

# Cyber intelligence systems based on adaptive regression splines and logical procedures of attack recognition

**Beketova G<sup>1\*</sup>, Akhmetov B<sup>1</sup>, Korchenko A<sup>2</sup>, Lakhno V<sup>3</sup>, Tereshuk A<sup>3</sup>**

<sup>1</sup>Kazakh National Research Technical University named after K.I.Satpayev, Kazakhstan

<sup>2</sup>National Aviation University, Ukraine

<sup>3</sup>European University, Ukraine

\*Corresponding author's e-mail: beketova2111@gmail.com

Received 20 April 2017, www.cmnt.lv

## Abstract

The article presents the results of research devoted to the further development of methods, models and algorithms for recognizing cyber threats, as well as the most common classes of cyber attacks and anomalies in critical computer systems (CCS). It is shown that the cyber security process for CCS controlled and analyzed by the values of several parameters of anomalies or signs of cyber attacks. This, in turn, makes it possible to carry out a preliminary assessment of information security with the help of two-stage recognition procedure in which initially used the methodology of adaptive regression splines for the processing of statistical data on the anomalies and cyber incidents in CCS, and then in the second stage are used designed logical recognition procedures based on the signs of matrix surfaces. This minimizes the number of training samples for the detection of objects in the framework, the relevant classes of cyber threats, attacks and anomalies.

The research on minimizing the amount of training samples of recognizing signs were performed. It is shown that for the recognition of objects within the known class of cyber threats, attacks and anomalies in the use of training facilities matrices used for training a representative set of long 3-5 attributes will allow to achieve maximum efficiency of the algorithm, reaching up to 98%.

Using the proposed method and models has allowed to reduce the amount of required object recognition rules within the class of 2.5-10 times, compared to the widely used in anomaly detection systems and methods of cyber attacks sequential sorting features and statistical algorithms states.

## Keywords:

intelligent recognition system, cyber threats, anomalies, signs of cyber attacks, adaptive regression splines, logical procedures, elementary classifier

## 1 Introduction

The widespread use of computer systems and information and communications technology improves business efficiency, reduce raw material costs, improve product quality, etc. Today, critical computer systems (CCS) play a key role in the deployment, operation and maintenance of information and communication infrastructure (ICI), responsible for the timely delivery to the consumers of energy resources, water, food, transport services and communications. The most important element of ICI are computerized systems and information technology, disruption of which can lead to serious or even explosive social and economic consequences in the country or a particular region, that is caused by a strong system interconnection between the various components CCS and life support systems. To ensure high performance, reliability and security CCS will need to proactively solve problems related to their information security (IS) and cyber defense.

Active extension applications of CCS, especially in the segment of mobile, distributed and wireless information technology, accompanied by the emergence of new threats to IS, as evidenced by the rapid growth in the number of incidents related to IS and cyber defense CCS and identified vulnerabilities in their software. Thus, the relevance of

studies aimed at the further development of models and methods of protection on the basis of intellectual recognition of threats of CCS and providing them by information security is one of the key problems of cyber critical infrastructure of any state.

## 2 The aim and tasks of the research

The aim of the work is the further development of models and methods of protecting of critical computer systems based on the use of adaptive, self-learning cyber capable of recognition systems, anomalies and attacks.

To achieve this goal it is necessary to solve the following tasks:

1. Develop the method of recognition of threats, anomalies and cyber attacks, allowing to provide cyber defense of CCS based on the application of innovative adaptive cyber defense systems to increase resilience of CCS to cyber attacks.

2. Develop the model of intellectual recognition using of adaptive regression splines and logical procedures for the identification of anomalies and cyber attacks, based on the signs of matrix surfaces (MS) and the concept of an elementary classifier (EC).

### 3 The review of the previous researches

According to various sources [1-3], for the period from 2009 to 2015 the number of cyber incidents, including cyber attacks directed at information system of countries, entering the torus 20, has grown by an average 15 times, Figure 1. And the tendency of a strong growth of number of cyberincidents and cyber attacks is fixed that, in particular, is explained by growth of quantity of CCS connected to wide area networks.

After, in industrial, energy and transport CCS were identified as complex viruses like the Stuxnet (2010), Duqu (2011), Flame (2012), Careto (2014), there was a sharp jump in interest in the IS critical automated control systems (ACS or SCADA). As a result, during the period from 2011 to 2015, in critical components in SCADA was found more than 130 vulnerabilities [3, 4].

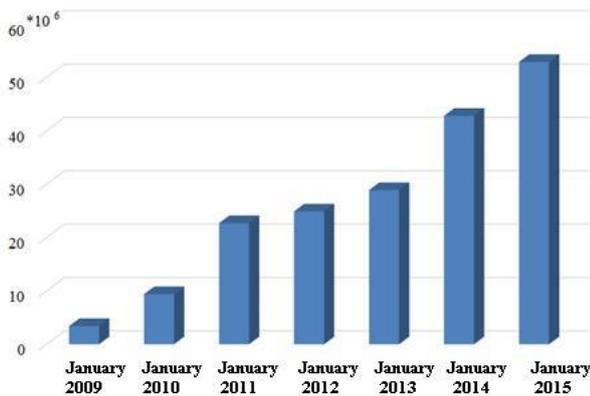


FIGURE 1 Dynamics of cyber incidents in CCS for the period from 2009 to 2015 (Sources: [1-3])

Growth of number of the fixed cyber threats, anomalies and cyber attacks become a powerful stimulus of development of research in the field of analysis and synthesis of various detection systems and detection of anomalies and cyber attacks.

Rather large numbers of works for the last decade are devoted, also to the problems of the development of intelligent intrusion detection systems (IDS). In particular, in works [5-7] presented reviews of anomaly detection methods, offered the principles of classification detection methods based on machine training and the statistical analysis. Overview of modern methods of machine training for systems to detect of cyber attacks (SDCA) is rather fully presented in works [8-10]. However, beyond these publications were some techniques such as k-average method [11] and its modifications [12, 13]. Methods for detection of cyber attacks based on finite state machine (FSM) are rather in detail stated in works [14-16]. Another perspective direction of development of adaptive systems of recognition cyber attacks (ASRCA) is a direction connected with the detection of abuse based on CCS states [17-19].

In work [20] considered a possibility of using in ASRCA IDA-splines, allow to build accurate approximation of behavior of the normal user or attacker on the set parameters.

Methods of computational intelligence, in particular, neural networks (NN) for problems of detection of cyber attacks are described in works [21, 22]. In [17, 23] describes the models and methods of adaptation of genetic algorithms

for the detection of the problem of cyber attacks. In works [24, 25] computing immune system, which can be used for the task of building ASRCA are described.

Typical disadvantage of most SDCA described in [17, 18, 21] works - erroneous operation during recognition. This is in particular due to the use, in most existing systems, a technology for detecting (identifying attacks). According to many authors [19, 20, 24, 25], the most perspective direction of development of cyber attacks and anomalies detection methods is to associate existing approaches in adaptive or hybrid SDCA with the ability to self-training.

