Запропоновано модель розпізнавання аномалій і кібератак, яка базується на використанні логічних процедур, покриттях матриць ознак і понятті елементарного класифікатора. Модель дозволяє мінімізувати кількість навчальних вибірок для ідентифікації кіберзагроз в критично важливих комп'ютерних системах. Виконано оцінку правил навчання й достатньої кількості вибірок з інформативних ознак для адаптивної системи розпізнавання. Запропоновано програму пошуку мінімально необхідної кількості ознак для різних класів кібератак, аномалій і загроз

Ключові слова: адаптивні системи розпізнавання кіберзагроз, ознаки кібератаки, логічні процедури, елементарний класифікатор

Предложена модель распознавания аномалий и кибератак, основанная на применении логических процедур, покрытиях матриц признаков и понятии элементарного классификатора. Модель позволяет минимизировать количество обучающих выборок для идентификации киберугроз в критически важных компьютерных системах. Выполнена оценка правил обучения и достаточного количества выборок из информативных признаков для адаптивной системы распознавания. Предложена программа поиска минимально необходимого количества признаков для различных классов кибератак, аномалий и угроз

Ключевые слова: адаптивные системы распознавания киберугроз, признаки кибератаки, логические процедуры, элементарный классификатор

UDC 004.056
DOI: 10.15587/1729-4061.2016.71769

DESIGN OF ADAPTIVE SYSTEM OF DETECTION OF CYBER-ATTACKS, BASED ON THE MODEL OF LOGICAL PROCEDURES AND THE COVERAGE MATRICES OF FEATURES

V. Lakhno
Doctor of Technical Science, Associate Professor
Department of Managing Information Security*
E-mail: lva964@gmail.com
S. Kazmirchuk
PhD, Associate Professor**
E-mail: sv.kazmirchuk@gmail.com
Y. Kovalenko
Candidate of Pedagogical Sciences, Associate Professor**
E-mail: yleejulee22@gmail.com
L. Myrutenko
Postgraduate student
Department of Information
Systems and Mathematical Disciplines*
E-mail: lara.mirutenko@yandex.ru
T. Zhmurko
Assistant**
E-mail: taniazhm@gmail.com
*European University
Academician Vernadskiy blvd., 16B, Kyiv, Ukraine, 03115
**IT-Security Academic Department
National Aviation University
Kosmonavta Komarova ave., 1, Kyiv, Ukraine, 03058

1. Introduction

Global development of mission-critical computer systems (MCCS) in energy, industry, communications and transport, infrastructure objects of major metropolitan areas, etc. requires constant monitoring of cyber threats, as well as vulnerabilities in the technical components and the software. The imperfection of the existing methods of cyber defense, as well as the changing nature of cyber-attacks, may lead MCCS to unsafe conditions. In addition, attackers increasingly are not individual hackers or a group of hackers, but the cyber armies from the countries – potential enemies. One of the priority areas for protection, contributing to the timely detection of cyber-attacks and prevention of their consequences, is the way of the development of adaptive systems of detection and prevention of cyber-attacks (ASDCA). One of the prospective and actual directions of ASDCA synthesis is the application of the models of logical procedures of recognition, based on the coverage matrix of features of anomalies, threats and cyber-attacks within existing and new classes of intrusion.

2. Analysis of scientific literature data and the problem statement

There are quite a large number of publications in this subject area. In particular, the papers [1–3] present reviews of methods of detection of anomalies, with proposed principles of classification of the methods for detection based on machine learning and statistical analysis. The overview of modern machine learning methods for cyber-attacks recognition systems (CARS) is well presented in the works [4–6]. However, certain methods,

such as k-means method [7] and its modifications [8–10] remain uncovered by these publications. The methods of detection of cyber-attacks on the basis of state machines (SM) is described in detail in [11, 12]. Another promising direction of development of ASDCA, covered in the works [13, 14], is the creation of systems to identify abuse on the basis of the analysis of states of MCCS [15].

The methods of computational intelligence, in particular neural networks (NN) for the tasks of detecting cyber-attacks, are described in the works [16, 17]. [13, 18] describe the models and methods of adapting genetic algorithms for the task of detection of cyber-attacks. The works [19, 20] describe the computational immune systems, which can be used for the task of setting up ASDCA.

The bayesian network for ASDCA, described in [21], is the model enabling collection of snapshots of a MCCS performance every few seconds for their subsequent analysis. [22] considers the possibility of application of MAR splines in ASDCA, enabling building of exact approximation of the behavior of a standard user, or of the attacking side, according to specified parameters. A large number of works is devoted to statistical analysis of the data in ASDCA [15, 23], to signature models [24] and theoretical aspects of the use of Markov chains [5, 6, 24] and the Petri nets [25] for the systems of cyber-attacks recognition.

A typical flaw of the most CARS described in [17, 19, 20, 24] is faulty triggering, because almost always only one technology of detection is involved (as a general rule, identification of attacks) in these systems. According to many authors [8, 10, 12, 16, 24, 26, 27], the most promising direction of the development of the methods for detection of cyber-attacks and anomalies is a combination of existing approaches in adaptive hybrid CARS with capacity for self-learning.

In the cited works, of certain interest in solving the tasks of providing a cyber defense of MCCS and the development of the systems of detection of cyber-attacks, the problem of the account of hard-to-explain and loosely connected features of threats, attacks and anomalies is not solved. Thus, further research is needed, aimed at developing methodological and theoretical bases for the creation of adaptive systems of detection of cyber-attacks, capable of fast learning or self-learning, and providing sustainable functioning of MCCS as an integral part of cybersecurity of the state.

3. The purpose and objectives of the study

The purpose of the study is to design a model for training the adaptive system of detection of cyber-attacks (ASDCA), which is being developed, based on the use of the apparatus of logical functions and elementary classifiers. The model allows taking into account the hard-to-explain features of threats, attacks and anomalies in the critically important computer systems, and it also reduces the time required for training ASDCA under conditions of the increase in the number of cyber threats.

To achieve the objectives of the work, the following tasks must be solved:

to design a model of logical procedures of detection of anomalies and cyber-attacks, based on the coverage matrices of features and the concept of an elementary classifier;

to minimize the number of training samples for the features which are located in the ASDCA repository.

4. The model of logical procedures of detection of anomalies and cyber-attacks based on the coverage matrices of features

To create an effective system of cyber defense (SCD) of MCCS, the choice and implementation of adequate technical components must be preceded by a stage of description, analysis and modeling of cyber threats and vulnerabilities of MCCS. Thus, it is clear that the cyber threats must be initially recognized, identified and categorized.

