Journal of Theoretical and Applied Information Technology
30th April 2017. Vol.95. No 8

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

APPLYING THE FUNCTIONAL EFFECTIVENESS INFORMATION INDEX IN CYBERSECURITY ADAPTIVE EXPERT SYSTEM OF INFORMATION AND COMMUNICATION TRANSPORT SYSTEMS

[1] LAKHNO V. A., [2] KRAVCHUK P. U, [3] PLESKACH V. L., [4] STEPANENKO O. P., [5] TISHCHENKO R. V., [6] CHERNYSHOV V.A.

[1,2,5,6] Department of Managing Information Security, European University, Ukraine
[3] Faculty of Information Technology, Taras Shevchenko National University of Kyiv, Ukraine
[4] Economics Information Systems Department, SHEE "Kyiv National Economic University named after Vadym Hetman", Ukraine
E-mail: [1]lva964@gmail.com, [2]p.kr@ukr.net, [3]v_pleskach@ukr.net, [4]olga_stepanenko@kneu.edu.ua, [5]tishchenko.roman@gmail.com, [6]geck@ukr.net

ABSTRACT

Developing a model for determining the functional effectiveness information criterion for expert system learning to determine the state of cybersecurity, while taking into account known statistical and distance clustering indicators of cyber threats, cyber-attacks (CA), anomalies and also errors of the third type, that may arise in the recognition of complex targeted CA on critical computer systems, including the transport sector.

The model for determining the functional effectiveness information criterion of machine learning expert system is developed. It is based on modified entropy and Kullback - Leibler divergence information criterion at clustering features of CA and anomalies that can receive an incoming fuzzy classified learning matrix, that is used as an object of the study, and to build correct decision rules for recognizing complex CA. Tests of the developed expert system were conducted. It is established that the proposed model can significantly increase the anomalies and CA detection effectiveness under constant increase in number and complexity of the destructive influences on computer systems information security.

The model for determining the functional effectiveness information criterion capable of self-learning information security expert system is developed. It takes into account potential errors of the third type that may arise and accumulate during the learning of the intellectual system of complex targeted CA detection.

Keywords: *Cyber-Attacks Recognition, Expert System, Sign Clustering, Functional Learning Effectiveness.*

1. INTRODUCTION

In recent decades cybersecurity (CS) becomes one of the most topical problems in society upon which, in particular, all modern computer systems depend. It is critically important, in particular, in industrial, energy, communications, transport and related sectors. Experience from recent years shows that cyber criminals are increasingly using unique, as yet unknown IT industry malware, vulnerabilities and methods of cyber-attacks (CA).

The transport sector information and communication environment (TSICE) is oriented towards engagement with other sectors of the economy to reduce delays in cargo transporting, processing vessels, containers, rail cars and other cargo through the use of electronic invoice information systems, 'Client-Bank', e-business and others.

Within the framework of the national and international transport industry (TI) information programs of leading countries, modern complexes of information systems, information management systems and automated control systems (ACS) are created.

Active TSICE expansion, especially in the segment of mobile, distributed and wireless technologies is accompanied by the emergence of new threats to CS. The threats are real, since criminals have the potential to intercept passwords, individual files, geolocation information, broadcast audio and video data, and control Wi-Fi networks, webcams, road, railway and airport information boards.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

It is possible to resist the constant increase in number and complexity of the destructive effects on computer systems, particularly in TSICE, using adaptive intelligent cyber threats recognition systems (ICTRS).

Development and implementation of the adaptive algorithms and models in ICTRS remains one of the existing problems in further increasing CS systems operation effectiveness.

The term «adaptation» in ICTRS can be interpreted as a process of deliberate change in the structure, algorithm or parameters of the system in order to improve its functioning effectiveness. The relevance of the work is in creating and researching an expert system (ES) with implemented adaptive algorithm of complex anomalies and CA recognition. A developed ES is based on models and algorithms of the intelligent learning technologies that can increase the probability of complex targeted CA detection within the known and new classes of CA.

