International Journal of Civil Engineering and Technology (IJCIET)
Volume 9, Issue 11, November 2018, pp. 95–104, Article ID: IJCIET_09_11_009
Available online at http://www.iaeme.com/ijciet/issues.asp?JType=IJCIET&VType=9&IType=10
ISSN Print: 0976-6308 and ISSN Online: 0976-6316

©IAEME Publication **Scopus** Indexed

DEVELOPMENT OF A CONCEPTUAL MODEL OF ADAPTIVE ACCESS RIGHTS MANAGEMENT WITH USING THE APPARATUS OF PETRI NETS

V. Lakhno
Department of Computer systems and networks,
National University of Life and Environmental Sciences of Ukraine, Kiev, Ukraine

V. Buriachok
Head of the Department of Information and Cybersecurity,
B. Grinchenko Kyiv University, Kiev, Ukraine

L. Parkhuts
Professor, Department of Information Security,
Lviv Polytechnic National University, Lviv, Ukraine

H. Tarasova
Associate Professor of the Department,
Kiev National University of Technology and Design, Kiev, Ukraine

L. Kydyralina
Doctoral Candidate,
Kazakh National Pedagogical University named after Abay, Almaty, Kazakhstan

P. Skladannyi
Senior Lecturer of the Department of Information and Cybersecurity,
B. Grinchenko Kyiv University, Kiev, Ukraine

M. Skrypnyk
Doctor of Science (Economics)
Kyiv National University of Technology and Design, Kyiv, Ukraine

A. Shostakovska
Associate Professor of Department of Management and Marketing
European University, Kiev, Ukraine

ABSTRACT

The paper describes the conceptual model of adaptive control of cyber protection of the informatization object (IO). Petri's Networks were used as a mathematical device to solve the problem of adaptive control of user access rights. The simulation model is proposed and the simulation in PIPE v4.3.0 package is performed. The possibility of automating the procedures for adjusting the user profile to minimize or neutralize cyber threats in the objects of informatization is shown. The model of distribution of user tasks in computer networks of IO is proposed. The model, unlike the existing, is based on the mathematical apparatus of Petri's Networks and contains variables that allow reducing the power of the state space. Access control method (ACM) is added. The addenda touched upon aspects of reconciliation of access rights that are requested by the task and requirements of the security policy and the degree of consistency of tasks and access to the IO nodes. Adjustment of rules and security metrics for new tasks or redistributable tasks is described in the notation of Petri nets.

Key words: Cybersecurity, access rights management, security policy, mathematical model, Petri nets, rule adjustment.

Cite this Article: V. Lakhno, V. Buriachok, L. Parkhuts, H. Tarasova, L. Kydyralina, P. Skladannyi, M. Skrypnyk, A. Shostakovska, Development of a Conceptual Model of Adaptive Access Rights Management with Using the Apparatus of Petri Nets, *International Journal of Civil Engineering and Technology (IJCIET)* 9(11), 2018, pp. 95–104.
http://www.iaeme.com/IJCIET/issues.asp?JType=IJCIET&VType=9&IType=11

1. INTRODUCTION

The modern level of application of information technology (IT) and systems (ITS) at various objects of informatization (IO) reached the highest level. At the same time, most specialists in the field of IT note the need for primary tasks to preserve the integrity, confidentiality and accessibility of information, regardless of its functional purpose [1, 2]. Almost annually detection of previously unknown cyber threats (Cth) [3, 4] and a steady trend for the formation of a new landscape Cth for digitalized technologies and systems, make the tasks of information protection (IPr), information security (IS) and cybersecurity (CS) priority in the whole world [1, 2, 5].

Despite the commonness of the tasks for CS for various IO (information-educational environment of the modern university, automated control system for complex production or banking system), has own specifics of cyber threats [1–5]. However, the initial task of creating effective protection systems and CS any IO, remains the task of examining a specific object of protection, modelling of a potential intruder (computer attacker – CA) and cyber threats [1–5]. Implementation of the above steps will provide adequate requirements for information security systems (ISS) IO.

In the context of the increasing complexity of cyber-attack scenarios on IO analysts of information security services (IS) need to respond quickly to cyber-attacks, threat anomalies. It makes the problem actual search for new ways to increase the effectiveness of decision-making in tasks to respond to attempts at destructive intervention by the CA or unscrupulous personnel in the work of IO. In this situation, a significant role can be played by various intellectualized decision support systems (IDSS) and expert systems (ES) in tasks of providing cybersecurity IO [5–7].

