International Journal of Civil Engineering and Technology (IJCIET)
Volume 10, Issue 02, February 2019, pp. 1–9, Article ID: IJCIET_10_02_001
Available online at http://www.iaeme.com/ijciet/issues.asp?JType=IJCIET&VType=10&IType=2
ISSN Print: 0976-6308 and ISSN Online: 0976-6316

MODEL OF INDICATOR OF CURRENT RISK OF THREATS REALIZATION ON THE INFORMATION COMMUNICATION SYSTEM OF TRANSPORT

V. Lakhno
Professor, Department of Computer Systems and Networks,
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine

O. Kryvoruchko
Professor, Head of Department of Software Engineering and Cyber Security National University of Trade and Economics, Kyiv, Ukraine

H. Mohylnyi
PhD., Department of Information Technologies and Systems,
Luhansk Taras Shevchenko National University, Starobilsk, Ukraine

M. Semenov
PhD., Department of Information Technologies and Systems,
Luhansk Taras Shevchenko National University, Starobilsk, Ukraine

I. Kiryeyev
PhD., Department of Information Technologies and Systems,
Luhansk Taras Shevchenko National University, Starobilsk, Ukraine

V. Matiievskyi
Department of Information Technologies and Systems,
Luhansk Taras Shevchenko National University, Starobilsk, Ukraine

V. Donchenko
Department of Information Technologies and Systems,
Luhansk Taras Shevchenko National University, Starobilsk, Ukraine

ABSTRACT

The paper proposed a model for estimating the quantitative indicator of current risks of threats and cyberattacks realization on information communication systems of transport (ICST), that differs from the existing models with ability to take into account the degree of influence of each threat or cyberattack within the class on the probability of an emergency situation that arises at cyber-attacks on components of

information communication systems of transport, which in many cases can be attributed to critical computer systems. For approbation of the proposed model the simulation experiment was conducted, the results of which also are presented in the article. Simulation modeling is also carried out for verification of adequacy of the proposed model and algorithm of estimation of current risks for components of ICST. It is considered that many components of ICST work in real time. It is shown that the proposed model takes into account current values of information security metrics and new classes of cyberthreats for ICST.

Key words: Information communication systems of transport, mathematical model, indicator of current risk, cybersecurity, information security.

Cite this Article: V. Lakhno, O. Kryvoruchko, H. Mohylnyi, M. Semenov, I. Kiryeyev, V. Matiievskyi, V. Donchenko, Model of Indicator of Current Risk of Threats Realization on the Information Communication System of Transport, *International Journal of Civil Engineering and Technology (IJCIET)* 10(2), 2019, pp. 1–9.
http://www.iaeme.com/IJCIET/issues.asp?JType=IJCIET&VType=10&IType=2

1. INTRODUCTION

Information security and cybersecurity of information communication systems of transport (ICST) requires accounting for all events that occur. In particular, events in the process of which digital information is created, modified, accessed or transmitted [1, 2]. Implementation of these measures is the requirement of the international standard ISO/IEC 27001:2013 “Information security management systems – Requirements”.

The need to use of monitoring systems for information security (IS) in ICST is determined by the fact that the use of conventional measures and mechanisms of information security is inadequate [3]. In particular, because they perform only basic functions and do not allow to control the safety of the systems functioning in conditions of permanent modifications of cyberattacks. Existing security monitoring systems are not able to conduct a comprehensive assessment of hackers' actions, build a sequence of implemented vulnerabilities, determine the ultimate goal of the attacker and assess the risks of threats realization to security systems, which can lead to repeated successful attacks, as well as to financial losses.

Existing monitoring tools of IS, such as, Intruder Alert, Real Secure Network Sensor [3–5] and others, have some drawbacks:

high level of type I and type II errors, that is, errors are not the definition of a cyberattack, when it occurs, and the formation of an "attack" situation in its absence;

lack of ability to adaptively manage system of IS and to conduct preventive actions.