Incomplete initial data about cyber threats to MCCS have a dual quality. First, it is the lack of prehistory (sometimes, partial), including, at the level of the data about the structure of the entire object of a cyber-attack [12, 14, 23, 24], prior to the start of activities of the attacking side. And, secondly, limited capabilities of monitoring a concrete target of a cyber-attack and identification of the threats, belonging in a particular class. In an extreme case, only general multitude of threats to information security (IS) of MCCS and the ways to implement them are known in advance. Incomplete monitoring and evaluation of IS incidents in adverse events means that the subject can only assess the feedback from the object from the point of view of its preference.

However, in the case of occurring new cyber threats and vulnerabilities to MCCS, such an approach may not always contribute to effective protection against the attacks. So we shall consider below a model of logical procedures for detection of cyber-attacks (cyber threats, anomalies) (LPDCA) to MCCS, proposed in this work.

Let there exists a set of cyber threats to MCCS, general classification of threats is provided in [2, 4, 15, 24]. The indicator of danger of each cyber threat depends on the values of a set of factors that increase or decrease the protection of MCCS from a given threat. The indicators, decreasing protection of MCCS are considered to be risk indicators [24], and those increasing it – protection indicators [4, 6]. To formalize the dependency of MCCS's degree of protection on corresponding values, one can apply one of the following approaches [16, 19, 24]:

1) a cyber threat within a class depends on one indicator, i.e. the relationships of one-to-one correspondence exist between the degree of threat and the values of the indicator (factor);

2) a cyber threat depends on the values of many indicators;

3) the same indicators influence the degree of protection of MCCS not from one but from many kinds of cyber threats.

To ensure clarity, completeness and integrity of classification, we introduce the following requirements to the classification of cyber threats:

– disjoint classes of threats (it defines the uniqueness of class selection based on an external rule, allowing to make a decision);

– applicability (adding a class should not cause splitting more than one class in two parts);

– objectivity (presence or absence of a class must be confirmed by known classifications);

– extensibility (adding a class is possible by splitting existing classes);

– the number of classes is finite.

The information, to be taken as the basis for building classifiers of cyber threats for adaptive systems of detection of cyber-attacks (ASDCA), may be presented in different forms, for example in the form of hard-to-explain features of

anomalies in the performance of the system, of a cyber-attack or a threat to IS of MCCS. The following indicators can be used with this aim: threshold values of parameters of incoming and outgoing traffic; unintended packet addresses; attributes of database queries, etc. As the attack grows in complexity, the information features can be rather blurred.

For example, in the course of a complex cyber-attack in late December 2015 on the MCCS of power system of Ukraine in Ivano-Frankivsk Region, the power substation's computer center operator on duty saw the cursor's arrow on the display shift, though he had not touched the mouse. The cursor then moved on to the virtual switch, responsible for the physical switch and switched it. The operator was not able to log in at that time. The investigation showed the attack had been prepared during an extended period (not less than six months). The hackers first embedded Blackenergy 3 software into computers of the substation, and then a malicious program, claiming control of the power substations. In addition to the introduction of the virus, the attacking side launched a snowballing flow of calls to the call center of "Prikarpattyaoblenergo" so that the people could not report interruptions of power supply. Simultaneously 30 substations were cut off.

In a general case, the problem of detection of anomalies, cyber-attacks or threats to MCCS boils down to the following [1, 3, 9, 14, 24, 28, 29]. Certain set of objects is explored, in our case this is PA – the number of possible targets from the side that attacks MCCS. The objects of this set are described by the features $\{s_{ax1},...,s_{axn}\}$, represented, for example, in a binary form. It is known that the set of PA is displayed in the form of the combination of disjoint subsets (classes) of cyber threats to MCCS – $(CT_1,...,CT_l)$. Let us assume that there is a finite set of objects $\{ss_{a1},...,ss_{am}\}$ from PA, about which we know which classes of anomalies, attacks or threats they belong in (these are precedents, i.e. the objects used for training, – OUT). It is required, based on a set of values of features, specified in the OUT, i.e. the description of a certain object ss_{an} from PA, to identify this class and to adjust the performance of ASDCA for MCCS, accordingly. It is not known in advance, to which class the object can be attributed to.

A distinctive feature of the logical procedures examined in the work is the ability to obtain a reliable result when there is no a priori information about the function of distribution of existing values of features of a threat, cyber-attack or anomaly. Hereinafter we shall refer to such procedures as logical procedures. And there is no need to specify the so-called metrics in the space of object descriptions, characterizing each class. Therefore, for each feature of a cyber-attack (anomaly, threat, vulnerability, etc.), a binary function of similarity between its values is defined, allowing distinguishing objects and their representations (sub descriptions).

As the informative fragments, it is advisable to use only those fragments in the ASDCA that reflect typical patterns in the descriptions of the objects used for training (OUT). Therefore, the presence (absence) of such fragments in the categorized object allows determining its belonging in the class. When the logical procedures of detection of cyber-attacks (LPDCA) are applied, we also accept as informative those fragments that are found in the descriptions of the objects of the same class of cyber-attacks, but missing from the descriptions of objects from other classes. The fragments used include also a meaningful description of the OUT in terms of designing ASDCA.

To build LPDCA, the so-called elementary classifiers (EC) [16, 19, 21, 28, 29] are used. EC is a fragment that briefly describes the object and which is used for training ASDCA. For the objects under consideration (cyber threats, anomalies, vulnerabilities, etc.) $(CT_1,...,CT_l)$, many EC with preset properties are designed. We believe that, firstly, in the OUT it is advisable to use the classifiers that are present in the descriptions of the objects of the same class but absent in the descriptions of other classes' objects. Secondly, the aggregate of features and classifiers, characterizing all the objects of the analyzed class, are to be applied to the OUT.

The next problem when designing ASDCA is the presence of the OUT in the sample with characteristics, which are bordering different classes of cyber-attacks $(CT_1,...,CT_l)$. Each of these OUT is not atypical for its class, because its description is not similar to the informative representations of the OUT from other classes. The presence of atypical OUT in the training sample increases the length of the informative representations that distinguish objects from different classes. And since the long informative descriptions are less often present in new objects, this increases the share of unrecognized cyber-attacks (cyber threats, anomalies, vulnerabilities) in MCCS, which is particularly characteristic for the sophisticated types of cyber-attacks discussed above.