Among the methods that are used in SDCA, researchers have identified the following areas: 1) the detection of anomalies in the system (anomaly detection system - ADS); 2) detection of abuses [5, 6, 22]. In works [9, 18] examined the peculiarities of SDCA, which used different methods and models. Applied aspects of commercial SDCA - IDES, NIDES, EMERLAND, JiNao, HayStack, etc., are considered in works [22, 23].

Anomalies detection methods (ADM), offer an opportunity for defense to perform detection with a high degree of accuracy and to make an informed opinion about the cause of changes in the state CCS. To create ADM decided to use: 1) controlled training; 2) uncontrolled training [5, 17]. The difference between the approaches is that the discrete set of features used in a controlled learning and training duration is determined previously. For uncontrolled training set of features usually change over time, and training can continue with the improvement of the system. Today, only a controlled training is used in commercial IDS [24].

Most modern SDCA and ADS based on models and methodologies which founded in pattern recognition theory [26-29]. In accordance with the basic principles of this theory to detect anomalies or cyber attacks, it is necessary to form an image of normal and abnormal behavior of CCS, for example, using expert assessment. So formed image, can be described as a set of values of the evaluation parameters i.e. signs, for convenience will be applied binary forms of describing features that are stored in the repository. If the image changes at some point of time, we can talk about abnormal functioning of the system. After, the anomaly or a cyber attack identified, and also assessed the degree of risk for functional tasks CCS, SDCA or ADS gives a conclusion on the possible cause of the changes. Thus, it is possible one of the following options for this conclusion: the change of state CCS - the result of cyber attacks; change of state - tolerance.

The difficulty in implementing of existing models of SDCA formalized device of recognition theory lays on that a particular informative complex for CCS often including unique software and information files, as well as its own IS subsystem which consists of heterogeneous components. However, carried out within this research, a specification of problems of cyber attacks recognition and application of models, which can to minimize the amount of training samples in the form of matrix signs, as well as elementary classifiers for each simulated class of cyber attacks, will optimize the work SDCA.

### 4 The use of adaptive regression splines in the intellectual system of cyber defense

Modern cyber attacks have become extremely complex.

Narrowly focused, systematic and specialized (targeted) attacks, able to hide from anti-virus systems, and are not always detected by firewalls and intrusion detection systems. Thus, further research is needed, which directed to develop the methodological and theoretical bases of creation of adaptive capacity to learn cyber attacks recognition systems that include the various technologies of detection and recognition, Figure 2. Within this research will consider the ASRCA, based on two landmark detected threats, cyber attacks and anomalies. The first stage uses the methodology of statistical data processing, which used adaptive splines. And on the second stage of the work of ASRCA are involved logical procedures.

RandomForest algorithm and the use of multivariate adaptive regression splines (multivariate adaptive regression splines - MARS).

RandomForest [20, 22, 28, 29] algorithm - an algorithm of machine learning, the essence of which is to construct a plurality of decision trees for the training sample. Each decision tree is constructed independently of the other as follows:

- For the beginning of the training sample generates a random subsample with repetitions. This procedure called bagging (bootstrap aggregating or bagging);
- Constructed decision tree for classification under this sub-sample, wherein the L signs used a limited subspace signs  $l = \sqrt{L}$  ;
- Construction of decision tree extends to the complete exhaustion of the subsample. The procedure pruning branches (pruning) are not carried out;
- Classification of objects is realized by the majority sampling: every tree set of attributes classified object to one of the classes, and wins the class for which chose the largest number of trees;
- Optimal number of trees selected in such a way as to minimize the error of the classifier on the test sample. In case of default, minimized error evaluation indicators that were classified incorrectly and, as a result, were not included in the sample (out-of-bag).

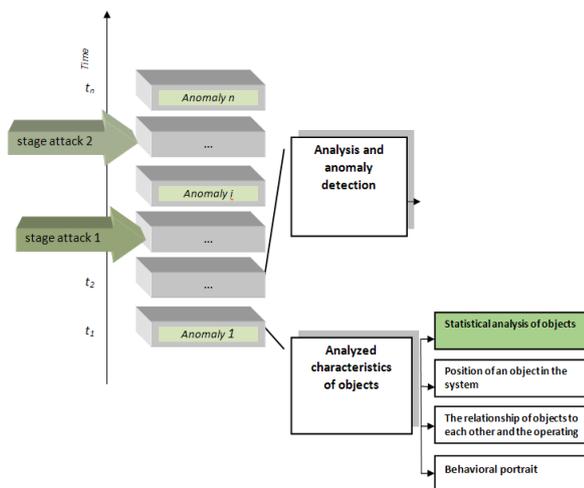


FIGURE 2 Scheme of work of multi-stage recognition adaptive system of threats, anomalies and cyber attacks

The main disadvantage of this method has high computational complexity of O (NP), where P is the number of trees. As a result of this method can be used for

vulnerability detection complex, but not for the problem of intrusion detection in real time.

Instead of decision trees, as a base model, we can use a variety of non-linear models, such as polynomial logistic regression [20] or multivariate adaptive regression splines (MARS).

The statistics of normal (or abnormal) activity are displayed in a sequence of vectors of this space. The task of MARS method is to construct the best approximation of conduct on the statistics in the given form of a training set of vectors, in this case as approximating functions used multivariate adaptive regression splines. Construction of MARS model comes in two approaches: forward and reverse. During the forward stroke criterion for adding vertices in the model the next step is optimal. Vertices to be added until the model reach the maximum level of complexity. In reverse stroke the course irrelevant peaks are removed from the model, leading to its simplification. Built spline is a "template" of attack or normal behavior of systems.

Suppose that a sample is set  $\{x_i; y_i\}$ ,  $i = \overline{1, N}$ , while the dependence between  $y_i$  and  $x_i$ , may be represented as

$$y_i = f(x_i) + \varepsilon, \tag{1}$$

where  $f(x)$  - unknown function,  $\varepsilon$  - approximation error.

MARS algorithm approximates the predicted value of the activity  $\tilde{f}$  in the form of an expansion in a row of basis functions

$$\tilde{f} = \alpha_0 + \sum_{k=1}^K \alpha_k F_k(x), \tag{2}$$

where  $\alpha_0$  - shift model;  $K$  - the number of basis functions;  $F_k$  and  $\alpha_k$  is k-th basis function and its coefficient [20].

Let  $\delta(y)$  - step function, defines a positive argument

$$\delta(y) = \begin{cases} 1, & \text{if } y \geq 0; \\ 0, & \text{if } y < 0. \end{cases} \tag{3}$$

In the one-dimensional case, the basis functions are selected piecewise-linear function of the form  $\delta(\pm(x-z))_+^r$ , where  $z$  - node coordinates;  $r \geq 0$  - the degree of the spline.

