UDC 004.056
DOI: 10.15587/1729-4061.2016.85600

DEVELOPMENT OF ADAPTIVE EXPERT SYSTEM OF INFORMATION SECURITY USING A PROCEDURE OF CLUSTERING THE ATTRIBUTES OF ANOMALIES AND CYBER ATTACKS

V. Lakhno
Doctor of Technical Science, Associate Professor
Department of Managing Information Security
European University
Academician Vernadskiy blvd., 16B, Kyiv, Ukraine, 03115
E-mail: lva964@gmail.com

Y. Tkach
PhD, Associate Professor*
E-mail: tkach_ym@ukr.net

T. Petrenko
Senior Lecturer*
E-mail: mail_taras@ukr.net

S. Zaitsev
Doctor of Technical Science, Associate Professor**
E-mail: serza1979@gmail.com

V. Bazylevych
PhD, Associate Professor*
E-mail: bazvlamar@gmail.com

*Department of Cybersecurity and Mathematical Simulation***
Department of Information and Computer Systems*
***Chernihiv National University of Technology
Shevchenka str., 95, Chernihiv, Ukraine, 14027

Запропоновано структурну схему здатної до самонавчання адаптивної експертної системи з інформаційної безпеки. Розроблена модель визначення інформаційного показника функціональної результативності, яка ґрунтується на ентропійному та інформаційно-дистанційному критерії Кульбака-Лейблера при кластеризації ознак загроз, аномалій та кібератак, що дозволяє скласти коректні вирішальні правила розпізнавання. Проведені тестові дослідження адаптивної експертної системи та порівняльний аналіз із існуючими методами та моделями, які використовуються у інтелектуальних системах розпізнавання кіберзагроз

Ключові слова: розпізнавання кібератак, експертна система, кластеризація ознак, функціональна результативність навчання

Предложена структурная схема самообучающейся адаптивной экспертной системы по информационной безопасности. Разработана модель для определения информационного показателя функциональной результативности, основанная на энтропийном и информационно-дистанционном критерии Кульбака-Лейблера при кластеризации признаков угроз, аномалий и кибератак, позволяющая составить корректные решающие правила процедуры распознавания. Выполнены тестовые исследования адаптивной экспертной системы и сравнительный анализ с существующими методами и моделями, используемыми в интеллектуальных системах распознавания киберугроз

Ключевые слова: распознавание кибератак, экспертная система, кластеризация признаков, функциональная результативность обучения

1. Introduction

Over the last decades one of the most urgent problems of society has been information security (IS) and its component – cyber security (CS), on which, in particular, is dependent the functioning of all modern computer systems (CoS) in industry, energy, communication, transport, etc. As the experience of recent years demonstrates, cybercriminals are increasingly using unique, not yet known for the IT-industry, malware, vulnerabilities and ways of cyber-attacks. Resisting a constant growth in the quantity and complexity of destructive effects on CoS is possible, using in particular adaptive inteligent systems of recognition of cyber threats (SIRCT). The term "adaptation" for SIRCT may be interpreted as a process of purposeful change of the structure of algorithm or system parameters in order to improve the efficiency of its functioning.

The relevance of the work is in the creation and examination of adaptive expert system (AES) of recognition of complicated anomalies and cyber-attacks. The system under design is based on the models and intelligent technologies of learning and makes it possible to increase the probability of detecting sophisticated targeted cyber-attacks.

2. Literature review and problem statement

The growing interest to investigating the topics of CS and IS has lead in the last decade to a surge of research into development of effective systems of detection and prevention of cyber threats. In particular, there has been quite a number of publications devoted to the synthesis of SIRCT based on the theory of finite automata [1], the theory of machine learning [2, 3], neural networks [4, 5], Bayesian networks [6], genetic algorithms [7], fuzzy logic [8], statistical data analysis [9]. But the majority of existing articles, devoted to the problem of recognition of CT, address only the basic features of cyber-attacks that, in particular, is due to the complexity of determining information distance between individual features. Papers [10, 11] propose to solve this task by applying preliminary clustering of features. As a measure of the closeness of objects in the process of clustering, the Bayesian information criterion is used [12], or the Kullback-Leibler divergence [13, 14]. But, to our regret, the authors examined cyber attacks of a certain class only that narrows the scope of application of the proposed models in contemporary intelligent systems of recognition of cyber attacks.

Many authors point out prospects of research related to the use in the CS tasks of different intelligent systems and technologies (IST). In particular, it is proposed to use the potential of the following systems: expert (ES) [15, 16]; decision making support [17, 18], adaptive [19, 20]. Such systems are still under development, and, unfortunately, the majority of papers on this topic do not include consideration of the question of evaluation of errors of the third kind, which may arise when the SIRCT models do not take into account certain recognition procedures. In addition, it should be noted that the procedure for splitting the set (space) of attributes that are considered in SIRCT is not the same for different CoS, dictated by the specifics of their performance and functional tasks.

Numerous discussions and publications [16, 17, 19, 21, 22], dealing with designing the criteria for splitting the set of attributes and evaluation of effectiveness, ES with CS, as well as the use of a variety of methods in SIRCT point to the fact that there is a need to create a model for the identification of information indicator of functional performance (IIFP) of AES learning, which takes into account the known statistical and deterministic optimization parameters when clustering the attributes of illegal activity of cyber-criminals in CoS.

3. The aim and tasks of the study

The aim of the work is to design a model for determining information indicator of functional performance of training ES with CS. The model takes into account the known statistical and distance clustering parameters for attributes of cyber threats, anomalies and cyber attacks, as well as errors of the third kind during procedure of ES machine learning.

To achieve the aim, the following tasks are to be solved:

– to develop a structural scheme of adaptive expert system (AES) with CS;

– to design a model for evaluation of functional effectiveness of the process of machine training of adaptive expert system of information security, which is based on the entropic and information-distance criterion of Kullback-Leibler when clustering the attributes of threats, anomalies and cyber attacks in CoS;

– to conduct AES testing and determine rational number of clusters in the space of attributes of anomalies or cyber attacks for CoS.

4. Structural scheme of adaptive expert system of information security

Construction of structural model of AES with IS is a part of a large-scale process of intelligent analysis and data processing in SIRCT.

To provide for highly reliable data processing in CoS under conditions of increasing number of destructive influences, in particular cyber attacks, it is necessary to find:

$$SI^{*}= \\ =\operatorname{Arg}\max_{CO^{ad}\in CO,CM^{ad}\in CM,ME^{ad}\in ME} SI\left[\left(CO^{ad},CM^{ad},ME^{ad}\right)\right]|\,\Lambda, \quad (1)$$

where CO^{ad} are the permissible parameters of the regulation of CoS; CM^{ad} are the permissible for possible application methods and models for resisting threats and cyber attacks based on SIRCT; ME^{ad} are the permissible for possible application means for prevention, detection and analysis of cyber attacks; Λ are the restrictions on the parameters that affect the efficiency of AES as a part of SIRCT (potentially vulnerable sections of CoS, the time period of cyber attacks activity, the cost of protection tools, etc.).

Within the framework of IIT, which are used for training the CS systems, the main objective of AES is a result-oriented procedure of the transformation of fuzzy splitting of the sets of attributes of anomalies, threats and cyber attacks to a clear-cut breakdown of classes of the objects of recognition (OR) [23–25]. This is achieved by using the iterative procedure, which allows optimization of the parameters of AES operation in the tasks of supporting high level of CoS IS. The training process takes place in two stages:

– the first stage implies purposeful search for global maximum value of the objective function with many extrema for statistical representation of IIFP in the working area of the OR attributes;

– the second stage allows determination and simultaneous renewal of optimal separate hypersurfaces [10, 13, 14, 23, 25], which were built in the binary space of recognition attributes (BSRA – RS) of anomalies, threats and cyber attacks.

Input fuzzy separation of implementations of the objects that are used during training are transformed into a clear division during optimization of testing permissible deviations on each class of anomalies, threats or cyber attacks [17, 19, 24, 25]. The result is a purposeful change in the values of RS in AES for the defined objects and construction of correct decisive rules by the multidimensional binary training matrix (MBTM). This allows, within the framework of IIT, combining the process of correction of the objects that are used for training (OUT) and the stage of learning itself. During the latter stage, the synthesis of correct decisive rules takes place.

A solution of the task on formation of the input symbol description of AES as a part of SIRCT is to create OUT, for example, in the form of a multidimensional learning matrix of attributes (MLMA) – learning matrix:

$$\left\| lm_{m,i}^{(j)} \mid m=\overline{1,M}; i=\overline{1,N}, j=\overline{1,n} \right\|.$$

In this case, it is necessary to solve the following tasks:

1) to form a glossary of attributes for each class of anomalies, cyber threats and attacks, as well as alphabet of classes in terms of OR;

2) to determine minimum level of representative training matrix for OUT;

3) to determine the normalized permissible deviations for RS.

As the primary attributes, one can use parameters which are read out of certain sensors or the experimental data obtained directly, for example, in the course of implementation of penetration tests in CoS.

As the secondary attributes to recognize anomalies, threats and cyber attacks, one can use a variety of statistical characteristics, for example, vectors of realization of a certain class $\{lm^{(j)}_{m,i} \mid i=\overline{1,N}\}$, a training sample $\{lm^{(j)}_{m,i} \mid j=\overline{1,n}\}$ for OUT, etc.

An alphabet of classes of OR for AES $\{lm^{o}_{m}\}$ is formed at the first stage by the developer of the system with involvement of specialists on IS.