The algorithms of the synthesis of workable implementations for LPDCA depend directly on the success of the research of metrical (quantitative) properties of many informative fragments, i. e. the features of a cyber-attack (cyber threat, anomaly, vulnerability). And it is necessary to transform the incoming uncategorized training matrix (OUT) into a categorized one and to design, in a training mode, a clear division of the features space of detection into the classes of detection $CT_m^0 \,|\, m=\overline{1,M}$, where M is the power of the alphabet of classes.

Technically, it appears difficult to implement the following tasks in ASDCA:

1) to calculate the asymptotic estimate of the number of blind coverings for integer matrix of the object's features;

2) to calculate the asymptotic estimate of accepted and maximum values of conjunctions of Boolean function that can be applied to the synthesis of schematic-technical solutions of the ASDCA hardware for MCCS.

Let us consider the task of designing LPDCA based on the principle of "nonoccurrence" of sets of acceptable values of the features of cyber-attacks (cyber threats, anomalies, vulnerabilities).

Let us define: Q – total number of cyber threats to MCCS; B_{s_a} – set of numbers of cyber threats, implemented by an attacking side for achieving p_a – target of the cyber-attack; NP_{s_a} – an acceptable set of discrete features (of threat, anomaly, cyber-attack, etc.) in the $\{s_{a_1},...,s_{a_{jQ}}\}$ form.

The algorithm for calculating the value (ACV) of the significance of a feature for ASDCA can be presented as follows. Let us define the combination of subsets of $NP_{s_a}=\{s_{aj_i},...,s_{a_Q}\}$, $r_{p_a}\le Q$ in the system of the features of OUT. We assume the subsets defined being the reference for ACV. Their total combination is ΩQ.

Let us assign additional parameters: po_{ss_a} – the significance of the target of an attack (object) ss_{ai}, $i=1,2,...,$ PA, $po_{NP_{sa}}$ – the significance of the object of the referent set $NP_{s_a}\in\Omega Q$.

Let us calculate for each class of cyber-attacks on MCCS $CT\in\{CT_1,...,CT_l\}$, the value of belonging $E(ss_a,CT)$ of the object ss_a to the class CT, which has the form:

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

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

The object ss_{an} belongs in the class with the highest value $E(ss_a, CT)$. If there are many similar classes, then the algorithm refuses to detect further. To improve the correctness of the algorithm, it is necessary to solve a system of inequalities of the following type:

$$\begin{aligned} &E(ss_{a1}, CT_i) > E(ss_{a1}, CT_2), \\ &\quad . \ . \ . \\ &E(ss_{aQ}, CT_l) > E(ss_{aQ}, CT_{l+1}). \end{aligned} \qquad (2)$$

In order to solve the system (2), the parameters $po_{ss_{ai}}$ $i = 1, 2,..., PA$ and $po_{NP_{sa}}$, $NP_{s_a} \in \Omega Q$ should be selected. In a situation when the system is incompatible, one must find the subsystem that is maximally compatible with it. Then determine the values $po_{ss_{ai}}$ and $po_{NP_{sa}}$ out of the solution of this subsystem.

An alternative way to improve correctness of the performance of the algorithm is the path of selection of the system of reliable reference sets for the object detection (anomalies, threats, vulnerabilities, or cyberattacks). For example, to choose a sample in such a way so that the condition $E(ss'_a, CT) = 0$ is valid for any OUT $ss'_a \notin CT$. In addition, for any OUT $ss''_a \in CT$, the inequality $E(ss''_a, CT) > 0$ would be valid. One can do it in the following way. Let us assume $NP_{s_a} = \{s_{aj_1},..., s_{a_Q}\}$ as being the reference set. The combination of features NP_{s_a} will be considered satisfying the requirements of the test, if for any OUT ss'_a, ss''_a, and belonging in different classes at that, the condition $BN(ss'_a, ss''_a, NP_{sa}) = 0$ holds true. Thus, our test is a combination (a group) of features, according to which only any two objects from different classes differ.

It should be mentioned at this point that at present the most aggressive method to test the effectiveness of SPI of MCCS against various cyber-attacks or attempts of unauthorized access (UAA) is the penetration tests, during which the side performing the role of the attacker can use all modern arsenal of means and ways of overcoming the cyber defense mechanisms of MCCS. The obtained results are subjected to comprehensive analysis that eventually improves the SPI of MCCS, eliminates vulnerabilities and replenishes the knowledge base on threats, anomalies in the systems' performance.

Let us define as MC – combination of all EC which were obtained by the totality of features from $\{s_{ax1},...,s_{axn}\}$, i. e.

$$MC = (\sigma_{DOP}, NP_{sa}),$$

where

$$NP_{sa} \subseteq \{s_{ax1},...,s_{axn}\},$$

$$\sigma_{DOP} = (\sigma_{DOP_1},...,\sigma_{DOP_r}),$$

$$\sigma_{DOP_i} \in NP_{s_{aj}}, \text{ for } i = 1,2,...,r_{s_a}.$$

Let us suppose that a series Z of measurements of the values of the controlled features in MCCS was performed, and we received the matrix of features:

$$S = \begin{pmatrix} s_{ax_{11}} & s_{ax_{12}} & \dots & s_{ax_{1i}} & \dots & s_{ax_{1n}} \\ s_{ax_{21}} & s_{ax_{22}} & \dots & s_{ax_{2i}} & \dots & s_{ax_{2n}} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ s_{ax_{l1}} & s_{ax_{l2}} & \dots & s_{ax_{li}} & \dots & s_{ax_{ln}} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ s_{ax_{Z1}} & s_{ax_{Z2}} & \dots & s_{ax_{Zi}} & \dots & s_{ax_{Zn}} \end{pmatrix},$$

for example, the matrix of features, available in the ASDCA repository, will look like this

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

Thus, a set of objects to be tested, belonging in a class, is specified by the binary features {1001...–01}. The dash points to the uncertainty of a feature in OUT.

Each algorithm used for detection in MCCS of cyber-attacks, threats, anomalies or vulnerabilities of MCCS, within a class, is specified as – AL. Then we shall consider the subset of $MC^{AL}(CT)$ of the set MC.

