DOI: 10.18372/2225-5036.25.13841

MECHANISMS OF CYBER SECURITY: THE PROBLEM OF CONCEPTUALIZATION

Oleksandr Milov[1], Nadiia Kazakova[2], Piotr Milczarski[3], Olha Korol[1]

[1]Kharkiv National University of Economics
[2]Odessa State Environmental University
[3]University of Lodz

MILOV Oleksandr, *PhD, Associate Professor*

Date and place of birth: 1955, Zaporozhye, Ukraine.
Education: Moscow Power Engineering Institute, 1978.
Position: associate professor, Department of Cyber Security and Information Technology.
Research interests: decision theory, coordination in distributed systems, cryptography, agent-based modeling.
Publication: monographs −17, scientific papers – 78, 10 textbooks.
E-mail: Oleksandr.Milov@hneu.net.
Orcid ID: 0000-0001-6135-2120.

KAZAKOVA Nadiia, *Dr. of Tech.Sc*

Date and place of birth: 1979, Odessa, Ukraine.
Education: Odesa National Academy of Telecommunications n. a. O.S. Popov, 2001.
Position: Professor of Information Technology Department.
Research interests: information and cyber security, information technology, information protection systems.
Publications: more than 200 scientific publications, including monographs, articles and patents.
E-mail: kaz2003@ukr.net.
Orcid ID: 0000-0003-3968-4094.

MILCZARSKI Piotr, *PhD*

Date and place of birth: 1969, Gostynin, Poland.
Education: University of Lodz, 1999 (PhD), 1995 (MSc).
Position: University of Lodz, Faculty of Physics and Applied Informatics, Department of Computer Science, Poland.
Work position: Head of Mobile Systems Lab.
Research interests: image processing, artificial intelligence, machine learning, deep learning.
Publications: more than 50 scientific publications.
Email: piotr.milczarski@uni.lodz.pl.
Orcid ID: 0000-0002-0095-6796.

KOROL Olha, *PhD, Associate Professor*

Date and place of birth: 1981, Crimea, Ukraine.
Education: Simon Kuznets Kharkiv National University of Economics, 2005.
Position: associate professor, Department of Cyber Security and Information Technology.
Research interests: ensuring the security of banking information resources.
Publication: monographs – 3, scientific papers – 36.
E-mail: olha.korol@m.hneu.edu.ua.
Orcid ID: 0000-0002-8733-9984.

Abstract. *The article discusses general approaches related to the use of the concept of "mechanism" in the cybersecurity system. The initial definition of the mechanism in systems of analytical dynamics is presented. The transformation of the concept of "mechanism" is traced from mechanical systems to economic, social and organizational-technological. The definition of a mechanism that can be used in the analysis and design of decision-making systems is formulated, the features of using this concept in cybersecurity systems are considered. The publications related to the concept of the mechanism in* *cybersecurity systems were analyzed, on the basis of which an ontological model was built, which can be considered as a carrier of knowledge about the corresponding subject area. Particular attention is paid to the analysis and development of algorithmic mechanisms used in auction theory, as well as applications based on the use of both the classical theory of games and the theory of dynamic games. Analysis of the model made it possible to track the main directions of development using a mechanism to ensure the protection of critical infrastructure. The system of characteristics and structural elements of mechanisms in the socio-economic and political contexts of the use of cyber defense mechanisms is presented, which was not previously presented in the literature on information security and cyber defense. Given this, it is proposed to consider the decision-making mechanism in cybersecurity systems as a system of relations and interactions of various (individual, group, organizational) agents, whose interaction is aimed at solving the security problem. It is indicated that a particular variant of this approach is the decision-making mechanism. The conditions are presented under which the cybersecurity system acquires pronounced features of socio-economic and political systems, which emphasizes the legitimacy of the approach proposed by the authors.*

Keywords: *mechanism, cyber security, ontology, mechanism design, auction, game theory.*

Introduction

The concept of "mechanism" is quite widely used lately in a context that is far from mechanics. Certain aspects of the analysis and synthesis of mechanisms to ensure cybersecurity are discussed in sufficient detail in the literature. However, in most works, the forms, methods, controls for specific conditions and levels of management are considered without specifying what the authors understand by the term "mechanism". Moreover, analysis of processes and decision-making systems should lead us to clarify the meaning that we put into the concept of a mechanism for making management decisions. The need for this (in the framework of second order cybernetics) is determined by the following reasons:

– the role of the decision maker in cybersecurity systems is increasing, that is associated with an increase in the variety of attacks on objects of critical infrastructure;

– the activity of the object under control becomes decisive, which makes it difficult to apply the methods of the classical theory of control.

