INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2019, VOL. 65, NO. 4, PP. 545–550
Manuscript received January 23, 2019; revised December, 2019. DOI: 10.24425/ijet.2019.129811

Development of decision support system based on feature matrix for cyber threat assessment

Timur Kartbayev, Bakhytzhan Akhmetov, Aliya Doszhanova, Valery Lakhno, Feruza Malikova and Sharapatdin Tolybayev

***Abstract*—The article herein presents the method and algorithms for forming the feature space for the base of intellectualized system knowledge for the support system in the cyber threats and anomalies tasks. The system being elaborated might be used both autonomously by cyber threat services analysts and jointly with information protection complex systems. It is shown, that advised algorithms allow supplementing dynamically the knowledge base upon appearing the new threats, which permits to cut the time of their recognition and analysis, in particular, for cases of hard-to-explain features and reduce the false responses in threat recognizing systems, anomalies and attacks at informatization objects. It is stated herein, that collectively with the outcomes of previous authors investigations, the offered algorithms of forming the feature space for identifying cyber threats within decisions making support system are more effective. It is reached at the expense of the fact, that, comparing to existing decisions, the described decisions in the article, allow separate considering the task of threat recognition in the frame of the known classes, and if necessary supplementing feature space for the new threat types. It is demonstrated, that new threats features often initially are not identified within the frame of existing base of threat classes knowledge in the decision support system. As well the methods and advised algorithms allow fulfilling the time-efficient cyber threats classification for a definite informatization object.**

***Keywords*—decision support system, cyber threat, intellectualized system, detecting the cyber threats, critically needed computer systems**

I. Introduction

With the globalization of information technologies and system usage scale one of the paramount tasks for their smooth operation has become the task of securing the information and cyber security of electronic resources from destructive interference and unauthorized penetration. Sufficiently long time ago at the cyber security market the different recognition systems or network attacks, as well as the attack features or anomalies detection occupied their niche[13]. Respectively as a new guideline has become developing the intellectualized systems of detecting the threats for information and cyber security, in particular, for critically needed computer systems [3, 4]. At that a sufficient part of analog software consists of the decision support systems modules [4] or expert systems [57], which help the information protection services analysts and cyber security, upgrade analysis performance and decision making speed upon hard attacks at information-communication systems of enterprises and organizations, as well as other critically needed computer systems [7]. Statistics of increasing the cyber attacks quantity and complexity and information and cyber security incidents investigation duration [2, 8, 9] of different informatization objects just confirms the thesis on the developments continuation necessity in the field of the new methods synthesis and new threats detection models for protecting information and cyber security. Cyber and information security intellectualized tasks, including the problems of decision support upon detecting threats and anomalies in informaization objects are paid sufficient attention all over the world nowadays. Researchers of the USA, European Community and China are the world leaders in elaborating the intellectualized decision support system in cyber security area. There at, the existing decisions are mainly based on using artificial neural networks, cognitive models and cluster analysis methods [811]. However in developing countries (in particular, Kazakhstan, Ukraine, etc., usage of the developed decisions worked out by them is considerably complicated due to a number of reasons: closed nature of methods and models the given products based on, high cost, absence of detailed scientific-technical documentation, insufficient customization to the cyber protection, and consequently, to the expected operation results. According to many researchers opinions the perspective is the guideline connected with the combined methods development which potentially is able to unite classical well approved themselves in practice approaches as well as the new methods, able adequately and efficiently recognize the new or modified cyber threats [2]. Therefore, it is possible to solve the contradiction, connected with complicating the recognition objects nature (cyber attacks, anomalies and cyber threats) and insufficient extent of involvement in detection procedures of intellectualized different types decision support systems modules and expert systems. Consequently, the task on elaborating the new models for intellectualized decision support systems to assess the threats and anomalies in information-communication systems informaization objects notably, under

The work is performed within grant financing of the AP05132723 project "Development of Adaptive Expert Systems in the field of Cyber Security of Crucial Objects of Informatization" (Republic of Kazakhstan).

B. Akhmetov is with Abai Kazakh National Pedagogical University, Almaty, Republic of Kazakhstan (e-mail:bakhytzhan.akhmetov.54@mail.ru).