At the second stage of the alphabet synthesis, using AES, the input data processing continues using the methods of clustering of the RS attributes.

As was previously demonstrated in articles [10, 14, 19], in the case of immutability in the glossary of attributes of OR and increase in the capacity of the alphabet, a change in the asymptotic characteristic of AES is possible. Accordingly, this factor may significantly affect functional effectiveness of the procedure of training similar systems. This, in particular, is due to the increasing degree of intersection of the classes of threats, anomalies and cyber attacks that are subject to recognition (later – objects of recognition or OR).

Let us formulate the following formalized statement of the problem of information synthesis of the AES elements. Suppose that we know the alphabet of classes $\left\{CT^{o}_{m} \mid m=\overline{1,M}\right\}$ and MBTM of OR which, accordingly, describes the m-th state, in which a CoS is. In this case, MBTM of OR for the class of recognition CT^{o}_{m} will take the following form:

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

In matrix (2) we adopted the following denotations: line of matrix – implementation of the "view" of OR

$$\left\{lm^{(j)}_{m,i} \mid i=\overline{1,N}\right\},$$

N is the number of attributes of OR; column – stochastic training sample

$$\left\{lm^{(j)}_{m,i} \mid j=\overline{1,n}\right\},$$

where n is the volume of the sample.

Fig. 1 demonstrates the process of formation of the structure of the training matrix, which in stages includes vectors of implementations

$$\left\{ct^{(j)}_{1}\right\} \in CT^{o}_{1} \text{ and } \left\{ct^{(j)}_{2}\right\} \in CT^{o}_{2},$$

respectively. To build such a matrix, it is necessary to define only meaningful properties of OR, which unequivocally distinguish one automatically found threat, anomaly or cyber attack within the class from another one. It is clear that for each AES, the classification of OR may be different. However, most of OR contain such properties as, for example, the type of vulnerability, protocol by which the vulnerability may be used, a channel of implementation within this protocol, the type of object, a path to the object, etc., Table 1.

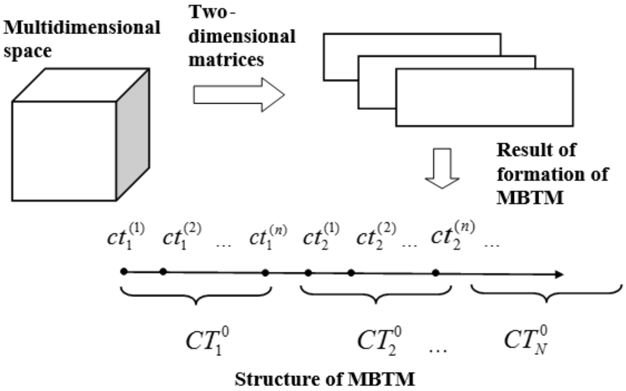

Multidimensional space
Two-dimensional matrices
Result of formation of MBTM
$ct_1^{(1)}$ $ct_1^{(2)}$ ... $ct_1^{(n)}$ $ct_2^{(1)}$ $ct_2^{(2)}$ ... $ct_2^{(n)}$ ...
CT_1^0 CT_2^0 ... CT_N^0
Structure of MBTM

Fig. 1. Scheme of work with a multidimensional information space of attributes for AES as a part of SIRCT

All of the possible values of each property of OR are possible to encode either in binary form [10, 19, 20, 23] or by using non–negative integers [7, 21, 22], where zero corresponds to an uncertain value of the property of OR. This allows us to take account of the missing, new or not yet predicted values of the OR property. More detailed results of research into the procedures of forming BSRA and binary training matrices (OUT) are represented in papers [23–25].

Table 1

An example of the formation of matrix of attributes

Threat	0	1	2	...
Type	Not known	SQL	XSS	...
Protocol	Not known	FTP	HTTP	...
Channel	Not known	Post	get	...
Object type	Not known	js	php	...
...				
Other	Not known	...	...	...

The attributes of cyber attacks are detected in a large volume of measured information, such as logs, data monitoring, etc. This, in turn, requires increasing the speed of information processing in SDI. Combining the data in compact clusters, it is possible to carry out the analysis of typical representatives of each cluster and make decisions about whether these data are an attribute of attack or not. Then this solution is transferred to all representatives of the examined cluster. This approach significantly reduces the volumes of information required for a successful attack classification (OUT).

Using the models for intelligent learning technologies (MILT), we will present IIFP of training AES as follows:

$$CE^{*}_{m} = \max_{IS} CE_{m}, \tag{3}$$

where CE_m are the IIFP procedures of machine training of AES as a part of SIRCT; IS are the permissible values of the CoS parameters.

Table 2 presents a list of the main data sources for AES and information that is subject to preliminary processing and analysis.

Fig. 2 demonstrates a functional scheme of AES as a part of SIRCT for CoS. For clarity, the scheme shows basic functional units and information flows, in particular, curly yellow arrows display relationships between functional modules of AES while normal arrows indicate control commands. Curly blue arrows show connections between the components of SIRCT and AES.

In the course of training AES and the formation of KB, the system's performance is regulated by a specialist on IS, who, in accordance with the recommendations of AES, forms the control commands (control commands) –

$$\left\{ CC\left\{ hy_m \right\} | \, m = \overline{1,M} \right\}.$$

Let us consider the procedure of functioning of AES as a SIRCT element in the mode of learning by a priori categorized training matrix (CTM). When a controlled process of learning is affected by stochastic factors rf(t) and arbitrary initial conditions of the formation of implementations

$$\left\{ ss^{(j)}, j = \overline{1,n} \right\}$$

of the functional state of CoS, in particular under conditions of cyber attacks, in the module of preliminary data processing (MPDP) there occurs the formation of classifying scale displaying the current implementation $ss^{(j)}$. This procedure aims at forming element $lm_m^{(j)}$, whose coordinates is the normalized results of monitoring of the CS state. In addition, MPDP checks statistical stability and uniformity of the training samples. It is based on the corresponding statistical criteria and minimal volume n_{min} of the representative learning sample. At the output of MPDP, a classified fuzzy learning matrix is formed, which is supplied to the input of the module of formation of binary vectors of recognition (MFBVR).

MFBVR performs binearization of vectors-implementations of the classes of OR by comparing the current attributes with their respective testing permissible deviations $\{ca_{K,i}\}$, which are contained in a database (DB) and determined based on the methods of multifractal analysis, the Hurst indicator, movable window, etc. [4, 9, 16, 19, 22]. Depending on the set mode, MFBVR creates a multidimensional binary vector (MBV), which is the parameter-implementation of the view of OR in AES. Each coordinate of MBV at algorithmic implementation of AES can be represented as a single predicate equal to "1" if the value of OR attribute belongs to the set of testing permissible deviations and is equal to "0" if it does not.

Table 2

List of main data sources for AES

Data source for building clusters	Information that is subject to processing and analysis
Log-files of working subsystems of CoS	Period and type of performed operations, essence of operations, password validity, failure to connect with remote machine, other
Network traffic	Load of network equipment, communication channels usage, network activity
Reference guides and journals of registration of users and events	ID-codes of users, password check, performed actions
List of functional tasks	Chains of interconnected tasks and processes
Access rights information	Compliance with guidelines of resources requests
Data on the performance of mailing system	Statistics, volume and addresses of sendings and mail in-coming messages, topics of messages
Test files	Content directions
Applied SW	Previous procedure of IS audit
Tables with attributes of performed files	Types of files, dates of creation and change, initiators of changes and their rights, control of immutability, addresses of reference modules, control sums
Other	Other sources

As a result, we will form in MFBVR a binary training matrix (BTM) –

$$\left\{ ct_m^{(j)} | \, j = \overline{1,M} \right\},$$

which consists of structured stochastic vectors–implementations of the representation of corresponding threat of anomalies or cyber attack:

$$ct_m^{(j)} = \left\langle ct_{m,1}^{(j)}, \ldots, ct_{m,i}^{(j)}, \ldots, ct_{m,N}^{(j)} \right\rangle. \quad (4)$$

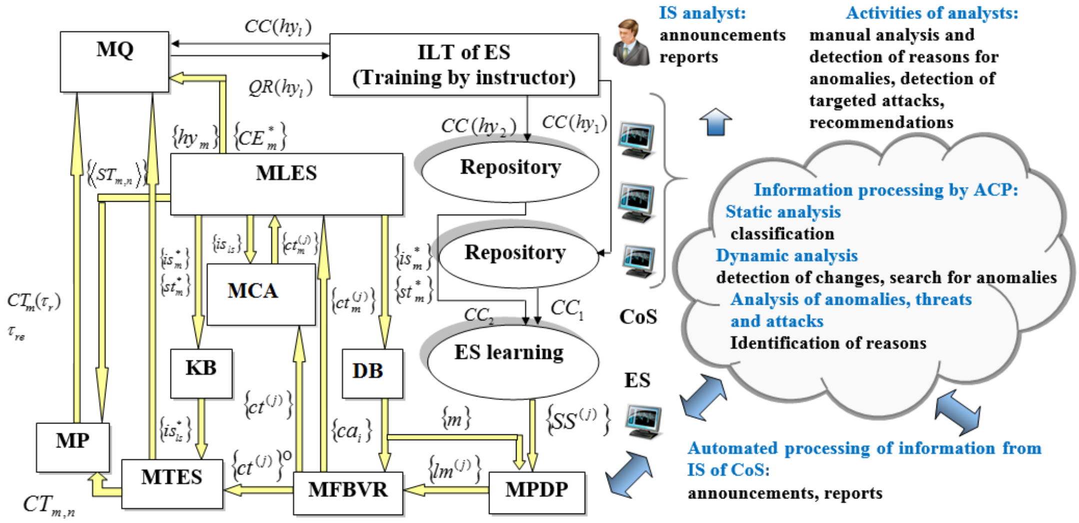


Fig. 2. Structural scheme of AES as a part of SIRCT

BTM is also used to assess the testing permissible deviations in the process of recognition (system of test/control permissible deviations – SCPD). SCPD

$$\left\{ca_{n,i} \mid i=\overline{1,N}\right\},$$

as well as parameters that determine levels of the sample $\{cl_m\}$ of coordinates of binary reference vectors of classes of OR, are entered into MFBVR from a database (DB).

