UDC 621.31I :658.284.011. 56:681.3 **doi: 10.26906/SUNZ.2019.5.072**

O. Milov[1], S. Milevskyi[1], S. Pohasii[1], K. Rzayev[2]

[1] Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
[2] Azerbaijan State Oil Academy, Baku, Azerbaijan

PROCEDURAL BASIS OF CYBERSECURITY SYSTEMS

The subject of the research is a system of procedures implemented within the framework of a cybersecurity system, which is analyzed and described in a formal form. **The aim** of this work is to develop a formal description of the system of procedures implemented within the security system, which would automate the analysis, adaptation and design of the entire complex of processes operating within the cybersecurity system. The technique is based on the use of set theory, as well as system and process analysis. **The tasks** that need to be solved are to analyze existing approaches to the analysis of ongoing processes to identify their advantages and disadvantages. Based on the analysis, to propose a new formal presentation and classification of security system processes. The following results were obtained: the general characteristics of the security system processes were identified, the information and model bases of the security system were formed, which made it possible to present an approach to the classification and formal presentation of procedures implemented in security systems. **Conclusion**: The approach to the classification and the formal description of the procedures implemented in the security system presented in the article allows us to formalize the approach to the analysis and subsequent synthesis of the necessary procedural basis for the design and reengineering of security systems, in a more understandable way to the decision-maker. Thus, the efficiency of managing the mechanisms for protecting the contour of business processes is increased.

Keywords: cybersecurity systems, decision maker, semiotic approach, cyberattack, decision making.

Introduction

Operational interaction of a decision maker (DM) with computer processing tools, presenting information and supporting the selection and application of tools to counter cyber attacks constitute one of the main operations of the entire technological cycle to ensure cybersecurity of business processes. At the same time, the characteristics of a person as an element of a contour are increasingly becoming a «bottleneck» in operational counteraction given the existing structure of means and methods of man-machine interaction.

A way out of this situation is the creation of a cybersecurity system structure that allows:

- collection and integration of information about potential threats and sources of their implementation;
- processing and storage of this information with acceptable degrees of aggregation;
- automatic and (or) man-machine assessment of the state of the level of protection and the environment of functioning of business processes with prediction of the emergence of new types of threats;
- automatic and (or) man-machine search for solutions on the choice of countermeasures, initiated by assessments of the state of the protected object and its environment, as well as unfavorable forecasts of development trends of cyberthreats;
- automatic and (or) man-machine optimization in terms of money spent and time for found and recommended solutions;
- human-machine decision-making with challenge capabilities for analyzing both the data underlying the search for proposed solutions to counter cyberattacks, and the logic and mathematical methods used, on which the search for proposed solutions was based.

The semiotic approach explores the pattern in which the control body knows:

- not always a certain set of parameters $\{x\}$, characterizing the current state of the object of protection and the environment of opposition;
- many ways to split $\{x\}$ on classes of states $K=\{k_1, k_2, ..., k_z\}$, requiring decisions;
- the set models of finding solutions $\{M\}$;
- the set mechanisms for finding solutions on models – $\{\varphi\}$.

When implementing such a scheme, dynamically formed sets $\{k\}$ and $\{M\}$, of the possibility of obtaining the necessary solutions in a reasonable time, but the nature of the solutions obtained is qualitative.

Methods of the theory of identification and planning of an experiment can be applied only to the extent that statistics can be collected on the reactions of the object of defense to attacks in the mode of its operation. This makes it difficult to use them directly in the systems under consideration.

Considering the many functions entrusted to the system, the existing approaches to automating decision-making processes, and the presence of decision-makers united in teams, the cybersecurity system for ensuring the contour of business processes should be based on the concept of human-machine control.

Features of building cyber security systems

Currently, there is no complete general theory of cybersecurity systems, and therefore there is no general model of such systems that have knowledge of cybersecurity and can use cybersecurity systems to organize purposeful behavior of the system while ensuring specified quality criteria [1].

