) \geq E_{s\min}$, where $E_{s\min}$ is specified by the administrator. Asserting that the degree of completeness of the information integrity controlling process is reversed to its duration, we will present this process in time as:

$$E_f = P(K_{dm} > K_{dm\min}) = 1 - P(\tau_{dm} \leq \tau_{\min f}) = 1 - E(\tau_{mf}),$$
$$E_s = P(K_{dm} \leq K_{dm\max}) = 1 - P(\tau_{dm} \leq \tau_{\max s}) = 1 - E(\tau_{ms}),$$

where $\tau_{dm} = v_{dm}c^{-1}$, $K_{dm} = v_{dm}V_{dm}^{-1} = c\tau_{dm}V_{dm}^{-1}$, a $K_{dm\min}$, $K_{dm\max}$, $\tau_{\min f}$, $\tau_{\max s}$ – the limit values of the corresponding variables set by the administrator. Let’s summarize the variables E_f and E_s in the form of a dynamic criterion of the IICS effectiveness:

$$E(\tau_m) = P(\tau_{dm} \leq \tau_{\max}(\tau_m)), \tag{41}$$

where the function $\tau_{\max}(\tau_m)$ is exponentially distributed with the mean $\overline{\tau_m}$.

Taking into account criterion (41), the random information integrity controlling process in ISCU is characterized in time by a sequence of random duration states with different probability distribution laws, that is the semi-Markov process [12, 13], which is characterized by a matrix $H(\tau) = \|H_{ij}(\tau)\|$, the arbitrary element of which $H_{ij}(\tau)$ is the probability that the simulated process while in a state i goes to the defined by the E-network architecture state j in a time less than τ, $i = \overline{1, n-1}$, $j = i+1$, $n = l_{\max} + 1$, $1 \leq l_{\max} \leq L$.

Consequently, the number of states $i = \overline{1, l_{\max}}$, the amount of information, whose integrity is controlled when the ISCU is in the state i, V_i, the basic distribution law $F_b(\tau)$ with parameters $\xi = \{P_0, P_1, a, b, d\}$, $P_0 \geq 0$, $P_1 \geq 0$, $P_0 + P_1 \leq 1$, $0 \leq a \leq b \leq 1$, $0 \leq d \leq \infty$, $(P_0 + P_1 \neq 1) \wedge (a = b = 1) \wedge (d = \infty)$, $(P_0 + P_1 \neq 1) \wedge (a = b = d = 0)$ and the density $f_b(\tau) = P_0\delta(\tau) + P_1\delta(\tau - 1) + f_l(0, a, 0, f_b(a), \tau) + f_l(a, b, f_b(a), f_b(b), \tau) + f_l(b, 1, f_b(b), 0, \tau)$ at $d < \infty \Rightarrow f_b(b) = df_b(a)$, $d = \infty \Rightarrow f_b(a) = 0$ and $f_l(x_1, x_2, y_1, y_2, x) = \begin{cases} 0, if\ x \in [0; x_1] \cup [x_2; \infty], \\ (y_2 - y_1)(x - x_1)(x_2 - x_1)^{-1} \\ + y_1, if\ x \in [x_1; x_2], \end{cases}$ are the input parameters for generating control decision, which is to choose a corresponding value $K_{\max i}$ for each from the $i = \overline{1, l_{\max}}$ states and the parameters of the basic probability distribution. Control influences are determined through the assignment of quantities $K_i = K_{\max i}\xi_i$.

To evaluate the criterion of the dynamic efficiency of the IICS, first we calculate the basic probability distribution density values

$$f_b(a) = \begin{cases} 0, if\ (d = \infty) \vee (a = b = d = 0), \\ 2(1 - P_0 - P_1)(b - ad + d)^{-1}, if\ else, \end{cases}$$
$$f_b(b) = \begin{cases} 2(1 - P_0 - P_1)(1 - a)^{-1}, if\ d = \infty, \\ df_b(a), if\ else. \end{cases} \tag{42}$$

DOI 10.15588/1607-3274-2019-1-13

for each state $i=\overline{1,l_{\max}}$ on the basis of values $\xi=\{P_0,P_1,a,b,d\}$.