2. LITERATURE DATA ANALYSIS AND PROBLEM STATEMENT

The growth of interest in the problems of CS and information security (IS) in the last decade has caused a surge of research in developing effective systems of cyber threats (CT) detection and prevention. In particular, many publications emerged, devoted to the ICTRS synthesis based on the finite automata theory [1], machine learning theory [2, 3], neural networks [4, 5], Bayesian networks [6], genetic algorithms [7], fuzzy logic [8] statistical data analysis [9]. But most of the existing works devoted to the issue of CT recognition cover only basic CA signs. That, in particular, is due to the complexity of determining the information distance between individual characteristics. This task in the works [10, 11] proposes a solution by applying clustering of the previous signs. As a measure of objects proximity in the process of clustering the Bayesian information criterion [12], the Kullback – Leibler divergence [13, 14], or informational entropy as a basic indicator of the attack are used [15]. But unfortunately, the authors examined only a certain class of CA, which narrows the applicability of proposed models in modern ICTRS.

Many authors mark as promising research related to using different Intelligent Systems and Technology (IST) in detection of threats, anomalies and CA in CS tasks. In particular, it is proposed to use the potential of these systems: expert (ES) [16]; decision support [17, 18], adaptive [19, 20]. Previous studies were mainly presented only as formal mathematical models and were not implemented as able-bodied software. Such systems are still under development and unfortunately most of these works do not cover the issue of evaluation of errors of the third type that can occur when ICTRS models ignore some procedures of anomalies or CA recognition in computer systems. In addition, it should be noted that the signs partitioning process considered in ICTRS for different computer systems is not the same, it is dictated by their work and functional tasks specifics.

Numerous publications [16, 17, 19, 21, 22] related to developing effectiveness evaluation criteria of the CS ES learning and also using a variety of methods in ICTRS indicate that there is a need to create a model of a functional effectiveness information index (FEII) of the ES machine learning procedure. This procedure should take into account known statistical and deterministic indicators of optimization the clustering procedure of illegitimate attackers' actions signs in critically important computer systems (CICS). However, authors of the studies [13, 14, 16, and 17] have not shown examples of practical use of similar decision support systems in cybersecurity tasks. Models proposed by the authors [19 - 21] are difficult for program implementation, in particular due to the difficulty of anomaly detection algorithm in computer systems.

After reviewing previous studies, we believe that to improve the efficiency of cybersecurity expert systems (ES) it's efficient to develop a model for definition of the functional performance information index of their machine learning. The model being developed should take into account the statistical parameters and remote clustering features of cyber threats, cyber attacks and anomalies signs. It also seeks to take into account possible errors of the third type during ES training. This will help to improve the quality and speed of cyber attacks detection.

3. FORMULATION OF THE RESEARCH PROBLEMS

The aim of this work is to develop a model to determine the functional effectiveness information index of the machine learning of the information and cyber security status determining expert system, taking into account known statistical and distance signs clustering indicators of cyber threats, CA, anomalies and errors of the third type that may arise during the recognition of targeted complex

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

CA on CICS. To meet the goal, it is needed to solve the following problem: to develop the FEII definition model, that is based on Kullback - Leibler divergence information criterion at clustering signs space of anomalies and cyberattacks in CICS.

4. MATERIALS AND METHODS

The construction of IS ES structural model is a part of the large-scale process of intellectual analysis and data processing in ICTRS.

Within the Intelligent Information Technologies (IIT) used for CS systems learning, the main ACS task is an efficient procedure of transformation of unclear anomalies and CA signs space partitioning into clear recognition objects (RO) class partitions. In particular, it is achieved by the use of an iterative procedure that allows optimization of the ES function parameters in support of high-level IS CICS. The learning process comprises two phases:

the first phase involves the purposeful search for the global maximum of multiextremal function for the statistical FEII of the CS ES learning in the RO signs workspace;

the second phase simultaneously determines and restores the optimal separate hyper-surfaces [10, 13, 14], which were built in binary space of anomalies and CA signs detection.

Unclear incoming objects realizations partitioning used for learning is transformed into clear partitions during the optimization of test tolerances for each class of anomalies or CA. As a result, a deliberate values change of ES recognition signs for certain objects happens and the correct decision rules for multivariate binary learning matrix (MBLM) is built. This allows within the IIT to combine the correction process of used for learning objects and the direct learning stage. The decision rules synthesis happens at the last stage.

To solve the task of forming the input mathematical description of the ES in ICTRS structure, the used for learning object – ULO has to be created (that is, a multidimensional educational signs matrix – learning matrix) – $\left\| lm_{m,i}^{(j)} \mid m=\overline{1,M}; i=\overline{1,N}, j=\overline{1,n} \right\|$.

In order to make this happen the following has to be done:

forming the signs dictionary for each class of anomalies, CT and CA, as well as forming the classes alphabet in terms of RO;

determining the minimum amount of representative learning matrix (RLM);

determining normed tolerances for recognition signs of illegitimate interference into the critically important information systems (CIIS) work.