We note that the mathematical component of the IDSS and ES in the CS tasks is various models and algorithms that enable specialists to intellectually support solutions.

Within the framework of the research, the possibility of synthesizing analytical models for the main types of unauthorized access to IO. The possibility of describing functional models of various IO in terms of the Petri nets theory [4, 5, 7, 8].

Such a presentation will allow analysts IS and IPr to detail threats in the defended IO. In addition, in the future, it is possible to identify states that potentially determine vulnerabilities IO to new cyber threats. We also consider the prospects of using this model on the basis of Petri (and Petri-Markov) networks and colored Petri nets as mathematical and algorithmic components, which projected IDSS in the process of analyzing cyber threats for various IO. In our opinion, these judgments make our paper relevant and increase the effectiveness of the work on the creation of IDSS in the tasks of IPr and CS for various IO.

2. LITERATURE REVIEW AND PROBLEM POSING

In the papers [3–5, 8, 9] were presented results of research, devoted to the application of Petri nets for the description of the threat model CS IO. Although these works have made an undeniable theoretical contribution to this issue, in our opinion, the models proposed by the authors are somewhat difficult to implement programmatically, especially IDSS and ES of IPr and CS IO.

Based on the papers [3, 5] of the threat model, it is possible to construct using a visual tabular form of displaying threats when updating the question of evaluating IO security. But, this approach to drawing up models of threats is laborious. In addition, the growing number of threats makes such a tabular presentation format difficult to comprehend, especially for specialists with little experience in the field of CS.

Petri nets (and Petri-Markov) were also successfully used to describe intruder models [10, 11]. However, the authors did not consider the possibility of correcting the intruder model (CA), in particular by combining it with models on the basis of graph theory, which would allow more accurately describe state transitions in the process of probable overcoming of CA perimeters (boundaries) of cyber protection for a particular object OI.

In the papers [3, 8, 9] models ISS for various IO were considered as preliminary allocated in Petri nets sequences of elementary operations, from which cyber-attack is possible. The models allowed calculating the possibility of implementing different attacks for a certain period of time. However, the models considered in [9, 10] did not allow us to calculate the time characteristics in the process of implementing new cyber threats.

In the papers [5, 12], models based on Petri nets were proposed and described the processes of implementing threats in information systems (IS). Although these models made it possible to evaluate many of the security parameters IO, in particular, the likelihood of the implementation of threats, the time to implement threats, the coherence of CA actions, they are not fully completed. In these papers, the issue of resolving conflict situations arising when IS states change during attacks has not been studied, belonging to different classes. This circumstance, in our opinion, limits the practical applicability of this research.

Thus, the synthesis of new models, as well as the addition of existing models and methods of adaptive cyber defense management of various IO with using of the capabilities of the apparatus of Petri nets and taking into account the potential of visualization of Petri nets, can become an effective tool for forecasting the state of security for particular IO. This will significantly simplify the understanding for new cyber threats and in the future possible the effective application of the proposed approaches by service analysts IPr, IS and CS of various IO.

3. GOAL AND OBJECTIVES OF THE STUDY

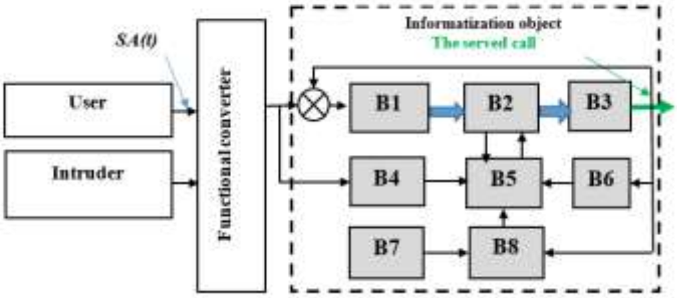
The goal is the development of models and methods that contribute to increasing the stability of the functioning of computer networks of various information objects on the basis of adaptive management of cybersecurity mechanisms in conditions of increasing the number and complexity of destructive unauthorized impact.