The simplest basis functions of MAR-spline order  $r = 1$  called reflected pairs. Often, these functions are in the form of

$$(x-z)_+ = \begin{cases} x-z, & \text{if } x \geq z, \\ 0, & \text{if } x < z; \end{cases} \tag{4}$$

$$(z-x)_+ = \begin{cases} z-x, & \text{if } x \leq z, \\ 0, & \text{if } x > z. \end{cases} \tag{5}$$

Example of reflexive pair is shown in Figure 3.

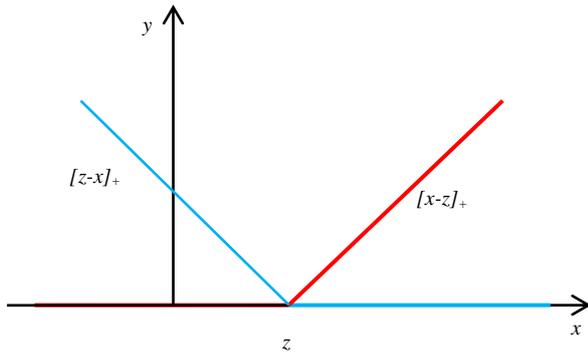


FIGURE 3 Schedule of basis functions of MAR-splines

In the multidimensional case the independent variable is a vector  $X = (x_1, x_2, \dots, x_i, \dots, x_s)$ . For each values  $x_i$  constructed reflective pairs with a node point  $z = x_{i,j}$ ,  $i = \overline{1, N}$ ,  $j = \overline{1, s}$ . According to the values of data can build a class of basic functions  $\Psi = \left\{ (x_j - z)_+^r; (z - x_j)_+^r \right\}$ ,  $z \in \{x_{1,j}; x_{2,j}; \dots; x_{N,j}\}_{j=1}^s$ .

As a result, the basis function  $F_k$  defined by an equation of the form

$$F_k(x) = \prod_{l=1}^{N_k} \delta \left[ \pm(x_{l,k} - z_{l,k}) \right]_+^r, \tag{6}$$

where  $N_k$  - number of functions in the class  $\Psi$ , which are part of  $k$ -th basis function,  $x_{l,k}$  - vector coordinate  $X$ , which is part of  $l$ -th linear function of  $k$ -th basic functions,  $z_{l,k}$  - the node that corresponds to  $x_{l,k}$ .

To construct the basis function  $F_k(x)$  can be used not only function in the class  $\Psi$ , but also functions that are derived from them. To find the coefficients  $\alpha_k$  can be used methods of discrepancy minimization, for example, discrete least squares method.

At the forward stroke MARS algorithm is finished. Next, you need to simplify this model by reducing the number of nodes. To do this, in every step of reverse stroke the node is removed, which the lack of that gives the smallest increase in the amount of residual squares.

The next stage of MARS algorithm has the choice of the optimal number of nodes that remain in the model of reverse stroke. To evaluate the value of the quantity  $K$  use a method of generalized cross-validation [5].

Let  $\tilde{f}_K$  - the function of optimal approximation values  $y_i$ .

We introduce the matrix  $F$  of dimension  $K \times N$  such that  $F_{ij} = F_i(x_j)$ .

$$T(K) = \text{tr}(F(F^T F)^{-1} F^T) + 1, \tag{7}$$

where  $\text{tr}(A)$  is the trace function of the matrix  $A$ .

$T(K)$  - the number of parameters, which is necessary to

determine, for its decision we can use the following equation

$$T(K) = q + aY, \tag{8}$$

where  $q$  - the number of basic linearly independent functions in the model,  $Y$  - the number of nodes that have been added to the model with the forward stroke,  $a$  - the parameter that shows estimates of optimization for each basis function.  $a$  parameter value are selected equally for two in adaptive model and  $a = 3$  for non-adaptive model.

Next, calculate the coefficient  $GCV$ , which is proportional to the mean square of residual.

$$GCV(K) = \frac{1}{N} \sum_{i=1}^N \frac{(y_i - \tilde{f}_K(x_i))^2}{\left(1 - \frac{T(K)}{N}\right)^2}. \tag{9}$$

Minimizing coefficient value  $GCV$  we find the optimal number of model nodes

$$K^* = \arg \min_K GCV. \tag{10}$$

Thus, in the first phase of the functioning ASRCA using the methodology of MARS allows to build the best approximation conduct on the given statistics of recognizing threats, anomalies, or cyber attacks in the form of a training set of vectors.

### 5 Using logical procedures in the adaptive system of cyber defense

The use of adaptive regression splines on the first stage of ASRCA allows to formulate a finite set of objects  $\{s_{a1}, \dots, s_{am}\}$ , which the analyst or system know to what classes of anomalies, attacks or threats they belong (it is precedents, i.e. the objects used for training – ITO). The next task of ASRCA is to identify a particular class of anomalies, threat or an object from a given set of features in the ITO values  $\{s_{ax1}, \dots, s_{axn}\}$ .

The use of the logical procedures in the second stage of ASRCA, makes it possible to obtain reliable results for situation, when there is no aprioristic information about the distribution function of the available values of threat, cyber attack or anomalies.

When using logical procedures of cyber attacks recognition (LPCAR), we will consider informative fragments which are found in the description of objects in one class of cyber-attacks, but absent in the descriptions of other classes.

In constructing LPCAR used so-called elementary classifiers (EC) [18, 28, 29]. EC is a fragment of a brief describing the object, and is used for training ASRCA. For these facilities (cyber threats, anomalies, vulnerabilities, etc.)  $(CT_1, \dots, CT_l)$  constructed the set of EC with predetermined properties.

Algorithms for synthesis of efficient implementations for LPCAR directly dependent on the success of the metric (quantitative) properties research of the set of informative fragments, i.e., signs of cyber attacks (cyber threats,

anomalies, vulnerabilities). It is necessary to turn the unclassified training matrix (UTM) as classified and in the learning mode to construct a clear partition space of recognition features to recognition of classes  $CT_m^0 | m = \overline{1, M}$ , where  $M$  - the power of alphabet classes.

Technically difficult implemented in ASRCA are the following problems. Determination of the asymptotic estimates of the number of deadlock coverings for integer matrix, containing signs of object recognition. Determination of the asymptotic evaluation of the permissible and maximum values of conjunctions of Boolean function, which can be applied to the synthesis circuit solutions of hardware ASRCA for the CCS.

In the article we consider the problem of constructing LPCAR based on the principle of "nonoccurrence" sets of permissible values of cyber attack signs (cyber threats, anomalies, vulnerabilities).