Further, on the basis of $T_i=K_{\max i}V_i c^{-1}$ – the maximum duration of the semi-Markov process in a state i, we calculate the value $v=T_i t_m^{-1}=K_{\max i}V_i(c\tau_m)^{-1}$ and the Laplace-Stieltjes transformation of the basic probability distribution function

$$\varphi_{bi}\left(T_i\tau_m^{-1}\right)=P_0+P_1e^{-v}+\varphi_{bl}(v)+\varphi_{bs}(v)+\varphi_{bn}(v), \quad (43)$$

where $\varphi_{bn}(v)=\begin{cases}0, if\ b=1,\\ vf_b(b)\left(2e^{-bv}-e^{-v}\right)\left(v(1-b)\right)^{-1}, if\ b<1,\end{cases}$

$$\varphi_{bl}(v)=\begin{cases}0, if\ a=0,\\ vf_b(a)\left(1-e^{-av}\right)\left(av-e^{-av}\right)^{-1}, if\ a>0,\end{cases}$$

$$\phi_{bs}(v)=\begin{cases}0, if\ a=b,\\ v\left(f_b(b)-f_b(a)\right)\left(e^{-av}-e^{-bv}\right)\cdot\\ \cdot\left(v(b-a)+f_b(a)e^{-av}-f_b(b)e^{-bv}\right)^{-1}, if\ a<b,\end{cases}$$

and represent the criterion (41) in the applied form

$$E(\tau_m)=\prod_{i=}^{l_{\max}}\varphi_{bl}(T_i\tau_m^{-1}). \quad (44)$$

Consequently, the expressions (42)–(43) formalize the associate with the E-network representation of SP of ISCU, adapted for practical application, a method for evaluating the effectiveness of the IICS functioning on the basis of a dynamic control of the information integrity (44). The criterion (44) is based on the mathematical model of semi-Markov networks for a comprehensive stochastic description of discrete states of the information integrity control at selected hierarchical levels of the ISCU during continuous discretionary access. The method allows us to select the maximum allowable values of information integrity control factors at sub-levels of the applied level of OSI allocated in the ISCU, at which value of the criterion (44) is maximized, based on the predetermined amount of controlled information, the speed of the information integrity control and the maximum duration of the system's presence in the appropriate state.

Now let's look at the work of ASU, for which we will generalize the model of SP of ISCU in the form of a tuple

$$\langle M_A,M_U,M_R,G\rangle. \quad (45)$$

The first position of the tuple (45) corresponds to the administrative sublevel of the application level of the ISCU from Table 1, the second – corresponds to the identification, the third – corresponds to the integration, the fourth – corresponds to the remaining sublevels and G is a set of subsets

$$G=\{G_E,G_R\cup G_A\cup G_M,G_I\}. \quad (46)$$

Given (45), (46), we isolate in the OSCU E-network the set of potential targets of intruders $Q_z=\{q_{z1},\dots,q_{zn}\}$, which on a system scale is formed as a result of the unification of disjoint sets of classes of information threats $Z=\{z_1,\dots,z_m\}$. The set of objects $D=\{d_1,\dots,d_m\}\in Q$, categorized by types of information threats is a set of precedents that we will use to train the ASU.

A trained ASU is represented in each block of the E-network structure of the ISCU by a set of classifiers that determine the weighted identity degree of the attributes of the analyzed object q_{zi}, $1\le i\le n$ to the classes of information threats z_j, $j=\overline{1,m}$, and compare these degrees with the corresponding threshold values. Situations of excess of the identity degrees of the threshold values are qualified as appropriate information threats, which initiates the reaction of the system described in the SP. With such a mechanism of functioning, the efficiency of the ASU will be determined by the type of classifiers used, the representativeness of the set of precedents used for their training, and the correct choice of weights for classes of information threats and threshold values for the ASU operation. Next, we will investigate the influence of the values of the third and fourth of the listed factors on the quality of the functioning of the ASU, because the first two factors were investigated in previous studies [14, 15].

5 RESULTS

Adjust the operation of the video surveillance center ISCU ASU and the DPU, the structure of which is organized in accordance with the information given in Table 1, so as to optimize the values of the criteria (44) and (45), respectively. The analytical form of expression (43) allows us to predict that the most appreciable dynamics of the value of the criterion (44) can be observed with significant segregation in terms of the volumes of information controlled for integrity by the levels of the hierarchy of the ISCU. However, as with most powerful ISs, more than 99% of all ISCU's data is located at the first (information) level of the ISCU (or at 7 level 1 sub level if consider the ISCU in the OSI model). In particular, in the described system the video archive is 10 Tb and the rest of the software together with the server operating system and all specialized software with the automated speaker recognition system for critical use is about 70 Gb. In this situation, the greatest imbalance in the volumes of information controlled for integrity on levels of ISCU can be observed when powerful data manipulation processes are initiated, the most common of which are: 1) the data backup process initiated by the administrator; 2) initiated by the authorized user process of searching information on the entire database of the ISCU. Let's analyze the relative volumes of information controlled for integrity on the sub-levels of the ISCU