At the same time, an analysis of the tasks to be solved in decision-making systems with intelligent mechanisms for automatically finding means to counter cyber threats shows that [2]:

a formal apparatus describing the processes of recognizing situations, developing and making decisions in a rapidly changing situation with elements of uncertainty should be extremely flexible;

the processes of making decisions are based not only on quantitative characteristics, but also on factors that do not always have quantitative measures (psycho-

logical, moral, etc.). Therefore, the preparation of information for decision-making on the means of counteraction should be viewed as a creative act of choice from a set of possible decisions, in which quantitative factors are combined with the heuristic abilities embedded in the computer that forms the decisions, i.e. decisions are formed on the basis of two components of decision-making and development (formal and creative);

Special attention should be paid to the decision-making procedure itself, i.e. it is important to know which components of the cybersecurity process should be controlled by the decision maker, and which components can be executed by the computer;

an important place is occupied by the problem of human and computer communication. This problem has two sides – the satisfaction of information needs on the information available in the system and participation in the procedure for developing and adopting decisions. A natural requirement for the means of presenting information is their informational content and perception to the language of communication – proximity to the language of professional vocabulary and its slang. The form of communication should be interactive;

the problem of learning or adapting the developed system to the emergence of a new class of threats (hybrid, synergistic) requires the development of a special procedure that allows the release of information presented formally (algorithmically) and informally (expertly). Such a procedure should be man-machine in nature and be applicable to a large class of situations;

the problem of designing and generating different versions of software for decision-making systems requires the development of a special human-machine technology for designing within this class of systems.

Taking into account the nature of the activities of the systems of this type, based on the ability to adapt and build targeted behavior, we will distinguish two types of information in the cybersecurity system [3]:

1) information that implements the targeted behavior of the system by organizing the processes of recognition of the type of cyber attack, search and decision-making on countering;

2) information that is elements of processing from the above-mentioned processes.

The first type of information is called *the knowledge of the system about the subject field of management* – models, tasks, algorithms.

The second type of information is called *data on the state of the system, the object and environment of the formation of threats* – the parameters of the system, the object, the environment and the area of definition of these parameters.

Analysis of decision-making processes allowed us to base the concept on the following notions [4]:

global logical model of knowledge as a set of tasks, models and methods of their use for organizing the processes of targeted recognition of situations of threats, developing and making decisions on counteraction;

the area of interpretation of the global logical model of knowledge as a structured and ordered dynamic set of attributes characterizing the parameters of the cybersecurity system, the object and the environment of functioning;

an army of system analysts, experts who, using means of recognition and communication, can define and describe the elements of a global logical model of knowledge and its area of interpretation in a volume sufficient to solve problems that can be posed in any problem situations.

When developing a concept, the following model characteristics should be taken into account:

Expertise – as a basis for shaping the goals of the cybersecurity system, models that are the area of search for solutions, rules for searching and making decisions on cyber defense of the contour of business processes.

Associativity – as the basis for automatic accumulation, generalization of information and adaptation of the cybersecurity system to the changing environment of functioning.

Many alternatives – as the basis for displaying all possible ways of finding solutions.

Semiotics – as the basis for the development of mechanisms for the integration of heterogeneous information about the object of protection and the environment of the formation of cyber-thunderstorms.

Sociability – as the basis for the implementation of dialogue means of communication system with decision makers.

Virtuality – as a basis for reflecting the globality of information, which is characterized by territorial disunity and multi-level sources of receiving, storing and using information.

Efficiency – as the basis for the implementation of the model of ensuring the necessary level of cybersecurity in software and hardware environments.

The resulting model has a number of new properties, for example, it is at the same time a means of solving problems arising before a system, and a methodology for designing and implementing such systems. The team of experts has both formal and informal knowledge of the subject area of management. In addition, each expert performs a specific learning function in the team. This allows him to easily construct and fill a knowledge model, highlight a specific local logical knowledge model and have access to global knowledge and data models.