Let:  $RA$  - the number of possible targets attacking from the side of CCS;  $Q$  - total number of cyber threats to CCS;  $\{s_{ax1}, \dots, s_{axn}\}$  - the set of object attributes, such as threats, anomalies, cyber attacks, (signs for convenience represented in binary form);  $(CT_1, \dots, CT_l)$  - an integration of disjoint subsets (classes) of cyberthreats to CCS;  $B_s$  - the set of numbers of cyber threats, implemented by the attacker to reach of  $p_a$ -th goal of cyber attacks;  $NP_{s_a}$  - a valid set of discrete signs (threats, anomalies, cyber attacks etc.)  $\{s_{a1}, \dots, s_{a_{jQ}}\}$  typed.

An algorithm for calculating estimates (ACE) of the importance of a sign for ASRCA is possible as follows. In GIA features system select a set of the type of subsets  $NP_{s_a} = \{s_{aj1}, \dots, s_{ajQ}\}$ ,  $r_{p_a} \leq Q$ . Presume that selected subsets supporting for ACE. We will designate all their set -  $\Omega Q$ .

We define the following additional parameters:  $po_{ss_a}$  - the significance of the attack target (object)  $ss_{ai}$ ,  $i=1, 2, \dots, PA$ ;  $po_{NP_{s_a}}$  - the significance of an object of a basic set  $NP_{s_a} \in \Omega Q$ .

For each class of cyber attacks on CCS  $CT \in \{CT_1, \dots, CT_l\}$ , calculate the estimate  $E(ss_a, CT)$  of the object  $ss_a$  class TT, which has the form:

$$E(ss_a, CT) = \frac{1}{|LW_{CT}|} \sum_{ss_{ai} \in CT} \sum_{NP_{s_a} \in \Omega Q} po_{ss_a} \cdot po_{NP_{s_a}} \cdot BN, \quad (11)$$

where  $|LW_{CT}| = |CT \cap \{ss_{a1}, \dots, ss_{aQ}\}|$ ,  $BN$  - the proximity of objects  $ss'_a$  and  $ss''_a$ .

The object  $ss_{am}$  belongs to the class, possessing the highest ratings  $E(ss_a, CT)$ . If there is a set of similar classes, then the algorithm refuses the subsequent recognition. In order to increase the correctness of the algorithm is necessary to solve a system of inequalities:

$$\begin{aligned} E(ss_{a1}, CT_1) &> E(ss_{a1}, CT_2), \\ &\dots \\ E(ss_{aQ}, CT_l) &> E(ss_{aQ}, CT_{l+1}). \end{aligned} \quad (12)$$

To solve the system (12) is necessary to choose parameters  $po_{ss_{ai}}$   $i = 1, 2, \dots, PA$ , and  $po_{NP_{s_a}}, NP_{s_a} \in \Omega Q$ .

In a situation where the system is inconsistent, it is necessary to find the most compatible subsystem for it. Then, from the decision of this subsystem determine the values of  $po_{ss_{ai}}$  and  $po_{NP_{s_a}}$ .

An alternative way to increase a correctness of algorithm work is the way of a selection of reliable basic sets system for object recognition (anomalies, threats, vulnerabilities, and cyber attacks). For example, to choose a selection so that the condition for any ITO. In addition, for each GIA  $ss''_a \in CT$ ,  $E(ss''_a, CT) > 0$  inequality was carried out. This can be done as follows. Let  $NP_{s_a} = \{s_{aj1}, \dots, s_{ajQ}\}$  - support set. The set of attributes  $NP_{s_a}$  will be considered to satisfy the test requirements, if each GIA  $ss'_a, ss''_a$ , and thus belonging to different classes,  $BN(ss'_a, ss''_a, NP_{s_a}) = 0$  condition satisfied. Thus, our test - is a set (group) of signs on which only any two objects from different classes distinguish [29].

Denote as  $MC$  - plurality of EC, which were obtained from a set of attributes  $\{s_{ax1}, \dots, s_{axn}\}$ , i.e.  $MC = (\sigma_{DOP}, NP_{s_a})$ , where  $NP_{s_a} \subseteq \{s_{ax1}, \dots, s_{axn}\}$ ,  $\sigma_{DOP} = (\sigma_{DOP_1}, \dots, \sigma_{DOP_r})$ ,  $\sigma_{DOP_i} \in NP_{s_{aj}}$ , at  $i = 1, 2, \dots, r_{s_a}$ .

Suppose that a  $Z$  series of measurements of controlled features in CCS is carried out, and received the matrix by a sign

$$S = \begin{pmatrix} s_{ax11} & s_{ax12} & \dots & s_{ax1i} & \dots & s_{ax1n} \\ s_{ax21} & s_{ax22} & \dots & s_{ax2i} & \dots & s_{ax2n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ s_{axr1} & s_{axr2} & \dots & s_{axri} & \dots & s_{axrn} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ s_{axz1} & s_{axz2} & \dots & s_{axzi} & \dots & s_{axzn} \end{pmatrix}, \text{ for example,}$$

$$S = \begin{pmatrix} 0 & 1 & \dots & 1 & \dots & 1 \\ 1 & 0 & \dots & - & \dots & 1 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ - & 1 & \dots & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & \dots & - & \dots & 0 \end{pmatrix}.$$

Thus, a set of checked objects, belonging to the class is given the binary signs  $\{1001\dots-01\}$ . A dash indicates the uncertainty of feature in GIA.

Each algorithm used for recognition in CCS cyber attacks, threats, anomalies or CCS vulnerabilities within the class, denoted -  $AL$ . Then, for each class will be considered a subset of  $MC^{AL}(CT)$  from set  $MC$ .

Let  $MC^{AL} = \bigcup_{j=1}^l MC^{AL}(CT_j)$ . The object of analysis

$sp_{an}$  is based on determining the value  $BN(\sigma_{DOP}, ss_a, NP_{sa})$  of each element  $(\sigma_{DOP}, NP_{sa})$  of the set  $MC^{AL}(CT)$ ,  $CT \in \{CT_1, \dots, CT_l\}$ . In addition, for each element  $MC^{AL}(CT)$  is performed calculation assessment, which determines  $ss_a$  accessory of  $CT$  class. Each algorithm AL, in turn, is characterized by set of EC  $MC^{AL}(CT)$  and in the way of calculation of assessment  $E(ss_a, CT)$ .

The classifiers used in algorithms  $\sigma_{DOP} = (\sigma_{DOP_1}, \dots, \sigma_{DOP_r})$ , are formed informational signs from  $NP_{sa}$ . Wherein, each EC should have at least one of the properties listed below: 1) fragment groups  $(ss'_a, NP_{sa})$ , where  $ss'_a \in CT$ , coincides with  $\sigma_{DOP} = (\sigma_{DOP_1}, \dots, \sigma_{DOP_r})$ ; 2) only a part of the fragments  $(ss'_a, NP_{sa})$ , where  $ss'_a \in CT$  coincides with  $\sigma_{DOP} = (\sigma_{DOP_1}, \dots, \sigma_{DOP_r})$ ; 3) fragments of the group  $(ss'_a, NP_{sa})$ , where  $ss'_a \in CT$ , not match with  $\sigma_{DOP} = (\sigma_{DOP_1}, \dots, \sigma_{DOP_r})$ .