It follows from this that the concept of a decision-making mechanism should reflect not only the psychological characteristics of the decision-maker, but also the social aspects of security, as well as the consequences of the decisions made [1, 2].

Therefore, the main purpose of the article is to attempt to formulate a definition of the mechanism that is directly related to ensuring the cybersecurity of critical infrastructures, as well as to present the characteristics and features of the mechanisms reflecting the socio-psychological aspects of the cybersecurity systems.

The concept of "mechanism" was originally proposed in the technical field, and only then was borrowed by the humanities and is now widely used not only in psychology and sociology, but also in economics, management, decision theory [3, 4].

The definition of the term "mechanism" usually begins with a reference to mechanics, where this term first appeared [5, 6, 7]. The encyclopedia [8] defines the mechanism as a set of bodies limiting the movement of each other by mutual resistance. In this case, such a characteristic is noted as the limitation of the number of degrees of freedom - the minimum number of its points, whose kinematic characteristics (trajectories and speeds of motion) uniquely determine the trajectories and speeds of all other points of the mechanism. As a motion transducer, the mechanism modifies speeds, or trajectories, or both. Such a generalized definition represents the mechanism of a phenomenon as a process, system, or tool (cross out) for solving certain problems.

Using the phase plane as a display space for any changes, including technical and economic system, which is a cybersecurity system, its behavior can be described in terms of coordinates and their rate of change [9]. Therefore, even with such a cybernetic approach, the mechanism for implementing a certain process can be defined as a set of rules and constraints determining the dynamic characteristics of the system (the trajectories of the system and the rate of change of variables that describe the state of the system) [10, 11]. The mechanism for implementing any process thus defined modifies (shapes) both trajectories and speeds (or both), determining the effectiveness of achieving the target state and the characteristics of management decisions made to implement the appropriate cybersecurity level management [12]. At the same time, it is possible to talk about decision-making mechanisms about goals (the goal setting mechanism) and decision-making mechanisms about actions (mechanisms of regulation, program management, stabilization depending on the tasks of management) [13-16].

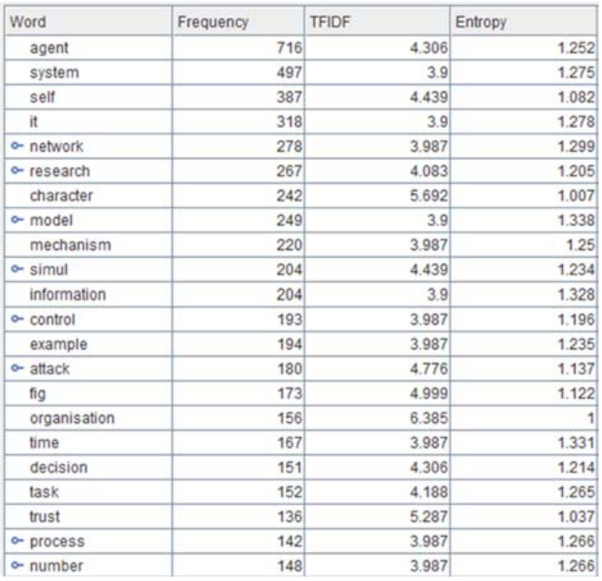
Unfortunately, despite the quite active use of this term, its exact and detailed definition is not always given in disciplines that are not related to mechanics. This causes not only its incorrect use, but also ambiguous interpretation, and, as a result, misunderstanding related to the mixing of concepts of mechanism and model.

Research results

To analyze the use of the concept of "mechanism" in cybersecurity systems, an ontology of the field of research related to the design and use of security mechanisms was built [16]. As a base for building ontology, articles related to cybersecurity were used in the title of which the term "mechanism" was encountered (the main ones are referenced in the list of references). As an instrumental approach, we have used one involving the extraction of basic concepts, the relations between them and the construction of ontology from natural language texts (articles, reports, monographs). Today, this approach is quite common for the formal presentation of subject areas.

