UDC 004.56

A. V. Skatkov, ScD.,
A. A. Briukhovetskyi, PhD.,
A. A. Selkin

AN ADAPTIVE FUZZY LOGIC MODEL FOR INTRUSION DETECTION IN COMPUTER NETWORKS BASED ON ARTIFICIAL IMMUNE SYSTEM

Abstract. *An adaptive model and the structure of the Intrusion Detection System (IDS), which is constructed based on immunological principles was proposed. Fuzzy rules classify objects belonging to several classes simultaneously with varying degrees of affiliation. Recognition of network traffic state is the shortage of a priori information about the properties of the source intrusion and the stochastic nature of recognizable events. To increase the level of confidence in the intrusion detection system was made adaptive tuning of decision rules for the classification of network traffic states. The system is designed for the detection and classification of network attacks classes: DoS, R2L, U2R, Probe . Setting up and testing of the model are based on the detection of anomalies in the data sets obtained from the real IP-traffic of computer networks and contained in a certain database KDD'99.*

Keywords: *adaptive model, intrusion detection, fuzzy rules, IP-traffic, IDS, immune system, quality rules, classifier, population, the optimization algorithm*

А. В. Скатков, д-р техн. наук,
А. А. Брюховецкий, канд. техн. наук,
А. А. Селькин

АДАПТИВНАЯ НЕЧЕТКАЯ МОДЕЛЬ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В КОМПЬЮТЕРНЫХ СЕТЯХ НА ОСНОВЕ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ

Аннотация. *Предлагается адаптивная модель и структура системы обнаружения вторжений, которая построена на основе иммунологических принципов. Нечеткие правила классифицируют принадлежность объектов нескольким классам одновременно с различной степенью принадлежности. Распознавание состояния сетевого трафика осуществляется в условиях дефицита априорной информации о свойствах источника вторжений и стохастической природы распознаваемых событий. Для повышения уровня достоверности обнаружения вторжений в системе производится адаптивная настройка правил принятия решений по классификации состояний сетевого трафика компьютерной сети. Настройка и тестирование модели выполнены на основе обнаружения аномалий в наборах данных, полученных из реальных IP-трафиков компьютерных сетей и содержащихся в известной базе данных KDD'99.*

Ключевые слова: *адаптивная модель, обнаружение вторжений, нечеткие правила, IP-трафик, иммунные системы, качество правил, классификатор, популяция, алгоритм оптимизации*

О. В. Скатков, д-р техн. наук,
О. О. Брюховецький, канд. техн. наук,
О. О. Селькин

АДАПТИВНА НЕЧІТКА МОДЕЛЬ ВИЯВЛЕННЯ ВТОРГНЕНЬ В КОМП'ЮТЕРНЫХ МЕРЕЖАХ НА ОСНОВЕ ШТУЧНИХ ИМУННИХ СИСТЕМ

Анотація. *Пропонується адаптивна модель і структура системи виявлення вторгнень, яка побудована на основі імунологічних принципів. Нечіткі правила класифікують приналежність об'єктів декількох класах одночасно з різним ступенем приналежності. Розпізнавання стану мережевого трафіку здійснюється в умовах дефіциту апріорної інформації про властивості джерела вторгнень і стохастичної природи подій які розпізнаються. Для підвищення рівня достовірності виявлення вторгнень в системі проводиться адаптивна настройка правил прийняття рішень щодо класифікації станів мережевого трафіку комп'ютерної мережі . Налагодження та тестування моделі виконані на основі виявлення аномалій в наборах даних , отриманих з реальних IP- трафіків комп'ютерних мереж і які знаходяться у відомій базі даних KDD'99 .*

Ключові слова: *адаптивна модель, виявлення вторгнень, нечіткі правила, IP-трафік, імунні системи, якість правил, класифікатор, популяція, алгоритм оптимізації*

Introduction. The problem of information security does not lose its relevance due to the fact that today networks are faced with an unprecedented range of computer threats that lead to the violation of the integrity, confidentiality and availability of resources. Nowadays there are many intrusion detection systems (IDS), which effectively perform detailed the research of the state of network traffic and the search for sources of intrusions [1, 2]. However, there is an urgent need for continuous improvement of the

IDS, because of continuously development of various types of attacks on the network objects.