A. Doszhanova is with Department IT-engineering, Almaty University of Power Engineering and Telecommunications , Almaty, Republic of Kazakhstan (e-mail:dalia.81@mail.ru).

T. Kartbayev is Director of the Institute of the Control systems and Information Technologies, Almaty University of Power Engineering and Telecommunications , Almaty, Republic of Kazakhstan (e-mail: Kartbaevt@gmail.com).

V. Lakhno is Head of Department of Computer systems and networks, National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine (e-mail: Valss21@ukr.net).

F. Malikova is with Department IT-engineering, Almaty University of Power Engineering and Telecommunications, Almaty, Republic of Kazakhstan (e-mail: feruza-malikova@mail.ru).

Sh. Tolybayev is with Department IT-engineering, Almaty University of Power Engineering and Telecommunications , Almaty, Republic of Kazakhstan (e-mail: tolybayev.sh@gmail.com).

the conditions of poorly structured data about the new cyber threats, anomalies and attacks still remains relevant.

II. Literature review and analysis of previous researchers

As it has been shown above, the research actuality has been defined by the world tendency of raising destructive effects complexity and quantity from the side of cyber abuses at information communication systems of different informaization objects. Growth of quantity and complicating the scenario of conducting cyber attacks at informaization objects, as well cyber threats variability, sparked interest to elaborating the efficient systems of intellectual detecting the cyber threats, anomalies and cyber attacks [1, 2, 11, 12]. Individual research direction in the field thereof has become the works on methods, software and models development for intellectualized decision support system [2, 4, 12] and expert system [5, 7, 1315] in the area of information and cyber security. The works [15, 16] consider Data Mining technologies in information security tasks, which allow detecting regularities of the situation evolution linked with information protection in informatization objects. Unfortunately, the works having been analyzed did not have practical implementation in the form of applied software. The works [2, 16, 17] have analyzed intellectual modeling methodology, designed for analysis and decision making in insufficient structured situations. Researches were not brought up to hardware or software implementation. Complication for analysis and decision support system, concerning the informaization objects information security are poorly falling for formalization and structuring tasks provision of cyber safety upon appearing the new attacks classes, anomalies or threats [18]. In case thereof cyber -information security state parameters might be presented with qualitative indices [12], which is not always efficient. According to the authors opinions [18, 19], information security protection degree analysis and elaboration of counteraction plan development against targeted cyber attacks shall be preceded with the stage of detecting the main threats and vulnerabilities. Thereat, as denote the researches themselves, the task of links formalization between the threats and vulnerabilities in information communication systems information security still exists. Major weaknesses of the works [10, 12, 13] are absence of expert or intellectualized decision support systems architectural implementation for complicated formalized problems of informaization objects cyber security. As the authors acknowledged [14, 19, 20], the majority of similar intellectualized decision support system and expert systems are on the stage of testing at present. The works [2, 17, 21] have considered shortages of existing intellectualized decision support and expert systems in the field of information and cyber security. Such shortages are: necessity in high quality experts upon forming knowledge database and knowledge field; separate methods and models algorithmization difficulties; impossibility to assess performance of a definite intellectualized decision support system, etc. [19, 20] Thus, taking into account the controversy in the considered papers, it is evident, that the researches on practically implemented models and intellectualized decision support system algorithms in the cyber and information security sphere shall be necessarily continued.

III. Goals and tasks of research

Goal Developing the methods and models for intellectualized decision support systems in the course of detecting and recognizing the cyber threats to electronic resources of different informatization objects. To reach the research aim there have been solved the tasks on development: methods and algorithms for intellectualized decision support systems that allow forming operationally the feature space for the initial cyber/information security; algorithms for the cyber threats operational classification and task solution, connected with the cyber threats classification of the new cyber threats for a definite informaization object.