In the mode of training AES, at the output of MFBVR during the period τ_{Bd}, MBTM

$$\left\{ct_m^{(j)} \mid m=\overline{1,M}; j=\overline{1,n_{\min}}\right\},$$

is created, which arrives at the input of the module "ES learning" (MLES). We will note that the formation of MBTM is performed by certain, predetermined in advance, confidence level [19, 21, 23–25].

At the output of MLES, in the knowledge base (KB) there enters the vector of optimal parameters (VOP) of AES performance:

$$\{is_k^*\}^O \mid k=\overline{1,O}; O=\overline{1,\Omega}\}, \qquad (5)$$

where O is the mapping of openness of the set, or, in the case of implementation of the procedure of recognition – a number of implementations of OR).

VOP provides for max value of IIFP of the AES learning in the permissible area of its determination. While testing AES, namely at the moment $\tau_{EC_{\max}}$ when $EC_m^*=\max$, the learning process for the recognition of implementation of class CT_m^0 stops. Also, for $\tau_{EC_{\max}}$, the current statistical parameters ST_m, which are the members of the corresponding variational series, are accepted as the extremum of functional distribution ST_m^*. In the AES testing mode, that is, while direct decision-making that allow recognition of threats, anomalies and sophisticated cyber attacks, from MFBVR to the module "Test" (MTES) the test matrix $\left\{ct^{(j)}\right\}^O$ is entered. At the same time, in MFBVR out of KB they find optimal values of the testing permissible deviations $\left\{ca_{K,i}^*\right\}$ and the levels of sample $\left\{sl_m^{(j)}\right\}$ for binary reference vectors of the OR classes. This allows us to ensure equivalent conditions for the formation of learning and examination matrices.

From the first output of MTES, IS analyst through the "Module of queries" (MQES) has a possibility to receive suspicions hy_m about membership of the corresponding state of CoS to the class CT_m^0 and, accordingly, to design adequate measures for responding to the arising threat, anomaly in behavior or a cyber attack.

In the cluster analysis mode (CA) of in-coming data to AES, and for solving the task of automating the procedure of forming the inbound classified learning matrix (ICLM or OUT), from MFBVR to the first input of MCA (module "cluster analysis" – MCA), a non-classified learning matrix (NLM) – $\{ct^{(j)}\}$ is supplied. NLM consists of implementations of all classes of OR and the appropriate alphabet.

CTM – $\left\{ct_m^o\right\}$, formed at each step of clustering of input data in AES, are delivered to the second input of the module MLES. Accordingly, this module is responsible for the process of assessment by IIFP the quality of the conducted clustering procedure and sends to the second input of MCA the values of parameters of clustering $\{is_k\}$ [14, 19].

Thus, the stage of CA of input data in AES and MILT is a part of the algorithm of operation of AES as part of SIRCT.

An important feature of AES with IS of CoS is the ability to predict the change in its functional efficiency in the process of recognition of OR, as well as to determine the moment when there is a need to re-train the system, for example, in cases when there are new, previously non-categorized, types of threats and cyber attacks. In this case, the first input of the module of prediction (MP) receives the current statistical data $ST_{m,n}$ that are processed by MTES. These data characterize statistical properties of binary examination matrix of class CT_m^o, which is defined by the corresponding decisive rules obtained in the course of AES training.

The second input of MP receives from KB a statistical array $\left\{<ST_m^*>\right\}$, which characterizes relevant statistical properties of the OR classes in the moment of the first training τ_1 of ES and has the property of invariance to the laws of probability distribution. The accuracy and reliability of prediction directly depends on the value of parameter $CE_m^*(\tau_r)$. received in the ES learning process in the moment of prediction τ_r.

The considered structure of AES is different from the existing ones by broad functional capabilities and allows dealing with complicated tasks of ensuring reliable cyber protection of CoS both with created KB for the known classes of OR and in the course of machine learning, in the case there are new, previously unknown, classed of cyber attacks.

5. A model for evaluation of functional effectiveness of the process of machine learning of adaptive expert system of information security

In the process of development of AES as a part of SIRCT, there is always a question about the assessment of functional efficiency of the process of machine learning. In particular, this makes it possible to define the maximum asymptotic reliability of decisions taken during testing of AES when detecting certain classes of threats, anomalies and cyber attacks. For the intelligent technology of AES learning, it is possible to use different criteria that satisfy certain properties of the information measures (IM) [13, 14, 19].

For AES as a part of SIRCT, we propose to apply as informational measures entropic measure [13] and the criterion of Kullback-Leibler [14].

Entropy may be considered as a measure of the "structuring" of some state SS_i or a measure of the distance of structure of one state from another one. Then the stochastic process (SP) in CoS, which characterizes state of the systems and functions in the interval of time from τ_0 to T, is described by a vector of variables of the IS state:

$$SS_i(\tau)=f(SX(\tau),he)+hl(\tau), \qquad (6)$$

where he, hl(τ) are the "noises" of a general nature; SX(τ) is the vector of variable CoS states, for example, as a result of a cyber attack or implementation of other threat.

An observation of the magnitude $SS_i(\tau)$ is carried out in time periods $\tau_i=\tau_0+j\Delta,\quad j=\overline{0,n},$ with discretization step $\Delta>0$.

Let us assign cluster in accordance with each of the selected state of CoS (for alternative assumptions $hy=\{hy_1, ..., hy_m\}$ that are a full group of events and physically interpret state of the system):

$$M\Theta_i = \{l_{M\Theta_i}(ss)\cdot ss \,|\, ss \in UK_{sig}, l_{M\Theta_i}(ss) \in ZR\}, \qquad (7)$$

where $l_{M\Theta_i}(ss)$ is the function of the number of instances of the cluster, which determines multiplicity of element of the system $ss \in UK_{sig}$; UK_{sig} is the set, the power of which is equal to the maximum level of the signal, characteristic of the object's attribute.

Let us generalize basic stages of recognition procedures in AES:

1. Define characteristic attributes for each OR.

2. Compile for each node of CoS a full group of states of the system – hy={hy_1,...,hy_m}, to which the original specifications $M\Theta_i$ will correspond.

3. Determine the evaluation of probability distribution P_{SS_i}, characteristic for states of the system, which it experienced as a result of a cyber attack.

4. Calculate the change in entropy of all subsystems of CoS by formula:

$$H_{SS^*} = -\sum_{i=1}^{max} P_{SS_i} \cdot \log_2 P_{SS_i}. \qquad (8)$$

5. According to the results of the observations, form

$$(SS^*_L = \{SS^*(\tau), SS^*(\tau+1), ..., SS^*(\tau+L-1)\}$$

appropriate cluster:

$$M\Theta^*_L = \{is^L_1, is^L_2, ..., is^L_M\}, \qquad (9)$$

where is^L_j is the total number of occurrence of signals specific to the j-th state of the system; L is the control "window" [13, 14].

6. Compute information distances between clusters

$$DIS(M\Theta_i, M\Theta^*_L) \;\; (i = \overline{0,I})$$

by $RS \geq 1$ attributes of difference.

7. Make decision in favor of the state, for which magnitude $DIS(M\Theta_i, M\Theta^*_L)$ is the lowest for each attribute RS_i. At the same time, calculate weight coefficients of individual decisions:

$$kf^j_1 = \arg\min_{i=\overline{0,I}} DIS(M\Theta_i, M\Theta^*_L),$$

$$kf^j_2 = \arg\min_{i=\overline{0,I},\, i\neq i^j_1} DIS(M\Theta_i, M\Theta^*_L), (j = \overline{1,J}). \qquad (10)$$

8. Choose according to the voting procedure [13, 14, 19, 26] the state of the system, for which the weight coefficient is larger:

$$kf_1 = \arg\min_{i=\overline{0,I}} kf^j_1,\; kf_2 = \arg\min_{i=\overline{0,I},\, i\neq i^j_1} kf^j_2. \qquad (11)$$

The magnitude of normalized entropic IIFP, with regard to a priori probability of approving the hypotheses for the OR recognition, we will represent as follows:

$$CE = 1 + 0{,}5 \sum_{l=1}^{2}\sum_{m=1}^{2} p(hy_m/hy_l)\log_2 p(hy_m/hy_l), \qquad (12)$$

where $p(hy_l)$ is the a priori probability of approval of assumption (hypothesis) hy_l; $p(hy_m/hy_l)$ is the a posteriori probability of approval of assumption hy_m, provided that the variant hy_l was chosen; M=2 is the number of considered assumptions in the process of recognition.