Let us define

$$MC^{AL} = \bigcup_{j=1}^{l} MC^{AL}(CT_j).$$

The analysis of object sp_{an} is carried out on the basis of calculation of value $BN(\sigma_{DOP}, ss_a, NP_{sa})$ for each element (σ_{DOP}, NP_{sa}) of set

$$MC^{AL}(CT), CT \in \{CT_1,...,CT_l\}.$$

Here for each element $MC^{AL}(CT)$, the calculation is carried out to evaluate $E(ss_a, CT)$, which defines the belonging of ss_a in the class CT. Each algorithm AL, in its turn, is characterized by the set of EC $MC^{AL}(CT)$ and the method of calculation of the value $E(ss_a, CT)$.

The classifiers used in the algorithms

$$\sigma_{DOP} = (\sigma_{DOP_1},...,\sigma_{DOP_r})$$

are created by information features from NP_{sa}. And each EC must have at least one of the following properties:

1) fragment of group (ss'_a, NP_{sa}), where $ss''_a \in CT$, coincides with $\sigma_{DOP} = (\sigma_{DOP_1},...,\sigma_{DOP_r})$;

2) only part of fragments (ss'_a, NP_{sa}), where $ss'_a \in CT$, coincides with $\sigma_{DOP} = (\sigma_{DOP_1},...,\sigma_{DOP_r})$;

3) fragment of group (ss'_a, NP_{sa}), where $ss'_a \in CT$, do not coincide with $\sigma_{DOP} = (\sigma_{DOP_1},...,\sigma_{DOP_r})$.

The situation corresponding to property 1 occurs rarely in ASDCA. Therefore, to apply groups of features, which the property 1 refers to, is impossible in SDCA of MCCS. Property 2 characterizes only a certain subset of OUT in the considered classes of objects. The situation described by property 3 involves the use of all the objects from CT. Thus when the class CT is considered in ASDCA without an association with another class, it can be assumed that the groups of features within the range of property 3 will be more informative. Then

in situation 3, the argument in favor of the object ss_a belonging in the class can be the values of the features of the group that are missing in all the objects belonging in class CT.

In the models described in the works [20, 24], the methodology of designing EC σ_{DOP_i} for a specific class of cyber-attacks, threats, anomalies or vulnerabilities of MCCS is based on the synthesis of coverage matrices σ_{DOP_i}, which is formed by the OUT descriptions for CT. The use of such models [24, 27] allows reducing to some extent the computational costs in the work of the algorithms, for example, when inequality $|CT|<|\overline{CT}|$ is performed, particularly when there is a large number of classes of cyber-attacks, threats, anomalies or vulnerabilities to MCCS – $(CT_1,...,CT_l)=(B_{s_{a1}},...,B_{s_{al}})$.

Let us associate the object's EC

$$(\sigma_{DOP}, NP_{sa}),$$

where

$$\sigma_{DOP}=(\sigma_{DOP_1},...,\sigma_{DOP_r}),$$

NP_{sa} is the set of features with numbers $j_1,...j_{r_{sa}}$ with elementary conjunction $\Re=s_{axj_1}^{\sigma_{DOP_1}}...s_{axj_{ra}}^{\sigma_{DOP_{ra}}}$. If $ss_a=(\alpha s_{a1},...,\alpha s_{aQ})$ – the object out of set PA, therefore $BN(\sigma_{DOP},ss_a,NP_{sa})=1$ when and only when $(\alpha s_{a1},...,\alpha s_{aQ})\in NI_{\Re}$, where $NI_{\Re}$ – interval of truth of elementary conjunction $\Re$.

When designing LPDCA, it should be noted that the definition of the set of EC boils down to finding acceptable and maximal conjunctions for a distinctive function of the class of object CT (i. e., cyber threat, anomalies, cyber-attack, etc.). And this function is a two-valued Boolean function that takes different values in OUT from CT_l and $\overline{CT_l}$.

Then the procedure of detection of the object $ss_a=(\alpha s_{a1},...,\alpha s_{aQ})$, for example, cyber-attack in MCCS, is carried out on the basis of the results of calculation by elementary conjunctions – $\Re$. During the study, the results of which are described in the work [27], it was justified that the most economical was the variant to use the algorithm for calculating the conjunctions for coverage of the class of a corresponding object (cyber threat, vulnerability or attack).

Then the distinctive (characteristic) function of the CT class will be presented in the form of a function of algebra of logic (Boolean function) F_{KL}, which equals zero (0) on the information descriptions of object $ss_{an}=(\alpha s_{an1},...,\alpha s_{anQ})$ from CT_l and equals one (1) on the remaining sets of features from E_{CT}^{Q}. Here E_{CT}^{Q} is a combination of sets, of the length r_{s_a}. Then the accepted for $F_{\overline{CT}}$ conjunction will match the class coverage. Maximal for $F_{\overline{CT}}$ conjunction will correspond to blind coverage. The acceptable $\Re$ in the matrices of features of the objects will determine the belonging of a specific object $ss_{an}=(\alpha s_{an1},...,\alpha s_{anQ})$ in the CT_l class, if the condition $(\alpha s_{a1},...,\alpha s_{aQ})\notin NI_{\Re}$. is valid.

In our case, the search for abbreviated disjunctive normal form of a function (ADNF) boils down to obtaining ADNF for F_{CT}, which takes the value 0 on the sets from $B_{F_{\overline{CT}}}$ and the value of 1 on the rest of the sets E_{CT}^{Q}. Once the ADNF for $F_{\overline{CT}}$ is received, the conjunctions $\Re$, which do not have the property of $NI_{\Re}\cap A_{F_{CT}}\neq 0$, must be deleted out of it.

For example, obtaining ADNF of the logical function is possible by way of transforming conjunctive function of the type $D_1\wedge D_2\wedge...\wedge D_u$, where

$$D_i=s_{ax1}^{\overline{\beta_{i1}}}\vee s_{ax2}^{\overline{\beta_{i2}}}\vee...\vee s_{axQ}^{\overline{\beta_{iQ}}}, i=1,2,..,mu$$

implements the function F_{CT}, β_{iQ} – elements of set $B_{F_{\overline{CT}}}$.