IV. Models and methods

In the process of many intellectualized decision support systems implementation in the tasks of cyber security the critical part of the protection systems development is, in whole, the correct problem selection threats detection and assessment for various informatization objects. Support of decision making procedure and qualitative expert evaluation allow solving the problems of information and cyber safety effectively to the fullest extent. Existing approaches to information and cyber security maintenance, assuming growth of means and measures on the closed information, do not always give appreciable effect. In the series of situations they only raise the companies and organizations personnel workload. Intellectualized decision support system does not eliminate the necessity in using the antivirus software, attacks detecting systems, anomalies and targeted cyber attacks, etc. But for difficult situations of informatization objects cyber protection, in which effectiveness of reaching the goals of informaization objects cyber security protection depends on the subjective knowledge, the performance of its introduction into complex systems is high enough. In the foundation of our model, used for producing intellectualized decision support system, the cyber threats detection tasks for different informatization objects and critically important computer systems lies the following assumption: To increase the performance of cyber threats classification, including beforehand unknown, it is effective to use methods combination based on recognition theory and classification apparatus, as well computational models upon forming the elementary classifiers for separate threats classes patterns. [3, 18, 21]. Such methods and models combination allow constructing the effective system for creating the intellectualized support systems knowledge database and synthesis of cyber threats pattern classes for informatization objects. Finally in aggregate with the existing and being designed attacks and anomalies detection systems, the offered intellectualized decision support system will permit to raise sufficiently the performance of detecting the new earlier unknown and unclassified cyber threats.

A. Prerequisites of forming knowledge database

Intellectualized decision support system knowledge database about threats is based on the table ≪Objectfeature≫. Line characterize recognition objects, for instance, threat, anomaly, or cyber attack class. Lines features (or attributes) recognition objects. We suppose that element of the corresponding line equals to one (≪1≫) if k recognition object already contains necessary features/attributes for classification and detection. If j equals to zero (≪0≫) then recognition object features in the database are absent or have insufficient parameters for recognition object classification procedure. Tables lines are given in the database as follows:

$$RO_i\,[at(i), at(j), at(k)] \tag{1}$$

where at=$\{1, 0\}$ attribute (feature) value; i, j, k - attributes number for recognition object (features in the order of their succession in the object, for example, cyber threat with a number i RO_i.Intellectualized decision support system foundation is presented with corresponding models and algorithms of cyber threats classification for informaization objects and critically needed computer systems Prerequisites and initial data for intellectualized support systems knowledge database algorithms and feature space:

1) accepted: $OT = \{OT_i : (i = 1, 2, ...m)\}$ - multiple sample objects for cyber security informatization objects (or critically needed computer systems) $\{TH1, TH2, ...THk\}$, where $TH_i = \left(RO_i^1, RO_i^2, ..., RO_i^n\right)$; RO_i^1 - j -feature of i - object of threat to informatization objects cyber security (or critically needed computer systems);

2)Recognition object is specified as n - dimensional vector $TH_i = \left(X_i^1, X_i^2, ..., X_i^n\right)$; where $\left\{X_i^1, X_i^2, ..., X_i^n\right\}$ - permissible set of features from the feature space of threats to informatization objects cyber security (or critically needed computer systems);

3) For algorithm $AL1$ we fix multiple pattern objects $\{TH1, TH2, ...THk\}$ and recognition object, which are presented in binary format for the lines with equal register length. Each binary format (≪1≫) corresponds to availability of a certain feature. A binary format (≪0≫) corresponds to unavailability;

4) We specify an adherence function $\Psi\,(TH_u, TH)$ of the sample object $TH_u, (u = 1, 2, ..., k)$ and recognition object (TH) for respective features:

$$\Psi(TH_u, TH) = \begin{cases} 1if l - (TH_u, TH) \le h < l; \\ 0if h < l - (TH_u, TH), \end{cases} \tag{2}$$

where l - line length with bits; $h = l - 2$ - amount of binary formats; (TH_u, TH) - scalar product of vectors TH_u, TH;

5) To classify available and mainly new objects in the database of intellectualized decision support system is possible based upon the procedure of breaking down an initial multitude OT (threats to informatization objects cyber security and critically needed computer systems) into non-overlapping sets (i.e., classes);

6) Above mentioned procedure has been implemented by means of algorithmic decision rule as well as models, which we have demonstrated in the papers [3, 18, 21, 22];

7) Decision rule for intellectualized decision support system has been formulated proceeding from the following provisions: two objects are considered similar, provided that amount of coinciding binary formats in the line of object number 1 is bigger or equal to the set binary formats quantity in the line of object number 2; there exists unambiguous correspondence between (≪dissimilarity≫) and distance in n dimensional space of recognition object properties; values of recognition object features symbols in the database (≪1≫) and (≪0≫) are equal.