The presence of experts allows, in addition to the recognition, development and decision-making procedures, to also build:

procedures for identifying consistent knowledge, using dynamically changing expert groups; create expert decision-making models for different classes of problem situations (threats);

simulate any combination of centralized and decentralized decision making; achieve greater generality, which allows for various methods of solving problems. In addition, in such a team, it is possible to formalize the connection between experts and build standard means of communication on this basis. With the help of these tools, various modes of interaction are organized – from the explicit reference of one expert to another to the implicit reference, when the addressee is determined by the function implemented by him.

The presence of a multitude of tasks, models and knowledge of the way they are used in various situations of decision making and development allows us to develop uniform means of describing such information and organizing their use by the system. Linguistic and software support tools are used as such tools: languages of logical knowledge model definition (LKM) and manipulation of elements of a logical knowledge model (KMM). The definition of knowledge involves the introduction of new types of information, such as model, task. Knowledge manipulation is based on planning decision-making processes in the global knowledge model by using, first of all, the goal setting mechanism.

The considered concept is in good agreement with the nature of complex human-machine decision-making systems and allows using the knowledge of experts and programmers:

1) generate threat classifiers for the corresponding contour of business processes;

2) to build models of recognition of cyber attacks, the classification of the state, targeting, development and adoption of governing decisions on countering cyber attacks;

3) o build a functionally complete set of computational algorithms characterizing a specific area of cyber defense;

4) "fill" the cybersecurity software system with specific content;

5) to design and generate software systems and organize its problem orientation.

Summarizing what has been said, it can be concluded that the considered concept fully meets the problems of human-machine management of complex technological objects, methods and the theory of building large control software packages, cybersecurity systems [5]. The task of the research is the formation and description of a variety of procedures, the implementation of which in the cybersecurity system of the business process contour will allow to realize the properties and features of the effective functioning of the cybersecurity system as a complex human-machine system.

Decision making procedures in cyber security systems

Ensuring the required level of cybersecurity of the business process contour will be considered as a man-machine activity to determine the state of the protected object, which requires making decisions related to the search and selection by targeted coordination of *behavioral patterns of all participants in cyber conflict* – M_1 and existing at the decision maker – M_2. Such a model representation is determined by the accumulated knowledge of methods and mechanisms for ensuring cybersecurity, the goals and limitations of each of the parties, objective and subjective preferences on the choice of ways to achieve goals and assess their degree of applicability. The interactivity of human interaction with the system is organized by introducing the concept of a man-machine situation that requires decisions S_y and defining this notion of a set of attributes. The nature of this activity, on the one hand, is set by man by controlling the processes of setting the task of tracking the progress of its solution. On the other hand, the system clarifies the correctness of the tasks set, proposes alternative ways of solving them, using the "knowledge and experience" of the search for solutions, reflected in its model. Thus, the person and the system interact as partners, coordinating their methods of solving the tasks of ensuring cybersecurity of the required level. Symbiosis will be optimal only when the work of the system is organized in the "intelligent" human advisor mode, performing the routine functions of automatic recognition of attacks as well as the search for countermeasures based on information obtained both from experts and using system knowledge. This knowledge exists in the system in the form of two types of structured sets {computational and set-theoretic}, {interactive and *expert logical-algebraic and logical-linguistic*} models of cyber-attack recognition and the search for means to counter it. The first type of models is defined on situations for which an algorithm can be found that connects the desired parameters with the given ones, and the search of variants is not very large. The second type of models is used to search for solutions that are highly dependent on situations and where the search is extremely It can be said that computational and set-theoretic models are analogs of computational operations when searching for solutions, and interactive and expert models are analogs of methods of searching for solutions.

The capabilities of each of the interacting parties to a cyber conflict are determined by the completeness of behavior models, decision-making procedures and the model basis for decision-making procedures. At the same time, decision-making and behavior processes are considered semiotic (sign). Used in this sequence of steps (related causal, temporal, spatial and other relationships) finding control solutions for each problem situation is considered as the *logic of finding solutions*.

At each step of interaction between the decision maker and the decision support system of one of the parties, a query is formed in the form of a problem situation and (or) a subset of the model's algebraic operations in accordance with the logic of the search for solutions. The task of the decision-making system is to find the interpretation of these operations in terms of their model, their implementation and in response to the formation of the request.