In models described in works [26, 29], the methodology of EC construction  $\sigma_{DOP_i}$  for a particular class of cyber attacks, threats, anomalies or CCS vulnerabilities, based on the synthesis of matrix covering  $\sigma_{DOP_i}$ , which is formed by GIA descriptions for CT. The use of such models [29] allow to reduce computing costs in work of algorithms in some ways, for example, when inequality is carried out  $|CT| < |\overline{CT}|$  (in particular, when a large number of classes of cyber attacks, threats, vulnerabilities or anomalies of CCS -  $(CT_1, \dots, CT_l) = (B_{s_{a1}}, \dots, B_{s_{al}})$ ).

We put the object in compliance EC -  $(\sigma_{DOP}, NP_{sa})$ , where  $\sigma_{DOP} = (\sigma_{DOP_1}, \dots, \sigma_{DOP_r})$ ,  $NP_{sa}$  - a set of signs with numbers  $j_1, \dots, j_{r_{sa}}$  elementary conjunction  $\mathfrak{R} = s_{axj_1}^{\sigma_{DOP_1}} \dots s_{axj_{r_{sa}}}^{\sigma_{DOP_{r_{sa}}}}$ . If  $ss_a = (\alpha_{s_{a1}}, \dots, \alpha_{s_{aQ}})$  - the object from a set of PA, therefore,  $BN(\sigma_{DOP}, ss_a, NP_{sa}) = 1$  in only case when  $(\alpha_{s_{a1}}, \dots, \alpha_{s_{aQ}}) \in NI_{\mathfrak{R}}$ , where  $NI_{\mathfrak{R}}$  - interval of the validity of elementary conjunction  $\mathfrak{R}$ .

During the creation of LPCAR, should be noted that the definition of the set of EC is reduced to finding the EC and permissible maximal conjunctions for the distinctive features of the object class (i.e., cyber threats, anomalies, cyber attacks, and so on). Moreover, this function is two-digit Boolean function that takes on different values of ITO from  $CT_l$  and  $\overline{CT_l}$ .

Then, an object recognition procedure  $ss_a = (\alpha_{s_{a1}}, \dots, \alpha_{s_{aQ}})$ , such as cyber attacks in SDCA is performed on the basis of the results of elementary

conjunctions  $\mathfrak{R}$  calculation. In the study, the results of which are described in works [29] proved that the most economical option is to use the algorithm for calculating the conjunctions to cover the corresponding object class (cyber threats, vulnerabilities or attack). Then, distinctive (characteristic) function of class  $CT_l$  - will be presented as a function of the algebraic logic (Boolean function)  $F_{KL}$ , which is equal to zero (0) on the informative descriptions of the object  $ss_{an} = (\alpha_{s_{an1}}, \dots, \alpha_{s_{anQ}})$  from  $CT_l$  and equal to one (1) on the remaining sets of signs from  $E_{CT}^Q$ . Where  $E_{CT}^Q$  is a set of signs, having a length  $r_{s_a}$ . Then, cover the class will correspond permissible for  $F_{\overline{CT}}$  conjunction. Maximum for the  $F_{\overline{CT}}$  conjunction corresponds to the deadlock cover. Acceptable  $\mathfrak{R}$  in matrices of attributes objects define the particular object  $ss_{an} = (\alpha_{s_{an1}}, \dots, \alpha_{s_{anQ}})$  belonging to the class  $CT_l$ , if the condition  $(\alpha_{s_{a1}}, \dots, \alpha_{s_{aQ}}) \notin NI_{\mathfrak{R}}$  performed.

In this case, getting the abbreviated disjunctive normal form (ADNF) of function reduces to finding ADNF for  $F_{CT}$ , which takes the value 0 on the sets from  $B_{F_{\overline{CT}}}$  and the value 1 on the remaining sets  $E_{CT}^Q$ . After getting ADNF for  $F_{\overline{CT}}$  conjunction  $\mathfrak{R}$  that do not possess  $NI_{\mathfrak{R}} \cap A_{F_{CT}} \neq 0$  property must be removed from it.

For example, to get logic function ADNF can be achieved by converting the conjunctive function of the form  $D_1 \wedge D_2 \wedge \dots \wedge D_u$ , where  $D_i = s_{ax1}^{\beta_{i1}} \vee s_{ax2}^{\beta_{i2}} \vee \dots \vee s_{axQ}^{\beta_{iQ}}$ ,  $i = 1, 2, \dots, mu$  realizes the function  $F_{CT}$ ,  $\beta_{iQ}$  - set of elements  $B_{F_{\overline{CT}}}$ .

Let:  $s_{ax}^\alpha = \bigvee_{\beta_i \neq \alpha_i} s_{ax}^\beta$ . Then conjunctive function takes

the form  $D_1^* \wedge D_2^* \wedge \dots \wedge D_u^*$ , where  $D_i^* = \bigvee_{t \neq \beta_{i1}} s_{ax1}^{\beta_{i1}} \vee \bigvee_{t \neq \beta_{i2}} s_{ax2}^{\beta_{i2}} \vee \dots \vee \bigvee_{t \neq \beta_{iQ}} s_{axQ}^{\beta_{iQ}}$ ,  $i = 1, 2, \dots, u$ .

During the recognition proximity of objects  $ss'_a = (\alpha'_{s_{a1}}, \dots, \alpha'_{s_{aQ}})$  and  $ss''_a = (\alpha''_{s_{a1}}, \dots, \alpha''_{s_{aQ}})$  from RA on a matrix of signs  $NP_{sa}$  was estimated by parameter

$$BN(ss'_a, ss''_a, NP_{sa}) = \begin{cases} 1, & \text{if } \alpha'_{s_{ai}} = \alpha''_{s_{ai}} \text{ at } ti = 1, 2, \dots, r_{s_a}, \\ 0 & \text{if else.} \end{cases} \quad (13)$$

Thus, obtaining LPCAR and a set of EC for the simulated class of objects (cyber threats, cyber attacks or anomalies) is as follows: 1) set the distinctive function; 2) find a DNF (or ADNF) that realizes this function; 3) find permissible (maximum) conjunction  $\mathfrak{R}$ , which defines the object belonging to the class.

To assess the effectiveness of the training algorithm ASRCA used informative criteria of functional efficiency (ICFE) index:

$$\bar{E}^* = (1/C) \cdot \sum_{c=1}^C \max_{\{w\}} E_c, \tag{14}$$

where  $E_c$  - ICFE value of ASRCA training for the implementation of the class of cyber threats, cyber attacks, or anomalies -  $CT_m^0$ ;  $\{w\}$  - a set of steps to study ASRCA.