B. Algorithms of forming feature for detecting cyber threats in make up of decision support system

Algorithms works steps and outcomes for forming intellectualized decision support system database are shown in the Table 1.

Classification of the object, which has not been previously described in intellectualized decision support system database for recognizing the cyber threats has been carried out in the following subsequence.

1. We fix the pattern for unknown recognition object being analyzed, i.e. classification object OCL.
2. Compare the pattern of recognition object being classified to $RS1$ (i.e., RS is the base pattern). In case OCL is similar to $RS1$, then the bit, corresponding to the base pattern thereof obtains the value (≪1≫). Otherwise (≪0≫). 3. Fulfilling comparing of recognition object signature with RS2. If OCL similar to $RS2$, then the bit, corresponding to RS, obtains the value ≪1≫. Otherwise ≪0≫.
4. The procedure continues until the comparison of the object being analyzed with all RS is finished.
5. Obtained by such a way a binary format for some object, further is considered to be the signature of the OCL thereof. All objects with similar signatures in intellectualized decision support system database are assigned to one class. Thus, the signature becomes ≪a noun≫ of the class thereof. The algorithm ascribes a signature to each object, and as well allows defining the signatures quantity. It gives the possibility to group together the objects with similar signatures. Sufficient and guaranteeing the effective recognition objects samples amount might be selected experimentally, for instance, altering the parameter h (i.e., similarity threshold). Or as it has been shown in our previous works [3, 18, 2125], in order to cut computation volume, we may use the methods and models , which permit to decrease matrix size with features [18, 21]. It reached by means of dropping out non-informational features. Outlined in [18, 2125] computation, as well as algorithms $AL1$, $AL2$ confirm an assumption about the fact, that additions to filter methods in minimization tasks of training excerpts in intellectualized decision support system will allow fulfilling more effectively the rating of informational attributes in the knowledge database. Previously we in the works [18, 21, 22] analytically and experimentally confirmed, that methods-filters and offered algorithms $AL1$, $AL2$ allow effective implementing the information assessment for multitudes, in particular, cutting less informative features, the analysis of which complicates the intellectualized decision support system

TABLE I
ALGORITHMS WORKS STEPS AND OUTCOMES FOR FORMING INTELLECTUALIZED DECISION SUPPORT SYSTEM DATABASE

Step (number)	Algorithm	
	AL1	AL1
1	Formed class object pattern.	Fix OCL 1 as a ≪base signature 1 ≫ $RS1$.
2	An object being detected TH is compared bit-by-bit with every model sample $TH_u(U = 1, 2, ..., k)$.	Comparing the OCL signature 2 with OCL 1 pattern.
3	Computation of adherence function value $\Psi\,(TH_u, TH)$.	Fulfilling checking. If patterns are similar, the object 2 is not considered. If otherwise the object pattern 2 is fixed as $RS2$.
4	Signature class binary format bit, in the i - bit of which is (ll 1 gg) , at identity with $i$sample bit means availability of threat feature in the analyzed model. Parameter (ll 0 gg) remains upon non-conformity .	Compare the OCL 3 signature successively with all OCL patterns, which are in intellectualized decision support system database.
5	-	Fulfilled checking. If the OCL 3 signature is similar to the signature of one of the obtained signatures, then it is not considered. If otherwise lets fix $RS3$ as a next base signature.
6		The procedure is repeated until all OCL will be considered
7		Lets return to OCL 1 from multitude G. Successively there is executed its comparison with every objectbase signatures.
	Outcome. For instance, 1) object 10111 enters into the class, described by the signature 011 (as all others, which have the given signature). In case we have n samples in intellectualized decision support system database, then there is no need to sort all 2^n classes. All classes not used by initial objects multitude are dropped out.	Outcome. Base signatures (RS) represent multiple vectors, which are used for recognition objects similarity analysis.