The following expression allows us to determine IIFP of training AES with IS:

$$CE^{(ls)}_m = 1 + 0{,}5 \times$$
$$\times\left(\frac{mis1^{(ls)}_m(cr)}{mis1^{(ls)}_m(cr) + AU^{(ls)}_{2,m}(cr)}\log_2\frac{mis1^{(ls)}_m(cr)}{mis1^{(ls)}_m(cr) + AU^{(ls)}_{2,m}(cr)} + \right.$$
$$+\frac{mis2^{(ls)}_m(cr)}{AU^{(ls)}_{1,m}(cr) + mis2^{(ls)}_m(cr)}\log_2\frac{mis2^{(ls)}_m(cr)}{AU^{(ls)}_{1,m}(cr) + mis2^{(ls)}_m(cr)} +$$
$$+\frac{AU_{1,m}(cr)}{AU^{(ls)}_{1,m}(cr) + mis2^{(ls)}_m(cr)}\log_2\frac{AU_{1,m}(cr)}{AU^{(ls)}_{1,m}(cr) + mis2^{(ls)}_m(cr)} +$$
$$+\frac{AU^{(ls)}_{2,m}(cr)}{mis1^{(ls)}_m(cr) + AU^{(ls)}_{2,m}(cr)}\log\frac{AU^{(ls)}_{2,m}(cr)}{mis1^{(ls)}_m(cr) + AU^{(ls)}_{2,m}(cr)} +$$
$$+\frac{mis1^{(ls)}_m(cr)}{mis1^{(ls)}_m(cr) + AU^{(ls)}_{3,m}(cr)}\log_2\frac{mis1^{(ls)}_m(cr)}{mis1^{(ls)}_m(cr) + AU^{(ls)}_{3,m}(cr)} +$$
$$\left.+\frac{AU^{(ls)}_{3,m}(cr)}{mis3^{(ls)}_m(cr) + AU^{(ls)}_{3,m}(cr)}\log_2\frac{AU^{(ls)}_{3,m}(cr)}{mis3^{(ls)}_m(cr) + AU^{(ls)}_{3,m}(cr)}\right), \qquad (13)$$

where $AU^{(ls)}_{1,m}(cr)$ is the procedure of the first validation; $AU^{(ls)}_{2,m}(cr)$ is the procedure of the second validation; $AU^{(ls)}_{3,m}(cr)$ is the procedure of the third validation; $mis1^{(ls)}_m(cr)$ are the errors of the first kind when approving the decision for the ls-th step of AES learning; $mis2^{(ls)}_m(cr)$ are the errors of the second kind when approving the decision for the ls-th step of AES learning; $mis3^{(ls)}_m(cr)$ are the errors of the third kind when approving the decision for the *ls*-th step of AES learning; cr is the radius of hyperspheric containers [13, 14, 19].

Provision of sustainable functioning of reliable processing of information in CoS in a random point in time under the influence of a cyber attack is achieved through the implementation of representation:

$$SO: SS \times CA \to SS_{res} = \{SS^i_{res}\}, \qquad (14)$$

where SS_{res} is the set of permitted states of CoS; CA={CA_0, CA_1,...,CA_N} is the set of implementation of cyber attacks.

A functionality that determines generalized indicator of effectiveness of resisting cyber attacks takes account of the indicator of effectiveness of recognition, as well as characterizes stability of functioning of CoS, will be represented:

$$IE = F[(SCA, CE), (SS, T_s, VIL), (CO, CM, ME)], \qquad (15)$$

where SCA are the scenarios for cyber attacks; CE is the criterion of effectiveness of recognition of OR; a set of parameters of CoS: T_s are the periods of time for performing functional tasks in CoS; VIL are the vulnerabilities of CoS; a set of parameters for resisting the threats and cyber attacks: CO are the parameters of regulation of CoS; CM are the methods of resisting threats and cyber attacks in CoS; ME are the means of prevention, detection, analysis and active counteraction to cyber attacks.

To determine how the Kullback-Leibler information measure depends on the AES parameters for the variant of applying control commands, which are based on three alternatives (a case when a decision is made about dynamics of the change in the IE parameter), we will introduce the following hypothesis:

1) the basic working hypothesis which (base) – $hy_{\gamma 1}$: an attribute (attributes) rc_i of OR (RS) and the IE indicator is within a normal CoS state;

2) hypothesis hy_{γ_2} – an attribute (attributes) rc_i of OR (RS) and the indicator IE allows drawing a conclusion that the values of indicator IE are lower than the norm;

3) hypothesis hy_{γ_3} – indicator IE allows drawing a conclusion that the values of indicator IE are larger than the norm.

According to the accepted assumptions, let us denote a posteriori hypotheses as: hy_{μ_1} – the value of attribute (attributes) belongs to the range of permissible deviations (RPD) ca, hy_{μ_2} – the value of attribute (attributes) is located to the left of RPD; hy_{μ_3} – the value of attribute (attributes) is located to the right of RPD.

Given previous calculations, for the AES solution, which allows three alternatives, we received the following characteristics, Table 3.

We will assume that: characteristics $mis2_{2,m}^{(ls)}$ and $mis3_{2,m}^{(ls)}$ are unlikely, which is why they can be disregarded. We also assume:

$$mis1_m^{(ls)} = mis1_{1,m}^{(ls)} = mis1_{2,m}^{(ls)};$$

$$mis2_m^{(ls)} = mis2_{1,m}^{(ls)}; mis3_m^{(ls)} = mis3_{1,m}^{(ls)}. \qquad (16)$$

Calculate full probabilities $P_{t,m}^{(ls)}$ and $P_{f,m}^{(ls)}$ with regard to assumptions (16)

$$P_{t,m}^{(ls)} = p\left(hy_{\mu_1}\right)AU_{1,m}^{(ls)} + p\left(hy_{\mu_2}\right)AU_{2,m}^{(ls)} + p\left(hy_{\mu_3}\right)AU_{3,m}^{(ls)}$$

and

$$P_{f,m}^{(ls)} = p\left(hy_{\mu_1}\right)mis1_m^{(ls)} + p\left(hy_{\mu_2}\right)mis2_m^{(ls)} + p\left(hy_{\mu_3}\right)mis3_m^{(ls)}. \qquad (17)$$

Then, on the basis of the Bernoulli-Laplace principle [13, 14] for the three adopted hypotheses, we obtain the following result:

$$CE_m^{(ls)} = \tfrac{1}{3} \cdot \left\{ \begin{matrix} \left[AU_{1,m}^{(ls)} + AU_{2,m}^{(ls)} + AU_{3,m}^{(ls)}\right] - \\ -\left[mis1_m^{(ls)} + mis2_m^{(ls)} + mis3_m^{(ls)}\right] \end{matrix} \right\} \times$$

$$\times \log_2 \frac{AU_{1,m}^{(ls)} + AU_{2,m}^{(ls)} + AU_{3,m}^{(ls)}}{AU_{1,m}^{(ls)} + AU_{2,m}^{(ls)} + AU_{3,m}^{(ls)}}. \qquad (18)$$

The decisive rule defines the assignment of the vector of parameters of implementation of the known or unknown scripts of cyber attacks SCA_m^{CT} for the m-th object and ct-th class to one of the known OR classes $RS_{m_j}^{CT}$ at the j-th step of the work of cyber protection tools. According to the Bayesian criterion, the decisive rule takes the following form:

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

$$\geq P\left(RS_{m_k}^{CT}\right) \cdot P\left(\overline{SCA_m^{CT}} / RS_{m_k}^{CT}\right), \qquad (19)$$

where $P\left(RS_{m_i}^{CT}\right)$ is the probability of assigning AES of OR (threats, anomalies, or cyber attacks) to the class of the known OR $RS_{m_i}^{CT}$;

$$P\left(\overline{SCA_m^{CT}} / RS_{m_i}^{CT}\right)$$

is the density of conditional probability of assigning AES of detected OR to the known class $RS_{m_i}^{CT}$; $P\left(RS_{m_k}^{CT}\right)$ is the probability of assigning AES of OR to the class of the unknown OR $RS_{m_k}^{CT}$;

$$P\left(\overline{SCA_m^{CT}} / RS_{m_k}^{CT}\right)$$

is the density of conditional probability of assigning AES of detected OR to the unknown class $RS_{m_k}^{CT}$.

Table 3

Characteristics of the accuracy of recognition in AES for the three accepted alternatives

No.	Name of parameter	Expression for calculation	Note
1	first validation of hypothesis	$AU_{1,m}^{(ls)} = p\left(hy_{\gamma_1}/hy_{\mu_1}\right)$	based on conclusions
2	second validation of hypothesis	$AU_{2,m}^{(ls)} = p\left(hy_{\gamma_2}/hy_{\mu_2}\right)$	based on comparison of deviations from $\left\{ca_{K,i}^{*}\right\}$
3	third validation of hypothesis	$AU_{3,m}^{(ls)} = p\left(hy_{\gamma_3}/hy_{\mu_3}\right)$	based on the results of processing a predicate form of calculation of the number of episodes, when it is established that the implementation of OR 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 established that the implementations of OR belong to the container $C_{1,m}^{o}$, if they really belong to the class CT_2^{o}
4	first error of the first kind	$mis1_{1,m}^{(ls)} = p\left(hy_{\gamma_2}/hy_{\mu_1}\right)$	number of false activites of AES in the process of detection of threats, anomalies or cyber attacks
5	second error of the first kind	$mis1_{2,m}^{(ls)} = p\left(hy_{\gamma_3}/hy_{\mu_1}\right)$	
6	first error of the second kind	$mis2_{1,m}^{(ls)} = p\left(hy_{\gamma_1}/hy_{\mu_2}\right)$	number of undetected threats, anomalies or cyber attacks in the process of AES performance
7	second error of the second kind	$mis2_{2,m}^{(ls)} = p\left(hy_{\gamma_3}/hy_{\mu_2}\right)$	
8	first error of the third kind	$mis3_{1,m}^{(ls)} = p\left(hy_{\gamma_1}/hy_{\mu_3}\right)$	may occur in case the model does not take into account certain elements of MILT
99	second error of the third kind	$mis3_{2,m}^{(ls)} = p\left(hy_{\gamma_2}/hy_{\mu_3}\right)$	