The parameters that are read from certain sensors or experimental data obtained directly, for example in the course of penetration testing at CIIS, can be used as primary signs.

As secondary signs to detect anomalies and CA, various statistical characteristics can be used, such as certain class realization vectors $\{lm_{m,i}^{(j)} \mid i=\overline{1,N}\}$, learning sample $\{lm_{m,i}^{(j)} \mid j=\overline{1,n}\}$ for ULO and others.

The alphabet for (RO) anomalies, threats or CA for the ES $\{lm_m^o\}$ is formed at the first stage by the system developer involving IS experts.

At the second stage of the alphabet synthesis, with the ES help, the input data processing using clustering methods continues.

As previously shown in works [10, 14, 19] in the case of RO signs dictionary immutability and the alphabet capacity increase, change of the ES asymptotic characteristics is possible. Respectively, this factor can significantly affect the learning procedures functional efficiency for such systems. This is particularly due to increasing the crossing degree of threats, anomalies and CA classes that are a subject of recognition (hereinafter - recognition object or RO).

Let's formalize the ES elements information synthesis. Supposing that the alphabet known classes $\left\{CT_m^o \mid m=\overline{1,M}\right\}$ and RO (type «object-feature») MBLM, which respectively describes the m system state. Herewith, RO MBLM for CT_m^o recognition class, will be as follows:

$$\left\| lm_{m,i}^{(j)} \right\| = \begin{vmatrix} lm_{m,1}^{(1)} & lm_{m,2}^{(1)} & \cdots & lm_{m,1}^{(1)} & \cdots & lm_{m,N}^{(1)} \\ lm_{m,1}^{(2)} & lm_{m,2}^{(2)} & \cdots & lm_{m,1}^{(2)} & \cdots & lm_{m,N}^{(2)} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ lm_{m,1}^{(j)} & lm_{m,2}^{(j)} & \cdots & lm_{m,1}^{(j)} & \cdots & lm_{m,N}^{(j)} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ lm_{m,1}^{(n)} & lm_{m,2}^{(n)} & \cdots & lm_{m,1}^{(n)} & \cdots & lm_{m,N}^{(n)} \end{vmatrix} \quad (1)$$

In the matrix (1), the following notations are accepted: matrix line - the RO "submission" realization $\left\{lm_{m,i}^{(j)} \mid i=\overline{1,N}\right\}$, N - RO signs number; column - stochastic study sample $\left\{lm_{m,i}^{(j)} \mid j=\overline{1,n}\right\}$ with capacity n.

All possible values of each RO feature can be encoded either in binary form [10, 19, 20], or using

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

integers [7, 21, 22], where zero corresponds to the unspecified value of the RO feature. In particular, it has the ability to take into account absent, new or not yet provided RO feature values.

CA signs are detected in large numbers of measured data, such as logs, monitoring data and others. This, in turn, requires increasing the information processing speed in ICTRS.

By combining the data into compact clusters, the analysis of typical representatives of each cluster can be done and the decision whether or not this data is a sign of an attack can also be done.

After that, this solution is transferred to all representatives of the studied cluster. This approach significantly reduces the volume required for the information attack successful classification (ULO).

Using intellectual learning technology models (ILTM) [10, 19], let's present FEII of the self learning capable CS ES as follows:

$$IND_m^* = \max_{IS} IND_m, \qquad (2)$$

where IND_m – FEII of machine learning ES procedure in the RO class recognition CT_m^0; IS – CICS permissible values.

While ES learning and knowledge base (KB) formation, the system's work is regulated by the IS specialist, who according to the ES recommendations generates control commands – $\left\{CC\{hy_m\} \mid m = \overline{1,M}\right\}$.

During the development of the ES as a part of ICTRS the question of evaluating the functional efficiency of machine learning procedures is unavoidably raised. In particular, it allows you to determine the maximum asymptotic reliability of decisions, that are taken during ES testing in the process of anomalies and CA specific classes detection. For the ES as a part of ICTRS, entropic measure [13] and the Kullback – Leibler criterion [14] are proposed to be used as information measures.