Depending on the source of intrusion the detection systems are distinguished level host-based (HBIDS) and network IDS (NIDS – network intrusion detection). The first, as a rule, are the monitor traffic and individual computer kernel [3, 4], the second examine network traffic and determine its state, which are normal (NS) or abnormal (AS) [5]. At the time, intrusion detection systems, depending on the technology used to identify attacks, are divided into two main types: detection of malicious behavior and abnormaly detection system. First are guided by the model of malicious behavior (for example, the pattern / signature attack), and compare the model with the flow of events. The existing signature-based intrusion detection systems can not be intercepted by the profiling data stream distributed intrusion for their classification and generating a signal to invade. Therefore, intrusion detection systems of the second type use methods to detect unknown attacks. Such IDS usually designed on the base of the models of normal behavior and abnormal occurrences, which are looking into the event flow.

The main problem in intrusion detection is to conduct an objective assessment of the controlled light intrusion in terms of correct classification [1 – 3]. Currently used to solve various statistical models estimating the probability of the occurrence of specified values (events) [6], hidden Markov models [7], a model based on fuzzy logic [8], as well as data mining techniques such as neural networks [9], association rules [10], decision trees [11], data clustering [12], artificial immune system (AIS) [13] and others.

The analysis shows that the further development of the results in the IDS is achieved with the following areas of research that we believe to improve the efficiency of the systems, make the recognition process more reliable traffic status in the early stages of intrusion detection, reduce the number of false alarms and others. These areas are:

• Improving the efficiency of IDS, which can be achieved by improving the combined methods of intrusion detection, including adaptive models, fuzzy logic and AIS.

• Using of adaptive IDS in a deficit of priori information about the properties of the source intrusion will increase the stability classification methods to some changes in the implementation of the attack. These systems respond to changes in the input data by adjusting the parameters of the rules and structure of the IDS.

• Application of the methods based on fuzzy logic has significant advantages over binary, deterministic classifiers intrusion. In particular, these classifications are not fully take into account the nature of the controlled events, which is stochastic. While monitoring events in the system, it is usually impossible to conclude unequivocally that they belong to a particular class: normal or abnormal. Therefore, the use of methods based on fuzzy logic is justified.

• Much of the teaching methods of fuzzy systems use genetic algorithms (GA) [14]. However, the classic GA and their varieties are not always effective in solving the problem of multimodal optimization. Therefore, improving the efficiency of learning algorithms of fuzzy models is carried out through the creation of new methods of using the ability to dynamically change the optimization algorithms. AIS meet these requirements, which are inherent properties such as pattern recognition, diversity, training, multidynamics and other.

The aim of this work is the development and improvement proposed in [13, 16] intrusion detection methods based on the use of adaptive models in combination with the methods of AIS and fuzzy logic.

Building Intrusion Detection Model (IDM). In constructing the model are based on the analysis of information obtained by treating the real IP-traffic, details of which are presented in a publicly samples network traffic KDD Cup 1999 [15]. Used, the database input structurally represent n – dimensional vector, which is known a priori that they belong to one of five classes of Cl (l = 1 .. 5) possible states of network traffic: DoS – Denial of Service, R2L – unauthorized access from a remote computer, U2R – unauthorized access to privileged user, Probing –port scanning to identify vulnerabilities in the system, NS –Normal.

We use the following decision rules fuzzy inference (hereinafter, the term “rule” means a rule of fuzzy inference) for the solution of k-

dimensional classification vectors $x = (x1, ..., xn)$ with n numeric attributes using Cl classes:

$$R_j: IF\ X_1\ is\ A_i\ AND\ ...\ AND\ X_n\ is\ A_n \quad then\ CLASS\ C_l \mid CF_j, f_j \quad , \qquad (1)$$

where R_j – mark j-th fuzzy rule, $j = 1, 2, ..., N$; N – the number of fuzzy rules; A_i — linguistic term (each input interval x_i-th numeric attribute splits using linguistic terms); CF_i – function defining the degree of membership of a particular class , $CF_j \in [0,1]$; f_j – quality metric classification rules, $f_j \in [-1; 1]$:

$$ff = w1 \bullet a_j / \mid AS \mid - w2 \bullet b_j / \mid NS \mid , \qquad (2)$$

where a_j – number of correct classification of the plant; b_j – the number of misclassified NS; $|AS|$ – total number of speakers ; $| NS |$ – total number of NS ; $w1$, $w2$ – nonnegative weights; $w1 + w2 = 1$. Values CF_j, f_j are determined during the training phase IDM.