Reducing the risks of unauthorized access to information resources of ICST can be achieved by solving the problem of assessing and analyzing the current threat of the process of computer attack in real time, in order to prevent the attack in a timely manner and thereby prevent the development of an unfavorable scenario for the development of this situation. Obviously, in order to take into account, the influence of numerous parameters of anomalies and cyberattacks on the degree of IS ICST, as well as their interconnections of systems in real time, special methods and corresponding organizational, technical and software tools are necessary. So, the topic of the study is relevant.

2. LITERATURE REVIEW AND PROBLEM POSING

Analysis of previous studies allowed to determine the list of potential current risks, which allows to determine the most topical threats for ICST and measures to counter them, as well as to optimize the cost of building a system of protection [5–7].

One of the most common methods of risk assessment is the method based on the full coverage of system, which is a triad "threats – information security measure– protection objects" in the form of a trilogy graph [8, 9].

During the risk assessment, three tasks can be distinguished, reflecting the goals of such an assessment:

1) risk assessment at the objects of ICST not equipped with modern information security measures (ISM), in order to find out the need to create complexes of information security systems (ISS);

2) risk assessment of cyber threats realization in order to modernize the existing complexes of ISS;

3) risk assessment in order to create a new complex of ISS.

It should be noted that a certain quantitative characterization of the risk of unauthorized access (UA) to ICST has already been introduced in the normative documentation and in the studies of a number of authors [3, 6, 8, 10]. According to these sources, as a quantitative characteristic of the risk of penetration in ICST, the risk is considered, measured, as a rule, in monetary units, which is not always of paramount importance for critical systems.

Consequently, it is necessary to calculate the risk for all three formulations of the design task. Consideration of the real connections between threats and resources leads to the fact that the risk should be determined with taking into account the values of elements of the matrix of relationships, the values of which are equal to 0 - if the threat cannot affect the resource, and equal to 1 - if the threat potentially can affect the information resource.

3. GOAL AND OBJECTIVES OF THE STUDY

Research goal is to develop a model of indicator for assessment of the current risk of threats realization on the information communication system of transport.

To achieve the research goal, it is necessary to develop:

1) obtain a quantitative indicator of the current risks (ICR) of the implementation of threats on ICST;

2) to develop algorithms for estimating ICR for ICST components operating in real time, taking into account current values of information security metrics and new classes of cyber threats.

4. MODELS AND METHODS

The current risks and threats of cyberattacks or unauthorized access are indicators of technological processes in ICST, which can acquire different values depending on various factors [7].

It is intuitively clear that current risks may be insignificant if all potentially dangerous ICST parameters are maintained within established limits or increased, becoming threatening, with the deviation of such parameters from the norm. Therefore, it is necessary to describe the degree of current risk of cyberattack threats realization with some quantitative indicator, the value of which would depend on the deviations of the parameters associated with the IS.

The introduction of such an indicator will allow for indirect measurement of the degree of current risks of cyberattack threat realization on ICST.

We propose to introduce a special indicator for the quantitative characterization of the current attack hazard level or unauthorized access to ICST, which can be calculated (measured) at any given time, in particular, using intelligent detection methods for threats [7, 10]. The results of the measurements of the indicator can be presented to the system administrator (administrator of ISS) or used for other tasks.

If processes in ICST are characterized by the risks of implementing IS threats, all of which lie in the zone of permissible values of ZS_0 (see Figure 1), then the current IS can be considered as zero. If one or more parameters are transferred to the zone of unsafe values ZS_1, the current risk increases, and it will increase with the parameters to the zone of critical values ZS_2.