To achieve the goal of the research, the following tasks are solved:

Conceptual model of adaptive management of cyber protection of the information object (IO) using the apparatus of Petri nets; models of distribution of user tasks in computer networks of information objects (IO); Additions to the Access Control Method in the Context of Reconciliation of Access Rights that are Requested by the Task and the Requirements of the Security Policy and the Degree of Consistency of the Task and Access Permitted Nodes IO.

4. MODELS AND METHODS

In accordance with the purposes of our research, this section of the article describes a conceptual model of adaptive cyber protection management IO.



Accepted designations: B1 - block information and measuring devices of OBI; B2 - block of multichannel control devices; B3 - OBI as object of access control to resources; B4 - state prediction unit in OBI; B5 - decision block on the right of access; B6 - the block of calculation of efficiency by quantity of the realized threats connected with infringement of access in OBI; B7 - block of a priori information; B8 - block of variable models.

Figure 1 Scheme of the conceptual model of adaptive control of cyber protection of the information object.

An example of a solution of the problem adaptive management of user access rights using apparatus of Petri nets and related software, which allows you to automate the adjustment of the user profile, and also through the integration of IDSS module to recommend ways to neutralize cyber threats in IO.

We formulated the tasks of managing access rights: 1) the model of access delimitation for a given IO is constructed; 2) determine the model parameters that are controlled; 3) parameterization of the risk of breach of confidentiality of information for IO to perform.

A formal mathematical statement of the problem of optimizing the scheme of access delimitation in IO. Initial data: 1) access objects of IO $-AO = \{ao_i\}, i = \overline{1, I}$; 2) subjects of access in IO – $SA = \{sa_j\}, j = \overline{1, J}$; 3) communication nodes (CN) in IO – $CN = \{cn_k\}, k = \overline{1, K}$; 4) an adaptive mechanism that responds allows you to maintain access security metrics in the IO at a given level $- AM^0 = \{am^0_{i,j}\}, i = \overline{1, I},\ j = \overline{1, J}$.

Suppose that an acceptable level of protection IO is achieved if the conditions are met, as shown in Table 1.

Table 1 The conditions under which an acceptable level of protection is achieved IO *(for setting optimization of access control of IO)* [with considering 8, 9, 12]

No	Parameter	Condition
1	An adaptive mechanism that allows you to maintain access security metrics in IO at a given level [5, 9].	$am_{i,j} = \begin{cases} 1, \text{if } am_i \text{ it is placed on} \\ \text{a node } cm_k; \\ 0, \text{Otherwise.} \end{cases}$
2	Damage from possible unauthorized access to resources – $DA^0 = \{da^0_{i,j}\},\ i = \overline{1,I},\ \ j = \overline{1,J}$ [8, 12].	See note.
3	The structure of the computer network IO – $NS = \{ns_{m,n}\},\ m,n = \overline{1,K}$	$ns_{m,n} = \begin{cases} 1, \text{if } (cn_m \in NS_o) \& (cn_n \in NS_o); \\ 0, \text{Otherwise.} \end{cases}$ $where \quad NS_o$ – Network objects.
Managed Parameters (are set by the administrator IP and CS)		
1	Symptoms of sharing resources IO – $SV = \{sv_i\}$ [6, 9].	$sv_i = \begin{cases} 1, \text{if the general access to} \\ \text{a node } sv_i \text{ is allowed}; \\ 0, \text{Otherwise.} \end{cases}$
2	Accommodation AO on nodes IO – $MP^1 = [mp^1_{i,k}]$	$mp^1_{i,k} = \begin{cases} 1, \text{if } ao_i \in cn_k; \\ 0, \text{Otherwise.} \end{cases}$
3	Accommodation SA on nodes IO –$MP^2 = [mp^2_{j,k}]$.	$mp^2_{j,k} = \begin{cases} 1, \text{if } sa_j \in cn_k; \\ 0, \text{Otherwise.} \end{cases}$
Note: The damage from the probable unauthorized access to resources (line 2) determines the degree of information resources on the IO node, and the user profile (taking into account the characteristics of probable intruders, look at Table 2).		

The conditions under which an acceptable level of protection is achieved IO (to specify the optimization of access control for IO) is subsequently considered in conjunction with the data in Table 2. We will assume that the objective function is the magnitude of the likely expected damage from unauthorized access to information resources (IR) IO (further IR and IO). This parameter is defined as a measure of the discrepancy between the real and optimal delineation of user access to IR for a particular IO.

$$TF = \sum_{i=1}^{I}\sum_{j=1}^{J} da^0_{i,j} \cdot \left| am_{i,j} - am^0_{i,j} \right|, \tag{1}$$

where $\{am_{i,j}\}$– elements of a set that displays already implemented access rights.