Intrusion detection model structure will represent a tuple $M = (X, Y, R, Pr, W, U, C, A, Pp)$, where X is the set of vectors that describe the current state (CS) of network traffic; Y – IDM output network traffic condition, wherein $Y = 1$ in the case where the hypothesis that CS corresponds to the AS (denoted as $CS = AS$), and $Y = 0$, else if $CS = NS$; R – set of fuzzy rules R_j, $j = 1 .. N$; Pr – pre-processing procedures in order to eliminate redundancy and to identify informative features of network traffic; W – many adjustable parameters of the rules; U – set parameters optimization procedures w rules; A – set of procedures adaptation parameters w rules; C – set of classification procedures CS; Pp – set of procedures for deciding on the status CS.

On the basis of the IDM proposed IDS structure is shown in Fig.1, where the following notation: X_{ts} – teaching sampling network traffic; X^* – updated training sample obtained during the operation of IDS; f_j – quality metric j-th CS classification rule; $R_w(NS)$ / $R_w(AS)$ – the set of optimized classification rules NS / AS, formed at the stage of setting up and testing the given parameters w; $Y(NS)$ / $Y(AS)$ – signal generated by a plurality of rules $R_w(NS)$ / $R_w(AS)$, $Y(NS)$, $Y(AS) = \{0,1\}$, DR / DR^* – likelihood of intrusion detection level in setup mode and test / operation of IDS ; FAR / FAR*– level IDS false positives in setup mode and test / operation of IDS; f^*_j – quality metric j-th CS classification rule in operation of IDS.

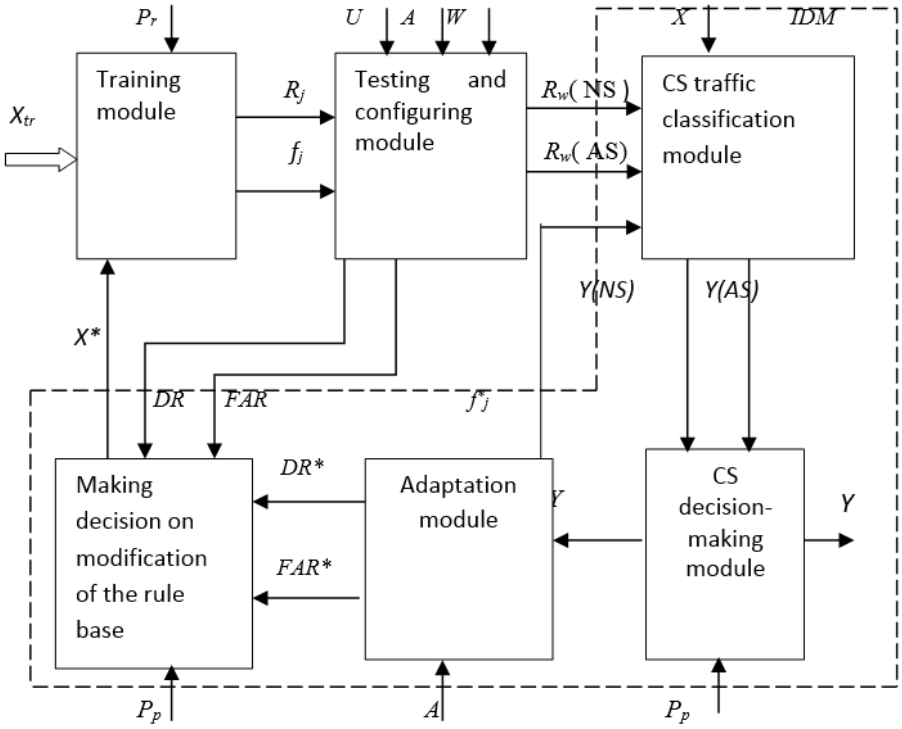


Fig. 1. Functional structure of adaptive IDS

Learning module. The module is designed to identify informative features of network traffic and the formation of fuzzy rules of the form (1). Functional conversion performed in the module, reduces the formation of a set of rules based on the learning sample examples: $X(d)$ -> $X(n)$ -> R, the dimension of the original vectors (d = 41), n – dimensional vector at the module output, $n < d$. With the pretreatment procedure identifies the most informative features of the network traffic. The main goal – to reduce the dimension of the processed vectors and increase the reliability of the classification of traffic status. The procedure is based on an assessment of a prior probability of the values of attributes and a posteriori probability vectors accessories specified classes [16].