Given a priori probability of the approval of RO detection hypotheses, the normed entropic FEII value is as follows:

$$IND = 1 + \\ + 0{,}5\sum_{l=1}^{2}\sum_{m=1}^{2} p(hy_m/hy_l)\log_2 p(hy_m/hy_l), \qquad (3)$$

where $p(hy_l)$ – is a priori approval probability of the assumption (hypothesis) hy_l; $p(hy_m/hy_l)$ – aposterior approval probability of the assumption hy_m provided that the adopted hypothesis hy_l; $M = 2$ – number of assumptions considered in the process of recognition.

Then normalized entropy FEII of IS ES learning, which takes into account the errors of the 1st and the 2nd type, is as follows:

$$IND_m^{(ls)} = 1 + 0{,}5 \cdot \left(\frac{mis1_m^{(ls)}(cr)}{mis1_m^{(ls)}(cr) + AU_{2,m}^{(ls)}(cr)} \cdot \log_2 \frac{mis1_m^{(ls)}(cr)}{mis1_m^{(ls)}(cr) + AU_{2,m}^{(ls)}(cr)} + \right. \\ + \frac{mis2_m^{(ls)}(cr)}{AU_{1,m}^{(ls)}(cr) + mis2_m^{(ls)}(cr)} \cdot \log_2 \frac{mis2_m^{(ls)}(cr)}{AU_{1,m}^{(ls)}(cr) + mis2_m^{(ls)}(cr)} + \\ + \frac{AU_{1,m}(cr)}{AU_{1,m}^{(ls)}(cr) + mis2_m^{(ls)}(cr)} \cdot \log_2 \frac{AU_{1,m}(cr)}{AU_{1,m}^{(ls)}(cr) + mis2_m^{(ls)}(cr)} + \\ \left. + \frac{AU_{2,m}^{(ls)}(cr)}{mis1_m^{(ls)}(cr) + AU_{2,m}^{(ls)}(cr)} \cdot \log_2 \frac{AU_{2,m}^{(ls)}(cr)}{mis1_m^{(ls)}(cr) + AU_{2,m}^{(ls)}(cr)} \right), \qquad (4)$$

where $AU_{1,m}^{(ls)}(cr)$ – is a first validation procedure; $AU_{2,m}^{(ls)}(cr)$ – second validation procedure; $mis1_m^{(ls)}(cr)$ – decisions approval errors of the first type for the ls automated expert system (AES) learning step; $mis2_m^{(ls)}(cr)$ – decisions approval errors of the second type for the ls AES learning step; cr - hyperspherical containers radius [13, 14, 19].

Ensuring the sustainable functioning and reliable information processing in CICS at a random time under the impact of CA is achieved by the realization of the display:

$$SO : SS \times CA \to SS_{res} = \left\{SS_{res}^{i}\right\}, \qquad (5)$$

where SS_{res} – is a set of CICS allowed states; $CA = \{CA_0, CA_1, ..., CA_N\}$ – is a CA realization set.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The functional that defines the general performance indicator of CA counteraction takes into account the recognition efficiency indicator and characterizes the CICS resistance functioning, will be as follows:

$$IE = F\begin{bmatrix}(SCA, CE), (SS, T_s, VIL),\\ (CO, CM, ME\end{bmatrix}, \quad (6)$$

where SCA – is CA scenarios; CE – is RO recognition effectiveness criterion; computer system parameters set: T_s – time periods of the computer system functional tasks performance; VIL – computer system vulnerabilities; the threats and CA counteraction parameters set: CO – computer system regulation parameters; CM – methods of counteraction to the threats and CA in a computer system; ME – means of preventing, detecting, analyzing and active counteraction to CA.

In order to determine how the Kullback - Leibler information measure depends on the ES parameters for the option of use of control commands that are based on three alternatives (a case when a decision on changing the dynamics of the parameter IE is taken), we introduce the following hypotheses: 1) the main working hypothesis (basic) – hy_{γ_1}: RO sign (signs) rc_i (*RS*) and IE indicator is within the CIIS normal state; 2) hypothesis hy_{γ_2} – RO sign (or signs) rc_i (*RS*) and IE indicator suggest that the IE indicator value is less than normal; 3) hypothesis hy_{γ_3} – IE indicator suggests that the IE indicator value is higher than normal;

According to the assumptions let's denote posteriori hypothesis as follows: hy_{μ_1} – signs (signs) value belongs to the tolerances field (TF) ca, hy_{μ_2} – sign (signs) value is to the left of the TF; hy_{μ_3} – sign (signs) value is to the right of the TF.