As a result of the text processing of articles from scientific journals, a list of basic concepts was originally received. Figure 1 shows the results of the work of the TextToOnto program [18, 19] on the extraction of concepts, which are ordered by the frequency of occurrence in the totality of the presented sources forming the lexicon (corpus) of the subject area. An analysis of the data obtained shows that the term "mechanism" is not the most used in the texts of articles, although it is in the title of the article. Moreover, in most articles this term is not even included on the list of keywords. Moreover, the word "model" is used even more often than "mechanism", and they are replaced each other and are used interchangeably. It should also be noted that the most repeated word in the articles of the relevant subject is "agent". This most likely indicates that the authors of scientific articles associate the implementation and functioning of mechanisms in cybersecurity systems with agent-based modeling, which share cybersecurity mechanisms with socio-psychological characteristics that distinguish this type of simulation from the rest (the character term, emerging in articles in the context of personality traits, indirectly confirms this assumption).

The emergence of the concept of "mechanism" in the constructed ontological model is also interesting one (Fig. 2). It appears in the combination of "designing mechanisms", with the leading term "designing". The basic articles on the development of algorithmic mechanisms (AMD) are [20, 21]. In these articles, a formal model of centralized computing was proposed, in which the stimulating part "development of the mechanism" was combined with the computational capability for processing (the "algorithmic" part). The articles [22, 23] present an extension of the mentioned model to the level of a distributed algorithmic mechanism (DAMD), in which there are the same goals, but, in addition, the agents, the corresponding information and the computational model are distributed in nature.



Word	Frequency	TFIDF	Entropy
agent	716	4.306	1.252
system	497	3.9	1.275
self	387	4.439	1.082
it	318	3.9	1.278
⊸ network	278	3.987	1.299
⊸ research	267	4.083	1.205
character	242	5.692	1.007
⊸ model	249	3.9	1.338
mechanism	220	3.987	1.25
⊸ simul	204	4.439	1.234
information	204	3.9	1.328
⊸ control	193	3.987	1.196
example	194	3.987	1.235
⊸ attack	180	4.776	1.137
fig	173	4.999	1.122
organisation	156	6.385	1
time	167	3.987	1.331
decision	151	4.306	1.214
task	152	4.188	1.265
trust	136	5.287	1.037
⊸ process	142	3.987	1.266
⊸ number	148	3.987	1.266

Fig. 1. List of concepts that form the ontology of "cybersecurity mechanism"

Till now, the work on the design of distributed algorithmic mechanisms (DAMD) has focused on the "truthful" mechanisms. The general approach, which is consistent with the approach in the economic literature, is to develop mechanisms that are compatible with incentives in the technical sense in the sense that strategic agents cannot improve their well-being by providing false information about their personal involvement. The prerequisite for this approach is that agents voluntarily disclose their personal information if a lie does not benefit from them.

Another feature of the constructed ontological model is also interesting. If we talk about the theoretical basis of the design and use of mechanisms, the theory in ontology appears only as a game theory. This may indicate a certain point of view of the authors of articles that use the mechanism in the context of the game strategy.

In essence, game theory is the study of what happens when independent agents act selfishly. The design engine asks how systems can be designed so that the selfish behavior of agents leads to the desired system-wide goals. The "mechanisms" in this area are output specifications and payments to agents that encourage them to behave in such a way as to produce the desired system-wide result [24].

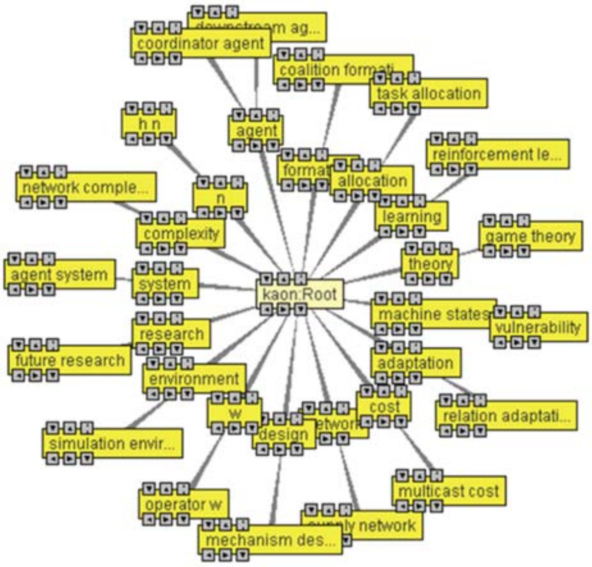


Fig. 2. The ontological model of "cybersecurity mechanism"

Attention should be paid to one more branch of the ontological model obtained, namely "coordination". There are several coordination mechanisms in the current literature, the most popular of which are an auction and a network of contracts. These mechanisms allow agents to allocate resources and tasks to achieve their goals.