At the second stage of training patterns are formed on fuzzy decision rules of the form (1). For each element of the Cartesian product of the set of examples and a set of rules score calculated CF_j. Moreover, for each value of the input variable fuzzy sets are formed, which correspond to the maximum values of the membership functions. The output value of the membership function CF_j example a certain class of sets $\{C_1\}$ is calculated as a result of the fuzzy operation 'AND' all input variables x_i. At this stage, the initial values of the metrics f_j rules using training samples with known responses of base KDD Cup. As a result, formed the basic set of rules $R_\alpha(AS)$ and $R_\alpha(NS)$ in classifying anomalous and normal traffic , of which eliminate duplicate rules and that have defined thresholds metrics CF_α, f_α, providing higher value of the likelihood DR intrusion detection and low value FAR indicator of false alarms. Formed a set of rules R_α can be considered in terms of AIS, as the population of antibodies. Quality rules included in R_α integrally valued metric F_α [16], which is constructed as an average value f_j quality metrics separate classification rules. The most effective subset of rules R_α has a maximum value of the metric F_α:

$$Fmax = \max_{R_\alpha} \{F_\alpha\}. \qquad (3)$$

Module testing and tuning. Main function of this module is associated with the formation of an optimized set of rules for each of the five classes: R -> Rw. The algorithm for generating and optimizing the structure and parameters of fuzzy rules based on the iterative procedure sequential processing examples of training sample based on the methods of AIS [16]. At the same time we have an antigen n – dimensional numerical vector of training sample, as antibodies – fuzzy rules. The model uses a triangular membership function with parameters a, b, c [8]. Input each interval x_i-th numeric attribute, which is broken by three linguistic terms. In the result, it is tuned the parameters a, b, c and shaped membership functions optimized structure of fuzzy rules in accordance with (1) and the criterion (3).

In test mode, the correction of the metric values f_j quality rules. Whenever triggered (activated) the rules included in the subset of R_α, produces a binary signal Y when the CS is classified correctly. This binary signal is compared with the binary signal S, which for each sample X priori determines its belonging to the class $\{NS, AS\}$. Using these binary signals are corrected values f_j quality metrics rules.

Classification module. The classifier can be represented as a two-tier structure and performs the following functional transformations: $X(n)$ -> R_α -> $\{Y(NS), Y(AS)\}$. On the first level there is recognition of the state of the input traffic X and concludes its normality / abnormality: $CS = \{NS, AS\}$. At the second level, the rules for detecting the abnormal traffic. Thus, the classifier performs object recognition, which may belong to one of five sets of rules. We define a reference to the classification procedure as:

$$(CS)\ CLASS\ (R_\alpha),$$

where $R_\alpha = R_\alpha(NS) \cup R_\alpha(AS)$.

Then the rules on recognition of CS using the classification procedures are defined as follows:

$$IF\ (CS)\ CLASS\ (R_\alpha\ (NS))\ then\ (NS);$$
$$IF\ (CS)\ CLASS\ (R_\alpha\ (AS))\ then\ (AS). \qquad (4)$$

In the classification of the CS current state to a set of rules Rα (NS) formed a binary signal Y(NS)= 1. In the classification of the CS current state to a set of rules Rα (AS) formed a binary signal Y(AS) = 1. Otherwise, the signals are formed Y(NS) = 0 and Y(AS) = 0, respectively. Then rule (4) take the form:

IF (CS) CLASS (R_α(NS)), then Y(NS) = 1
else Y(NS) = 0;

IF (CS) CLASS (R_α(AS)) then Y(AS) = 1 (5)
otherwise Y(AS) = 0.

In accordance with the mechanism of the 2-level classification of the current state of vehicle traffic is detected on the sets of rules Rα(NS) and Rα(AS).Taking into account this fact, we define multigrain recognition NS traffic based on rules of the form (5):

$$IF(CS)CLASS(R\alpha(NS))=1 \quad And \quad IF\ (CS)\ CLASS\ (R\alpha(AS)\ ) = 0 \quad then\ Y(NS) = 1\ ,\ Y = 0. \qquad (6)$$

Similar rules can be constructed for the classification of the current state as the AS. Invited output signal Y appraisal of the current state vehicle traffic is based on the maximum total scores f_j activated rules for each class:

$$Fmax(C_l)=max\{F(C_l)\}, \qquad (7)$$

where $F(C_l)$ – the total value of metrics f_i activated rules – $R_{ac}(C_l)$ for each of the five classes of possible states of the network traffic C_l = { *NS* , *Probe*, *DoS*, *R2L*, *U2R*}. This approach allows us to take into account more fully a posteriori information.

Adapting module. In order to improve of the classification quality system in a mode of adaptation to the rules of the current traffic. Adapting unit corrects metrics rules depending on the CS traffic: Y-> $f_i \in R_{ac}$ (C_l). By introducing a feedback signal values Y analyzed activated rules and signal S. Correction rules implemented in the translation function values quality rules activated by the formula (2).