Thus, as a result of research developed a method of intellectual detection of threat, anomaly and attack, the essence of which is to determine the conjunctions for coverings class of object recognition, and which differs from the existing use of adaptive regression splines on the first stage of the statistical analysis of anomalies in CCS, as well as the application of the second stage of discrete treatments using the apparatus of logic functions and matrix signs and elementary classifiers of object recognition, which will allow to create effective analytical, hardware and software solutions for adaptive systems cyber defense of CCS.

**6 The simulation results**

The results obtained in the simulations led to make a conclusion that objects belonging to different classes of anomalies, threats or cyber attacks is often difficult to separate from each other. Quite number of features (for some classes of cyber attacks to 50%) have a weight of information [29] is almost equal to 0. In the case of using a set of attributes for the formation of GIA is advisable to waive the requirement of its deadlock. This is done to increase the speed of algorithm work. For example, in case of increasing the number of features from 3 to 6, the average number of inspections on the object was from 150 to 800, respectively. The use of representative sets with length 3-5 in GIA matrices allows achieving maximum effectiveness of the algorithm recognition works for the majority of the known anomalies, cyber attacks and threats. In a situation if the features of object class (e.g., cyber attacks) arranged with decreasing informational content, there is a set of features with a large informational content for each object (I) [29], and then, the information content of the group

gradually decreased, Figure 4.

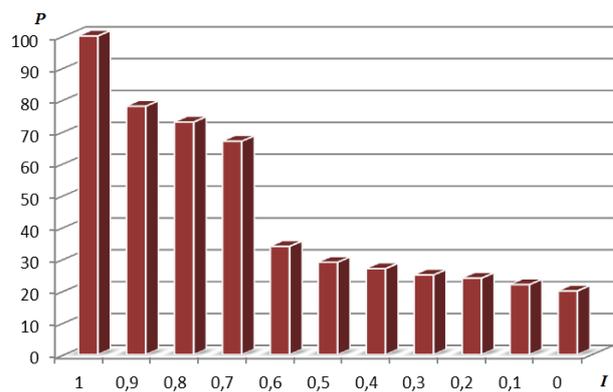


FIGURE 4 Visualize the importance of signs in a training matrix of GIA for network attacks

Thus interesting feature of the matrixes which forming GIA has been revealed, the informative content of control set for some classes of the attacks, for example, Dos/DDos, U2R, R2L or cyber attacks to the GPS system, several times greater than the weight of features forming this set. Thus the level of cyber attack recognition for which GIA training matrix were composed ranged from 25% to 30% for 2 features, 85-87% for 3-5 features, 92-98% for 6-9 features, Figure 5.

In this way GIA described by fragments of 3-4 features, belonging to different object classes is better characterized analyzed class than each of the features separately.

During the studies carried out comparison of the effectiveness of the proposed model by criteria - the average number of rules for training, Table 1.

The information about features of object recognition (cyber attacks) was adopted on the data from different sources (sensors) of software and hardware CCS. In particular, discussed the reports about the attacks generated by complex antiviral agents; analyzed log files, dumps of access memory AWP and PC, reports on the hard disk works, login logs into the system, database queries, etc. Some signs of attack are accepted on works [30, 31].

TABLE 1 The average number of rules, matrices and ASRCA training steps for the recognition of typical classes of cyber attacks in CCS

Object Class Recognition (Cyber attacks)  (According to:: [1, 2, 15, 24, 28, 29])	Number of features (features and their informative content on works [29, 30, 31])	The average number of rules, matrices and steps for learning object (Rules / Matrix / learning steps)		
		Models and algorithms for sequential sorting features [10, 12, 16, 24]	Statistical Forecasting model [16, 18, 24]	A model based on the MARS, training samples and EC Class
Network attacks through the corporate system	11	200/30/2000	350/65/2000	60/10/2000
Attacks on standard software components of software CCS	19	350/50/3500	450/35/3500	30/15/1500
Network investigation	15	320/40/2500	120/30/2500	70/20/2000
Attacks aimed at the selection of passwords	12	230/15/1500	180/25/1300	25/20/1500
Attacks such as Man-in-the-Middle	9	300/40/4000	350/30/3000	40/20/2000
DoS/DDoS attacks	9	150/25/2500	170/25/2000	30/15/1500
Virus attacks	21	400/50/2700	400/60/2500	35/25/1700
Attacks on the ERP system through a HARD protocol	5	170/30/2700	210/50/2300	60/35/1900
Attacks on the LAN components	9	260/25/2400	200/40/2500	45/35/2000
Attacks SCADA systems	7	600/70/4000	800/60/3000	150/50/3500
Attacks on the HMI	3	500/50/3000	400/60/3000	70/30/2600
Node substitution attacks ("funnel attack")	15	150/35/1500	100/55/1500	30/15/1500
Compromise of knot of data collection	5	250/30/1700	190/35/1800	30/20/1300
Substitution of the router	11	300/40/2300	380/60/2500	35/20/1700
Removing the data from peripherals	15	150/25/1500	75/20/1400	45/10/1000
Attacks on the satellite navigation system	9	90/30/4000	150/50/4000	20/15/1500

Figure 5 shows a histogram according to the maximum value of ICFE for the matrix dictionary of signs of anomalies and cyber attacks on the amount of learning algorithm steps ASRCA -  $\{w\}$ . Figure 6 shows the dependence of ICFE on the number of steps used for learning ASRCA.

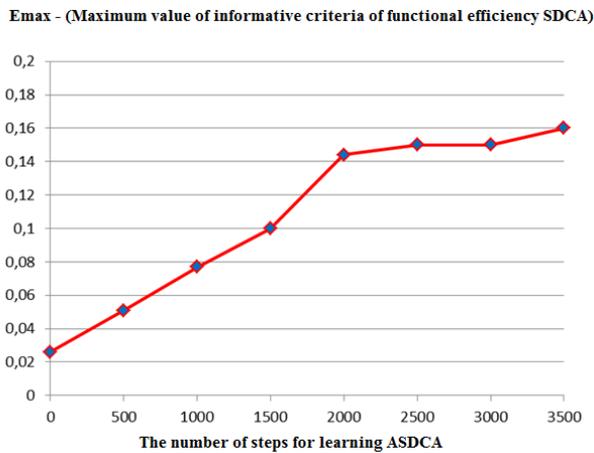


FIGURE 5 Dependence of the maximum value of ICFE for the matrix dictionary of signs of anomalies and cyber attacks on the amount of learning algorithm steps ASRCA

Analysis of the results shown in Figures 5 and 6, led to make a conclusion that quite effective in ASRCA is the use of algorithms with 4-10 features to train the system. In this case, ICFE reaches the maximum value, which gives grounds to speak about the possibility of constructing unmistakable

decision rules and signs of matrices to recognize threats, cyber attacks and anomalies within the class.