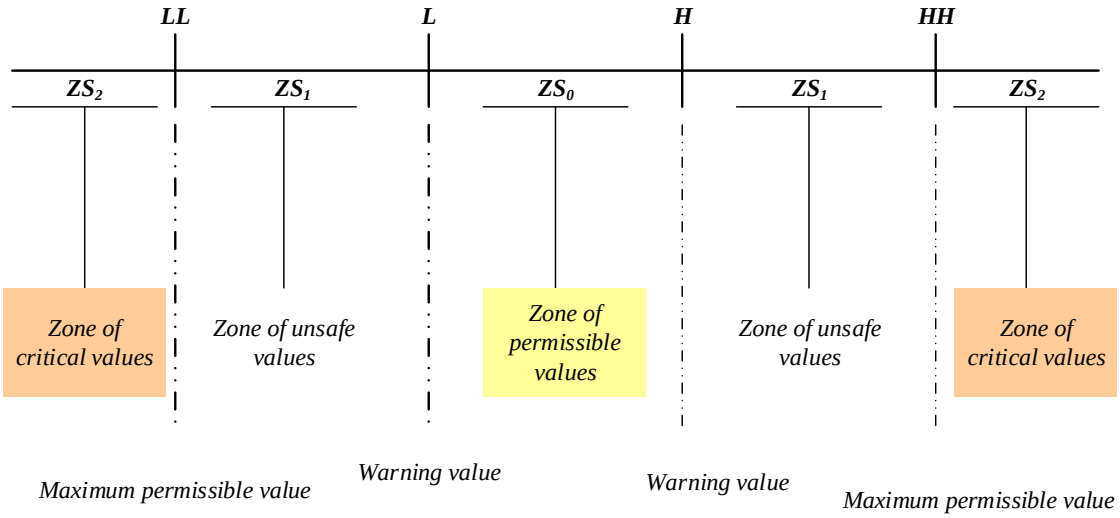

Figure 1 Risks of the threat's realization to information security of ICST

It is clear that the current danger of penetration in ICST should depend on the total number of threats of information - MI, which are simultaneously in the zone ZS_1, from the degree of approximation of each parameter to the zone ZS_2 and the degree of exposure of each threat to the possibility of an unordinary situation emergence, for example, gaining access to resources of ICST.

Denote ICR through $C_{CRI} = C_{CRI}(\bar{X})$, where $\bar{X}_{CRI} = (x_{CRI1},...,x_{CRI\,i},...,x_{CRI\,MI})$ - the vector values of the ICR, MI - the number of threats to information.

The current risk indicator C_{CRI} should meet these requirements.

1. Be scalar with a non-dimensional variable that varies from 0 to 1 ($C_{CRI} = (0 \div 1)$) taking into account the algorithm work of DDP IS.

2. Be the function of the parameters x_{CRIi} $C_{CRI} = f((x_{CRI1},...,x_{CRIi},...,x_{CRI\,M})$.

3. Values of C_{CRI} should depend on the values of all the risks of threats realization to the components and processes in ICST, when they are in the zone of unsafe values $0 < C_{CRI} < 1$.

$$\begin{aligned} &if \quad \exists(x_{CRIi}) : ZS_i = ZS_1,\ i = 1..MI; \\ &or \quad \exists(x_{CRI\,i}) : (x_{CRI\,ill} > x_{CRI\,i} > x_{CRI\,il}) \vee \\ &\vee (x_{CRI\,ih} > x_{CRI\,i} > x_{CRI\,ihh}), \end{aligned} \tag{1}$$

where $x_{CRI\,il}, x_{CRI\,ih}$ – warning values of indicators;

$x_{CRI\,ill}, x_{CRI\,ihh}$ – maximum permissible values of indicators.