Correction values for f_j rules R_j R_{ac} invited to perform in accordance with the following rule:

$$IF\ \ Y\ \&\ S\ then\ CORRECT\ (R_j \in R_{ac}), \qquad (8)$$

where $CORRECT\ (R_j \in R_{ac}\ )$ – correction procedure values f_i quality rules $R_j \in R_{ac}$ based on the analysis of signal values Y and S. Thus realized adaptation mechanism.

Consider a typical situation, the correction procedure are processed values f_j quality rules:

$$IF\ Y = 1\ and\ S = 1\ then\ CORRECT\ (R_j \in R_{ac}\ (AS)\ ) \qquad (9)$$

Procedure $CORRECT\ (R_j \in R_{ac}(AS)$ will increase the value f_j rules $R_j \in R_{ac}(AS)$ in accordance with the expression (2), which are activated correctly.

Similar rules correction can be constructed for other values of the signals Y and S. Thus, the values of the functions of quality rules are adjusted during operation of intrusion detection systems and adapt to the analyzed traffic.

Decision module modification of the rule base is designed to assess the level of similarity metric values (denoted in Figure 1 — DR) and the level of false positives (FAR), which were originally formed at the stage of testing and optimization: *DR*, *FAR*-> F_{ids} -> *X**. To assess the quality classification of traffic states operation adaptive IDS occurs as a self-test system. With this purpose in the operation of IDS formed the current values of output parameters of DR*, FAR*, which are compared with the values DR, FAR. Deciding on a modification of the rule base is based on the criteria:

$$F_{ids}=(DR*/DR)\bullet(FAR/FAR*). \qquad (10)$$

If $F_{ids} < 1$, then it means that the quality of the classification of IDS deteriorated and requires modification of the rule base. In this case, the decision to transition the IDS learning mode on an updated sample *X** and further optimization mode, and then repeated testing. On this basis, the updated values are formed metrics CF_j, f_j and define as well as the new values of the parameters of *DR*, *FAR*.

Interoperability developed modules IDS are represented in Figure 1. The proposed model is implemented in the IDS software environment MS Visual Studio 2013 Express for Windows Desktop. The programming language is C # v 5.0, platform .NET v. 4.5.

Experimental study effectiveness of the IDS model.

The purpose of experimental research is to assess the quality of the classification of CS traffic at different levels of testing of samples at varying thresholds CF_α, f_α, influence adaptation mode and others. 14 of the 41 informative signs are used and identified on the basis of decision trees [16].

Figure 2 shows the three fuzzy variables: --- Low, — Middle, • • • High, which are used to feature a numeric interval duration (Normal) with the corresponding values of the parameters a1 — c3. Learning for all classes conducted in a

mixed sample volume of 494 004 vectors, which was 10 % of the full sample used in the test.

Table 1 summarizes the specifications that were obtained during the formation of fuzzy rule base for different values CFα. As a result, when the values CFα = 0.5 and 0.6, respectively, is formed the 717 rules and 447 after the procedure of "compression".

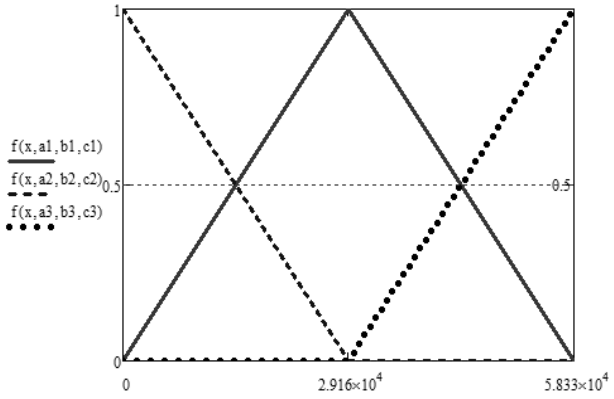


Fig. 2. The view of membership functions for duration attributes (Class Normal)

Table 1. Cardinality of the rule numbers subset

Class C_l	Number of rules N		
	Before compress	after compress	
		CF_α =0,5	CF_α =0,6
Normal	97 278	346	227
U2R	35	29	18
R2L	1 126	60	33
Probe	4 107	137	80
DoS	391 458	145	89
Total	494 004	717	447

Below are some of the results of the use of fuzzy rules for different states of network traffic, as well as numerical values of power supplies. Here, the following notations of linguistic variables are: 1 – Low, 2 – Middle, 3 – High. Representative examples of the structures of fuzzy rules show that for each state traffic rules contain characteristic values of linguistic variables:

N	Traffic state	Fuzzy rules	*CF*
1	Normal	11111221211111	0,69
2	Normal	11111322211111	0,94
3	DoS	11133332212111	0,96
4	DoS	11111332212111	0,78
5	R2L	11121311312222	0,80
6	R2L	11133311313221	0,97
7	U2R	21312311313211	0,81
8	U2R	12112311313211	0,76

On the basis of the use of the entire set of such rules R_α analyzed data from the database KDD CUP'99 [15]. Table 2 shows the characteristics of four test samples are randomly retrieved from the database.