Let us consider:

$$\overline{s_{ax}^{\alpha}}=\bigvee_{\beta_i\neq\alpha_i}s_{ax}^{\beta}.$$

Then the conjunctive function takes the form:

$$D^*_1\wedge D^*_2\wedge...\wedge D^*_u,$$

where

$$D^*_i=\bigvee_{\iota\neq\beta_{i1}}s_{ax1}^{\eta}\vee\bigvee_{\iota\neq\beta_{i2}}s_{ax2}^{\eta}\vee...\vee\bigvee_{\iota\neq\beta_{iQ}}s_{axQ}^{\eta}, i=1,2,..,u.$$

During the detection, the proximity of objects

$$ss'_a=(\alpha s'_{a1},...,\alpha s'_{aQ}) \text{ and } ss''_a=(\alpha s''_{a1},...,\alpha s''_{aQ})$$

from PA on the features matrix NP_{s_a} was measured by the parameter:

$$BN(ss'_a,ss''_a,NP_{sa})=\begin{cases}1, & \text{if } \alpha s'_{j_{ti}}=\alpha s''_{j_{ti}} \text{ at } ti=1,2,...,r_{s_a},\\ 0 & \text{if else.}\end{cases} \quad (3)$$

Thus, obtaining LPDCA and sets of EC for the modelled class of objects (cyber threats, anomalies or cyber-attacks) is reduced to the following:

1) we set the distinctive function;

2) we find DNF (or ADNF) that implements this function;

3) we find acceptable (maximal) conjunction $\Re$ that defines the belonging of the object in the class under consideration.

Since EC and OUT are limited in quantity, the following rules of training were used in ASDCA. Let there exists a priori categorized training matrix in the form of OUT is

$$\left\|s_{axi}^{(j)}\right\|, i=\overline{1,N}, j=\overline{1,n},$$

where N, n is the number of features of detection (for example, of an attack) and tests, respectively. It is necessary to modify a training matrix for OUT under the condition of minimizing the number of features, its columns and rows, in accordance with the following rules of training:

$$H_{1,m}^{(k)}[0]=0; H_{2,m}^{(k)}[0]=0;$$

$$s_{ax_{m,i}}^{(j)}=\begin{cases}1, \text{if } \zeta_b\le\Delta_{m,i}^{(j)}\le\zeta_t;\\ 0, \text{if else.}\end{cases}$$

$$I(s_{ax_i})=1+\sum_{i=1}^{G}(P_i\cdot\sum_{ct=1}^{CT}P_{i,ct}\cdot\log_{ct}P_{i,ct});$$

$$\text{if } s_{ax_m}^{(j)}\in CT_m^0 \text{ then } H_{1,m}^{(k)}[j]:=H_{1,m}^{(k)}[j-1]+1;$$
$$\text{if } s_{ax_c}^{(j)}\in CT_m^0 \text{ then } H_{2,m}^{(k)}[j]:=H_{2,m}^{(k)}[j-1]+1, \quad (4)$$

where $H_{1,m}^{(k)}$, $H_{2,m}^{(k)}$ is the number of events that characterize the belonging of the OUT implementations to the combination of features for EC of the considered class of objects (anomalies, threats, cyber-attacks) and the number of events that characterize the affiliation of the OUT implementations to the combination of features for EK of a "foreign" class of objects, respectively; ζ_b,ζ_t – upper

and lower control tolerances for a feature; $\Delta^{(j)}_{m,i}$ – selected mean value of the i feature in the vectors of OUT of the basic class of object; $I(s_{ax_i})$ – informational content of the feature within the limits of the class of an object; G – the number of gradations of the feature of an object; P_i – the probability of the i-th gradation of the feature; $P_{i,ct}$ – the likelihood of the occurrence of the i-th gradation of the feature in the class of objects CT.

Thus, the algorithm of training ASDCA is in an iterative procedure of finding DNF for the distinctive function of the object of detection by the feature matrix (3) and minimizing the number of features, the columns and rows of the OUT matrix (4) to its limit value, which includes acceptable (maximal) conjunction that defines the belonging of the object in the studied class of anomalies, threats and cyber-attacks.

6. The program of the search of the minimally needed numbers of features of detection for different classes of cyber-attacks

In the course of the research, a program was designed for evaluation of the complexity of the search algorithm of the minimally needed number of features for different classes of cyber-attacks, threats, anomalies and threats, Threat Analyzer, Fig. 1–3.

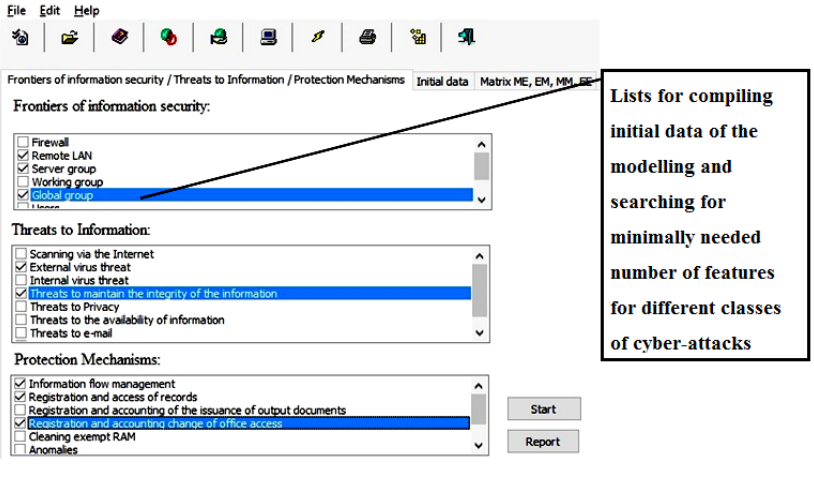

Fig. 1. The interface of the program Threat Analyzer, form 1

The form 1 sets analyzed classes of attacks and anomalies, Fig. 1. The form 2 shows the calculation results for training matrices in the form of OUT, taking into account the information content of each of the 3–21 features. The form 3 visualizes the results of calculation in the form of histograms, as well as the evaluation of the complexity of the algorithm of forming OUT depending on the class of an attack (anomaly, threat), Fig. 3.

The modelling allowed drawing the conclusion that the objects belonging in different classes of anomalies, threats or cyber-attacks are often difficult to separate from each other. A rather large number of features (for certain classes of cyber-attacks, up to 50 %) have the information weight almost equaling zero. In the case of using a set of features for the formation of the OUT, it is advisable to reject the requirement of its futility. This is done in order to increase the speed of the algorithm.

For example, in the case of an increase in the number of features from 3 to 6, the average number of checks per object ranged from 150 to 800, respectively. The use of representative sets with length of 3–4 features in the matrices of OUT made it possible to achieve maximum efficiency of the performance of the algorithm of detection for the majority of the known anomalies, cyberattacks and threats. In the situation when the features of the class of an object (e. g., cyber-attack) were positioned according to the decreasing information content (I), for every object there was a combination of features with greater information content and then the information content of the group decreased smoothly, Fig. 4. Thus the less meaningful features (PS<60 %) were not included in OUT.