Based on the Bayesian criterion, we also determine an average “price” of risk of making a decision in AES on the assignment of vector of parameters of the unknown OR to the class $RS_{m_k}^{CT}$:

$$PR\left(RUL_i / \overline{SCA_m^{CT}}\right) = \sum_{j=1}^{\gamma} np\left(\frac{RUL_i}{RS_{m_k}^{CT}}\right) \cdot P\frac{RS_{m_k}^{CT}}{\overline{SCA_m^{CT}}}, \qquad (20)$$

where RUL_i is the decisive rule by which a binary training vector (BTV) of OR $\overline{SCA_m^{CT}}$ specifies membership of the object to $RS_{m_k}^{CT}$;

$$np\left(\frac{RUL_i}{RS_{m_k}^{CT}}\right)$$

is the conditional “price” of making a decision by AES RUL_i;

$$P\frac{RS_{m_k}^{CT}}{\overline{SCA_m^{CT}}}$$

is the conditional probability that $\overline{SCA_m^{CT}}$ is assigned by AES to the class $RS_{m_k}^{CT}$.

For the case when AES runs a comparative analysis of two BTM, the decisive rule using the Bayesian criterion can be written down as the following ratio:

$$\frac{P\left(\overline{SCA_m^{CT}} \big/ RS_{m_1}^{CT}\right)}{P\left(\overline{SCA_m^{CT}} \big/ RS_{m_2}^{CT}\right)} \geq \frac{P\left(RS_{m_2}^{CT}\right)}{P\left(RS_{m_1}^{CT}\right)}. \qquad (21)$$

Therefore, the derived expressions (18), (21), which take into account the modified entropic criterion and the Kullback-Leibler measure is a functional of the decisions made in the course of recognition of respective OR. In addition, expression (18) takes into account the known statistical and deterministic (distance) criteria of optimization of the procedure of clustering the attributes of OR at the preceding stage of operation of SIRCT that are capable of learning.

6. Adaptive expert system “Threat Analyzer”

In the course of the research we developed AES “Threat Analyzer “, Fig. 3–5. The AES user interface is intended for professionals on IS. Through the interface, analyst of the status of IS of CoS receives necessary information and reports the requested data to AES. Through the same interface, preliminary selection and analysis of the threats to IS is conducted by the attributes. AES uses the user interface to compile summary reports of the results of analysis of the IS state and suggested recommendations.

The expert’s interface is designed to transfer the knowledge of experts on IS to KB, as well as to correct the knowledge and the rules for recognition of anomalies, threats or cyber attacks. Through the interface, a change in decisive modules for making decisions for different OR is carried out. This happens only if there were errors detected in the performance of EC.

For the development of interfaces and functional modules of AES, we used the Delphi language and programming environment. We chose the shell program CLIPS for the design of ES.

According to these tasks, the AES structure implemented the modules that make it possible: to automate the procedure of audit of CoS IS; to improve the procedure of recognition of the threats to IS in CoS; to receive expert information on the computers’ status in the network; to scan the programs running on PC; to determine levels of IS of individual PCs in CoS; to facilitate work of the experts on IS; to use previously gained experience on evaluation of the state of IS; to assess current risks of UAA to the IS of an enterprise; to present recommendations on how to improve the level of protection of IS; to reduce the time for conducting inspections and audit of the status of CoS IS.

For knowledge representation in ES we used frame model for decision-making – direct logical conclusion.

The basis of EC is the assumption that the elements of a set of security features might not fully meet the IS requirements at an enterprise and, consequently, lead to an increase in the indicator of current information risks. A level of current risk is assigned, which is considered acceptable and does not require the use of expensive means to resist attempts of UAA in CoS.

7. Results of testing the adaptive expert system

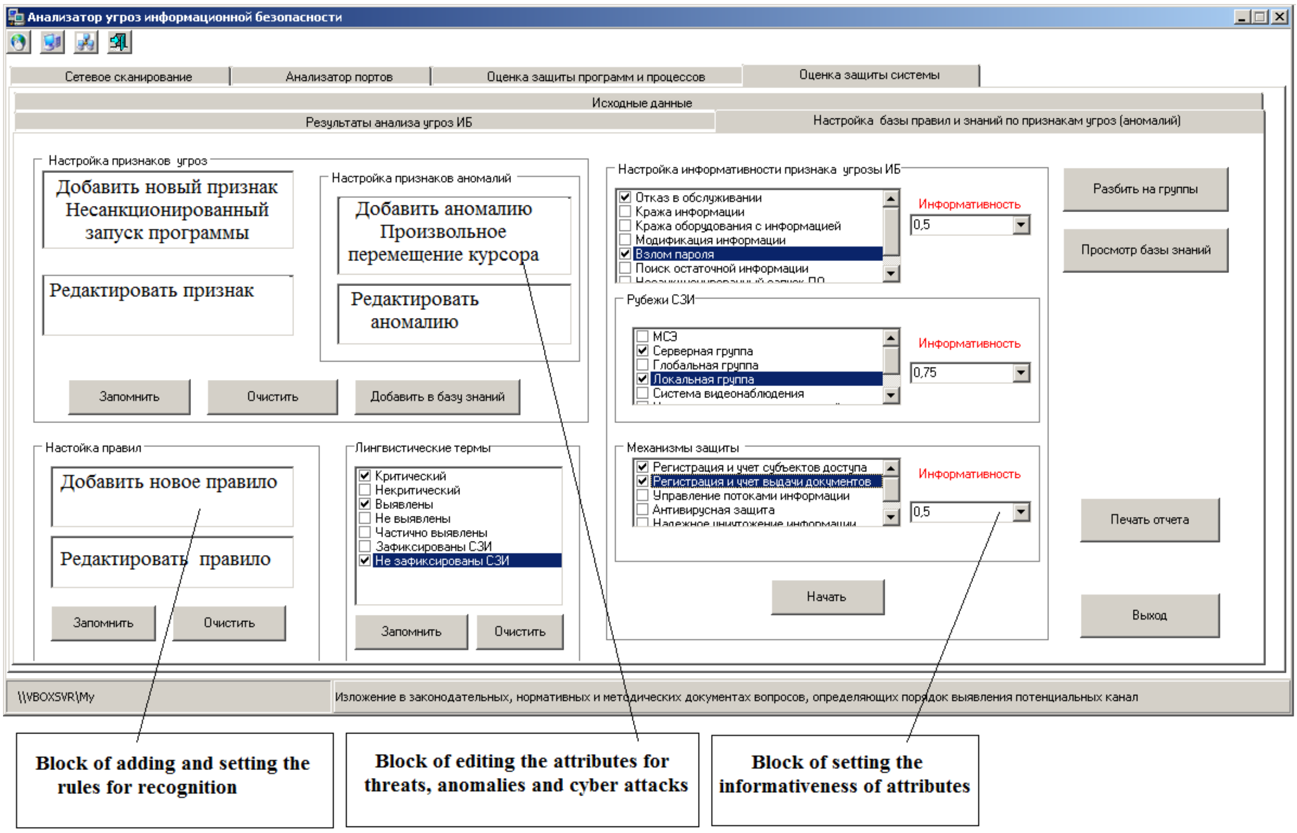
The testing of AES “Threat Analyzer” was carried out for CoS of a few enterprises in the cities of Kyiv, Dnipro and Chernihiv (Ukraine).

Fig. 6 demonstrates the main results obtained in the course of simulation of indicator CE for the network classes of cyber attacks listed in Table 4.

The research revealed that for the “voting” model MILT by the representative sets of attributes of threats, anomalies and cyber attacks, it is sufficient to confine with the construction of representative sets of lengths to 5–7 attributes. Compared with the method of supporting vectors [1, 4], MILT for a small number of the OR attributes (2–4) has a significant advantage in the indicator CE by 25–50 %, but is inferior by 20–55 % to the indicator CE, obtained for a hybrid neural network model [5, 7].

Comparative analysis, Fig. 7, was carried out based on the data obtained during test trials of AES “Threat Analyzer” and the data contained in [7, 9, 13, 14, 20]. Error values of the first $mis1_m^{(ls)}(cr)$ and second kind $mis2_m^{(ls)}(cr)$ when detecting cyber attacks were tested compared to the network intrusion detection systems (SDI) AIDS – application based IDS, and the combined solutions IDS & IPS (Intrusion prevention system).

The proposed approach of recognizing anomalies, threats and cyber attacks, based on MILT, makes it possible to increase the level of detection of network cyber attacks in CoS. Detection of different types of attacks when using AES reaches the probability of 77–99 % with an insignificant level of false action. In addition, the proposed method is not IS resource demanding and is capable of detecting unknown types of cyber attacks in CoS.