Then

$$am_{i,j} = \sum_{k=1}^{K} ns_{i,k} \cdot w^0_{k,j}; \tag{2}$$

$$w^0_{k,j} = w^1_{k,j} + sv_i \cdot \left(1 - w^1_{k,j}\right); \tag{3}$$

$$w^1_{k,j} = \sum_{k=1}^{K} \left(mp^2_{i,k} \cdot mp^1_{k,j}\right). \tag{4}$$

Table 2 Characteristics of potential intruders [9, 10, 13]

Classification	**Characteristic**
For reasons of violation	Violation of integrity, confidentiality, accessibility with mercenary or other purpose.
According to the level of awareness and qualification of CA	Intruder (or CA): 1) a high level of knowledge; 2) sufficient knowledge to gather information, use of known exploits and write your own software for cyber attacking; 3) CA is not an authorized user of IO.
By location	Without physical access to the IO territory. The intruder acts remotely, for example, through public networks.

Thus, the formulation of the task of differentiating access rights was obtained. This problem relates to the tasks of non-linear optimization of the vector of controllable parameters in Boolean variables:

$$UD = \min \sum_{i-1}^{I} \sum_{j=1}^{J} da^{0}_{i,j} \cdot \left| am_{i,j} - am^{0}_{i,j} \right| \tag{5}$$

for the following restrictions

$$\sum_{k-1}^{K} da^{1}_{i,j} \le 1 \tag{6}$$

$$\sum_{k-1}^{K} da^{2}_{i,j} \le 1. \tag{7}$$

Constant adjustment of the profile of the active user assumed the use of a special iterative algorithm [14]. This algorithm based on the implicit server feedback with the user specific IO resources. The key factor is the query statistics. The evaluation of the current user profile was used to rank users into groups by the degree of danger for IR and IO. Accepted: a) user; b) a potentially dangerous user; c) dangerous user; d) the intruder.

Optimization of access control procedures was carried out on the basis of the definition of such parameters: 1) Intensity of transitions (determined on the basis of regression models) [14]; 2) Parameterization of the risk associated with violation of confidentiality of information IO. It is defined as a multifactorial regression model of the 2-nd order [15]:

$$P_r(\tau) = da_0 + \sum_{k=1}^{m} da_k \cdot h_k + \sum_{ao=1}^{m} da_{ao,ao} \cdot h^2_{ao} + \sum_{i,j=1}^{m} da_{i,j} \cdot h_i \cdot h_j, \; i \ne j,$$

where $h = (h_1,\ldots,h_m)^T -$ managed parameters that regulate the rules of delineating access in networks of specific IO: $\tau -$ time.

With respect to any IO with a distributed resource access scheme, the subscriber task model is defined as follows

$$\sum = (PN, PIS, AT, s_0, FTR, MRT, RES), \tag{8}$$

where $PN = (TGR, T, MPN, F) -$ IR and IO (are represented by the Petri nets); $TGR = \{tgr\} -$ set of vertices graph (top - supplier IR and IO); $T = \{t\} -$ number of transitions between vertices; $MPN = (mpn_1,\ldots,mpn_n) -$ Petri nets marking; $F -$ neighbor ratio; $PIS -$ information security policy; $AT -$ active tasks initiated by users IR IO; $s_0 -$ initial state $S = \{s\}$; $FTR : PN \times AT \times MRT \times PIS \times A \to S -$ transition function between states IR OI; $MRT = \langle CL, U \rangle -$ markers in Petri nets, $CL -$ class of resources that subscribers (users) request (*U*); $RES -$ current position in the access rights to IR in IO.