© Bisikalo O. V., Kovtun V. V., Yukhimchuk M. S., 2019
DOI 10.15588/1607-3274-2019-1-13

hierarchy for these two processes, presenting the result of the analysis in the form of Table 3.

On the basis of the data obtained in Table 3 on the relative volumes of information controlled for integrity on the corresponding sublevels of the application level of the ISCU let's find the relationship between the value of the dynamic performance criterion DPU (44) and the values of the duration and the coefficient of the of the ISCU information integrity control for the processes 1 and 2, which are performed during the corresponding discretionary accesses The results of the study is shown in the Fig. 1.

The purpose of the operation of ASU of the above-described video surveillance center ISCU is to identify and correctly classify attacks that aim either to obtain unauthorized access to the information resources of the ISCU or to violate their integrity. To test the performance of the ASU, typified attacks were formulated to check the adequacy of the global SP (attacks on the content of user roles, 5 types of attacks), the local SP (attack on the hardware and software components of the ISCU interaction processes, including at different levels of its hierarchy, 12 types of attacks), the discretionary SP (attacks with attempted unauthorized authentication of users by password, identity card, individual voice parameters and attacks on the combined authentication procedure, 6 types of attacks, details are in [16]). The total number of types of attacks was 23.

The number of functions of the ISCU, described by the corresponding superblocks of different order, and related to the tasks of collecting, registering, storing, processing, updating and presenting of system information resources, was 41. The number of attributes whose values were evaluated by the classifiers for the recognition of the attack types were 9. The number of attacks of each type was 100 times, parameters of 40 of which for each type of attack were used to train ASU. The results of ASU's work on attack recognition were summarized in the form of a set of recommended weights for classifiers who are responsible for detecting attacks on the global, local and discretionary SP, respectively. The threshold of classifier sensitivity to detect the attack, given the critical use of IS, was set to 0.1.

Table 3 – Relative volumes of information controlled for integrity on the sub-levels of the ISCU hierarchy for the processes 1 and 2

Sub-levels of the ISCU hierarchy →	1. Information	2. Management	3. Applied	4. Server	5. Navigation	6. Dispatcher	7. Integration	8. Identification	9. Administrative
Process 1									
Relative volume of information controlled for integrity $V_i / \sum V$, %	1	1	1	1	1	1	1	1	92
Process 2									
Relative volume of information controlled for integrity $V_i / \sum V$, %	5	5	10	10	10	10	10	10	30