TABLE II
OUTCOMES OF ALGORITHM WORK AND EXAMPLES OF RECORDS FOR INTELLECTUALIZED DECISION SUPPORT SYSTEM DATABASE

Scheme of obtaining class signature at h=3				
Object	Model samples	Number of coincidence	$s(TH_u, TH)$	Class signature
10111	01010, 10011, 11100	1, 3, 2	0, 1, 1	011
An example of breaking down the objects into classes according to model samples				
Class		Class signature	Class objects	
1		100	01010	
2		011	10001, 10111, 10001	
3		110	01011	
4		001	11100	
5		101	01110	
Scheme of obtaining base signatures				
Initial set of objects			Base signatures RS (For h=3)	
00011, 01011, 10111			00011	
11001, 11100, 01110			11001	
01110, 01010, 00000			01110	
Scheme of obtaining the signature using the algorithm of defining the similarity				
Object under classification (OCL)	Base signatures	Coinciding bits	Class name	
11100	00011, 11001, 01110	0, 3, 3	011	

work, which can be used jointly with information protection complex systems.

V. EXPERIMENT

The table 2 demonstrates the results of computational and simulation experiments [25] in the course of algorithms checking AL1, AL2. Especially there were shown the examples of outcomes on the schemes of obtaining, recognition the object pattern class and the one for obtaining the pattern upon using the algorithm for similarity definition. Experiments, in particular, on detecting cyber threats ≪Threats analyzer≫ for the segment of the enterprises computation network. As a platform there were used MATLAB 7/2009 and SIMULINK. The results thereof have been outlined earlier in details in the work [25]. Fragment of pattern obtaining scheme using the algorithm of similarity definition in the lower part of the Table illustrates an example situation, when the object ≪11100≫ refers to class ≪011≫, as all other objects having the signature thereof. Thereat, each object is similar, at least, to one base signature in the intellectualized decision support system knowledge database. Consequently, an analyst on cyber security of a definite informatization object will have an assurance, that there is no class, represented by the signature all bits of which equal to zero.

It is, in its turn, will upgrade the effectiveness of situation analysis, in which the amount of initial features to cyber threat or anomalies does not raise the informaization objects protection extent without attracting additional financial or material resources.

VI. Discussion

Therefore during computation and simulation experiments there was stated the following:

1) every recognition object, which was analyzed by means of intellectualized decision support system and being available in the knowledge base was at least similar to one base signature. Hence, probability of recognition object class absence in intellectualized decision support system is high, which will be described in the database by means of a signature only with zero bits;

2) for recognition objects classification (cyber threats and anomalies) it is enough to use merely a fragment of space measurement, in which de factor reside the most informative attributes-features $at = \{1, 0\}$, which characterize recognition object. Paragraphs 1) and 2) might be referred to the stated method advantages, in particular, in comparison with outlined outcomes in [18, 2125].

In the process of test computations in the tasks of detecting the threats to informatization objects and critically needed computer systems, there were found out algorithms flaws $AL1$, $AL2$. It has become clear, that $AL1$, $AL2$ algorithms usage is not always an optimal means for recognition objects classification and detection with the help of intellectualized decision support system, when this means that the features amount less than 2 [21]. Based on experimental researches and practical approbation there has been made a conclusion on practicability of uniting $AL1$, $AL2$, which operate in two stages. At the first stage for detecting a random recognition object, there has been used an algorithm AL2, further AL1. After results correction there were formulated final conclusions to refer the recognition objects to classes. It allows compensating and minimizing the total number of mistakes while working in intellectualized decision support systems algorithms $AL1$, $AL2$. Additional advantage of solutions, offered in the article is the circumstance, that developed intellectualized decision support systems cost will be equal only to the software price and server for the knowledge database. The product being developed also allows upgrading the decision making operational efficiency, also increasing decision making performance under the conditions of growing the destructive, including targeted effects at informatization objects. Introducing the results of the research herein will give a possibility to widen functional potentials of being produced, modernized and existing cyber protection complex systems; to upgrade the quality and efficiency of decision making under condition of destructive effects amount growth, including targeted at informatization objects; to involve the potential of territorially remote experts and analysts in the information security field at the expense of intellectualized decision support system operation in on-line regime [23]. The peculiarity of being developed intellectualized decision support system is the ability to the self training and adaptation settable upon appearing the new types of threats to informatization objects.