Taking into account the previous calculations, such rules were obtained for the software product "Threat Analyzer" (described in detail [14]) to make a decision on the possibility of the user's access to the IR:

subscriber *U* (user IR and IO) authorized access to IR owner *OWR*, if the mutual authentication procedure is correct. For the owner IR *OWR* a local account is defined. In this case, this entry shows all subscribers and their access type in accordance with the security program:

$$Has\,COMP\;Ass\,Ri\left(U,OWR,PIS\right)=\begin{pmatrix}Is\,TRU\;\;By\,U\left(U,OWR\right)\wedge Is\,TRU\;\;By\,TGR\left(OWR,U\right)\wedge\\ \left(MapU\;To\,UD\left(OWR,U\right)\neq 0\right)\end{pmatrix}\wedge \qquad (9)$$
$$Is\,Acc\;\;AL\;By\;PIS\left(U,OWR,PIS\right),$$

and in relation to IR IO, local accounts on the nodes, which subscribers are displayed, must also have the right of access – *RI* to the object *Ob*:

$$Has\;FC\;\;Ass\;Ri\left(U,OWR,PIS,Ob,RI\right)=\begin{pmatrix}Is\,TRU\;\;By\,U\left(U,OWR\right)\wedge\\ \wedge\;Is\,TRU\;\;By\,TGR\left(OWR,U\right)\wedge\\ \left(ListU=MapU\;To\,UD\left(OWR,U\right)\neq 0\right)\end{pmatrix}\wedge \qquad (10)$$
$$Is\;Acc\;\;AL\;\;By\;\;PIS\left(U,OWR,PIS\right),$$

where: Acc – access; RI – right of access to IR; AL – allowed; TRU – is reliable; $MapU$ – subscriber/user card; $ListU$ – local subscriber account; $MapU\;To\;UD$ – function, which displays a lot of users IR in IO in the format of local owner accounts IR – *OWR*.

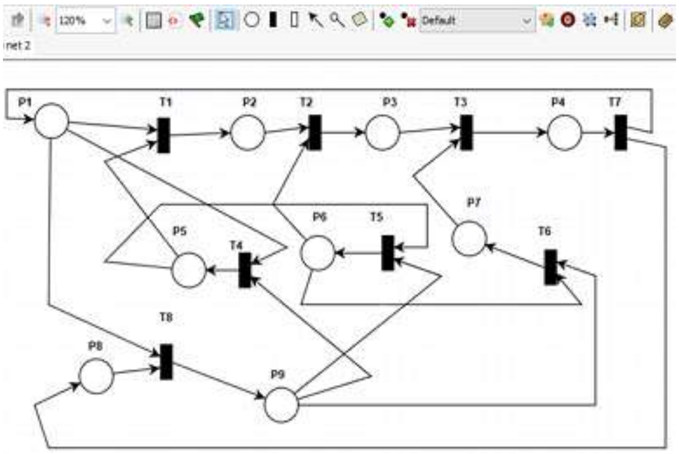
Taking into account the papers [5, 9, 12, 13] refinements to the method control and access management (CAM) were proposed, taking into account the specifics of the network IO. Refined and supplemented method CAM is to reconcile access rights, which are requested by the task and requirements of the security policy, and in addition, the coordination of the task and access-authorized nodes IO. For IO nodes, there is also a procedure for reconciling access rights for all subscribers who have the appropriate rights. As a result, a lot of nodes will be received, at which subscriber tasks are allowed to be performed. This takes into account the current security policy indicators for a specific IO and security metrics. It is possible to adjust the rules for new tasks or redistributed tasks. This, adjustment or redistribution of tasks can be described in the notation of Petri nets and taking into account the mathematical model, which is described by expressions (8) – (10).

5. SIMULATION EXPERIMENT

Based on the above reasoning, on the basis of modified Petri nets (MPN) the model for adaptive role-based access control to resources was developed IO (Access Control System – ACS). And simulation modelling was performed in the package PIPE v4.3.0 (Platform Independent Petri nets Editor). This approach allowed us to correctly describe conflict situations, in addition, the peculiarity of processing requests that arise on most IS IO in the multi-user mode. Figure 2. the scheme of the simulation model is presented. The diagram shows the logical structure of the operating system model of the access rights (for the variant of three-stage control). Positions and transitions in the network model based on MPN are shown in Table 3.