One of the reasons why an auction has become so popular is that it is an extremely simple interaction scenario, and therefore it is easy to automate. The auction mechanism includes a group of agents, where one agent plays the role of an auctioneer, and the remaining agents are bidders [25]. The classic scenario assumes that the auctioneer wants to sell the item at the highest possible price, while the Bidders want to buy at the lowest price.

Formal auction models are presented in [26]. Auction and contract networks are presented as coordination mechanisms in multi-agent systems based on FIPA (Foundation for Intelligent Physical Agents) protocols. Mathematical equations are presented that describe various parameters characterizing the mechanisms of the auction and the network of contracts; they allow you to define the general structure of each mechanism, and groups of agents can create several copies of them to coordinate their needs.

In [27], an approach was proposed to increase the productivity of agents using real-time auction mechanisms, based on the idea of setting tasks; here the agent may receive a large fine if he is not assigned to the task. On the other hand, in [28], a mechanism was developed based on market and trading strategies for intelligent networks, in particular, using continuous double auction.

Negotiations are necessary to reach agreements between agents. In this case, agents do not have common goals, therefore negotiation mechanisms are necessary to achieve their goals. A framework for developing and analyzing auction-based coordination mechanisms for cooperation between agents is presented in [29].

The mechanisms of auction and contractual networks have been used in many computer science applications, which include the distribution of goods, tasks and resources. Formalization of these mechanisms using mathematical models allows us to represent them in different forms (English auction, Dutch auction, etc.). This is important because we can generalize the description of these protocols, it is very important when it is required to optimize their use in this context. Study cases allow you to test both models. In addition, models can describe specific cases of coordination mechanisms, we can easily characterize the scenarios in which they want to be used. These formal models of auctions and contractual networks pursue the goal of proposing an optimization model for agent community coordination schemes, which is a multi-agent learning mechanism that supports the evolution of a multi-agent system.

An interesting combination of a conceptual approach to the design of security mechanisms and their practical use in the form of the security model of the Android system is presented in [30, 31, 32]. In these works, the concept of a reference monitor (reference monitor), first introduced in [33], is used. This concept defines the project requirements for the implementation of the so-called link checking mechanism, which should ensure that the system can be used to control access to the system. To ensure the proper operation of this mechanism, three design requirements are set: i) a link verification mechanism (full mediation) must always be activated; ii) a verification and protection mechanism against unauthorized access; and iii) the validation mechanism should be small enough to be analyzed and tested.

Android provides two mechanisms by which an application can delegate its own authority to another application. The developed Android security model is formalized as an abstract finite-state machine (another concept in the constructed ontological model).

The behavior of the security mechanisms during the execution of a session of the device is represented by a sequence of system states (a trace of execution), resulting from the execution of a sequence of actions starting in the (initial) state of the system.

This article describes the problems that arise when trying to apply formal methods to analyze and verify the security mechanisms defined by Android to ensure compliance with access control policies based on permissions. The idealized model developed by the authors allows a logical inference to provide certified guarantees that the stated access control policy is effectively provided by these mechanisms. It is also shown that, in the presence of vulnerabilities, it is possible to use a model to formally define and confirm the conditions that must be met in order to mitigate or even prevent the exploitation of these vulnerabilities.

The constructed ontological model lacks concepts related to the social and political aspects of cybersecurity. Among the publications reflecting this aspect of the problem, we can single out an article representing the consequences of a fall in trust in the company as a result of breach of confidentiality of customer data [34, 35]. However, the mentioned article is an exception rather than a rule for publications dealing with information security issues.

Trying to fill this gap in research, the authors propose their own vision of the characteristics and structural elements of security mechanisms, reflecting the socio-political features of the mechanisms.

Since decision-making processes are directly related to human mental activity, the question of decision-making mechanisms has been particularly intensively studied in psychology. And the result of the mental activity of a manager in management literature is increasingly considered from the point of view of its intellectual content. A brief formulation of this approach can be expressed by the formula "Managerial decision – choice of manager". The proposed formula should be changed and the adoption of a management decision as an activity of an individual, empowered for this purpose, in the conditions of the functioning of the system-organization.