4. The value of the ICR of the IS of ICST is zero if all the parameters of the information processes in the ICST are in the zone of permissible values $C_{CRI} = 0$,

$$if \quad \forall(\mathrm{x}_{CRI\,\mathrm{i}}) : ZS_i = ZS_0, i = 1..MI.$$

5. The value of ICR is equal to one if at least one technological parameter of the ICST (see [7, 10, 11]) is in the zone of critical values $C_{CRI} = 1$,

$$if \quad \exists(\mathrm{x}_{CRI\,\mathrm{i}}) : ZS_i = ZS_2, i = 1..MI. \tag{2}$$

6. The value of C_{CRI} should be increasing function of its arguments.

If $C_{CRI\,1}$ – the value of the indicator C_{CRI} when $x_{CRI\,i} = x_{CRI1}$,

$C_{CRI\,2}$ – the value of the indicator C_{CRI} when $x_{CRI\,j} = x_{CRIj1}$, and if degree of influence of $x_{CRI\,i}$ is less than degree of influence $x_{CRI\,j}$, then $C_{CRI\,1} < C_{CRI\,2}$.

7. The value of C_{CRI} should increase with an increase in the number of threats and attacks – data on incidents of IS in the zones ZS_1, ZS_2.

If $C_{CRI\,1}$ – the value of the indicator C_{CRI} when $x_{CRI\,i} = x_{CRI\,i1}$, $ZS_i = ZS_1$, $C_{CRI\,2}$ – the value of the indicator C_{CRI} when

$$\begin{aligned} & x_{CRI\,i} = x_{CRI\,i1}, \\ & x_{CRI\,j} = x_{CRI\,j1}, \\ & ZS_i = ZS_1, \\ & ZS_j = ZS_1 \; else \; C_{CRI\,1} < C_{CRI\,2}. \end{aligned} \tag{3}$$

8. Indicator C_{CRI} should take into account the degree of influence of each threat within the class $\mathrm{KL_i}$ to the possibility of an emergency situation that occurs when attacking components of ICST.

If $C_{CRI\,1}$ – the value of the indicator C_{CRI} when $x_{CRI\,i} = x_{CRI1}$,

$C_{CRI\,2}$ – the value of the indicator C_{CRI} when $x_{CRI\,j} = x_{CRIj1}$, and if degree of influence of $x_{CRI\,i}$ is less than degree of influence then $x_{CRI\,j}$, then $C_{CRI\,1} < C_{CRI\,2}$.

9. The value C_{CRI} should be applicable in any mode of operation of ICST.

Calculations of ICR of UA in ICST are based on this dependence:

$$C_{CRI}(\bar{X}) = \sqrt{\frac{x_{CRI1}^2}{\prod_{i=2}^{MI}(1+x_{CRIi}^2)} + \sum_{i=2}^{MI}\frac{x_{CRIi}^2}{\prod_{k=i}^{MI}(1+x_{CRIk}^2)}}. \tag{4}$$

The formula for calculating of C_{CRI} the value when used in ICST requires special algorithm for valuation and ordering of parameters MI.

Research of the algorithm and the main properties of the ICR is carried out with the help of the software package Mathcad.

Suppose that any C_{CRI} can have one or two areas of dangerous values (H – high and L – low).

If the parameter $x_{CRI\,i}$ $(1 \le i \le MI)$ has one or two zones of dangerous values, then the conversion of its current value to the normalized value θ_i is performed by the formula (5):

$$\theta_i = \begin{cases} 1, & if \quad x_{CRI\,i} \le x_{CRI\,i}^{ll}, \\ \dfrac{x_{CRI\,i} - x_{CRI\,i}^{ll}}{x_i^{l} - x_i^{ll}}, & if \quad x_{CRI\,i}^{ll} < x_{CRI\,i} < x_{CRI\,i}^{l}, \\ 0, & if \quad x_{CRI\,i}^{l} \le x_{CRI\,i} \le x_{CRI\,i}^{h}, \\ \dfrac{x_{CRI\,i} - x_{CRI\,i}^{h}}{x_{CRI\,i}^{hh} - x_{CRI\,i}^{h}}, & if \quad x_{CRI\,i}^{h} < x_{CRI\,i} < x_{CRI\,i}^{l}, \\ 1, & if \quad x_{CRI\,i} > x_{CRI\,i}^{hh}, \end{cases} \tag{5}$$

where $x_{CRI\,i}$ – current value of indicator;

$x_{CRI\,i}^{l}$, $x_{CRI\,i}^{h}$ – warning values of indicators;

$x_{CRI\,i}^{ll}$, $x_{CRI\,i}^{hh}$ – maximum permissible values of indicators.