Due to the previous calculations, we get nine characteristics for allowing three alternative AES solutions:

$AU_{1,m}^{(ls)} = p\left(hy_{\gamma_1}/hy_{\mu_1}\right)$ – the first hypothesis validation based on the findings;

$AU_{2,m}^{(ls)} = p\left(hy_{\gamma_2}/hy_{\mu_2}\right)$ – the second hypothesis validation based on a $\left\{ca_{K,i}^{*}\right\}$ deviations comparison;

$AU_{3,m}^{(ls)} = p\left(hy_{\gamma_3}/hy_{\mu_3}\right)$ – the second hypothesis validation based on the results of processing the predicate type of a number of episodes calculation when it is determined that the RO realization does not belong to the container $C_{1,m}^{o}$ if indeed $\left\{ct_1^{(j)}\right\} \in CT_1^{o}$ and the number of episodes when it is determined that the RO realization belongs to the container $C_{1,m}^{o}$, if they really belong to the CT_2^{o} class;

$mis\,1_{1,m}^{(ls)} = p\left(hy_{\gamma_2}/hy_{\mu_1}\right)$ and $mis1_{2,m}^{(ls)} = p\left(hy_{\gamma_3}/hy_{\mu_1}\right)$ – the number of ES false positives in the process of anomaly or CA detection, respectively;

$mis\,1_{2,m}^{(ls)} = p\left(hy_{\gamma_3}/hy_{\mu_1}\right)$ and $mis\,2_{1,m}^{(ls)} = p\left(hy_{\gamma_1}/hy_{\mu_2}\right)$ – the number of undetected CA or anomalies in the process of ES work, respectively;

$mis3_{1,m}^{(ls)} = p\left(hy_{\gamma_1}/hy_{\mu_3}\right)$ and $mis3_{2,m}^{(ls)} = p\left(hy_{\gamma_2}/hy_{\mu_3}\right)$ – errors of the third type can occur if the model does not take into account some elements of the ES ILTM.

We also accept:

$$\begin{aligned} &mis\,1_{m}^{(ls)} = mis\,1_{1,m}^{(ls)} = mis\,1_{2,m}^{(ls)};\\ &mis\,2_{m}^{(ls)} = mis\,2_{1,m}^{(ls)};\\ &mis\,3_{m}^{(ls)} = mis\,3_{1,m}^{(ls)}. \end{aligned} \quad (7)$$

Let's calculate the full probabilities $P_{t,m}^{(ls)}$ and $P_{f,m}^{(ls)}$ taking assumptions into account (7)

$$\begin{aligned} P_{t,m}^{(ls)} &= p\left(hy_{\mu_1}\right)AU_{1,m}^{(ls)} +\\ &p\left(hy_{\mu_2}\right)AU_{2,m}^{(ls)} + p\left(hy_{\mu_3}\right)AU_{3,m}^{(ls)}; \end{aligned} \quad (8)$$

$$\begin{aligned} P_{f,m}^{(ls)} &= p\left(hy_{\mu_1}\right)mis\,1_{m}^{(ls)} +\\ &p\left(hy_{\mu_2}\right)mis\,2_{m}^{(ls)} + p\left(hy_{\mu_3}\right)mis\,3_{m}^{(ls)}. \end{aligned} \quad (9)$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Then, based on the Bernoulli-Laplace principle [13, 14] for three accepted hypotheses we get the following result:

$$IND_m^{(ls)} = 1/3 \cdot \left\{ \left[\begin{array}{l} AU_{1,m}^{(ls)} + AU_{2,m}^{(ls)} + \\ + AU_{3,m}^{(ls)} \end{array} \right] - \left[\begin{array}{l} mis1_m^{(ls)} + mis2_m^{(ls)} + \\ + mis3_m^{(ls)} \end{array} \right] \right\} \cdot \log_2 \frac{AU_{1,m}^{(ls)} + AU_{2,m}^{(ls)} + AU_{3,m}^{(ls)}}{AU_{1,m}^{(ls)} + AU_{2,m}^{(ls)} + AU_{3,m}^{(ls)}}. \quad (10)$$

Thus, the received expression (10) which takes into account the modified entropy criterion and the Kullback – Leibler measure is functional from decisions characteristics taken during the recognition of relevant anomalies or CA in CICS.