Due to the fact that management decision-making in the field of cybersecurity is a social process, decision-making mechanisms can be considered as a particular type of social mechanisms with specific characteristics. Sociologists understand social mechanisms as "specific social systems, the functioning of which generates certain social changes in the sphere of economics, politics, population reproduction". There are a number of common features of social mechanisms, analyzing which you can understand and formalize the structure of the decision-making mechanism in the field of cybersecurity (Table 1). The formalization of the structure of the decision-making mechanism can be obtained by analyzing the general features of social mechanisms.

Thus, the cybersecurity mechanism should be considered as an integral system of relations between social subjects regarding the regulation of not only information, but also social processes, overcoming dysfunctions of social institutions, etc., taking into account the motivational, cultural, regulatory and value conditions of life and activities of these subjects.

The decision-making mechanism in the organization is a private variant of management mechanisms. The management literature often contains descriptions of specific management mechanisms in any areas, business sectors, or "technologies" of decision-making in specific management situations. In some works, there is an attempt to analyze the essence, structure, and the role of organizational mechanisms in the functioning and development of the organization. In particular, the "organizational-economic mechanism" of the enterprise's functioning is considered as a purposeful process of solving particular tasks of its operation based on a stable set of methods, norms and rules of forming and regulating relations between the elements of an organizational structure.

Table 1

General characteristics of social mechanisms

	Characteristic	Description
1	Functional role	Regulation of social processes in accordance with public needs – the acceleration of some, the containment or overcoming of others.
2	Subjects	Certain social groups, depending on the type of mechanism, form specific systems based on the exchange of the results of any activity. These subjects can be represented by social institutions (for example, the state represented by regional authorities), individual organizations, representatives of various social groups (for example, employees of organizations) and others.
3	The foundation	Social institutions that act as an established regulatory framework that defines and supports the necessary forms of social behavior, in particular, through a network of formal organizations.
4	Composition	Material and spiritual values are phenomena of social being and social consciousness.
5	Character	Systemic, as indicated by the nature of the internal links between the elements of the mechanism and the nature of the functional links of the mechanism itself with the external social environment.

Under the conditions of cyber-terrorism, decisions are made politically motivated. Therefore, it is logical to draw an analogy between decision-making mechanisms for ensuring information security and political decision-making mechanisms. The concept of a political decision-making mechanism is considered either as a certain institution within the framework of the production of any (political, managerial, economic, etc.) activities, consisting of components of different quality (social groups, communication systems, information systems, normative components, etc.), or – as local "procedures" of interaction, "activities", in turn, consisting of a series of specific operations aimed at achieving the goal. In the political context, the mechanism is considered as a multi-level system consisting of a social-goal-oriented, orientation-regulatory, and organizational-instrumental subcomplexes. The proposed definition should reflect the strengths of various methodological approaches to the study of decision making; reflect the participation of decision-making agents of all levels – individual, group, organizational; take into account formal and informal, rational and irrational decision-making factors; take into account the instrumental component of decision making – ways to achieve the goal, including organizational forms and procedures, methods and resources, types of interactions and communications between agents.

Political decisions are also managerial; therefore, turning to an analysis of their mechanisms allows us to concretize the process of making management decisions in economic organizations.

So, the "decision-making mechanism" is interpreted in quite a variety of ways: both as elementary information processes and complex thinking programs, as a process of regular change of any system states, and as an internal connection and interdependence of system elements, and as individual specific social systems. The analysis of various existing approaches leads to the conclusion that as a mechanism for making management decisions one should consider the system of relations and interactions of various (individual, group, actually organizational) agents with the aim of solving a problem. In this case, the head acts as a person authorized to make the

The structure of the management decision-making mechanism is presented in Table 2.

Table 2

Structural elements of the mechanism

№	Element	Characteristic
1	Subjects and actors of decision making	- decision maker; - the owner of the problem; - members of the active group; - voters or group member; - expert; - decision-making consultant.
2	Problem-target component	The problem facing the decision maker and the purpose of its resolution.
3	Regulatory component	Regulatory conditions: - subjective (motives, values, installations of decision makers); - objective (norms, rules of the social environment, the expectations of the team).
4	Process Interactive Component	Stages of managerial decision-making, represented by operations and actions of agents, schemes of their interaction in time.
5	Instrumental component	Individual and group methods, technologies, methods of making management decisions.