Анализатор угроз информационной безопасности
Сетевое сканирование
Анализатор портов
Оценка защиты программ и процессов
Оценка защиты системы
Исходные данные
Результаты анализа угроз ИБ
Настройка базы правил и знаний по признакам угроз (аномалий)
Настройка признаков угроз
Добавить новый признак
Несанкционированный запуск программы
Редактировать признак
Настройка признаков аномалий
Добавить аномалию
Произвольное перемещение курсора
Редактировать аномалию
Запомнить
Очистить
Добавить в базу знаний
Настойка правил
Добавить новое правило
Редактировать правило
Запомнить
Очистить
Лингвистические термы
Запомнить
Очистить
Настройка информативности признака угрозы ИБ
Рубежи СЗИ
Механизмы защиты
Начать
Разбить на группы
Просмотр базы знаний
Печать отчета
Выход
Block of adding and setting the rules for recognition
Block of editing the attributes for threats, anomalies and cyber attacks
Block of setting the informativeness of attributes

Лингвистические термы

☑ Критический
□ Некритический
☑ Выявлены
□ Не выявлены
□ Частично выявлены
□ Зафиксированы СЗИ
☑ Не зафиксированы СЗИ

Настройка информативности признака угрозы ИБ

☑ Отказ в обслуживании
□ Кража информации
□ Кража оборудования с информацией
□ Модификация информации
☑ Взлом пароля
□ Поиск остаточной информации

Информативность: 0,5

Рубежи СЗИ

□ МСЭ
☑ Серверная группа
□ Глобальная группа
☑ Локальная группа
□ Система видеонаблюдения

Информативность: 0,75

Механизмы защиты

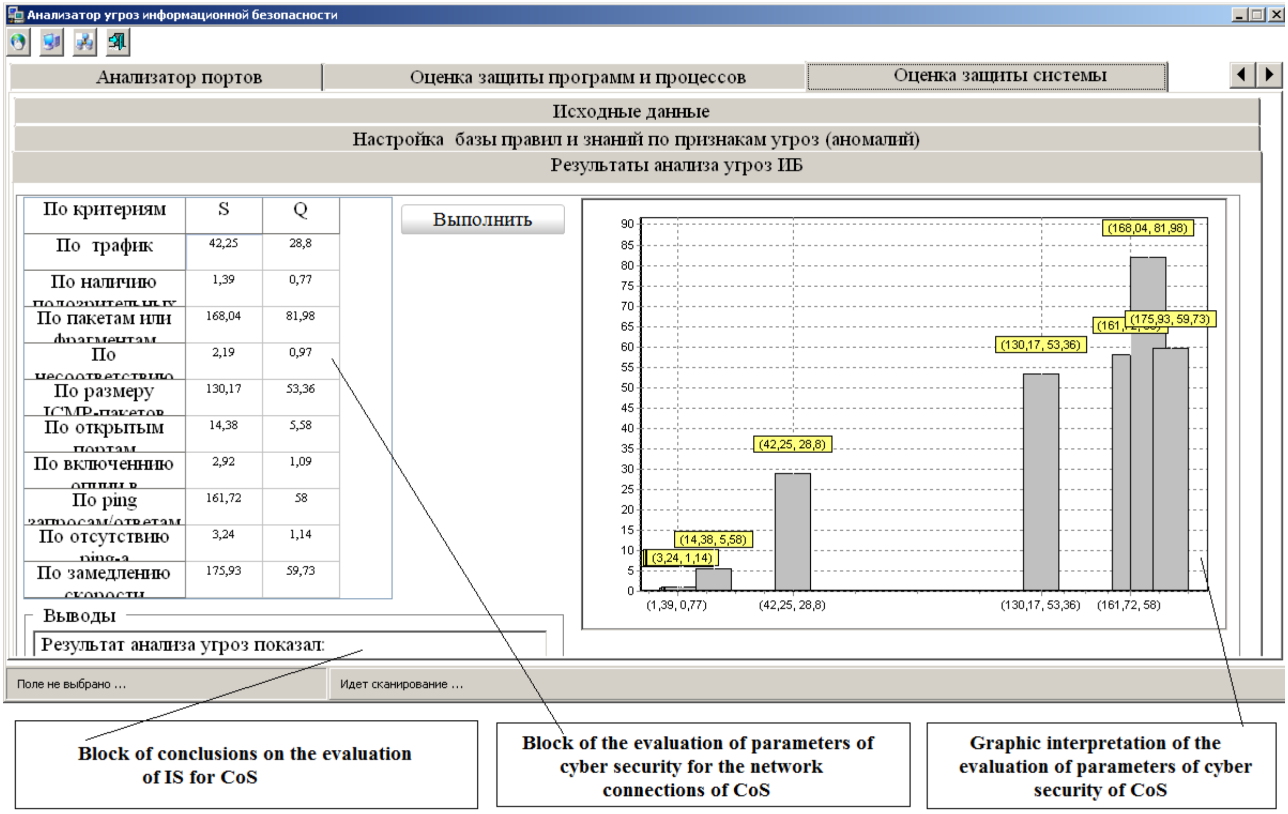
☑ Регистрация и учет субъектов доступа
☑ Регистрация и учет выдачи документов
□ Управление потоками информации
□ Антивирусная защита

Информативность: 0,5

\\VBOXSVR\My

Изложение в законодательных, нормативных и методических документах вопросов, определяющих порядок выявления потенциальных канал

Fig. 3. Bookmark for setting the rules of recognition and evaluation of anomalies, threats and cyber attacks


Анализатор угроз информационной безопасности
Анализатор портов
Оценка защиты программ и процессов
Оценка защиты системы
Исходные данные
Настройка базы правил и знаний по признакам угроз (аномалий)
Результаты анализа угроз ИБ
Выполнить
Выводы
90
85
80
75
70
65
60
55
50
45
40
35
30
25
20
15
10
5
0
(168,04, 81,98)
(161,72, 58)
(175,93, 59,73)
(130,17, 53,36)
(42,25, 28,8)
(14,38, 5,58)
(3,24, 1,14)
(1,39, 0,77)
(42,25, 28,8)
(130,17, 53,36)
(161,72, 58)
Block of conclusions on the evaluation of IS for CoS
Block of the evaluation of parameters of cyber security for the network connections of CoS
Graphic interpretation of the evaluation of parameters of cyber security of CoS

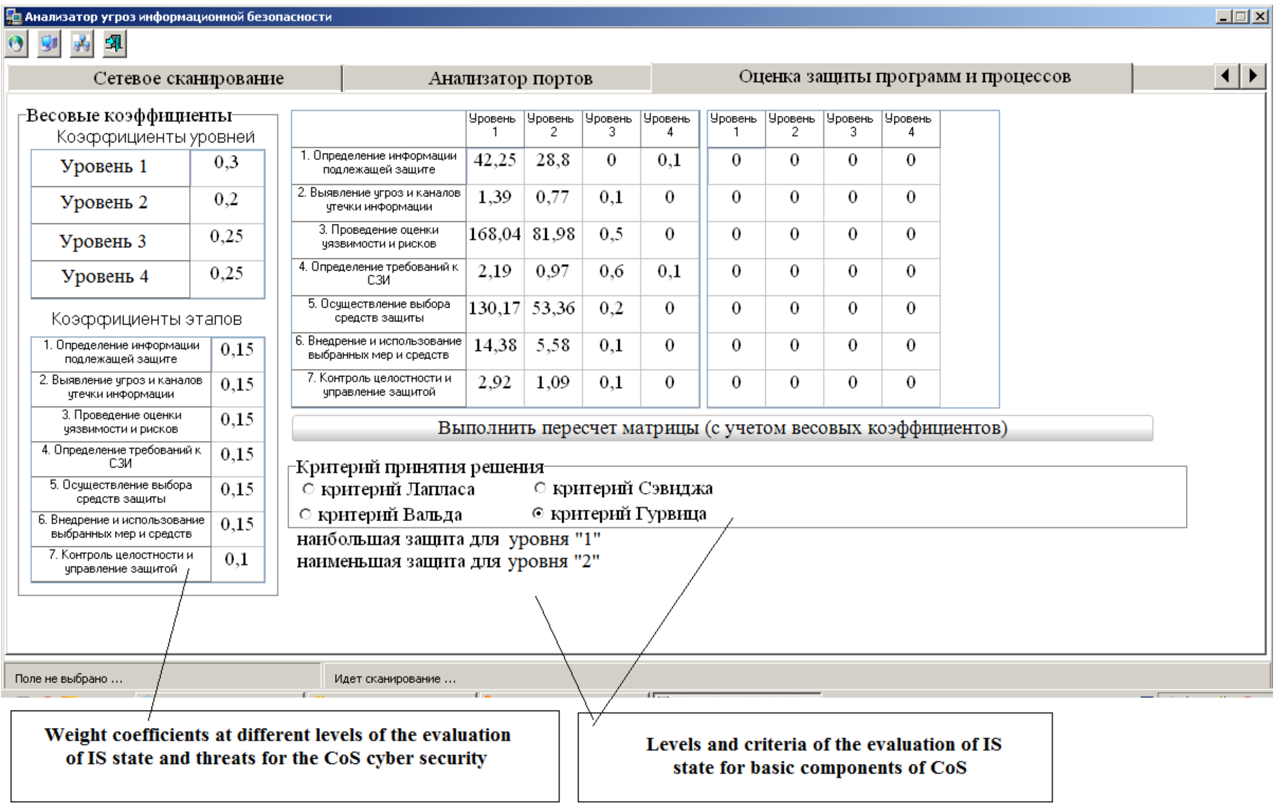
По критериям	S	Q
По трафик	42,25	28,8
По наличию подозрительных	1,39	0,77
По пакетам или фрагментам	168,04	81,98
По несоответствию	2,19	0,97
По размеру ICMP-пакетов	130,17	53,36
По открытым портам	14,38	5,58
По включеннию опции в	2,92	1,09
По ping запросам/ответам	161,72	58
По отсутствию ping-a	3,24	1,14
По замедлению скорости	175,93	59,73