VII. Conclusion

The article herein describes the following main results of our research, namely, developed for the first time and improved: method and algorithms of forming the feature space of detecting the cyber threats to informational resources, which in distinction from the existing ones are based on the system of threats sample classes and adaptive feature space of cyber threats. Feature space might be dynamically added, which allows reducing the time of their detection, in particular, for the cases of hard-to-explain features and cutting the amount of false responses in the recognition system; cyber threats analysis algorithm in the make up of adaptive intellectualized decision support system for anomalies assessment in critically needed computer systems and consequences of different threat classes implementation especially under poorly structured data about cyber threats features. Algorithm, in distinction from the existing, allows considering separately the threat detection task in the framework of known classes and in case of necessity adding the feature space for new types of threats. It is shown, that the new threats features were not specified initially by the frame of the available threat class database in the decision support system. Apart from that, the suggested method and algorithms allow fulfilling the operative cyber threats classification for a definite informatization object.

References

[1] J.Petit, S.E.Shladover, "Potential Cyberattacks on Automated Vehicles", *IEEE Transactions on Intelligent Transportation Systems*,Vol. 16 Iss. 2, 546–556 (2015) DOI: 10.1109/TITS.2014.2342271.

[2] F. Miao, Q. Zhu, M.G.Pajic, J. Pappas, "Coding Schemes for Securing Cyber-Physical Systems Against Stealthy Data Injection Attacks", *IEEE Transactions on Control of Network Systems*, Vol. PP,Iss. 99, 1 (2016) DOI: 10.1109/TCNS.2016.2573039.

[3] O. Petrov, B. Borowik, M. Karpinskyy, "Immune and defensive corporate systems with intellectual identification of threats, Pszczyna : Slaska Oficyna Drukarska", 222 p. ISBN: 978–83–62674–68–8 (2016).

[4] T. Sawik, "Selection of optimal countermeasure portfolio in it security planning",*Decision Support Systems*, 2013, Vol. 55, Iss. 1, P. 156164. http://dx.doi.org/10.1016/j.dss.2013.01.001

[5] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, F. Smeraldi, "Decision support approaches for cyber security investment", *Decision Support Systems*,2016, Vol. 86, P. 1323. http://dx.doi.org/10.1016/j.dss.2016.02.012

[6] L. Atymtayeva, K. Kozhakhmet, G. Bortsova, "Building a Knowledge Base for Expert System in Information Security", *Chapter Soft Computing in Artificial Intelligence of the series Advances in Intelligent Systems and Computing*,2014, Vol. 270, P. 5776. DOI:10.1007/978-3-319-05515-27

[7] M.M. Gamal, B. Hasan, A.F. Hegazy, "A Security Analysis Framework Powered by an Expert System", *International Journal of Computer Science and Security (IJCSS)*,2011, Vol. 4, No. 6, P. 505527.

[8] S. Dua, X. Du, "Data Mining and Machine Learning in Cybersecurity", UK, CRC press, 2016, p. 225.

[9] A.L. Buczak, E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection", *IEEE Communications Surveys and Tutorials*, 2016, Vol. 18, Iss. 2. P. 1153-1176. DOI: 10.1109/COMST.2015.2494502

[10] O. Al-Jarrah, A. Arafat, "Network Intrusion Detection System using attack behavior classification", *2014 5th International Conference on Information and Communication Systems (ICICS)*, 2014,. DOI: 10.1109/iacs.2014.6841978

[11] N. BenAsher, C. Gonzalez, "Effects of cyber security knowledge on attack detection",*Computers in Human Behavior*, (48), 51-61, (2015).