The formal representation of the model of behavior of the decision maker in the operational decision making is given by the expression

$$M_1=<BT, DM, I>,$$

where

$$BT=<L_{BT}, ACS, \Theta>$$

- behavior theory (system knowledge model);

$$DM =< x^Z, b^Z, f^Z, p^Z >.$$

- information data model describing the system;

$$I =< UI_1, CI_2 >.$$

- interpretation of BT in DM, here $L_{BT}=L_{KDL} \cup L_{DDL}$ – a language for describing a behavior model that is a combination of knowledge and data definition languages; ACS – theory axioms; Θ – rules of inference statements in theory; x^z, b^z – set of variables and state constants; f^z, p^z –

a set of function and predicate of state variables; UI_1 – user interpretation of the elements of the system knowledge model, which defines expertly the correspondence rule between the syntaxes structure of the language elements L_{BT} and their meaning in the field of cybersecurity (semantics of decision makers); CI_2 – machine interpretation of elements, which specifies expertly the algorithm for establishing the correspondence between the semantic structure of language elements L_{BT} and their truth at every current moment of the search for solutions (pragmatics of the field of cyber security).

Formal model of the behavior of a participant in a cyber conflict, depending on the restrictions imposed on the rules for deriving statements Θ, can be described by means of first-order predicate logic, production and algorithmic systems. Indeed, in the predicate logic there are no restrictions on the use of inference rules. Any withdrawal rule fits any statement already deduced if this statement allows its use. In production systems that are also based on the logic of predicates, there are additional conditions on the applicability of a particular inference rule. These conditions may change during the operation of the production system, depending on the receipt of this or that information in the process of withdrawal. In algorithmic systems, the sequence of application of the rules is uniquely determined. As a language for describing control theory, a first-order predicate logic language and an information processing algorithm language are used. The rules of inference of statements in the theory are the rules of inference in the logic of predicates, their modifications in the system of products and algorithmic rules.

The relationship of the model of behavior with problem situations and problems of finding solutions that appear when they appear is taken into account by taking into account the logical sequence of decision makers working stages while ensuring the security of business processes and identifying a variety of decision-making procedures characteristic of decision makers. The specified set of procedures can be represented in the following sequence:

procedure of situation classification:

$$P_1 =< S, J, K_p, K_s >,$$

where S – situation defined by some relation on the set of elements I; J – set of expert preferences for the choice of classification rules, given on the set $\{S \times K_s\}$; K_p — set of classification rules – decision procedure; K^*, —classes of situations set for which there are models for finding solutions;

procedure of the model classification allows to define a set of decision-making models, organizing the calculations on which you can find the required solutions to ensure the required level of cybersecurity:

$$P_2 =< S, K_s, A_1, M_1 >,$$

where A_1 — a set of alternatives for choosing solution search models whose weights depend on S and K_s, can be set by the person in an interactive mode of work with the system; M_1 — a set of models of finding solutions;

procedure of forming strategies for the goal of finding solutions allows to define a set of local and / or global goals of the cybersecurity system that must be achieved with the help of solutions found in this class of situations:

$$P_3 =< S, K_s, G, C_r, S_{tr} >,$$

where G — a set of current targets facing the control system; Cr — a set of criteria for achieving goals (both goals and criteria can vary and change over time); Str — a set of strategies to find solutions;

procedure for finding target management solutions allows to organize a search for solutions for each of the problem situations in accordance with the goals and criteria for ensuring the security of the business process loop:

$$P_4 =< S, S_{tr}, M_1, R_G >,$$

where R_G — a set of target control solutions that can be found in the decision search model (knowledge base) M_1, tuned to the current situation $s_i \in S$ when using strategy $str_i \in Str$. This procedure performs two functions — a computational sequence finder and a solver scheduler. The first function is to form a crucial program sequence, the second is to organize the execution of these programs and receive management recommendations in a specific computing environment;