Результат анализа угроз показал:

Поле не выбрано …

Идет сканирование …

Fig. 4. Bookmark for representation of results of the analysis of detected anomalies, threats and cyber attacks



Анализатор угроз информационной безопасности

Весовые коэффициенты

Коэффициенты уровней

Уровень 1	0,3
Уровень 2	0,2
Уровень 3	0,25
Уровень 4	0,25

Коэффициенты этапов

1. Определение информации подлежащей защите	0,15
2. Выявление угроз и каналов утечки информации	0,15
3. Проведение оценки уязвимости и рисков	0,15
4. Определение требований к СЗИ	0,15
5. Осуществление выбора средств защиты	0,15
6. Внедрение и использование выбранных мер и средств	0,15
7. Контроль целостности и управление защитой	0,1

	Уровень 1	Уровень 2	Уровень 3	Уровень 4	Уровень 1	Уровень 2	Уровень 3	Уровень 4
1. Определение информации подлежащей защите	42,25	28,8	0	0,1	0	0	0	0
2. Выявление угроз и каналов утечки информации	1,39	0,77	0,1	0	0	0	0	0
3. Проведение оценки уязвимости и рисков	168,04	81,98	0,5	0	0	0	0	0
4. Определение требований к СЗИ	2,19	0,97	0,6	0,1	0	0	0	0
5. Осуществление выбора средств защиты	130,17	53,36	0,2	0	0	0	0	0
6. Внедрение и использование выбранных мер и средств	14,38	5,58	0,1	0	0	0	0	0
7. Контроль целостности и управление защитой	2,92	1,09	0,1	0	0	0	0	0

Критерий принятия решения

○ критерий Лапласа ○ критерий Сэвиджа

○ критерий Вальда ● критерий Гурвица

наибольшая защита для уровня "1"

наименьшая защита для уровня "2"

Поле не выбрано ...

Идет сканирование ...

Weight coefficients at different levels of the evaluation of IS state and threats for the CoS cyber security

Levels and criteria of the evaluation of IS state for basic components of CoS

Fig. 5. Bookmark for representation of results of the evaluation of the IS state for the basic components of CoS

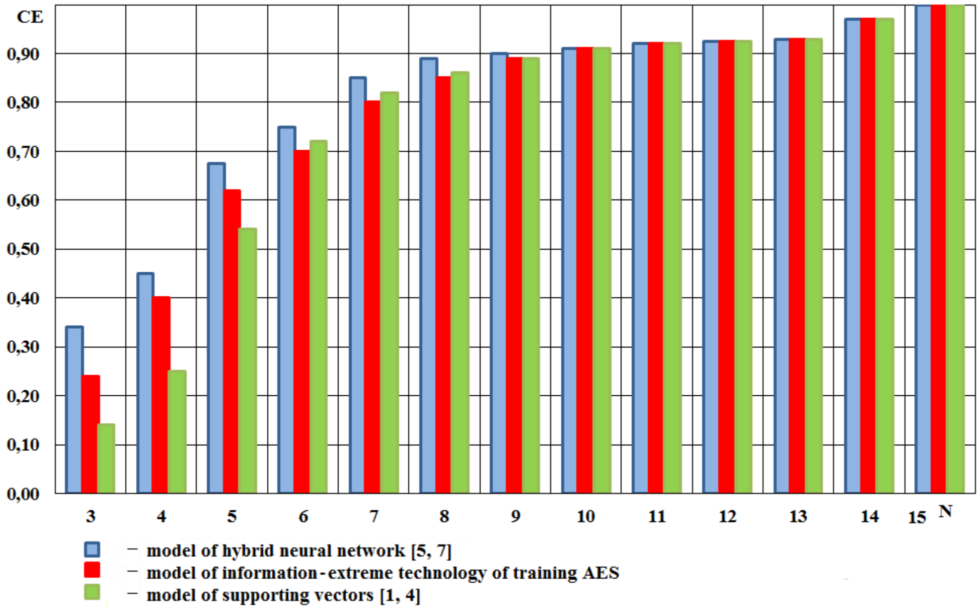


Fig. 6. Graph of dependence of IPFR on the number of attributes that are used for training SIRCT

As a result of the described experiment for the designed AES and the method of intelligent recognition of cyber attacks and anomalies [10, 19], we obtained the following results:

– for the DoS/DDoS attacks – for errors of the first kind (number of false actions) – 10.2 %) and for errors of the second kind (number of undetected attacks) – 2.86 %;

– for the Probe attacks – for errors of the first kind – 12.1 % and for errors of the second kind – 3.15 %;

– for the R2L attacks – for errors of the first kind – 9.4 % and for errors of the second kind – 2.75 %;

– for the U2R attacks – for errors of the first kind – 11.3 % and for errors of the second kind – 3.5 %.

In the course of research we found an optimal number of clusters to determine max value of the IPFR indicator when training AES, which is equal to 3.

These results allow us to compare the developed model with those, examined previously in papers [7, 9, 13, 14, 20, 23, 25], methods and mathematical models that are used in SDI, Table 4.

According to the data represented in Fig. 7 and in Table 4, the proposed model of ES training "Threat Analyzer" makes it possible to achieve results of the recognition of the standard classes of cyber attacks at the level from 76.5 % to 99.1 %, which is at the level of efficiency of recognition by hybrid neural networks and genetic algorithms.

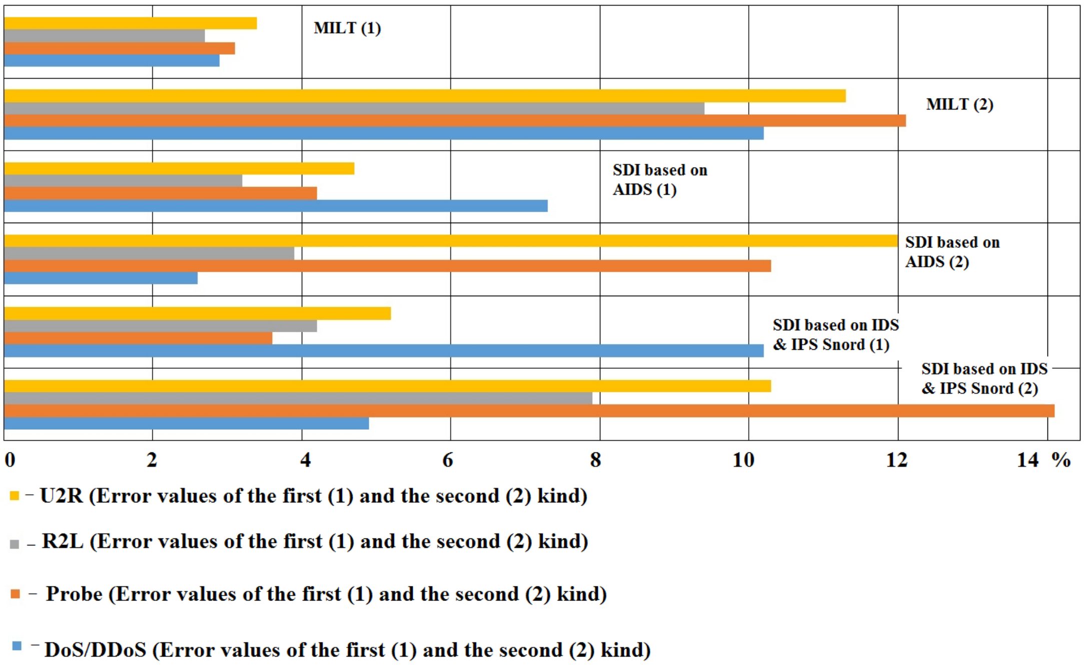


Fig. 7. Error values of the first (1) and the second (2) kind when detecting cyber attacks by different systems

Table 4

Comparative analysis of intrusion detection techniques

No. of entry	Model or method	Work under conditions of fuzzy attributes of attack and capability to adapt the algorithm to the errors of the third kind	Database	Number of input data	Search for intrusions of normal behavior, %	Search for new attributes	Source

1	Hierarchical map	–	KDD-99		Norm – 96,4;
					DoS – 96,2;
					U2R – 37,1;
					R2L – 43,1; Probe – 94,3
						–	[9, 11, 18]

2	Method of supporting vectors	–		41	Norm – 99,8;
					DoS – 97,5;
					U2R – 86,6;
					R2L – 81,3; Probe – 92,8
						–	[1, 4]

3	Kohonen neuron	–			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, 23]

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, 24]

7	MILT for AES	+		10–12	Norm – 98,7;
					DoS – 99,1;
					U2R – 76,5;
					R2L – 90; Probe – 84,2
						+	[10, 19]

8. Discussion of results of testing the model and prospects for further research

Scientific and practical research results in the form of AES "Threat Analyzer", were implemented at the State Enterprise "Design-Engineering Technological Bureau on Automation of Control Systems in the Railway Transport of Ukraine" of the Ministry of Infrastructure, as well as in information security services of several computing centers at industrial and transport enterprises in the cities of Kyiv, Dnipro, and Chernyhiv.

Implementation of the proposed AES made it possible to significantly change the approaches to the organization of work of a specialist on information security at the enterprises at which the test research was conducted, in particular, the status of cyber protection of CoS and information systems was greatly improved, as well as a vertically integrated system of IS was created. The proposed model of ES training was deliberately implemented with regard to a large amount of specialized data in the field of IS and cyber defence and, accordingly, it will require considerable time for systematization and transfer in the form of MBTM of the templates for threats, anomalies and cyber attacks with the subsequent introduction to AES.