The following feature of the matrix forming the OUT was identified. The information content of the control set formed by the two features, characteristic for different classes of attacks, such as Dos/DDos, U2R, R2L, may describe the object of detection better than each of the features and the EC class separately. And the level of detection of cyber attacks, for which the training matrices of OUT were compiled, ranged from 25 % to 30 % for 2 features, 85–87 % for 3–4 features, 92–98 % for 5–9 features, Fig. 5.

Thus the OUT, described by a fragment of 2–3 features, belonging in different classes of objects, better described the studied class than each of the features separately. For example, in the tasks of assessing the impact of a cyber-attack on the systems of satellite navigation of MCCS of the transport, the most informative was the following group of features:

1) signal level (because the GPS signal at the Earth's surface is around 163 dB·Wt., at the same time the signals of simulators tend to be higher, which may indicate the attack);

2) the same level of signal from different satellites (signals of the different GPS satellites tend to differ significantly).

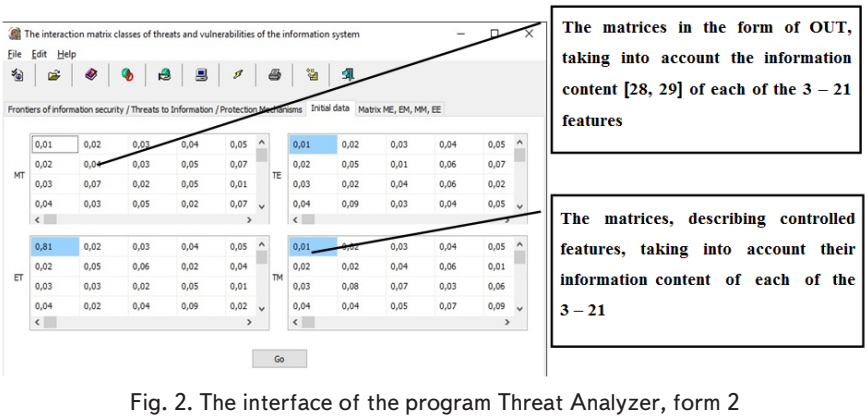

Fig. 2. The interface of the program Threat Analyzer, form 2

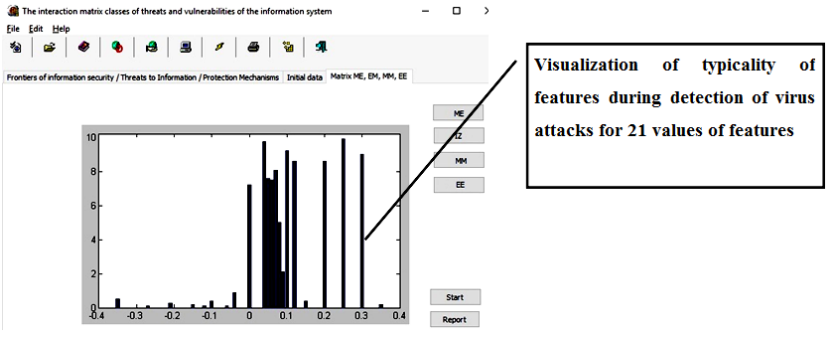

Fig. 3. The interface of the program Threat Analyzer, form 3

The information about the features of detection of the objects (cyber-attacks) was received from the data from various sources (sensors) of MCCS software and hardware. In particular, the reports were considered about the attacks generated by the integrated antivirus technologies, log files were analyzed, as well as dumps of RAM and PC, hard drives' reports, system entry logs, databases, queries, and so forth. The part of features of the attacks was admitted according to [28, 29].

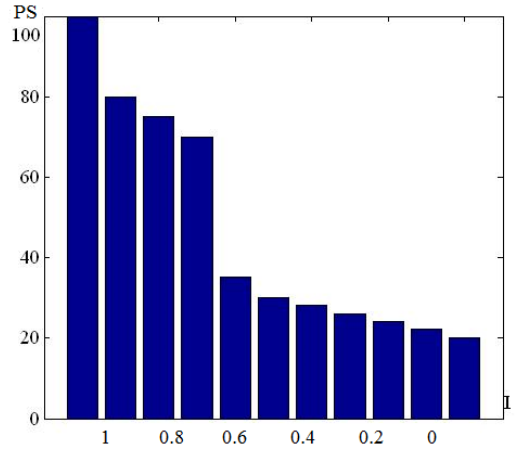

Fig.4. Visualization of the significance of the features (PS) and their information content (I) in the training matrix of OUT for network attacks

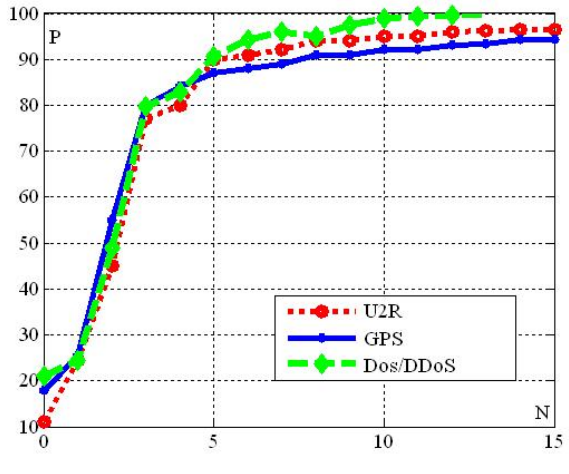

Fig. 5. Visualization of the accuracy of detection (P, %) for attacks of classes U2R, DOS/ DDoS and attacks on satellite systems of GPS, depending on the number of features (N) in the OUT training matrix

The features – noise and the satellites' numbers were less informative, although a joint application in the OUT of total described features in terms of combined information content did not lose to more significant feature – the level of signal.

The research compared the effectiveness of the proposed model based on the criterion of average number of rules for training, Table 1.