The correct decision rule determines the classification of a parameters vector of known or unknown CA scenarios realization SCA_m^{CT} for m object and ct class to one of the known classes RO $RS_{m_j}^{CT}$ from j-th step in the the work of CS means. According to the Bayes criterion the decision rule is as follows:

$$P\left(RS_{m_i}^{CT}\right) \cdot P\left(SCA_m^{CT} / RS_{m_i}^{CT} \right) \geq \geq P\left(RS_{m_k}^{CT}\right) \cdot P\left(\overline{SCA_m^{CT}} / RS_{m_k}^{CT} \right), \quad (11)$$

where $P\left(RS_{m_i}^{CT}\right)$ – is a probability of ES RO (anomalies or cyber-attacks) classification to a class of known RO $RS_{m_i}^{CT}$; $P\left(\overline{SCA_m^{CT}} / RS_{m_i}^{CT}\right)$ – is a conditional probability density of ES classification of the detected RO to a known class $RS_{m_i}^{CT}$; $P\left(RS_{m_k}^{CT}\right)$ – is a probability of AES RO classification to an unknown RO class $RS_{m_k}^{CT}$; $P\left(\overline{SCA_m^{CT}} / RS_{m_k}^{CT}\right)$ – is a conditional probability density of the detected RO ES classification to the unknown class $RS_{m_k}^{CT}$

Also based on the Bayes criterion we determine the average decision risk taking «price» in ES as for classifying the unknown RO parameters vector to a class $RS_{m_k}^{CT}$:

$$PR\left(RUL_i / \overline{SCA_m^{CT}}\right) = \sum_{j=1}^{\gamma} np\left(\frac{RUL_i}{RS_{m_k}^{CT}} \right) \cdot P \frac{RS_{m_k}^{CT}}{\overline{SCA_m^{CT}}}, \quad (12)$$

where RUL_i – is the final rule according to which the RO binary learning vector (BLV) $\overline{SCA_m^{CT}}$ determines the identity of the object to $RS_{m_k}^{CT}$; $np\left(\frac{RUL_i}{RS_{m_k}^{CT}} \right)$ – the ES decision taking nominal «price» RUL_i; $P \frac{RS_{m_k}^{CT}}{\overline{SCA_m^{CT}}}$ – conditional probability that $\overline{SCA_m^{CT}}$ is assigned by AES to class $RS_{m_k}^{CT}$.

For the case when ES takes a comparative analysis of the two binary learning matrices (BLM), the decision rule using Bayes criterion can be written as the following correlation:

$$\frac{P\left(\overline{SCA_m^{CT}} / RS_{m_1}^{CT} \right)}{P\left(\overline{SCA_m^{CT}} / RS_{m_2}^{CT} \right)} \geq \frac{P(RS_{m_2}^{CT})}{P(RS_{m_1}^{CT})}. \quad (13)$$

Thus, the proposed model takes into account known statistical and deterministic (distance) criteria of RO signs clustering optimization procedures at the previous phase capable of learning ES functioning in ICTRS.

5. RESULTS

Fig. 1 shows the main results obtained during the IND indicator modeling for CA network classes. Fig. 2 shows the results obtained during the IND indicator modeling for CA on SCADA systems of the transport industry.

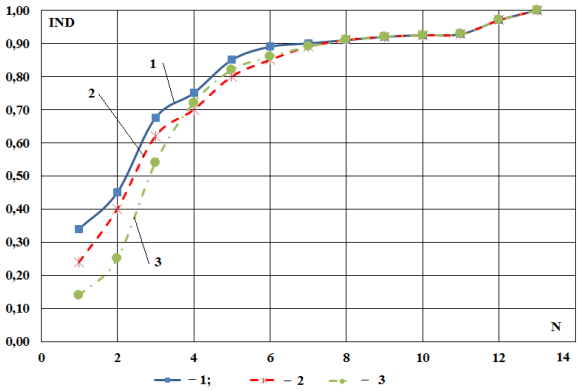
During the study it was found that it is sufficient to restrict to building the representative length sets 5-7 in the model of «voting» for representative sets of anomalies and CA signs. In comparison to the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

method of support vectors [1, 4] ILTM for the small RO signs number (2-4) has a significant advantage index *IND* by 25-50%, but yields at 35-55% to the index *IND*, that was received for the hybrid neural network model [5, 7].