the procedure for determining the possible outcomes of the implementation of solutions allows to set the reachability of local and (or) global management goals in the implementation of certain solutions to counter cyber attacks. This is done by organizing calculations on a model of an admissible decision area – M_{ADA}, defining this area — O_{ACA}, in accordance with the objectives G and criteria – Cr, characteristic of this level of decision making. This procedure is set by

$$P_{11} =< P_1, P_2, P_3, P_4 >,$$

where R_{G1} – the set of those governing decisions that are satisfactory outcomes, i.e. outcomes that can achieve local and / or global management objectives.;

procedure of the decision substantiation allows assessing the quality of decisions (their optimality) by organizing calculations on a model for determining the optimal decision-making area (M_{ODA}) to select the area of optimal control solutions (O_{OD}) in accordance with the goals and criteria. Tuple element R_{G1} is the set of those control solutions that satisfy O_{OD} and can be primarily recommended for implementation. This procedure

$$P_6 =< S, R_{G1}, G, C_r, M_{ODA}, O_{OD}, R_{G2} > -$$

procedure of the solution synthesis allows reducing the number of simultaneously recommended solutions for counteraction, regardless of how many situations are simultaneously analyzed by the system. In addition, the procedure ranks decisions issued by the decision maker as according to the information received from the procedures P_5, P_6, so using the set of preferences for the "narrowing" of the set R_G. These preferences can be set expertly.

The procedure is given as

$$P_7 =< S, R_{G2}, O_{ACD}, O_{ODR}, R >.$$

Information for the decision maker after the operation of this procedure is issued in the form <{*S*}=> {*R, O_{ACD}, O_{ODR}*}.

The decision maker can associate the current situation with the necessary decisions, taking into account their belonging to O_{ACD} or O_{ODR}, setting R_{G2};

procedure of the decision-making allows to organize the process of man-machine interaction in order to make one decision to be implemented. In this case, the decision maker may choose one of the means of counteraction recommended by the system or accept his own, different from the recommended, R_G, what he should inform the system. If $R_G \bigcap \overline{R} = 0$, then this solution can be implemented. Here $\overline{R} = R_G \bigcap R_{G1} \bigcap R_{G2}$ – forbidden set of solutions. Formally, this procedure,

$$P_8 =< S, R, \overline{R}, R_G, >,$$

procedure for evaluating the results of the implementation of the decisions allows to evaluate the effectiveness of the adopted and implemented decisions for the purpose of correcting (in the mode of training or self-study) the model of knowledge of the system and translating part of the information { <situation> – <decision>} from the sphere of the decision-making system to the sphere of automatic implementation of the decision. This procedure

$$P_9 =< S, R \cup R_G, M_1, P_{13} >,$$

where P_{13} – procedure for learning (self-study) of the system and correction of its knowledge model M_1;

procedure of the solution tracing makes it possible to organize the tracking of the logic of machine reasoning when searching for solutions and the information basis used for this. This procedure returns the DMP the observability property, i.e. the possibility of establishing any relationship on the elements of decision-making procedures. The tracing procedure is based on the modification of an ordered sequence φ_1-φ_9 – procedures. The modification consists in introducing into each procedure i an assertion about the correctness of obtaining results with its help. Formally, this procedure

$$P_{10} =< \mu_1 : P_1, \mu_2 : P_2, ..., \mu_9 : P_9, C_{or} >,$$

where μ_1, μ_2, ..., μ_9 — conditions of performance (validation statement) of procedures P_1, P_2, ..., P_9 respectively, recorded as μ_i:P_i. With the help of the elements of this tuple, a person can, through interaction with the system, psychologically believe in the correctness of the solutions found. Statements owned by *Cor,* determine the consistency of logic embedded in the database of models and procedures of a computer and a decision maker, i.e. they allow the system to inform the decision maker that the next cycle of search and decision-making is completed;

procedure of the information dialogue organizes the human-machine interaction of the decision maker with the system in order to obtain the necessary information. This procedure

$$P_{11} =< P_1, P_2, P_3, P_4 >,$$

where P_1-P_4 – considered procedures in which the following substitutions were made: S/R_A, M_1/M_A, C/C_D, G/G_D; R/R_0; $R_Д$ – many requests from the decision maker; $M_A \in M_1$ – a variety of response search models by query definition areas; Str_D – a set of strategies aiming for finding solutions ranked by a set M_A; G_D – a set of current goals; R_O – a set of answers issued by the decision maker when the system responds to a request;