The efficiency of application of the designed model will be the higher, the more informative attributes will be introduced to CTM, formed at every stage of clustering the AES input data. With a small amount of attributes in CTM, the effect of application of the model will be insignificant. Therefore, the prospects for further research are to improve knowledge base of the attributes in the form of their matrix representation, as well as to explore the model on a larger quantity of objects that are stored in databases and knowledge bases of AES.

The developed model, compared with the results obtained for the models represented in Table 4, provides for a significantly smaller number of required attributes to classify sophisticated targeted cyberattacks in CoS.

At the moment we are working to fill the knowledge base and to further test AES under real conditions of the CoS functioning.

9. Conclusions

1. We proposed a structural scheme of adaptive expert system of information security, capable of self-learning, which takes into account potential errors of the third kind, which may arise and accumulate in the course of training the system and splitting a space of attributes of the objects of recognition.

2. We designed a model of the information criterion of functional effectiveness, based on entropic and information-distance criteria of Kullback-Leibler when clustering the attributes of threats, anomalies and cyber attacks in CoS, that makes it possible to receive input fuzzy classified training matrix, which is used as an object of learning, as well as to build correct decisive rules for the recognition of cyber attacks.

3. The test examination of AES was conducted and it was found that the proposed model of ES training "Threat Analyzer" enabled us to achieve results of recognition of the common classes of cyber attacks at the level from 76.5 % to 99.1 %, which is at the level of recognition effectiveness by hybrid neural networks and genetic algorithms. We also found that the optimal number of clusters to determine the max value of IPFR when training AES and splitting a space of attributes of anomalies or cyber attacks for CoS is equal to 3.

References

1. Khan, L. A new intrusion detection system using support vector machines and hierarchical clustering [Text] / L. Khan, M. Awad, B. Thuraisingham // The VLDB Journal. – 2006. – Vol. 16, Issue 4. – P. 507–521. doi: 10.1007/s00778-006-0002-5
2. Zhang, Y. Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids [Text] / Y. Zhang, L. Wang, W. Sun, R. C. Green, M. Alam // IEEE Transactions on Smart Grid. – 2011. – vol. 2, Issue 4. – P. 796–808. doi: 10.1109/tsg.2011.2159818
3. Valenzuela, J. Real-Time Intrusion Detection in Power System Operations [Text] / J. Valenzuela, J. Wang, N. Bissinger // IEEE Transactions on Power Systems. – 2013. – vol. 28, Issue 2. – p. 1052–1062. doi: 10.1109/tpwrs.2012.2224144
4. Al-Jarrah, O. Network Intrusion Detection System using attack behavior classification [Text] / O. Al-Jarrah, A. Arafat // 2014 5th International Conference on Information and Communication Systems (ICICS), 2014. – p. 1–6. doi: 10.1109/iacs.2014.6841978
5. Selim, S. Detection using multi-stage neural network [Text] / S. Selim, M. Hashem, T. M. Nazmy // International Journal of Computer Science and Information Security (IJCSIS). – 2010. – Vol. 8, Issue 4. – P. 14–20.
6. Shin, J. Development of a cyber security risk model using Bayesian networks [Text] / J. Shin, H. Son, R. Khalil, G. Heo // Reliability Engineering & System Safety. – 2015. – Vol. 134. – P. 208–217. doi: 10.1016/j.ress.2014.10.006
7. Pawar, S. N. Intrusion detection in computer network using genetic algorithm approach: a survey [Text] / S. N. Pawar // International Journal of Advances in Engineering Technology. – 2013. – Vol. 6, Issue 2. – P. 730–736.
8. Linda, O. Fuzzy logic based anomaly detection for embedded network security cyber sensor [Text] / O. Linda, M. Manic, T. Vollmer, J. Wright // 2011 IEEE Symposium on Computational Intelligence in Cyber Security (CICS), 2011. – p. 202–209. doi: 10.1109/cicybs.2011.5949392
9. Zhan, Z. Characterizing Honeypot-Captured Cyber Attacks: Statistical Framework and Case Study [Text] / Z. Zhan, M. Xu, S. Xu // IEEE Transactions on Information Forensics and Security. –2013. – Vol. 8, Issue 11. – P. 1775–1789. doi: 10.1109/tifs.2013.2279800
10. Lakhno, V. A. Improving of information transport security under the conditions of destructive influence on the information-communication system [Text] / V. A. Lakhno, O. S. Petrov, A. V. Hrabariev, Y. V. Ivanchenko, G. S. Beketova // Journal of theoretical and applied information technology. – 2016. – Vol. 89, Issue 2. – P. 352–361.

11. Louvieris, P. Effects-based feature identification for network intrusion detection [Text] / P. Louvieris, N. Clewley, X. Liu // Neurocomputing. –2013. – Vol. 121. – P. 265–273. doi: 10.1016/j.neucom.2013.04.038
12. Ye, J. Single valued neutrosophic cross-entropy for multicriteria decision making problems [Text] / J. Ye // Applied Mathematical Modelling. – 2014. – Vol. 38, Issue 3. – P. 1170–1175. doi: 10.1016/j.apm.2013.07.020
13. Xiang, Y. Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics [Text] / Y. Xiang, K. Li, W. Zhou // IEEE Transactions on Information Forensics and Security. – 2011. – Vol. 6, Issue 2. – p. 426–437. doi: 10.1109/tifs.2011.2107320
14. Callegari, C. Improving PCA-based anomaly detection by using multiple time scale analysis and Kullback-Leibler divergence [Text] / C. Callegari, L. Gazzarrini, S. Giordano, M. Pagano, T. Pepe // International Journal of Communication Systems, – 2014. – Vol. 27, Issue 10. – P. 1731–1751. doi: 10.1002/dac.2432
15. Ericsson, G. N. Cyber Security and Power System Communication – Essential Parts of a Smart Grid Infrastructure [Text] / G. N. Ericsson // IEEE Transactions on Power Delivery. – 2010. – Vol. 25, Issue 3. – p. 1501–1507. doi: 10.1109/tpwrd.2010.2046654
16. Chang, L.-Y. Applying fuzzy expert system to information security risk Assessment – A case study on an attendance system [Text] / L.-Y. Chang, Z.-J. Lee // 2013 International Conference on Fuzzy Theory and Its Applications (iFUZZY), 2013. – p. 346–351. doi: 10.1109/ifuzzy.2013.6825462
17. Atymtayeva, L. Building a Knowledge Base for Expert System in Information Security [Text] / L. Atymtayeva, K. Kozhakhmet, G. Bortsova. – Advances in Intelligent Systems and Computing, 2014. – p. 57–76. doi: 10.1007/978-3-319-05515-2_7
18. Kanatov, M. Expert systems for information security management and audit. Implementation phase issues [Text] / M. Kanatov, L. Atymtayeva, B. Yagaliyeva // 2014 Joint 7th International Conference on Soft Computing and Intelligent Systems (SCIS) and 15th International Symposium on Advanced Intelligent Systems (ISIS), 2014. – p. 896–900. doi: 10.1109/scis-isis.2014.7044702
19. Lakhno, V. Design of adaptive system of detection of cyber-attacks, based on the model of logical procedures and the coverage matrices of features [Text] / V. Lakhno, S. Kazmirchuk, Y. Kovalenko, L. Myrutenko, T. Zhmurko // Eastern-European Journal of Enterprise Technologies. – 2016. – Vol. 3, Issue 9 (81). – p. 30–38. doi: 10.15587/1729-4061.2016.71769
20. Ben-Asher, N. Effects of cyber security knowledge on attack detection [Text] / N. Ben-Asher, C. Gonzalez // Computers in Human Behavior. – 2015. – Vol. 48. – P. 51–61. doi: 10.1016/j.chb.2015.01.039
21. Goztepe, K. Designing Fuzzy Rule Based Expert System for Cyber Security [Text] / K. Goztepe // International Journal of Information Security Science. – 2012. – Vol. 1, Issue 1. – p. 13–19.
22. Gamal, M. M. A Security Analysis Framework Powered by an Expert System [Text] / M. M. Gamal, B. Hasan, A. F. Hegazy // International Journal of Computer Science and Security (IJCSS). – 2011. – vol. 4, Issue 6. – p. 505–527.
23. Chinh, H. N. Fast detection of ddos attacks using non-adaptive group testing [Text] / H. N. Chinh, T. Hanh, N. Dinh Thuc // International Journal of Network Security & Its Applications. – 2013. – Vol. 5, Issue 5. – p. 63–71. doi: 10.5121/ijnsa.2013.5505
24. Ismail, M. N. Detecting flooding based DoS attack in cloud computing environment using covariance matrix approach [Text] / M. N. Ismail, A. Aborujilah, S. Musa, A. Shahzad // Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication - ICUIMC '13, 2013. – p. 1–7. doi: 10.1145/2448556.2448592
25. Thai, M. T. On Detection of Malicious Users Using Group Testing Techniques [Text] / M. T. Thai, Y. Xuan, I. Shin, T. Znati // 2008 The 28th International Conference on Distributed Computing Systems, 2008. – P. 206–213. doi: 10.1109/icdcs.2008.75
26. Ivakhnenko, A. G. Problemy induktivnogo dvukhurovnevogo monitoringa slozhnykh protsessov [Text] / A. G. Ivakhnenko, Ye. A. Savchenko, G. A. Ivakhnenko, V. L. Sinyavskiy // Upravlyayushchie sistemy i mashiny. – 2007. – Vol. 3. – P. 13–21.