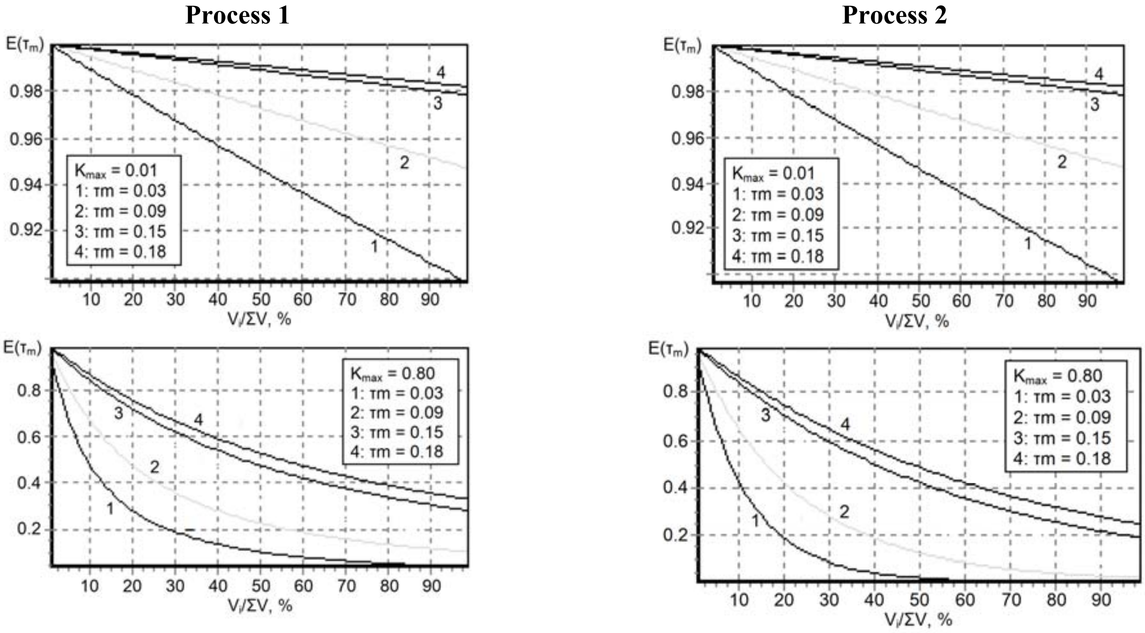

Figure 1 – Dependence of the functional criterion (44) on the input parameters of DPU of ISCU

© Bisikalo O. V., Kovtun V. V., Yukhimchuk M. S., 2019
DOI 10.15588/1607-3274-2019-1-13

6 DISCUSSION

The conducted experiments proved the adequacy of the proposed model for the formation of SP of ISCU on the basis of its representation in the form of an E-network graph, which simulates the hierarchical structure of IS, describes in the form of superblocks the corresponding roles of users, which correspond functions in the form of software services, information integrity controlling processes and the processes for separating of the to system resources access. The analysis of the results of experiments allowed to reveal a number of regularities in the work of ASU and DPU of ISCU, in particular:

1. The influence of the $K_{\max i}$ parameter of the i-level of the ISCU on the value of the criterion $E(\tau_m)$ depends on the volume of information controlled for integrity V_i at the i-level relative to the total volume of information controlled for integrity ΣV during the current discretionary access;

2. At close values of the V_i significant changes in the value of the criterion $E(\tau_m)$ can be achieved by changing the values $K_{\max i}$ at the appropriate levels of ISCU;

3. By changing the values of τ_m and the values of $K_{\max i}$ in one direction we can improve the dynamics of changing the value of the criterion $E(\tau_m)$;

4. At values of parameters $K_{\max i}$ close to zero IICS as a part of DPU ceases to perform its functions, and at values $K_{\max i}$ close to one an efficiency of IICS as a part of DPU is completely determined by the value of the parameter τ_m;

5. The change of the level parameters $K_{\max i}$ leads to a synchronous change in the mathematical expectation of the duration of information integrity control in the ISCU, affecting the quality of the work of IICS, accordingly;

6. It is possible to improve the efficiency of the access separation process implemented in the ASU with the use of sets of classifiers by teaching them methods created for ensembles of decision rules.

CONCLUSIONS

The article presents a mathematical apparatus for a complex unified description of static and dynamic, controlled by integrity and authenticity, processes of the information system for critical use in its hierarchical representation.

The scientific novelty of the results can be attributed to the fact that for the first time a mathematical modeling of a critical information system was implemented, in which, unlike existing ones, a single approach was introduced for describing information processes in the framework of global, discretionary and local security policies with anchoring to a hierarchical structure of information system, which allows to perform analysis and synthesis of functions of support services for user roles based on the object-relational model of information management system organization with the possibility of integration and interoperability induction within a single security policy to control data integrity and authenticity of static and dynamic access.

The practical consequence of the obtained theoretical results is the methods of optimizing the operation of data processing unit and access separation unit, which are responsible for information integrity controlling and access authenticity controlling to the ISCU, respectively. In particular, it is formally adapted for practical use, the method of dynamic information integrity control with the corresponding criterion, which is based on the mathematical apparatus of semi-Markov networks for the complex stochastic description of the discrete states of the information integrity control at selected hierarchical levels of the ISCU during continuous discretionary access. The method allows to select the maximum allowable values of information integrity control coefficients at the sub-levels of the application level OSI allocated in the ISCU, based on the pre-set volume of information controlled for integrity, the speed of its integrity control and the maximum duration of the system's stay in a suitable state.

The article describes a method for controlling access to information processes that are described by superblocks on the E-network representation of the ISCU using sets of classifiers integrated into each block of the superblock that capture the fact of exceeding the corresponding thresholds by weighted degrees of identity of the attributes of the object that wants to access, which allows us to classify the identified information threat and initiate the corresponding reaction described in the system SP. The analysis of the experiments results allowed obtaining the optimal parameters of groups of classifiers, which, in the framework of global, local and discretionary SP, prevent the receipt of unauthorized access to information resources of the ISCU or attempts to violate their integrity.