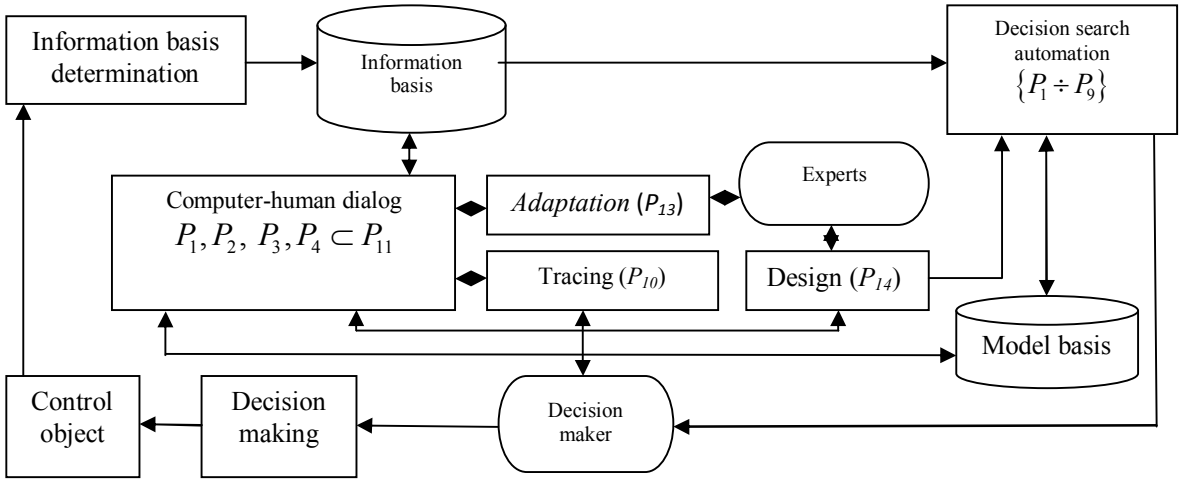

Fig. 1. The logical sequence of cybersecurity system procedures

procedure for determining the information basis for making decisions communicates with the information collection system in order to organize the processing of this information and record it in the information model (database) of the systems. Formally, this procedure:

$$P_{12} =< S, P_1, P_2, P_3, P_4, M_1, M_D >,$$

where M_D – information model storing the current state of the object;

the adaptation / training procedure allows to organize an automated system setup for the cyber security area.

This procedure

$$P_{14} =< S, L_{DKL}, L_{DML}, L_{LDL}, M^{Comp} >,$$

where L_L — a mechanism for correcting knowledge and data base models (means for describing knowledge and data), which allows to bind information in its machine

representation; E_K, E_D — set of elements of the model level of knowledge and data;

procedure of a computer-aided design, or, alternatively, an interactive cyber-security system computer-aided design system. For decision makers and system analysts, designers is the procedure

$$P_{14} =< S, L_{DKL}, L_{DML}, L_{LDL}, M^{Comp} >,$$

where S — design situation from a class of man-machine design situations, reflecting the subject-oriented formulation of the problem of constructing an information-model basis; L_{DKL}, L_{DML}, L_{DDL} language means of describing the elements of the model basis of knowledge and data; M^{Comp} – machine representation of information model basis.

Conclusions

The developed and cited procedural basis of cyber-security systems will significantly improve the efficiency of the development and implementation of modern cybersecurity methods. The use of the developed models will significantly formalize the process of creating cybersecurity systems and thus eliminate the subjectivity of the decisions made.