Table 1

Average number of rules, matrices and training steps of ASDCA for detection of typical classes of cyber-attacks in MCCS

Class of objects for detection (of cyber-attacks)*	Number of features**	The average number of rules, matrices and steps for training per object (Rules/Matrices/Steps for learning)		
		Models and algorithms for consecutive option of features***	Statistical models of forecasting the states****	Model, based on training samples and EC class
Network attacks through the corporate system	11	200/30/2000	350/65/2000	60/10/2000
Attacks on standard components of MCCS SW	19	350/50/3500	450/35/3500	30/15/1500
Network Intelligence	15	320/40/2500	120/30/2500	70/20/2000
Attacks aimed at passwords selection	12	230/15/1500	180/25/1300	25/20/1500
Attacks of Man-in-the-Middle type	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 ERP systems via HARD protocol	5	170/30/2700	210/50/2300	60/35/1900
Attacks on components of LCS	9	260/25/2400	200/40/2500	45/35/2000
Attacks on SCADA systems	7	600/70/4000	800/60/3000	150/50/3500
Attacks on HMI	3	500/50/3000	400/60/3000	70/30/2600
Attacks of the substitution («Funnel attack»)	15	150/35/1500	100/55/1500	30/15/1500
Compromising the data collection site	5	250/30/1700	190/35/1800	30/20/1300
Change of a router	11	300/40/2300	380/60/2500	35/20/1700
Copying information from peripheral devices	15	150/25/1500	75/20/1400	45/10/1000
Attacks on the satellite navigation systems	9	90/30/4000	150/50/4000	20/15/150

*Note: * – according to data [1, 2, 15, 24, 28, 29]; ** – features and their information content according to data [28, 29]; *** – according to data [1, 2, 16, 24]; **** – according to data [6, 8, 15, 19, 24]*

To test the effectiveness of the proposed model, a series of experiments for main attacks was conducted, shown in Table 1. The example of test results for attacks on SCADA systems is shown in Fig. 6.

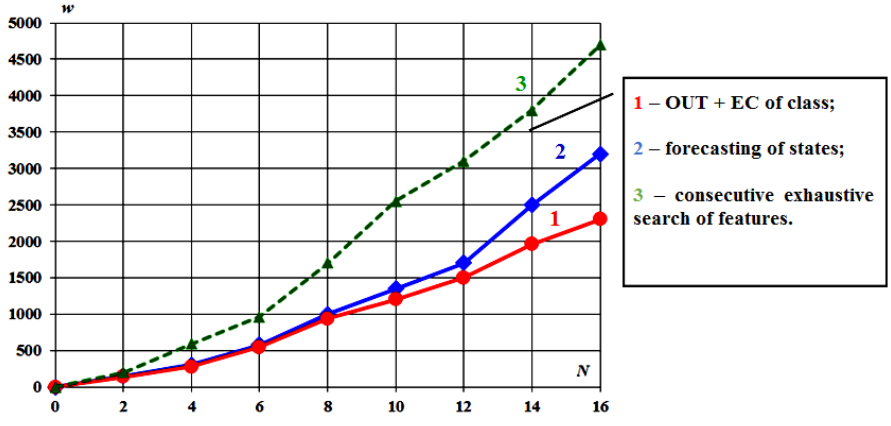

Fig. 6. Compared effectiveness of the proposed model for the detection of attacks on SCADA systems (N – the number of features; w – the number of training steps of ASDCA)

It was experimentally found that, compared to the methods of consecutive exhaustive search of features and statistical algorithms of states, the proposed model allows:

– reducing the number of necessary rules of object detection within a class by 2.5–12 times (depending on the class of objects – anomalies, cyber-attacks, threats);

– reducing by 7–9 % the time of detection of anomalies and cyber-attacks.

In the test mode of training ASDCA, the rational number of steps of training OUT for the proposed model amounted to $w \approx 3000$ for the known classes of objects and $w \approx 3500...4500$ for more sophisticated cyber-attacks and anomalies.

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

The complexity of training ASDCA using the apparatus of logical functions and EC relates solely to the stage of obtaining DNF out of maximal conjunctions of distinctive function for each of the classes.

The effectiveness of the application of the designed model will increase as more informative features are included into a representative set of OUT and as more copies will join the original matrix of data characterizing a certain class of anomalies, attacks or cyber threats. With a small number of features in OUT, the effect of the model's implementation will be negligible. Thus, the prospects of further research are in the improvement of the knowledge base of features in the form of their matrix representation, as well as conducting of the research of the model on a larger number of objects stored in the ASDCA repository.

The designed model, if compared to the results obtained for the models, presented in Table 1, provides significantly less number of necessary features for categorization of threats, while reducing training time of adaptive SDCA. In addition, the developed program *Threat Analyzer* can automatically create dimensions of the training matrix of features of anomalies, cyber threats or cyber-attacks, without requiring the participation of experts.

Scientific and practical results of the research in the form of hardware and software applications and methodical materials have been implemented at the State Enterprise "Design and Construction Technological Bureau of Automating of Systems of Control of Railway Transport of Ukraine" of the Ministry of Infrastructure of Ukraine, as well as in the departments of information security of several computer centres of industrial and transport enterprises.

At present, based on the proposed model and the test results, a system of decision-making support and an expert system is being developed, able for adaption and self-learning in the process of solving complex tasks of providing cyber defense of MCCS.

8. Conclusions

As a result of the research:

– the model of detection of cyber attacks, anomalies and threats to mission critical computer systems was designed, which is based on the application of training samples in the form of feature matrices and elementary classifiers for each of the modeled class;

– the studies were carried out on minimizing the number of training samples from the informative features for the ASDCA being developed. It was found that for detection in training matrices of OUT it was sufficient to use representative sets of 3–4 features long. The effectiveness of detection of anomalies and cyber-attacks reached 98 %. The proposed model reduces the number of necessary rules for ASDCA by 2.5–12 times and reduces the time of detection of anomalies and cyber-attacks by 7–9 %.

References

1. Jyothsna, V. A review of anomaly based intrusion detection systems [Text] / V. Jyothsna, V. V. Prasad Rama // International Journal of Computer Applications. – 2011. – Vol. 28, Issue 7. – P. 26–35. doi: 10.5120/3399-4730
2. Baddar, S. A.-H. Anomaly detection in computer networks: a state-of-the-art review [Text] / S. A.-H.Baddar, A. Merlo, M. Migliardi // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications. – 2014. – Vol. 5, Issue 4. – P. 29–64.
3. Gyanchandani, M. Taxonomy of anomaly based intrusion detection system: a review [Text] / M. Gyanchandani, J. L. Rana, R. N. Yadav // International Journal of Scientific and Research Publications. – 2012. – Vol. 2, Issue 12. –P. 1–13.