Further research is planned to be devoted to the collection and analysis of empirical data on the results of practically implemented ISCUs on the basis of the proposed mathematical apparatus for the purpose of factor analysis of the characteristic parameters of its objects and optimization of the set of user roles and corresponding set of functions.

ACKNOWLEDGEMENTS

The work was carried out within the framework of the cathedral scientific research work number 46K4 “Methods of modelling and optimization of complex systems on the basis of intellectual technologies” at the department of computer control systems of the Vinnytsia National Technical University with the support of the staff of the department and related department of automation and information and measuring technology VNTU.

DOI 10.15588/1607-3274-2019-1-13

REFERENCES

1. Conceptual Modeling of Information Systems [Electronic resource]. Access mode: http://infocat.ucpel.tche.br/disc/mc/cmis.pdf
2. Peltier T. Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. Auerbach Publications, CRC Press, 2001, 312 p.
3. ISO/IEC 27001 Information Security Management Standard [Electronic resource]. Access mode: http://pqm-online.com/assets/files/pubs/translations/std/iso-mek-27001-2013(rus).pdf
4. ISO/IEC 2382:2015 Information technology Standard [Electronic resource]. Access mode: https://webstore.iec.ch/publication/22380
5. Alani M. Guide to OSI and TCP/IP Models. Springer Publishing Company, 2014, 50 p. DOI: 10.1007/978-3-319-05152-9
6. Discrete System Models [Electronic resource]. Access mode: http://laser.inf.ethz.ch/2004/papers/abrial/discrete_system_models.pdf
7. Chen Y.-L., Feng Lin Modeling of discrete event systems using finite state machines with parameters*, Proc. of the 2000. IEEE International Conference on Control Applications. (Cat. No.00CH37162), 27–27 Sept. 2000 : proceedings, USA, Anchorage,* 2000, P. 941–946. DOI: 10.1109/CCA.2000.897591
8. Nikolaidou M. Dimosthenis Anagnostopoulos Exploring Web-Based Information System Design: A Discrete-Stage Methodology and the Corresponding Model, *International Conference on Advanced Information Systems Engineering CAiSE 2003*. Berlin, Springer, 2003, pp. 159–174. DOI 10.1007/3-540-45017-3_13
9. Mehler A., Kühnberger K.-U., Lobin H., Lüngen H., Storrer A., Witt A. *Modeling, Learning, and Processing of Text-Technological Data Structures.* Berlin, Springer-Verlag, 2012, XVI, 400 p. DOI 10.1007/978-3-642-22613-7
10. Balle B., Castro J., Gavaldà R. Learning probabilistic automata: A study in state distinguishability, Theoretical Computer Science, 2013, Vol. 473, pp. 46–60. DOI 10.1016/j.tcs.2012.10.009
11. Kim D., Solomon M. Fundamentals of Information System Security, Third Edition. Jones & Bartlett Publishers, 2010, 514 p.
12. Analysis of Probabilistic Processes and Automata Theory [Electronic resource]. Access mode: http://homepages.inf.ed.ac.uk/kousha/etessami-prob-processes-chapter-handbook-of-automata-theory-DRAFT.pdf
13. Falley P. Categories of Data Structures, *Journal of Computing Sciences in Colleges, Papers of the Fourteenth Annual CCSC Midwestern Conference and Papers of the Sixteenth Annual CCSC Rocky Mountain Conference*, 2007, Vol. 23, Iss. 1, pp. 147–153.
14. Bisikalo O. V., Grischuk T. V., Kovtun V. V. Optimizatsiya klasifikatora avtomatizovanoyi sistemi rozpiznavannya movtsya kritichnogo zastosuvannya, *Radio Electronics, Computer Science, Control,* 2018, No. 2, pp. 30–43. DOI 10.15588/1607-3274-2018-2-4
15. Bikov M. M., Gafurova A. D., Kovtun V. V. Doslidzhennya komitetu neyromerezh u avtomatizovaniy sistemi rozpiznavannya movtsiv kritichnogo zastosuvannya, Visnik Hmelnitskogo natsionalnogo universitetu, seriya: Tehnichni nauki. Hmelnitskiy, 2017, No. 2(247), pp. 144–150.
16. Grischuk T. V., Kovtun V. V. Kontseptsiya vprovadzhennya avtomatizovanoyi sistemi rozpiznavannya movtsya u protses avtentifIkatsiyi dlya dostupu do kritichnoyi sistemi, Visnik vinnitskogo politehnichnogo institutu, 2018, No. 6, pp. 98–110.