According to the degree of combination of individual and group participation in decision-making, we can distinguish levels of managerial decision-making. Combining elements with different characteristics leads to different mechanisms, allowing for a collegial discussion of the problem (Table 3).

Table 3

Examples of management decision-making mechanisms

№	Mechanism	Characteristic
1	formalized	standard, "programmed" (i.e. having a clear sequence of actions), repetitive decisions are made with the help of streamlined organizational procedures prescribed in the established regulatory acts.
2	democratic	whenever possible, all interested people are involved in the decision making, the opinion of both the subjects and the addressees of the decision made is taken into account. In this regard, different instrumental methods of coordination and decision-making are used.
3	eliminative	delegation of responsibility for the preparation and partial decision making on subordinates, prevention and prevention of "difficult" choice situations, minimizing the number of choice situations, etc.

Conclusion

The review allows us to conclude that cybersecurity decision-making mechanisms are a complex system of interactions of various organizational agents, aimed at achieving specific goals and performing a number of obvious and specific security functions within existing rules, norms and restrictions in organizations. Most of the works represent specific developments of models, technologies, rules. At the same time, there is no uniform classification of the mechanisms used and being developed, and the concept itself is used as a synonym for the model, the system of rules, and technology. The paper analyzes publications related to the concept of the mechanism in cyber security systems. Based on the analyzed publications. An ontological model was constructed, which is the carrier of knowledge about the relevant subject area. Analysis of the model made it possible to track the main directions of development by the mechanism for ensuring the protection of critical infrastructure facilities. The authors presented a system of characteristics and structural elements of mechanisms in the socio-economic and political contexts of the use of cyber defense mechanisms, which previously was practically not presented in the literature on information security and cyber defense. With this in mind, the authors proposed to consider the decision-making mechanism in cybersecurity systems as a system of relations and interactions of various (individual, group, organizational) agents, the interaction of which is aimed at solving the security problem.

References

[1]. Р. Грищук, Ю. Даник, *Основи кібернетичної безпеки : Монографія,* за заг. ред. проф. Ю. Г. Даника, Житомир : ЖНАЕУ, 2016, 636 с.

[2]. A. Milov, "Mehanizmy prinyatiya upravlencheskih resheniy: problemi konceptualizacii", *Upravlinnya rozvitkom*, № 17, pp. 119-122, 2008.

[3]. P. Hedström, P. Ylikoski, "Causal mechanisms in the social sciences", *Annual Review of Sociology* 36, pp. 49-67, 2010.

[4]. P. Machamer, L. Darden, C. Craver, "Thinking about mechanisms", *Philosophy of Science 67*, pp. 1-25, 2000.

[5]. N. Sclater N. Chironis, *Mechanisms and Mechanical Devices Sourcebook,* New York : McGraw-Hill New York, 2007, 551 p.

[6]. *New Oxford American Dictionary*, Oxford University Press, 2010, 2096 p.

[7]. *The Merriam-Webster Dictionary*, Merriam-Webster, Inc. 2016, 960 p.

[8]. D. Subbu, *Encyclopedia of Mechanical Engineering,* London : SBS Publishers, 2007, 393 p.

[9]. A. Milov, S. Milevsky, "Formalizaciya mechanizmov koordinacii resheniy v korporativnih structurah", *Bisnes-Inform*, № 2(2), pp. 129-132, 2009.

[10]. A. Milov, "Planirovanie v pronstranstve situaciy", *Modeli upravleniya v rinochnoy ekonomike. Sbornik nauchnih trudov; Donetskiy nacionalniy universitet.* – Donetsk: DonNU, Vol. 4, pp. 165-172, 2000.

[11]. A. Milov, "Planirovanie resheniy v prostranstve palach", *Modeli upravleniya v rinochnoy ekonomike Sbornik nauchnih trudov; Donetskiy nacionalniy universitet*, Donetsk: DonNU, 2002.

[12]. A. Milov, S. Milevsky, "Corporative Decision-Making Multiagent Models", *Економіка розвитку*, № 3(79), С. 79-84, 2016.

[13]. "Lingvisticheskie struktury mnogourovnevih system podderdzky reshenie", *Trudy Kaluzkogo filial MGTU im. N. E. Baumana Materialy mezdunarodnoy nauchno-practicheskoy konferencii «Priborostroenie-99»,* Kaluga, 1999.