The degree of influence of each factor on the possibility of threat realization to IS at deviation of this parameter from the norm, is determined by ranking, that is, assigning a parameter to a certain coefficient (rank). The rank of the parameter K_r represents a positive integer value: K_r = 1, 2, ... The model was tested during the simulation experiment.

5. SIMULATION EXPERIMENT

Figure 2, 3 show, for example, the dependencies of ICR C_{CRI} on the parameters of the parameters $x_{CRI\,i}$ and θ_i for *MI =1, 2* and K_r = 1, 2 (for example, the key abduction for the GSM-R communication system and the organization of the DoS / DDoS attack on the train control system).

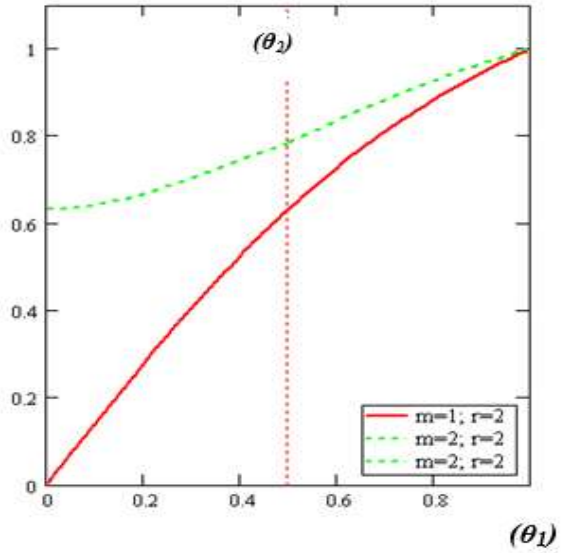

Figure 2 Dependencies $C_{CRI\,i}(\theta_1)$ for *MI=1* i 2 & $Kr_1 = Kr_2 = 2$

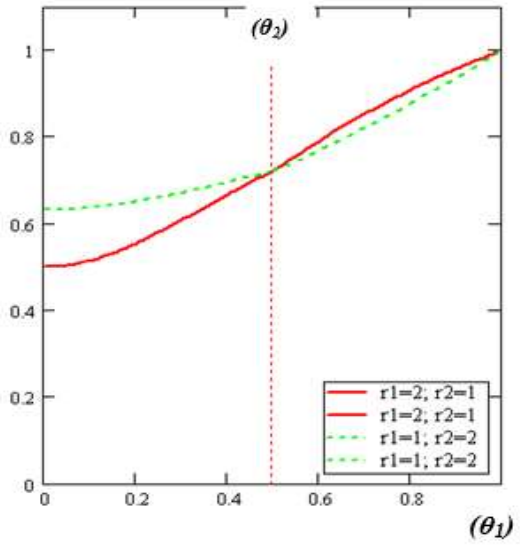

Figure 3 Dependencies $C_{CRI\,i}(\theta_1)$ for *MI=2*, $Kr_1 > Kr_2$ & $Kr_1 < Kr_2$

6. RESULTS AND DISCUSSION

As a result of the analysis of these and other dependencies obtained during the simulation experiment, as well as those investigated in papers [5, 7, 11–22], the following conclusions were made:

1. $C_{CRI} = 0$, if all θ_i are equal to 0.

2. $C_{CRI} = 1$, if at least one parameter θ_i is equal to 1.

3. $0 < C_{CRI} < 1$, if at least one parameter θ_i is greater than zero and less than 1 (the corresponding parameter x_i is in the danger zone).

4. If, when one or more parameters are found in the zone of unsafe values, another parameter also enters this zone, then the indicator C_{CRI} increases.