Received 01.11.2018.
Accepted 26.12.2018.

УДК 681.327.12

МОДЕЛЮВАННЯ ПОЛІТИКИ БЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ КРИТИЧНОГО ЗАСТОСУВАННЯ

Бісікало О. В. – д-р техн. наук, професор, декан факультету комп’ютерних систем і автоматики Вінницького національного технічного університету, Вінниця, Україна.

Ковтун В. В. – канд. техн. наук, доцент, доцент кафедри комп’ютерних систем управління Вінницького національного технічного університету, Вінниця, Україна.

Юхимчук М. С. – канд. техн. наук, доцент, доцент кафедри комп’ютерних систем управління Вінницького національного технічного університету, Вінниця, Україна.

АНОТАЦІЯ

Актуальність. Порівняно із універсальними інформаційними системами, інформаційна система критичного застосування має спрощену структуру інформаційного середовища і специфічні вимоги щодо обсягів і характеру інформаційних ресурсів. Це факт дозволяє відмовитися від надмірної деталізації і звузити об’єкт моделювання до процесу формування політики безпеки інформаційної системи критичного застосування, адекватний проблемний опис якого є досяжним за умови раціонального вибору математичного апарату.

Мета роботи. Синтез математичного апарату для комплексного уніфікованого опису статичних і динамічних, контрольованих за цілісністю та автентичністю, процесів у інформаційній системі критичного застосування у її ієрархічному представленні.

Метод. У статті отримано нові комплексні математичні моделі процесів оброблювання інформації та розмежування доступу до неї, які, на відміну від існуючих, описують в рамках математичного апарату Е-мереж механізми убезпечення середовища та ресурсів інформаційної системи критичного застосування і дозволяють кількісно оцінити цілісність її інформаційних ресурсів. Розроблено математичні моделі синтезу політики безпечної взаємодії інформаційних процесів у інформаційній системі критичного застосування, які дозволяють гарантувати дотримання локальних політик безпеки на різних структурних елементах системи і інтегрувати їх у глобальну політику безпеки із дотриманням єдиної дискреційної політики скрізь у системі.

DOI 10.15588/1607-3274-2019-1-13

Результати. Практичним наслідком отриманих теоретичних результатів є методи оптимізації роботи блоків оброблювання даних і розмежування доступу, які відповідають у інформаційній системі критичного застосування за контроль цілісності інформації та автентичність доступу до неї відповідно. Зокрема, формалізовано асоційований із моделлю політики безпеки інформаційної системи критичного застосування, адаптований для практичного застосування, метод динамічного контролю цілісності інформації із відповідним критерієм, який базується на математичному апараті напівмарковських мереж для комплексного стохастичного опису дискретних станів контролю цілісності інформації на вибраних ієрархічних рівнях системи під час неперервного дискреційного доступу. Метод дозволяє вибрати максимальні допустимі значення коефіцієнтів контролю цілісності інформації на підрівнях прикладного рівня OSI, виділених у інформаційній системі критичного застосування, на основі попередньо заданого обсягу контрольованої інформації, швидкості контролю її цілісності та максимальної тривалості перебування системи у відповідному стані. Також представлено метод контролю доступу до системних інформаційних процесів, який виконується множинами інтегрованих класифікаторів, які фіксують факти перевищення відповідних порогових значень зваженими ступенями ідентичності атрибутів об'єкта, який бажає отримати доступ, класифікують виявлені таким чином інформаційні загрози і ініціюють описані в системній політиці безпеки сценарії. Аналіз результатів проведених експериментів дозволив отримати оптимальні параметри для множин класифікаторів, які, в рамках глобальної, локальної і дискреційної політики безпеки, запобігають отриманню несанкціонованого доступу до системних інформаційних ресурсів або спробам порушення їх цілісності.