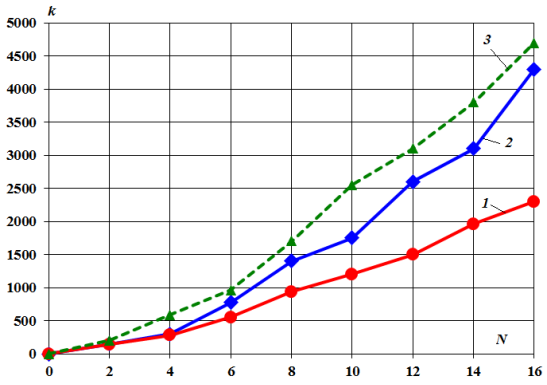
The proposed approach of anomalies and CA recognition based on ES ILTM can increase the network CA detection rate in CICS.

Identifying some types of attacks occurs with probability 77-99% with a slight level of false positives. In addition, the proposed method is not IS resource demanding and is capable of detecting unknown types of CA in the computer systems.



1 – hybrid neural network model [5, 7];
2 – SC ES CICS ILTM;
3 – the support vectors method [1, 4]

Fig. 1. The graph of correlation between capable of learning ES FEII learning (IND) and signs number (N) used for training



1 – ES based on ILTM;
2 – states forecasting methods;
3 – sequential signs search

Fig. 2. Comparative effectiveness of the proposed model for detecting attacks on SCADA system

The optimal number of clusters for determining FEII max value in ES learning during the research is established, which is 3.

The comparative analysis made on the basis of obtained data during the "threat analyzer" AES test trials [23] and the data contained in [7, 9, 13, 14, 20], for intrusion detection systems (IDS) AIDS - application based IDS, and combined solutions IDS & IPS (Intrusion prevention system), that allow to monitor the network or computer system in real time to detect, prevent or block malicious activity.

These results can be compared with the model developed in previous studies in [7, 9, 13, 14, 20, etc.] methods and mathematical models used in IDS Table 1.

6. PROSPECTS FOR THE DIRECTION DEVELOPMENT

At each step of AES input data clustering, the developed model becomes more effective as more informative signs form into classified learning matrices (CLM).

With a small amount of signs in CLM the effect of the model application will be minor.

The proposed adaptive expert system (AES) realization, compared to the results presented in [4, 7, 9] helped to significantly change approaches to the organization of information security specialist surveyed companies.

The developed model compared with the results obtained for the models presented in works [6, 8, 9, 16, 19, 21], provide significantly fewer required signs for classification of complex targeted cyber attacks on computer systems companies.

Thus, prospects of further research lie in improving the signs knowledge base in the form of a matrix representation and conducting model research on more objects stored in knowledge and databases of the ES.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1: Comparative characteristics of intrusion detection methods

№	Model or method	Work in fuzzy signs of attack and the possibility of the algorithm adaptation to the errors of the third type	New signs search	Database to identify anomalies and cyber attacks in the system	The number of input data	Intrusions and normal behavior search , %	Source
1	The hierarchical map	–	–	KDD– 99	41	Norm–96,4; DoS–96,2; U2R–37,1; R2L–43,1; Probe–94,3	[9, 11, 18]
2	Support vector machines method	–	–			Norm–99,8; DoS–97,5; U2R–86,6; R2L–81,3; Probe–92,8	[1, 4]
3	Neural Kohonen	–	–			Norm–97,2; DoS–98; U2R–30,8; R2L–36,5; Probe–92,8	[8, 9, 20]
4	Neural classifier	–	–			Norm–98,5; DoS–98,5; U2R–76,3; R2L–89; Probe–82,5	[5,7]
5	Genetic neural algorithm	–	+			Norm–96,3; DoS–97,3; U2R–29,8; R2L–9,6; Probe–88,7	[7]
6	Hybrid neural network	+	+			Norm–96; DoS–98,8; U2R–72,8; R2L–33,45; Probe–86,2	[5,7]
7	Proposed model for adaptive expert system	+	+		10–12	Norm–98,7; DoS–99,1; U2R–76,5; R2L–90; Probe–84,2	[10, 19]

7. CONCLUSIONS

The following conclusions are the research result in this section:

1) the model of the functional efficiency information criterion is developed. It is based on entropy and Kullback - Leibler divergence information criterion at clustering the anomalies and CA signs in CICS, particularly TSICE. The model is capable of receiving a fuzzy incoming classified learning matrix that is used as an object of study, and also to build the correct decision rules for recognizing CA on TSICE;

2) ES tests were conducted in data centers of several railways of Ukraine. It is established that the proposed model and ES «threats analyzer» learning algorithm can achieve recognition results of CA standard classes in the range of 76.5% to 99.1%. Obtained figures are at the level of recognition efficiency of hybrid neural networks and genetic algorithms. It was established that the optimal number of clusters to determine $\max$ FEII value in ES learning and partitioning signs space of anomalies or CA for computer systems, equals 3.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REFERENCES:

[1] L. Khan, M. Awad, B. Thuraisingham, "A new intrusion detection system using support vector machines and hierarchical clustering", *The International Journal on Very Large Data Bases*, Vol. 16, Iss. 4, 2007, pp. 507–521.