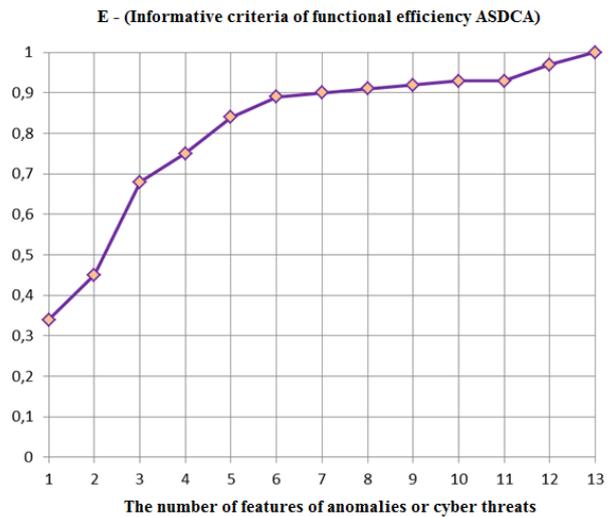


FIGURE 6 Schedule of the dependence of ICFE on the number of steps used for learning ASRCA

If in the algorithm recognition use representative sets of features of greater length ( $s_{axi} > 5$ ), the efficiency of the algorithm provided the same. When using a representative set of features at the reduced length the effectiveness of the algorithm is decreased. To test the effectiveness of proposed model is performed a series of experiments for the major attacks shown in Table 1. Examples of test for attacks aimed at SCADA system shown in Figure 7.

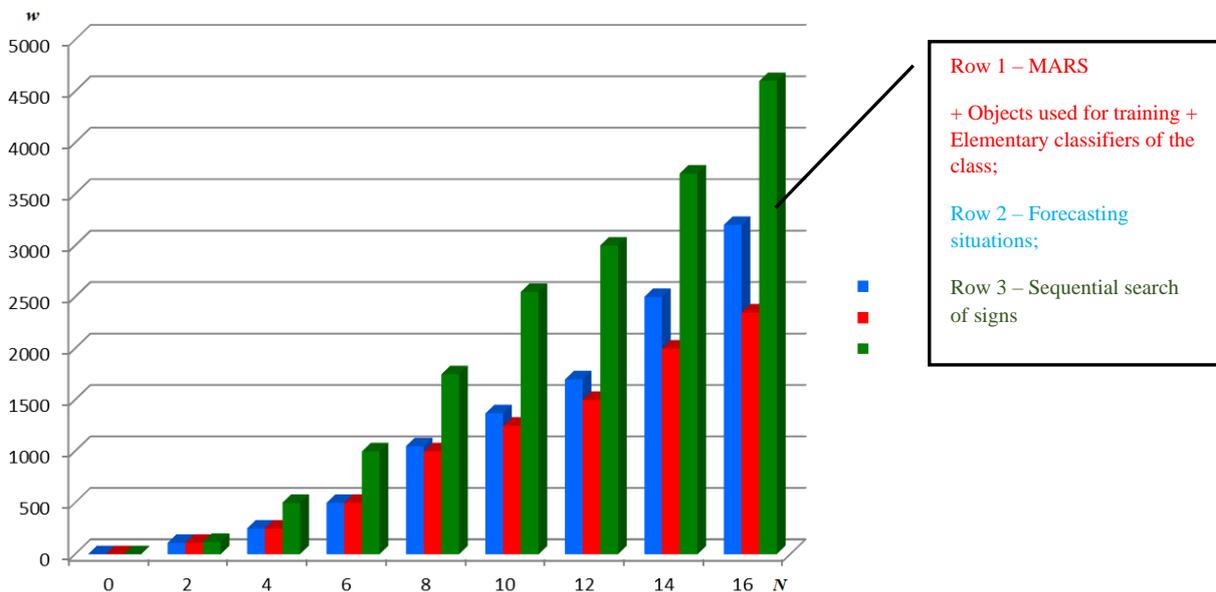


FIGURE 7 Comparative effectiveness of the proposed model for the recognition of attacks on SCADA system (N - number of signs; w - number of steps for learning ASRCA)

Compared to commonly used in ASRCA by sequential sorting features methods and statistical algorithms states, the use of models based on training samples and EC class allow to reduce the amount of required object recognition rules within the class of 2.5-10 times (depending on the class of objects - anomalies, cyber attacks, threats), and thus significantly reduce

the time recognition of anomalies, cyber attacks or threats. In the test training mode of ASRCA for the proposed model is a rational number of training steps of GIA made  $w \approx 3000$  for known classes of objects, and  $w \approx 3500...4500$  for more complex cyber attacks and anomalies.

## 7 Discussion of test results model and the prospects for further research

Difficulties of learning of ASRCA with the use of the device of adaptive regression splines, logic functions and elementary classifiers, exclusively associated with the stage of obtaining the disjunctive normal form (DNF) from maximal conjunctions of distinctive functions for each of the classes. However, the developed model compared with the results obtained for the models discussed in section 3, on the basis of finite automation [14-16], random sampling [4, 9], Bayesian networks, neural networks [21, 22], provide significantly a smaller number of relevant features for classifying threats, while reducing the time of ASRCA training.

At this stage of research, testing model made only for certain classes of anomalies, threats to information security and cyber-attacks. This is a definite disadvantage of the work.

Thus, the prospects for further research is to improve the knowledge base signs in the form of their matrix representation, as well as to conduct research model on a larger number of objects stored in the repository of ASRCA.