[14]. A. Milov, "Informacionnaya model prinyatiya reseniq", *Economika rozvitku*, № 4(28), 2003.

[15]. A. Milov, "Model gruppy lits, prinimayuchih resheniya", *Ekonomika rozvitku*, № 1(29), 2004.

[16]. A. Milov, O. Zaharova, "Modeli korporativnogo planirovaniya v IT-autsotsinge", *Radioelectronics and Informatics*, KhTURE, № 1, pp. 116-118, 2013.

[17]. Fong-Hao Liu, Wei-Tsong Lee, "Constructing Enterprise Information Net-work Security Risk Management Mechanism by Ontology", *Tamkang Journal of Science and Engineering*, Vol. 13, No. 1, pp. 79-87, 2010.

[18]. A. Maedche, S. Staab, "Discovering conceptual relations from text", In W. Horn (ed.): *ECAI 2000 Proceedings of the 14th European Conference on Artificial Intelligence*, IOS Press, Amsterdam, 2000.

[19]. A. Maedche, S. Staab, "Semi-automatic engineering of ontologies from text", *In Proceedings of the 12th Internal Conference on Software and Knowledge Engineering, Chicago, USA, July, 5-7, 2000*, KSI, 2000.

[20]. N. Nisan, "Algorithms for Selfish Agents", *in Proceedings of the Symposi-um on Theoretical Aspects of Computer Science, LNCS 1563*, Springer, Berlin, pp. 1-17, 1999.

[21]. N. Nisan, A. Ronen, "Algorithmic mechanism design", *Games and Economic Behavior 35,* pp. 166-196, 2001.

[22]. J. Feigenbaum, C. Papadimitriou, R. Sami, S. Shenker. "ABGP-based Mechanism for Lowest-Cost Routing", *in Proceedings of the 2002 ACM Symposium on Principles of Distributed Computing.*

[23]. D. Akinwumi, G. Iwasokun, B. Alese, S. Oluwadare, "A review of game theory approach to cyber security risk management", *Nigerian Journal of Technology (NIJOTECH),* Vol. 36, No. 4, pp. 1271-1285, 2017.

[24]. Р. Грищук, *Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень: Монографія*, Житомир : Рута, 2010, 280 с.

[25]. M. Wooldridge, "An Introduction to Multi Agent Systems", *Department of Computer Science*, University of Liverpool, WILEY & SON, LTD, Copy-right 2002.

[26]. J. Teran, J.L. Aguilar, M. Cerrada. "Mathematical Models of Coordination Mechanisms in Multi-Agent Systems", *CLEI Electronic Journal*, Vol. 16, No. 2, pp. 5, 2013

[27]. S. Koenig, X. Zheng, C. Tovey, R. Borie, P. Kilby, V. Markakis, P. Keskinocak, "Agent Coordination with Regret Clearing", *In Proceedings of the AAAI Conference on Artificial Intelligence (AAAI),* pp. 101-107, 2008.

[28]. P. Vytelingum, S. Ramchum, T. Voice, A. Rogers, N. Jennings, "Trading agents for the smart electricity grid", *In The Ninth International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2010)*, pp. 897-904, 2010.

[29]. S. Koenig, P. Keskinocak, C. Tovey, "Progress on Agent Coordination with Cooperative Auctions", *Proceedings of the Twenty-Fourth AAAI Con-ference on Artificial Intelligence, Atlanta, Georgia, USA, July 11-15*, 2010.

[30]. G. Betarte, J. Campo, M. Cristiá, F. Gorostiaga, C. Luna, C. Sanz, *Towards formal model-based analysis and testing of Android's security mechanisms*, 2017.

[31]. G. Betarte, J. D. Campo, C. Luna, A. Romano, "Formal analysis of android's permission-based security model", *Sci. Ann. Comp. Sci.*, Vol. 26, No. 1, pp. 27-68, 2016. [Electronic resource]. Available: http://dx.doi.org/10. 7561/SACS. 2016.1.27.

[32]. GSI, "Formal verification of the security model of Android: Coq code". [Electronic resource]. Available: http://www.fing.edu.uy/inco/grupos/gsi/documentos/proyectos/Android6-Coq-model.tar.gz.

[33]. J. P. Anderson, "Computer Security technology planning study", *Deputy for Command and Management System, USA, Tech. Rep.*, 1972. [Electronic resource]. Available: http:// csrc.nist.gov/ publications/ history/ ande72.pdf.