[2] Y. Zhang, L. Wang, W. Sun, R.C. Green, M. Alam, "Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids", IEEE *Transactions on Smart Grid*, Vol. 2, No. 4, 2011 pp. 796–808.

[3] J. Valenzuela, J. Wang, N. Bissinger, "Real-Time Intrusion Detection in Power System Operations", *IEEE Transactions on Power Systems*, Vol. 28, No. 2, 2013, pp. 1052–1062.

[4] O. Al-Jarrah, A. Arafat, A. "Network Intrusion Detection System using attack behavior classification", *Information and Communication Systems (ICICS), 2014 5th International Conference 2014*, pp. 1–6.

[5] S. Selim, M. Hashem, T. M. Nazmy, "Detection using multi-stage neural network", *International Journal of Computer Science and Information Security (IJCSIS)*, Vol. 8, No. 4, 2010, pp. 14–20.

[6] J. Shin, H. Son, R. Khalil, G. Heo, "Development of a cyber security risk model using Bayesian networks", *Reliability Engineering & System Safety*, Vol. 134, 2015, pp. 208–217.

[7] S.N. Pawar, "Intrusion detection in computer network using genetic algorithm approach: a survey", *International Journal of Advances in Engineering Technology*, Vol. 6, Iss. 2, 2013, pp. 730–736.

[8] O. Linda, M. Manic, T. Vollmer, J. Wright, "Fuzzy logic based anomaly detection for embedded network security cyber sensor", *Computational Intelligence in Cyber Security (CICS),* IEEE Symposium on 11–15 April 2011, pp. 202–209.

[9] Z. Zhan, M. Xu, S. Xu, "Characterizing Honeypot–Captured Cyber Attacks: Statistical Framework and Case Study", *IEEE Transactions on Information Forensics and Security*, Vol. 8, Iss. 11, 2013, pp. 1775 – 1789.

[10] V. Lakhno, "Creation of the adaptive cyber threat detection system on the basis of fuzzy feature clustering", *Eastern–European Journal of Enterprise Technologies*, Vol. 2, No 9(80), 2016, pp. 18–25.

[11] P. Louvieris, N. Clewley, X. Liu, "Effects-based feature identification for network intrusion detection", *Neurocomputing*, Vol. 121, Iss. 9, 2013, pp. 265–273.

[12] J. Ye, "Single valued neutrosophic cross-entropy for multicriteria decision making problems", *Applied Mathematical Modelling*, Vol. 38, Iss. 3, 2014, pp. 1170–1175.

[13] Y. Xiang, K. Li, W. Zhou, "Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics", *IEEE Transactions on Information Forensics and Security*, Vol. 6, Iss. 2, 2011, pp. 426 – 437.

[14] C. Callegari, L. Gazzarrini, S. Giordano, M. Pagano, T. Pepe, "Improving PCA-based anomaly detection by using multiple time scale analysis and Kullback–Leibler divergence", *International Journal of Communication Systems*, Vol. 27, Iss. 10, 2014, pp. 1731–1751.

[15] V. Lakhno, A. Petrov, A. Hrabariev, Y. Ivanchenko, G. Beketova, "Improving of information transport security under the conditions of destructive influence on the information-communication", *Journal of theoretical and applied information technology*, Vol. 89, Iss.2, pp. 352–361.

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

[17] 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*, Vol. 270, 2014, pp. 57–76.

[18] 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),* 15th International Symposium on 3–6 Dec. 2014, pp. 896 – 900.

[19] 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*, No 3/9 (81), 2016, pp. 30–38.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[20] N. Ben–Asher, C. Gonzalez, "Effects of cyber security knowledge on attack detection", *Computers in Human Behavior*, Vol. 48, 2015, pp. 51–61.

[21] K. Goztepe, "Designing Fuzzy Rule Based Expert System for Cyber Security", *International Journal of Information Security Science*, 2012, Vol. 1, No 1, pp.13–19.

[22] 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)*, Vol. 4, No. 6, 2011, P. 505–527.