4. Vinchurkar, D. P. A review of intrusion detection system using neural network and machine learning technique [Text] / D. P. Vinchurkar, A. Reshamwala // International Journal of Engineering Science and Innovative Technology (IJESIT). – 2012. – Vol. 1, Issue 2. – P. 54–63.
5. Tsai, C.-F. Intrusion detection by machine learning: a review [Text] / C.-F. Tsai, Y.-F. Hsub, C.-Y. Linc, W.-Y. Lin // Expert Systems with Applications. – 2009. – Vol. 36, Issue 10. – P. 11994–12000. doi: 10.1016/j.eswa.2009.05.029
6. Omar, S. Machine learning techniques for anomaly detection: an overview [Text] / S. Omar, A. Ngadi, H. H. Jebur // International Journal of Computer Applications. – 2013. – Vol. 79, Issue 2. – P. 33–41. doi: 10.5120/13715-1478
7. Riadi, I. Log Analysis Techniques using Clustering in Network Forensics [Text] / I. Riadi, J. E. Istiyanto, A. Ashari, Subanar // International Journal of Computer Science and Information Security. – 2013. – Vol. 10, Issue 7. – P. 23.
8. Ranjan, R. A new clustering approach for anomaly intrusion detection [Text] / R. Ranjan, G. Sahoo // International Journal of Data Mining Knowledge Management Process (IJDKP). – 2014. – Vol. 4, Issue 2. – P. 29–38. doi: 10.5121/ijdkp.2014.4203
9. Guan, Y. Y-means: a clustering method for intrusion detection [Text] / Y. Guan, A. A. Ghorbani, N. Belacel // CCECE 2003 – Canadian Conference on Electrical and Computer Engineering. Toward a Caring and Humane Technology (Cat. No.03CH37436). – 2003. – Vol. 2. – P. 1083–1086. doi: 10.1109/ccece.2003.1226084
10. Li, W. A New intrusion detection system based on knn classification algorithm in wireless sensor network [Text] / W. Li, P. Yi, Y. Wu, L. Pan, J. Li. // Journal of Electrical and Computer Engineering. – 2014. – Vol. 2014. – P. 1–8. doi: 10.1155/2014/240217
11. Ilgun, K. State transition analysis: a rule-based intrusion detection approach [Text] / K. Ilgun, R. A. Kemmerer, P. A. Porras // IEEE Transactions on Software Engineering. – 1995. –Vol. 21, Issue 3. – P. 181–199. doi: 10.1109/32.372146
12. Khan, L. A new intrusion detection system using support vector machines and hierarchical clustering [Text] / L. Khan, M. Awad, B. Thuraisingham // The VLDB Journal. – 2007. – Vol. 16, Issue 4. – P. 507–521. doi: 10.1007/s00778-006-0002-5
13. Wu, S. X. The use of computational intelligence in intrusion detection systems: a review [Text] / S. X. Wu, W. Banzhaf // Applied Soft Computing. – 2010. – Vol. 10, Issue 1. – P. 1–35. doi: 10.1016/j.asoc.2009.06.019
14. Kabiri, P. Research on intrusion detection and response: a survey [Text] / P. Kabiri, A. A. Ghorbani // International Journal of Network Security. – 2005. – Vol. 1, Issue 2. – P. 84–102.
15. Ameziane El Hassani, A. Integrity-OrBAC: a new model to preserve Critical Infrastructures integrity [Text] / A. Ameziane El Hassani, A. Abou El Kalam, A. Bouhoula, R. Abassi, A. Ait Ouahman // International Journal of Information Security. – 2014. – Vol. 14, Issue 4. – P. 367–385. doi: 10.1007/s10207-014-0254-9
16. 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
17. 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.
18. 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.
19. Zhou, Y. P. Hybrid Model Based on Artificial Immune System and PCA Neural Networks for Intrusion Detection [Text] / Y. P. Zhou // Asia-Pacific Conference on Information Processing. – 2009. – Vol. 1. – P. 21–24. doi: 10.1109/apcip.2009.13
20. Komar, M. Development of Neural Network Immune Detectors for Computer Attacks Recognition and Classification [Text] / M. Komar, V. Golovko, A. Sachenko, S. Bezobrazov // 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS). – 2013. –Vol. 2. – P. 665–668. doi: 10.1109/idaacs.2013.6663008
21. Heckerman, D. A tutorial on learning with bayesian networks. Innovations in Bayesian Networks [Text] / D. Heckerman // Theory and Applications. – 2008. –Vol. 156. – P. 33–82.
22. Mukkamala, S. Intrusion detection systems using adaptive regression splines [Text] / S. Mukkamala, A. H. Sung, A. Abraham, V. Ramos // Sixth International Conference on Enterprise Information Systems. – 2006. – P. 211–218. doi: 10.1007/1-4020-3675-2_25
23. 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
24. Raiyn, J. A survey of Cyber Attack Detection Strategies [Text] / J. Raiyn // International Journal of Security and Its Applications. – 2014. – Vol. 8, Issue 1. – P. 247–256. doi: 10.14257/ijsia.2014.8.1.23
25. Jasiul, B. Detection and Modeling of Cyber Attacks with Petri Nets [Text] / B. Jasiul, M. Szpyrka, J. liwa // Entropy. – 2014. – Vol. 16, Issue 12. – P. 6602–6623. doi: 10.3390/e16126602
26. Peddabachigari, S. Modeling intrusion detection system using hybrid intelligent systems [Text] / S. Peddabachigari, A. Abraham, C. Grosan, J. Thomas // Journal of Network and Computer Applications. –2007. – Vol. 30, Issue 1. – P. 114–132. doi: 10.1016/j.jnca.2005.06.003
27. Lahno, V. Information security of critical application data processing systems [Text] / V. Lahno // TEKA. Commission of motorization and energetics in agriculture. – 2014. – Vol. 14, Issue 1. – P. 134–143.
28. Rid, T. Attributing Cyber Attacks [Text] / T. Rid, B. Buchanana // Journal of Strategic Studies. – 2015. – Vol. 38, Issue 1-2. – P. 4–37. doi: 10.1080/01402390.2014.977382
29. Guitton, C. The Sophistication Criterion for Attribution [Text] / C. Guitton, E. Korzak // The RUSI Journal. – 2013. – Vol. 158, Issue 4. – P. 62–68. doi: 10.1080/03071847.2013.826509