Table 2. Characteristics of the test samples

Класс C_i	Number and amounts of test samples			
	1-й	2-й	3-й	4-й
	1133972	2450997	3422298	4898431
Normal	607222	712264	736838	972778
DoS	608566	1704936	2649613	3883370
U2R	9	29	32	52
R2L	105	581	834	1129
Probe	18070	33187	34981	41102

Table 3contains the results of experiments on the classification of states for each set of traffic rules.

Table 3. Traffic state classification experiments results

Class C_i	IDS characteristics							
	1st		2nd		3rd		4th	
	A	FAR	A	FAR	A	FAR	A	FAR
Normal	97.50	2.69	97.64	2.34	96.53	2.40	88.48	3.50
DoS	97.99	2.39	98.61	1.48	99.01	1.13	96.02	3.11
U2R	97.83	1.24	97.37	0.72	97.76	0.55	95.04	2.53
R2L	92.00	4.48	89.81	3.15	88.64	2.56	85.62	3.97
Probe	96.77	1.79	95.71	1.16	96.12	0.90	95.33	2.20

Likelihood level (% correctly classi-fied traffic states – A) and false positives (% misclassified traffic states – FAR) were calculated according to the expressions [17, page 220]. For

each of four experiments, a sample of an individual whose number corres-ponds to the number of the experiment. Best results marked in bold color.

Intermediate likelihood of false positives and in intervals of variation ΔA and ΔFAR classes in experiments with number No.1 – No. 3.

Class	A	ΔA	FAR	ΔFAR
Normal	97,22	1,11	2,48	0,35
DoS	98,54	1,02	1,67	1,26
U2R	97,65	0,46	0,84	0,69
R2L	90,15	3,36	3,40	1,92
Probe	96,20	1,06	1,28	0,89

Table 4 contains information about the runtime test experiments.

Table 4. Testing time

	Number and amounts of test samples			
	1st	2nd	3rd	4th
	1133972	2450997	3422298	4898431
Time	13 min 54 s	28 min 41 s	40 min 38 s	59 min 17 s

Obtained by solving the problem of CS traffic classification results are statistically robust and broadly reflect the presentational features of the proposed approach.

Conclusions. According to the study of adaptive fuzzy model, we suggest the following conclusions.

• Usage of the adaptation mode significantly increases the likelihood classify-cation of network conditions. Thus, with increa-sing sample sizes the length of the confidence interval level and the likelihood of false positives is well approximated by a power function of the square root of the ratio magnification scope. This is caused by f_i quality function productive correction and increases its evaluation. During the estimation of FAR classes U2R, R2L, Probe and DoS such behavior was observed in all three experiments. Experiment №4 was conducted without adaptation mode. In comparison with other experiments shown in Table 3, the quality classification is deteriorated for all classes of 2 – 9 %.

• The fact of reducing the same for some cases could be explained by the influence of distribution inhomogenety of examples in classes because of two possible reasons: 1) significantly uneven distribution of vectors in classes, 2) the effect of situations that have not been activated by any of the rules, and therefore the correction of f_i have not been performed. For example, in experiment No. 3, it decreased to attacks such as *R2L* in comparing with experiment No.1 ~ 3.5 at % and to the attacks on the type of Probe~ 1,06 %.

Similar experiments were planned and performed for the other samples to determine the quality of classification, the influence of the modification frequency of the rule base, the values of the coefficients *w*1 and *w*2, and others. In these experiments we used different amounts of test samples, optimized parameters *a*, *b*, *c* fuzzy rules, as well as varied thresholds CF_α, f_α, which were set by an expert and others.

The experimental results confirmed that the proposed model is locally stable within the limits of selected attacks, as well as sensitive to the adjustable parameters of fuzzy rules and thresholds CF_α, $f\alpha$ forming a subset of effective rules R_α, which allows the expert to make a choice of adjustable parameters, taking into account the specific features of the administration of computer networks, including the facts of the early detection of these classes of attacks.