5. If the number of current threats IS *MI = 1* and $Kr_1 = 1$, then $C_{CRI} = \theta_1$, that is, the ICR C_{CRI} is proportional to the parameter θ_1.

6. If *MI = 1* and $K_{r1} = 2$, then the dependence C_{CRI} from θ_1 is nonlinear. In this case, C_{CRI} more than with $K_{r1} = 1$ for the same values θ_1.

7. If *MI> 1*, then all dependencies C_{CRI} from θ_1 are nonlinear. At the same time, the value of the indicator C_{CRI} is higher, the more parameters are in the unsafe zone.

8. The higher the rank of parameters, which are in the unsafe zone, the higher level has indicator C_{CRI} for other equal conditions [23–25].

A certain disadvantage of work at this stage of research is insufficient approbation of results. But our research is continuing and eventually their results will be presented in the following publications.

7. GRATITUDES

The research and the article were done within the framework of promising scientific and technical programs of the Department of Computer Systems and Networks of the National University of Life and Environmental Sciences of Ukraine, as well as the grant of the Republic of Kazakhstan, registration number AP05132723 “Development of adaptive expert systems in the area of cybersecurity of critical objects of informatization”.

8. CONCLUSIONS

Thus, according to the results of the research, the following results were obtained:

The model was developed to assess the quantitative indicator of current risks of threats and cyberattacks realization on information communication systems of transport (ICST), which differs from existing ones by ability to take into account the degree of influence of each threat or cyberattack within the class, on the probability of emergencies that occurs when cyberattacks on ICST components;

Simulation modeling was performed to verify the adequacy of the proposed model and algorithm for assessing the current risk indicator for ICST components operating in real time, taking into account current values of information security metrics and new classes of cyber threats for ICST.

REFERENCES

[1] Al Hadidi, M., Ibrahim, Y. K., Lakhno, V., Korchenko, A., Tereshchuk, A., & Pereverzev, A. (2016). Intelligent systems for monitoring and recognition of cyberattacks on information and communication systems of transport. International Review on Computers and Software, 11(12), pp. 1167-1177.

[2] Alcaraz, C., Zeadally, S. (2013). Critical control system protection in the 21st century, Computer, 46 (10), pp. 74-83.

[3] Vacca, J.R. (2010). Managing Information Security, Syngress, p. 320.

[4] Lopez, I., Aguado, M. (2015). Cyber security analysis of the European train control system, *IEEE Communications Magazine*, **53**(10), pp. 110-116.

[5] Lakhno, V., & Hrabariev, A. (2016). Improving the transport cyber security under destructive impacts on information and communication systems. *Eastern-European Journal of Enterprise Technologies*, **1**(3), 4, pp. 4-11.

[6] Dunn, W. (2002). Practical Design of Safety-Critical Systems, Reliability Press, Cambridge.

[7] Lakhno, V. (2016). Creation of the adaptive cyber threat detection system on the basis of fuzzy feature clustering, *Eastern-European Journal of Enterprise Technologies*, Vol. **2**, Iss. 9, 2016, pp. 18-25.

[8] Beketova, G. S., Akhmetov, B. S., Korchenko, A. G. etc. (2017). Optimization backup model for critical important information systems. *Bulletin of the national academy of sciences of the republic of Kazakhstan*, (5), pp. 37-44.

[9] Lakhno, V.A., Kravchuk, P.U., Malyukov, V.P., Domrachev, V.N., Myrutenko, L.V., Piven, O.S. (2017). Developing of the cyber security system based on clustering and formation of control deviation signs, *Journal of Theoretical and Applied Information Technology*, Vol. 95, Iss. 21, pp. 5778-5786.

[10] Lakhno, V., Zaitsev, S., Tkach, Y. etc. (2019). Adaptive expert systems development for cyber-attacks recognition in information educational systems on the basis of signs' clustering, Advances in Intelligent Systems and Computing, 1st International Conference on Computer Science, Engineering and Education Applications, ICCSEEA2018; Kiev; Ukraine; 18 January 2018, Vol. 754, pp. 673-682.