Висновки. У статті вперше представлено математичну модель інформаційної системи критичного застосування, у якій, на відміну від існуючих, введено єдиний підхід для опису інформаційних процесів у рамках глобальної, дискреційної та локальної політик безпеки із прив'язкою до ієрархічної структури інформаційної системи, що дозволяє виконувати аналіз і синтез функцій сервісів підтримки ролей користувачів на основі об'єктно-реляційної моделі організації інформаційних ресурсів системи, виконувати їх інтеграцію, індукуванням і забезпечувати сумісність в рамках єдиної політики безпеки, контролювати в системі цілісність інформації та автентичність статичного і динамічного доступу до неї.

КЛЮЧОВІ СЛОВА: інформаційна система критичного застосування, політика безпеки, блок оброблювання даних, блок розмежування доступу, автоматизована система розпізнавання мовців критичного застосування.

УДК 681.327.12

МОДЕЛИРОВАНИЕ ПОЛИТИКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ КРИТИЧЕСКОГО ПРИМЕНЕНИЯ

Бисикало О. В. – д-р техн. наук, профессор, декан факультета компьютерных систем и автоматики Винницкого национального технического университета, Винница, Украина.

Ковтун В. В. – канд. техн. наук, доцент, доцент кафедры компьютерных систем управления Винницкого национального технического университета, Винница, Украина.

Юхимчук М. С. – канд. техн. наук, доцент, доцент кафедры компьютерных систем управления Винницкого национального технического университета, Винница, Украина.

АННОТАЦИЯ

Актуальность. По сравнению с универсальными информационными системами, информационная система критического применения имеет упрощенную структуру информационной среды и специфические требования по объемам и характеру информационных ресурсов. Это факт позволяет отказаться от чрезмерной детализации и сузить объект моделирования в процесс формирования политики безопасности информационной системы критического применения, адекватное проблемное описание которого является достижимым при условии рационального выбора математического аппарата.

Цель работы. Синтез математического аппарата для комплексного унифицированного описания статических и динамических, контролируемых на предмет целостности и аутентичности, процессов в информационной системе критического применения в ее иерархическом представлении.

Метод. В статье получены новые комплексные математические модели процессов обработке информации и разграничение доступа к ней, которые, в отличие от существующих, описывают в рамках математического аппарата E-сетей механизмы защиты среды и ресурсов информационной системы критического применения и позволяют количественно оценить целостность ее информационных ресурсов. Разработаны математические модели синтеза политики безопасного взаимодействия информационных процессов в информационной системе критического применения, которые позволяют гарантировать соблюдение локальных политик безопасности на различных структурных элементах системы и интегрировать их в глобальную политику безопасности с соблюдением единой дискреционной политики в системе в целом.

Результаты. Практическим следствием полученных теоретических результатов являются методы оптимизации работы блоков обработки данных и разграничения доступа, которые отвечают в информационной системе критического применения за контроль целостности информации и аутентичность доступа к ней соответственно. В частности, формализовано ассоциированный с моделью политики безопасности информационной системы критического применения, предназначенный для практического применения, метод динамического контроля целостности информации с соответствующим критерием, который базируется на математическом аппарате полумарковских сетей для комплексного стохастического описания дискретных состояний контроля целостности информации на выбранных иерархических уровнях системы при непрерывном дискреционном доступе к ее информационным ресурсам. Метод позволяет выбрать максимально допустимые значения коэффициентов контроля целостности информации на подуровнях прикладного уровня OSI, выделенных в информационной системе критического применения, на основе предварительно заданного объема контролируемой информации, скорости контроля ее целостности и максимальной продолжительности пребывания системы в соответствующем состоянии. Также представлен метод контроля доступа к системным информационным процессам,

DOI 10.15588/1607-3274-2019-1-13

который осуществляется множествами интегрированных классификаторов, которые фиксируют факты превышения соответствующих пороговых значений взвешенными степенями идентичности атрибутов объекта, который желает получить доступ, классифицируют выявленные таким образом информационные угрозы и инициируют описанные в системной политике безопасности сценарии. Анализ результатов проведенных экспериментов позволил получить оптимальные параметры для множеств классификаторов, которые, в рамках глобальной, локальной и дискреционной политик безопасности, предотвращают получению несанкционированного доступа к системным информационных ресурсам или попытки нарушения их целостности.

Выводы. В статье впервые представлена математическую модель информационной системы критического применения, в которой, в отличие от существующих, введен единый подход для описания информационных процессов в рамках глобальной, дискреционной и локальной политик безопасности с привязкой к иерархической структуры информационной системы, что позволяет выполнять анализ и синтез функций сервисов поддержки ролей пользователей на основе объектно-реляционной модели организации информационных ресурсов системы, выполнять их интеграцию, индуцирование и обеспечивать совместимость в рамках единой политики безопасности, контролировать в системе целостность информации и аутентичность статического и динамического доступа к ней.