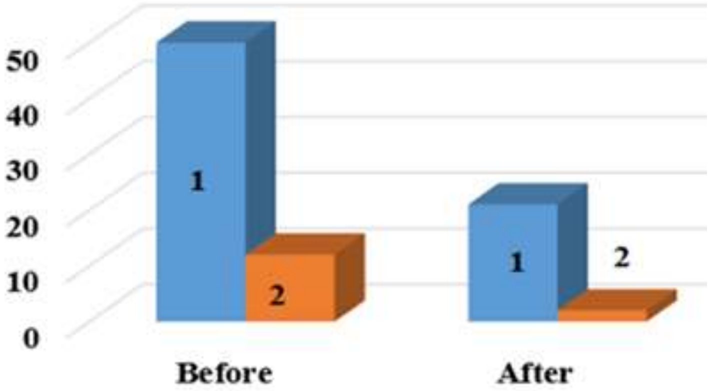
During researches have been performed to evaluate the effectiveness of the proposed models and refinements to the method of monitoring access rights. To evaluate the effectiveness of the proposed solutions, an indicator was used that characterizes the reduction of time spent on decision-making. Accordingly, the estimated time spent on processing data before and after application, models and method, which proposed. The simulation experiment was carried out for 400 computational nodes.

Table 3 Positions and transitions in the network model of the system with access rights in the basis of modernized Petri nets

<table>
<tr><td rowspan="14">

120%
Default
net 2
P1
T1
P2
T2
P3
T3
P4
T7
P5
T4
P6
T5
P7
T6
T8
P8
P9

Figure 2. Scheme of the simulation model of adaptive access rights management taking into account role regulation</td><th colspan="2">Positions</th></tr>
<tr><td>Symbol</td><td>Description of position for the user</td></tr>
<tr><td>*P*1</td><td>Active state</td></tr>
<tr><td>*P*2</td><td>Allowed to work in the project</td></tr>
<tr><td>*P*3</td><td>Allowed to work with functional components</td></tr>
<tr><td>*P*4</td><td>Allowed to files of information resources of IO</td></tr>
<tr><td>*P*5</td><td>Checking the rights for the job</td></tr>
<tr><td>*P*6</td><td>Checking the access rights to functional components</td></tr>
<tr><td>*P*7</td><td>Checking access to files</td></tr>
<tr><td>*P*8</td><td>Restoration of the initial state ACS</td></tr>
<tr><td>*P*9</td><td>Limitation of activity in time (for example, during job adjustments)</td></tr>
<tr><th colspan="2">Transitions</th></tr>
<tr><td>Symbol</td><td>Description</td></tr>
<tr><td>*T*1...*T*8</td><td>Represent a set of conditions for the transition (and modification) of markers from one network position to another. The conditions are determined by a set of a priori data.</td></tr>
</table>



1- The total number of cyber threats that were implemented in IO;

2- Cyber threats associated with violation of access rights and abuse of authority.

Figure 3 Information Security Assessment IO

The statistical data obtained in the course of simulation modeling (in particular, concerning the dynamics of markers, gave grounds to establish specific characteristics ACS for companies that participated in the approbation of the model.

6. RESULTS AND DISCUSSION

The advantage of our research is the fact that the proposed solutions, in particular, the developed conceptual model of adaptive access rights management using Petri nets apparatus, as well as models and method, have been successfully tested in the subsystem of the administration of information and cybersecurity of several large universities in Ukraine, as well as in commercial enterprises of Kiev and Dnipro. On the basis of the proposed solutions, software products have been created, which made it possible to automate the control, maintenance and modification of subscriber accounts of IO networks. At the same time, in these software products (especially the “Threat Analyzer” [14]), the opportunity has been laid to adjust subscriber access levels to information resources.

The disadvantage of this paper is not a large degree of approbation of the proposed solutions, but research and work in the chosen direction continues.

The prospect of further research is the possibility of applying the results obtained for the subsequent algorithmization of the processes associated with the analysis IS and CS of various IO, in particular, for solving applied problems that are related to the problem of management and access control in critical computer systems and information objects. In this context, our work continues previous publications of the authors [14, 15].

7. GRATITUDES

The research and the article were carried out within the framework of promising scientific and technical programs of the Department of Computer Systems and Networks of National University of Bioresources and Natural Resources Use of Ukraine as well as a grant of the Republic of Kazakhstan registration number AP05132723 "Development of adaptive expert systems in the field of cybersecurity of very important information objects".