The proposed adaptive model of intrusion detection and possible vulnerabilities in adapting computer networks based on the methods of artificial immune systems in combination with fuzzy logic can be the basis for building IT- technology computer security for rapid changes in the state of network traffic. Using the adaptive model of decision-making system can significantly improve the likelihood of recognition events, minimize the number of false alarms, as well as provide a high reactivity of the system, which is especially important for early detection stages. In a further refinement of the proposed approach is promising to consider the multidimensional problem of classification on a set of alternative characters, Pareto approach for multidimensional optimization problems, and the feasibility of prefiltering traffic.

Список использованной литературы

1. Дасгупты Д. Искусственные иммунные системы и их применение / Под ред. Д. Дас-

гупты: пер. с англ. – М. : Физматлит, 2006. – 344 с.

2. Информационные технологии для критических инфраструктур: моногр. / Под ред. А. В. Скаткова – Севастополь : СевНТУ, 2012. – 306 с.

3. Varghese S.M., and Jacob K.P. Anomaly Detection Using System call Sequence Sets, (2007), *Journal of Software,* No. 2(6), pp.14 – 21.

4. Yeung D.Y., and Ding Y. Host-Based Intrusion Detection Using Dynamic and Static Behavioral Models, 2003, *Journal of Pattern Recognition,* No.36, pp. 229 – 243.

5. Shon T.A., and Moon J. Hybrid Machine Learning Approach to Network Anomaly Detection, (2007), *Journal of Information Sciences,* No. 177, pp. 3799 – 3821.

6. Kabiri P., and A. Ghorbani Research in Intrusion Detection and Response. –A Survey, (2005), *International Journal of Network Security,* No. 1, pp. 84 – 102.

7. Khanna R., and Liu H. System Approach to Intrusion Detection Using Hidden Markov Model, *IWCMC, July 3–6, Vancouver, British Columbia, Canada*, pp. 349 – 354.

8. Castro P.A., Coelho G.P., Von Zuben F.J. Designing Ensembles of Fuzzy Classification Systems: An Immune-Inspired Approach, (2005), *Proceedings of the 4th International Conference on Artificial Immune Systems (ICARIS), Lecture Notes in Computer Science, Springer-Verlag, Berlin,* No. 3627, pp. 469 – 482.

9. Beghdad R. Critical Study of Neural Networks in Detecting Intrusions, (2008), *Journal of Computers and Security,* No. 27, pp. 168 – 175.

10. Sheikhan M., and Jadidi Z. Misuse Detection Using Hybrid of Association Rule Mining and Connectionist Modeling, (2009), World Appl. Sci. J., Vol. 7 (Special Issue of Computer & IT), pp. 31 – 37.

11. Chen Y., Abraham A., and Yang B. Hybrid Flexible Neural-Tree-Based Intrusion Detection Systems, (2007), *International Journal of Intelligent Systems,* No. 22, pp. 337 – 352.

12. Abraham A., and Jain R. Soft Computing Models for Network Intrusion Detection Systems. Classification and Clustering for Knowledge Discovery Studies, (2005), *Journal Computational Intelligence,* pp. 191 – 207.

13. Брюховецкий А. А. Адаптивная модель обнаружения вторжений в компьютерных сетях на основе искусственных иммунных систем / А. А. Брюховецкий, А. В. Скатков // Электротехнические и компьютерные системы. – К. : – 2013. – № 12 (88).– С. 102 – 111.

14. Hansen J.V, Lowry P. B., Meservy R. D., and McDonald D. M. Genetic Programming for Prevention of Cyberterrorism through Dynamic and Evolving Intrusion Detection, (2007), *Journal of Decision Support Systems,* No. 43, pp. 1362 – 1374.

15. KDD cup 99 Intrusion detection data set [Электронный ресурс]. – Электрон. текстовые данные (752 Мб). – Darpa: Irvine, CA 92697-3425, 1999. – Режим доступа: / http: // kdd.ics.uci.edu/ databases/kddcup99, (Monday, 17 March 2013 19:07:34).

16. Брюховецкий А. А. Обнаружение уязвимостей в критических приложениях на основе решающих деревьев /А. А. Брюховецкий, А. В. Скатков, П. О. Березенко // Радиоэлектронные и компьютерные системы. – Харьков : – 2013. Изд-во ХАИ. – № 5(64). – С. 18 – 23.

17. Zainal A., Maarof M., Shamsuddin S. et al. Ensemble Classifiers for Network Intrusion Detection System, (2009), *Journal of Information Assurance and Security,* –Vol. 4, pp. 217 – 222.

Received 25.04.2014

References

1. Dasgupta D. (ed.), (2006), Iskusstvennye immunnye sistemy i ikh primenenie [Artificial Immune Systems and Applications], *Fizmatlit,* Moscow, Russian Federation, 344 p. (In Russian).