REFERENCE

1. Грищук Р. В., Даник Ю. Г. Основи кібернетичної безпеки : Монографія / Р. В. Грищук, Ю. Г. Даник ; за заг. ред. проф. Ю. Г. Даника. – Житомир : ЖНАЕУ, 2016. – 636 с.: іл.
2. Cayirci E., GhergherehchiR. “Modeling cyber attacks and their effects on decision process” Proceedings of the 2011 Winter Simulation Conference, 2011.
3. Hryshchuk R. The synergetic approach for providing bank information security: the problem formulation // R. Hryshchuk, S. Yevseiev/ Безпека інформації. – 2016. – № 22 (1). – С. 64–74.
4. Balke T., Gilbert N. “How Do Agents Make Decisions? A Survey”, Journal of Artificial Societies and Social Simulation, # 17 (4), 2014.
5. Kott, A., Wang, C., Erbacher, R.F.: Cyber Defense and Situational Awareness. Springer (2014).

Рецензент: д-р техн. наук, проф. С. Г. Семенов,
Національний технічний університет “ХПІ”, Харків
Received (Надійшла) 22.08.2019
Accepted for publication (Прийнята до друку) 16.10.2019

Процедурний базис систем кібербезпеки

О. Мілов, С. Мілевський, С. Погасій, Х. Рзаєв

Предметом дослідження є система процедур, що реалізується в рамках системи кібербезпеки, яка аналізується і описується в формальному вигляді. **Метою** даної роботи є розробка формального опису системи процедур, що реалізуються в рамках системи безпеки, яке дозволило б автоматизувати процеси аналіз, адаптації та проектування всього комплексу процесів, що функціонують усередині системи кібербезпеки. Методика заснована на використанні теорії множин, а також системного і процесного аналізу. **Завдання**, які необхідно вирішити - проаналізувати існуючі підходи до аналізу реалізованих процесів для виявлення їх переваг та недоліків. На основі проведеного аналізу запропонувати нове формальне подання та класифікацію процесів системи безпеки. Були отримані наступні **результати**: виявлено загальні характеристики процесів системи безпеки, сформовані інформаційний і модельний базиси системи безпеки, що дозволило представити підхід до класифікації і формальному поданням процедур, реалізованих в системах безпеки. **Висновок**: Представлений в статті підхід до класифікації і формальному опису процедур, реалізованих в системі безпеки, дозволяє формалізувати підхід до аналізу і подальшого синтезу необхідного процедурного базису при проектуванні і реинжиниринге систем безпеки, у вигляді більш зрозумілою особі, що приймає рішення. Таким чином збільшується ефективність управління механізмами захисту контуру бізнес-процесів.

Ключові слова: система кібербезпеки, особа, яка приймає рішення, семіотичний підхід, кібератака, прийняття рішень.

Процедурный базис систем кибербезопасности

А. Милов, С. Милевский, С. Погасий, Х. Рзаев

Предметом исследования является система процедур, реализуемая в рамках системы кибербезопасности, которая анализируется и описывается в формальном виде. **Целью** данной работы является разработка формального описания системы процедур, реализуемых в рамках системы безопасности, которое позволило бы автоматизировать процессы анализ, адаптации и проектирования всего комплекса процессов, функционирующих внутри системы кибербезопасности. Методика основана на использовании теории множеств, а также системного и процессного анализа. **Задачи**, которые необходимо решить – проанализировать существующие подходы к анализу реализуемых процессов для выявления их преимуществ и недостатков. На основе проведенного анализа предложить новое формальное представление и классификацию процессов системы безопасности. Были получены следующие **результаты**: выявлены общие характеристики процессов системы безопасности, сформированы информационный и модельный базисы системы безопасности, что позволило представить подход к классификации и формальному представлению процедур, реализуемых в системах безопасности. **Вывод**: Представленный в статье подход к классификации и формальному описания процедур, реализуемых в системе безопасности, позволяет формализовать подход к анализу и последующему синтезу необходимого процедурного базиса при проектировании и реинжиниринге систем безопасности, в виде более понятном лицу, принимающему решение. Таким образом увеличивается эффективность управления механизмами защиты контура бизнес-процессов.

Ключевые слова: система кибербезопасности, лицо, принимающее решение, семиотический подход, кибератака, принятие решений.