[34]. Whan-Seon Kim, "Effects of a Trust Mechanism on Complex Adaptive Supply Networks: An Agent-Based Social Simulation Study", *Journal of Artificial Societies and Social Simulation,* (3) 4.

[35]. F. Lin, Y. Sung, Y. Lo, "Effects of trust mechanisms on supply-chain performance", *International Journal of Electronic Commerce*, 9(4), pp. 91-112, 2005.

УДК 681.32:007

Милов А., Казакова Н., Мильчарский П., Король О. Механизмы кибербезопасности: проблема концептуализации

Аннотация. *В статье рассмотрены общие подходы, связанные с использованием понятия «механизм» в системе кибербезопасности. Представлено первоначальное определение механизма в системах аналитической динамики. Прослежена трансформация понятия «механизм» от механических систем до экономических, социальных и организационно-технологических. Сформулировано определение механизма, которое может быть использовано при анализе и проектировании систем принятия решений, рассмотрены особенности использования этого понятия в системах кибербезопасности. Проанализированы публикации, связанные с концепцией механизма в системах кибербезопасности, на основании которых была построена онтологическая модель, которую можно рассматривать как носитель знаний о соответствующей предметной области. Особое внимание уделено анализу и разработке алгоритмических механизмов, используемых в теории аукционов, а также приложений, основанных на использовании как классической теории игр, так и теории динамических игр. Анализ модели позволил отследить основные направления развития с помощью механизма обеспечения защиты критически важных объектов инфраструктуры. Представлена система характеристик и структурных элементов механизмов в социально-экономическом и политическом контекстах использования механизмов киберзащиты, которая ранее практически не была представлена в литературе по информационной безопасности и киберзащите. Учитывая это, предложено рассматривать механизм принятия решений в системах кибербезопасности как систему отношений и взаимодействий различных (индивидуальных, групповых, организационных) агентов, взаимодействие которых направлено на решение проблемы обеспечения безопасности. Указано, что частным вариантом такого подхода является механизм принятия решений. Представлены условия, при которых система кибербезопасности приобретает ярко выраженные черты социально-экономических и политических систем, что подчеркивает правомерность предлагаемого авторами подхода.*

Ключевые слова: *механизм, кибербезопасность, онтология, проектирование механизма, аукцион, теория игр.*

Мілов О., Казакова Н., Мільчарський П., Король О. Механізми кібербезпеки: проблема концептуалізації

Анотація. *У статті розглянуто загальні підходи, пов'язані з використанням поняття «механізм» в системі кібербезпеки. Представлено первинне визначення механізму в системах аналітичної динаміки. Простежено трансформацію поняття «механізм» від механічних систем до економічних, соціальних і організаційно-технологічних. Сформульовано визначення механізму, яке може бути використано при аналізі і проектуванні систем прийняття рішень, розглянуті особливості використання цього поняття в системах кібербезпеки. Проаналізовано публікації, пов'язані з концепцією механізму в системах кібербезпеки, на підставі яких була побудована онтологічна модель, яку можна розглядати як носій знань відповідної предметної області. Особливу увагу приділено аналізу та розробки алгоритмічних механізмів, використовуваних в теорії аукціонів, а також додатків, заснованих на використанні як класичної теорії ігор, так і теорії динамічних ігор. Аналіз моделі дозволив відстежити основні напрями розвитку за допомогою механізму забезпечення захисту критично важливих об'єктів інфраструктури. Представлена система характеристик і структурних елементів механізмів в соціально-економічному і політичному контекстах використання механізмів кіберзахисту, яка раніше практично не розглядалась в літературі з інформаційної безпеки і кіберзахисту. З огляду на це, запропоновано розглядати механізм прийняття рішень в системах кібербезпеки як систему відносин різних (індивідуальних, групових, організаційних) агентів, взаємодія яких спрямована на вирішення проблеми забезпечення захисту належного рівня. Зазначено, що одним з варіантів такого підходу є механізм прийняття рішень. Представлені умови, при яких система кібербезпеки набуває яскраво виражені риси соціально-економічних і політичних систем, що підкреслює правомірність запропонованого авторами підходу.*

Ключові слова: *механізм, кібербезпека, онтологія, проектування механізму, аукціон, теорія ігор.*

Отримано *13 липня 2019 року*, затверджено редколегією *26 липня 2019 року*