## References

- [1] 2015 Cyber Attacks Statistics (2016). Available at: <http://www.hackmageddon.com/2016/01/11/2015-cyber-attacks-statistics/>
- [2] Cyber Attacks Statistics. Available at: Available at: [https://securelist.ru/files/2015/12/KSB\\_2015\\_Stats\\_FINAL\\_RU.pdf](https://securelist.ru/files/2015/12/KSB_2015_Stats_FINAL_RU.pdf)
- [3] MITRE Research Program. Available at: <http://www.mitre.org>
- [4] Raiyn J 2014 A survey of Cyber Attack Detection Strategies *International Journal of Security and Its Applications* **8**(1) 247–56 doi: /10.14257/ijssia.2014.8.1.23
- [5] Jyothshna V, Prasad Rama V V 2011 A review of anomaly based intrusion detection systems *International Journal of Computer Applications* **28**(7) 26–35 DOI: 10.5120/3399-4730
- [6] Baddar S A-H, Merlo A, Migliardi M 2014 Anomaly detection in computer networks: a state-of-the-art review *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* **5**(4) 29–64
- [7] Gyanchandani M, Rana J., Yadav R N 2012 Taxonomy of anomaly based intrusion detection system: a review *International journal of scientific and research publications* **2**(12) 1–13 ISSN 2250-3153
- [8] Vinchurkar D P, Reshamwala A 2012 A review of intrusion detection system using neural network and machine learning technique *International Journal of Engineering Science and Innovative Technology (IJESIT)* **1**(2) 54–63 ISSN: 2319-5967
- [9] Tsai C-F, Hsub Y-F, Linc C-Y, Lin W-Y 2009 Intrusion detection by machine learning: a review *Expert Systems with Applications* **36**(10) 11994–2000 doi: 10.1016/j.eswa.2009.05.029
- [10] Omar S, Ngadi A, Jebur H H 2013 Machine learning techniques for anomaly detection: an overview *International journal of computer applications* **79**(2) 33–41 doi:10.5120/13715-1478
- [11] Riadi I, Istiyanto J E, Ashari A, Subanar 2013 Log analysis techniques using clustering in network forensics *International journal of computer science and information security* **10**(7) 1–7
- [12] Ranjan R, Sahoo G 2014 A new clustering approach for anomaly intrusion detection *International journal of data mining knowledge management process (IJDKP)* **4**(2) 29–38 DOI: 10.5121/ijdkp.2014.4.203
- [13] Guan Y, Ghorbani A A, Belacel N 2003 Y-means: a clustering method for intrusion detection *In canadian conference on electrical and computer engineering* **2** 1083–6 DOI: 10.1109/CCECE.2003.1226084
- [14] Li W, Yi P, Wu Y, Pan L, Li J 2014 A new intrusion detection system based on knn classification algorithm in wireless sensor network *Journal of electrical and computer engineering* **2014** DOI: 10.1155/2014/240217
- [15] Ilgun K, Kemmerer R A, Porras P A 1995 State transition analysis: a rule-based intrusion detection approach *IEEE transactions on software engineering* **21**(3) 181–99
- [16] Khan L, Awad M, Thuraisingham B 2007 A new intrusion detection system using support vector machines and hierarchical clustering *The international journal on very large data bases* **16**(4) 507–21 doi: 10.1007/s00778-006-0002-5
- [17] Wu S X, Banzhaf W 2010 The use of computational intelligence in intrusion detection systems: a review *Applied soft computing* **10**(1) 1–35 doi: 10.1016/j.asoc.2009.06.019
- [18] Kabiri P, Ghorbani A A 2005 Research on intrusion detection and response: a survey *International journal of network security* **1**(2) 84–102
- [19] Ameziane El Hassani A, Abou El Kalam A, Bouhoula A, Abassi R, Ait Ouahman A 2014 Integrity-OrBAC: a new model to preserve Critical Infrastructures integrity *International journal of information security* **14**(4) 367–85 doi: 10.1007/s10207-014-0254-9
- [20] Mukkamala S, Sung A H, Abraham A, Ramos V 2006 Intrusion detection systems using adaptive regression splines *Sixth international conference on enterprise information systems Part 3* 211–8 DOI:10.1007/1-4020-3675-2\_25
- [21] Al-Jarrah O, Arafat A 2014 Network Intrusion Detection System using attack behavior classification *Information and communication systems (ICICS) 5th International Conference* 1–6 DOI: 10.1109/IACS.2014.6841978
- [22] Selim S, Hashem M, Nazmy T M 2010 Detection using multi-stage neural network *International journal of computer science and information security (IJCSIS)* **8**(4) 14–20
- [23] Pawar S N 2013 Intrusion detection in computer network using genetic algorithm approach: a survey *International journal of advances in engineering technology* **6**(2) 730–6
- [24] Zhou Y P 2009 Hybrid Model Based on Artificial Immune System and PCA Neural Networks for Intrusion Detection. *Asia-Pacific Conference on Information Processing* **1** 21-4 DOI: 10.1109/APCIP.2009.13
- [25] Komar M, Golovko V, Sachenko A, Bezobrazov S 2013 Development of neural network immune detectors for computer attacks recognition and classification *IEEE 7th Intern. Conf. on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS)* **2** 665–8 DOI: 10.1109/IDAACS.2013.6663008

## 8 Conclusions

During the research, the results which are presented in the article:

Developed recognition model of cyber attacks, anomalies and threats to critical computer systems, which is based on the use of cyber defense of adaptive regression splines in intelligent systems, training samples in the form of a matrix signs and elementary classifiers for each of the modeled classes;

Performed a study on minimizing the number of training samples of recognizing signs. It is shown that for the recognition of objects within the known class of cyber threats, attacks and anomalies, the use of training matrices of GIA representative sets with length 3-5 features allows to achieve maximum efficiency of the algorithm, reaching up to 98%. Compared to commonly used in ASRCA by sequential sorting features methods and statistical algorithms states, the use of models based on training samples and EC class allowed to reduce the amount of required object recognition rules within the class of 2.5-10 times.

- [26] Zhan Z, Xu M, Xu S 2013 Characterizing honeypot-captured cyber attacks: statistical framework and case study *IEEE transactions on information forensics and security* **8**(11) 1775–89 DOI: 10.1109/TIFS.2013.2279800
- [27] Bartosz Jasiul, Marcin Szpyrka, Joanna Śliwa 2014 Detection and modeling of cyber attacks with petri nets *Entropy* **16**(12) 6602-23 doi: 10.3390/e16126602
- [28] Peddabachigari S, Abraham A, Grosan C, Thomas J 2007 Modeling intrusion detection system using hybrid intelligent systems *Journal of network and computer applications* **30**(1) 114–32 doi: 10.1016/j.jnca.2005.06.003
- [29] 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**, No 9(80): Information and controlling system 18–25 DOI: 10.15587/1729-4061.2016.66015
- [30] Rid T, Buchanana B 2015 Attributing cyber attacks *Journal of strategic studies* **38**(1–2) 4–37 DOI: 10.1080/01402390.2014.977382
- [31] Guitton C, Korzak E 2013 The sophistication criterion for attribution *The RUSI journal* **158**(4) 62–8 DOI: 10.1080/03071847.2013.826509

AUTHORS	
	<p><b>Beketova Gulzhanat</b></p> <p><b>Current position, grades:</b> PhD student of Kazakh National Technical University. (Kazakhstan)  <b>University studies:</b> Master degree in Computer Science  <b>Scientific interests:</b> Information security</p>
	<p><b>Akhmetov Bakhytzhan</b></p> <p><b>Current position, grades:</b> professor of Kazakh National Research Technical University after K.I.Satpayev, Doctor of Technical Sciences. (Kazakhstan)</p>
	<p><b>Oleksandr Korchenko</b></p> <p><b>Current position, grades:</b> professor of National Aviation University, Doctor of Technical Sciences (Ukraine)</p>
	<p><b>Lakhno Valery</b></p> <p><b>Current position, grades:</b> associate professor of European University, Doctor of Technical Sciences (Ukraine)</p>
	<p><b>Tereshuk Anna</b></p> <p><b>Current position, grades:</b> Senior lecturer of Department of Information Systems and Mathematical Disciplines, European University(Ukraine)</p>