[11] Akhmetov, B., Lakhno, V., Akhmetov, B., Alimseitova, Z. (2019). Development of sectoral intellectualized expert systems and decision-making support systems in cybersecurity, Advances in Intelligent Systems and Computing, 2nd Computational Methods in Systems and Software, CoMeSySo 2018; Szczecin; Poland; 12 September 2018, Vol. 860, pp. 162-171.

[12] Akhmetov, B., etc. (2018). Models and Algorithms of Vector Optimization in Selecting Security Measures for Higher Education Institution's Information Learning Environment. In Proceedings of the Computational Methods in Systems and Software (pp. 135–142). Springer, Cham.

[13] Lakhno, V., Tkach, Y., Petrenko, T., Zaitsev, S. & Bazylevych, V. (2016). Development of adaptive expert system of information security using a procedure of clustering the attributes of anomalies and cyber-attacks. Eastern European Journal of Enterprise Technologies, 6/9 (84), pp. 32–44.

[14] Lakhno, V., Akhmetov, B., Korchenko, A., Alimseitova, Z., Grebenuk, V. (2018). Development of a decision support system based on expert evaluation for the situation center of transport cybersecurity. Journal of Theoretical and Applied Information Technology, 96 (14), pp. 4530–4540.

[15] Lakhno, V., Buriachok, V., Parkhuts, L. etc. (2018). Development of a conceptual model of adaptive access rights management with using the apparatus of Petri nets. International Journal of Civil Engineering & Technology (IJCIET), Vol. 9, Iss. 11, pp. 95–104.

[16] Akhmetov, B., Kydyralina, L. etc. (2018). Model for a computer decision support system on mutual investment in the cybersecurity of educational institutions, International Journal of Mechanical Engineering & Technology (IJMET), Vol. 9, Iss. 10, pp. 1114–1122.

[17] Borowik, B., Karpinskyy, M., Lahno, V., & Petrov, O. (2012). Theory of Digital Automata (Vol. 63). Springer Science & Business Media.

[18] Smirniy, M., etc. (2009). The research of the conflict request threads in the data protection systems. Proceedings of Lugansk branch of the International Academy of Informatization, 2(20), pp. 23–30.

[19] Akhmetov, B. B. etc. (2018). The Choice of Protection Strategies during the Bilinear Quality Game on Cyber Security Financing. Bulletin of the national academy of sciences of the republic of Kazakhstan, (3), pp. 6–14.

[20] Petrov, A., etc. (2016). Models, methods and information technologies of protection of corporate systems of transport based on intellectual identification of threats. Decision Making in Manufacturing and Services, 9(2), pp. 117–135.

[21] Lakhno V., Tsiutsiura S., Ryndych Y., Blozva A., Desiatko A., Usov Y. and S. Kaznadiy. (2019). Optimization of information and communication transport systems protection tasks. International Journal of Civil Engineering & Technology (IJCIET), Vol. 10, Iss. 1, pp. 1–9.

[22] V. Lakhno, D. Kasatkin, V. Kozlovskyi, S. Petrovska, Y. Boiko, P. Kravchuk, N. Lishchynovska (2019). A Model and algorithm for detecting spyware in medical information systems, International Journal of Mechanical Engineering & Technology, Vol. 10, Iss. pp. 287–295.

[23] Akhmetov, B. 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)), 4–15.

[24] Smirniy, M. etc. (2009). The research of the conflict request threads in the data protection systems. Proceedings of Lugansk branch of the International Academy of Informatization, 2(20), pp. 23–30.

[25] Petrov, B. B., & Karpinskyy, M. (2016). Immune and defensive corporate systems with intellectual identification of threats. Śląska Oficyna Drukarska, Pszczyna, 222 p.