8. CONCLUSIONS

The results of this paper:

The conceptual model of adaptive management of cyber protection of the object of informatization (IO) is described. An example of solving the problem of adaptive management of user access rights using the apparatus of Petri nets is considered. A corresponding model was implemented and simulations were performed in the PIPE v4.3.0 package. The possibility of automation of user profile adjustment procedures for minimizing or neutralizing cyber threats in IO is shown;

the distribution model of tasks assigned by users in computer networks of information objects is described. The basis for the model was the mathematical apparatus of Petri nets. Unlike the existing ones, the model contains variables that allow reducing the power of the state subspace. Also, the effectiveness of modeling has been improved, in particular by reducing the time spent on making decisions related to the regulation of access rights;

the method of access control was updated and supplemented (ACM). The model takes into account the current security policy indicators for specific IO and security metrics with possible adjustments of the latter. Correction of rules and security metrics for new tasks or redistributed tasks is described in Petri nets notation.

REFERENCES

[1] Gupta, Brij, Dharma P., Agrawal, & Shingo, Yamaguchi, eds. (2016). Handbook of research on modern cryptographic solutions for computer and cyber security, IGI Global.

[2] Liu, X., Zhu, P., Zhang, Y., & Chen, K. (2015). A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure, IEEE Transactions on Smart Grid, 6(5), pp. 2435–2443.

[3] Jasiul, B., Szpyrka, M., & Śliwa, J. (2014). Detection and modeling of cyber-attacks with Petri nets, Entropy, 16(12), pp. 6602–6623.

[4] Liu, X., Zhang, J., & Zhu, P. (2017). Modeling cyber-physical attacks based on probabilistic colored Petri nets and mixed-strategy game theory. International Journal of Critical Infrastructure Protection, 16, pp. 13–25.

[5] Jasiul, B., Szpyrka, M., & Śliwa, J. (2015). Formal specification of malware models in the form of colored Petri nets. In Computer Science and its Applications, Springer, Berlin, Heidelberg, pp. 475–482.

[6] Akhmetov, B., Lakhno, V., Boiko, Y., etc. (2017). Designing a decision support system for the weakly formalized problems in the provision of cybersecurity. Eastern-European Journal of Enterprise Technologies, (1(2)), pp. 4–15.

[7] Arendt, D. L., Burtner, R., Best, D. M., Bos, N. D., Gersh, J. R., Piatko, C. D., & Paul, C. L. (2015). Ocelot: user-centered design of a decision support visualization for network quarantine. In Visualization for Cyber Security (VizSec), IEEE Symposium, IEEE, pp. 1–8.

[8] Alheeti, K. M. A., Gruebler, A., McDonald-Maier, K. D., & Fernando, A. (2016). Prediction of DoS attacks in external communication for self-driving vehicles using a fuzzy petri net model. In Consumer Electronics (ICCE), IEEE International Conference, IEEE, pp. 502–503.

[9] de Carvalho, M. A., & Bandiera-Paiva, P. (2017). Evaluating ISO 14441 privacy requirements on role based access control (RBAC) restrict mode via Colored Petri nets (CPN) modeling. In Security Technology (ICCST), International Carnahan Conference, IEEE, pp. 1–8.

[10] Appel, M., Konigorski, U., & Walther, M. (2018). A Graph Metric for Model Predictive Control of Petri nets, IFAC-PapersOnLine, 51(2), pp. 254–259.

[11] Gao, Z., Zhao, C., Shang, C., & Tan, C. (2017). The optimal control of mine drainage systems based on hybrid Petri nets. In Chinese Automation Congress (CAC), IEEE, pp. 78–83.

[12] Narayanan, M., & Cherukuri, A.K. (2018). Verification of Cloud Based Information Integration Architecture using Colored Petri nets. International Journal of Computer Network and Information Security, 10(2), 1.

[13] Lakhno, V.A., Nikolaievskyi, O.Y. etc. (2017). Models and tools for automatization of the linguistic research, ournal of Theoretical and Applied Information Technology, Vol. 95, Iss. 5, pp. 989–999.

[14] Tikhonov, U., Lakhno, V., etc. (2016). Development of ontological approach in e-learning when studying information technologies, Eastern-European Journal of Enterprise Technologies, No 5 (2), pp. 13–20.

[15] Lytvynenko, L., Nikolaievskyi, etc. (2017). Development of knowledge-oriented system of machine translation based on the analytic-synthetic text processing, Eastern-European Journal of Enterprise Technologies, No 1(2), pp. 15–24.