КЛЮЧЕВЫЕ СЛОВА: информационная система критического применения, политика безопасности, блок обработке данных, блок разграничения доступа, автоматизированная система распознавания диктора критического применения.

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Conceptual Modeling of Information Systems [Electronic resource]. – Access mode: http://infocat.ucpel.tche.br/disc/mc/cmis.pdf
2. Peltier T. Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management / Thomas R. Peltier. Auerbach Publications: CRC Press, 2001. – 312 p.
3. ISO/IEC 27001 Information Security Management Standard [Electronic resource]. – Access mode: http://pqm-online.com/assets/files/pubs/translations/std/iso-mek-27001-2013(rus).pdf
4. ISO/IEC 2382:2015 Information technology Standard [Electronic resource]. – Access mode: https://webstore.iec.ch/publication/22380
5. Alani M. Guide to OSI and TCP/IP Models / Mohammed M. Alani. – Springer Publishing Company, 2014. – 50 p. DOI: 10.1007/978-3-319-05152-9
6. Discrete System Models [Electronic resource]. – Access mode: http://laser.inf.ethz.ch/2004/papers/abrial/discrete_system_models.pdf
7. Chen Y.-L. Modeling of discrete event systems using finite state machines with parameters / Yi-Liang Chen, Feng Lin // Proc. of the 2000. IEEE International Conference on Control Applications. (Cat. No.00CH37162), 27–27 Sept. 2000 : proceedings. – USA, Anchorage, 2000. – P. 941–946. DOI: 10.1109/CCA.2000.897591
8. Nikolaidou M. Exploring Web-Based Information System Design: A Discrete-Stage Methodology and the Corresponding Model / Mara Nikolaidou, Dimosthenis Anagnostopoulos // International Conference on Advanced Information Systems Engineering CAiSE 2003. – Berlin : Springer, 2003. – P. 159–174. DOI 10.1007/3-540-45017-3_13
9. Mehler A. Modeling, Learning, and Processing of Text-Technological Data Structures / [A. Mehler, K.-U. Kühnberger, H. Lobin et al.]. – Berlin : Springer-Verlag, 2012. – XVI, 400 p. DOI 10.1007/978-3-642-22613-7
10. Balle B. Learning probabilistic automata: A study in state distinguishability / Borja Balle, Jorge Castro, Ricard Gavaldà // Theoretical Computer Science. – 2013. – Vol. 473. – P. 46–60. DOI 10.1016/j.tcs.2012.10.009
11. Kim D. Fundamentals of Information System Security, Third Edition / David Kim, Michael Solomon. – Jones & Bartlett Publishers, 2010. – 514 p.
12. Analysis of Probabilistic Processes and Automata Theory [Electronic resource]. – Access mode: http://homepages.inf.ed.ac.uk/kousha/etessami-prob-processes-chapter-handbook-of-automata-theory-DRAFT.pdf
13. Falley P. Categories of Data Structures / P. Falley // Journal of Computing Sciences in Colleges, Papers of the Fourteenth Annual CCSC Midwestern Conference and Papers of the Sixteenth Annual CCSC Rocky Mountain Conference. – 2007. – Vol. 23, Iss. 1. – P. 147–153.
14. Бісікало О. В. Оптимізація класифікатора автоматизованої системи розпізнавання мовця критичного застосування / О. В. Бісікало, Т. В. Грищук, В. В. Ковтун // Радіоелектроніка, інформатика, управління. – 2018. – № 2. – С. 30–43. DOI 10.15588/1607-3274-2018-2-4
15. Биков М. М. Дослідження комітету нейромереж у автоматизованій системі розпізнавання мовців критичного застосування / М. М. Биков, А. Д. Гафурова, В. В. Ковтун // Вісник Хмельницького національного університету, серія: Технічні науки, Хмельницький. – 2017. – №2 (247). – С. 144–150.
16. Грищук Т. В. Концепція впровадження автоматизованої системи розпізнавання мовця у процес автентифікації для доступу до критичної системи / Т. В. Грищук, В. В. Ковтун // Вісник Вінницького політехнічного інституту. – 2018. – № 6. – С. 98–110.

DOI 10.15588/1607-3274-2019-1-13