[12] A.Kh. Nishanov, K.F.Kerimov, "Methods of Counteraction from Attacks Carried out Against Users in a Network the Internet",*ICEIC-Electronics, news and communications*,IX-the conference, Tashkent, 2008, P. 298299.

[13] M.M. Gamal, B.Hasan, A.F.Hegazy "A Security Analysis Framework Powered by an Expert System",*International Journal of Computer Science and Security (IJCSS)*, 2011, Vol. 4, No. 6, P. 505527.

[14] Li-Yun. Chang, Zne-Jung. Lee, "Applying fuzzy expert system to information security risk Assessment", A case study on an attendance system, International Conference on Fuzzy Theory and Its Applications (iFUZZY), 2013,346 – 351. DOI: 10.1109/iFuzzy.2013.6825462

[15] M.Kanatov, L.Atymtayeva, B.Yagaliyeva "Expert systems for information security management and audit",*Implementation phase issues, Soft Computing and Intelligent Systems (SCIS), Joint 7th International Conference on and Advanced Intelligent Systems (ISIS)*, 2014, P. 896 900. DOI:10.1109/SCIS-ISIS.2014.7044702

[16] Kuo-Chan.Lee, C.-H. Hsieh, L.-J. Wei, C.-H. Mao, J.-H. Dai, Y.-T. Kuang, "Sec-Buzzer: cyber security emerging topic mining with open threat intelligence retrieval and timeline event annotation", *Soft Computing*, 2016, P. 114. DOI:10.1007/s00500-016-2265-0

[17] S. Pan, T.Morris, U.Adhikari "Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems",*IEEE Transactions on Smart Grid*, 2015, Vol. 6, Iss. 6, P. 3104 3113. DOI: 10.1109/TSG.2015.2409775

[18] V. Lakhno, S. Kazmirchuk, Y. Kovalenko, L. Myrutenko,T. Zhmurko, "Design of adaptive system of detection of cyber-attacks, based on the model of logical procedures and the coverage matrices of features",*Eastern-European Journal of Enterprise Technologies*, 2016, No 3/9(81), P. 3038. DOI: 10.15587/1729-4061.2016.71769

[19] P. Louvieris, N. Clewley, X.Liu "Effects-based feature identification for network intrusion detection",*Neurocomputing*, 2013, Vol. 121, Iss. 9, P. 265273. DOI:10.1016/j.neucom.2013.04.038

[20] Z. Wang, X. Zhou, Z. Yu, Y. Zhang, D. Zhang,"Inferring User Search Intention Based on Situation Analysis of the Physical World",*Chapter Ubiquitous Intelligence and Computing*, 2010, Vol. 6406, P. 3551. DOI: 10.1007/978-3-642-16355-56

[21] V. Lakhno, S. Zaitsev, Y. Tkach, T. Petrenko, "Adaptive Expert Systems Development for Cyber Attacks Recognition in Information Educational Systems on the Basis of Signs Clustering",*Part of the Advances in Intelligent Systems and Computing book series (AISC)*, 2018, Vol. 754, P. 673682.

[22] B. Akhmetov, V. Lakhno, Y. Boiko, A. Mishchenko, "Designing a decision support system for the weakly formalized problems in the provision of cybersecurity", *Eastern-European Journal of Enterprise Technologies*, 1(2(85)), 4-15 (2017).

[23] V. Lakhno, B. Akhmetov, A. Korchenko, Z. Alimseitova, V. Grebenuk, "Development of a decision support system Based on expert evaluation for the situation center of transport cybersecurity", *Journal of theoretical and applied information technology*, 2018, Vol.96. No 14, P. 45304540.

[24] M. Al Hadidi, Y.K.Ibrahim, V. Lakhno, A. Korchenko, A. Tereshchuk, A. Pereverzev "Intelligent systems for monitoring and recognition of cyber attacks on information and communication systems of transport", *International Review on Computers and Software*, 2016, Vol. 11, No 12, P. 11671177.

[25] G. Beketova, B. Akhmetov, A. Korchenko, A. Lakhno, "Simulation modeling of cyber security systems in MATLAB and SIMULINK",*Bulletin of the national academy of sciences of the republic of Kazakhstan*, 2017, Vol. 3, P. 5464.