2. Skatkov A.V. (ed.), Informacionnye tehnologii dlja kriticheskih infrastruktur: monogr, [Information Technology for Critical Infrastructures: Monograph], (2012), *SevNTU*, Sevastopol, 306 p. (In Russian).

3. Varghese S.M., and Jacob K.P., (2007), Anomaly Detection Using System call Sequence sets, *Journal of software*, pp. 14 –21.

4. Yeung D.Y., and Ding Y., (2003), Host-Based Intrusion Detection Using Dynamic and Static Behavioral Models, *Journal of Pattern Recognition*, pp.229 – 243.

5. Shon T., and Moon J., (2007), A Hybrid Machine Learning Approach to Network Anom-

aly Detection, *Journal of Information Sciences*, pp. 3799 – 3821.

6. Kabiri P., and Ghorbani A., (2005), Research in Intrusion Detection and Response, *International Journal of Network Security*, pp. 84 – 102.

7. Khanna R., and Liu H., (2006), System Approach to Intrusion Detection Using Hidden Markov Model, *IWCMC, July 3 – 6, Vancouver, British Columbia, Canada*, pp. 349 – 354.

8. Castro P.A., Coelho G.P., and Von Zuben F.J., (2005), Designing Ensembles of Fuzzy Classification Systems: An Immune-Inspired Approach, *4th International Conference on Artificial Immune Systems (ICARIS), Springer-Verlag, Berlin,* pp. 469 – 482.

9. Beghdad R., (2008), Critical Study of Neural Networks in Detecting Intrusions, *Journal of Computers and Security*, pp. 168 –175.

10. Sheikhan M., and Jadidi Z., (2009), Misuse Detection Using Hybrid of Association Rule Mining and Connectionist Modeling, World Appl. Sci. J., Vol.7 (Special Issue of Computer & IT), pp. 31 – 37.

11. Chen Y., Abraham A., and Yang B., (2007), Hybrid Flexible Neural-Tree-Based Intrusion Detection Systems, *International Journal of Intelligent Systems*, pp. 337 – 352.

12. Abraham A., and Jain R., (2005), Soft Computing Models for Network Intrusion Detection Systems. Classification and Clustering for Knowledge Discovery Studies, *Journal Computational Intelligence*, pp. 191 – 207.

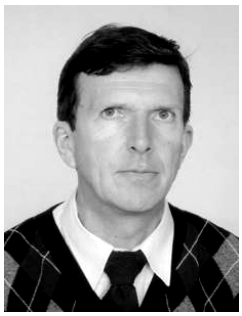
13. Bryukhovetskyi A.A., and Skatkov A.V. Adaptivnaja model' obnaruzhenija vtorzhenij v komp'juternyh setjah na osnove iskusstvennyh immunnyh system, [An Adaptive Model of Intrusion Detection in Computer Networks base on Artificial Immune System], (2013), *Journal Electrotechnic and Computer Systems*, Odessa, Ukraine, Vol. 12 (88), pp. 102 – 111.

14. Hansen J.V., Lowry P.B., Meservy R.D., and McDonald D.M., (2007), Genetic Programming for Prevention of Cyber terrorism through Dynamic and Evolving Intrusion Detection, *Journal of Decision Support Systems,* Vol. 43, pp. 1362 –1374.

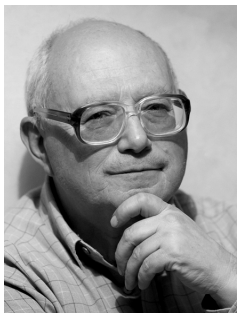
15. Irvine CA 92697-3425, (1999), KDD cup 99 Intrusion Detection data set, Available at: /http:// kdd.ics.uci.edu /databases/kddcup99/ (accessed 17 March 2013) .

16. Bryukhovetskyi A.A., Skatkov A.V., and Berezenko P.O., Obnaruzhenie ujazvimostej v kriticheskih prilozhenijah na osnove reshajushhih derev'ev, [The Discovery of Vulnerabilities in Critical Applications Based on Decision trees], (2013), *Journal Electronic and Computer Systems*, Kharkov, Vol. 5 (64), pp. 18 – 23.

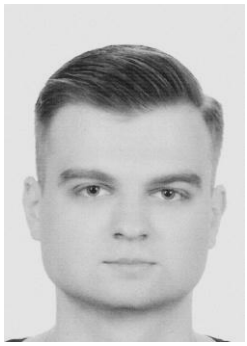
17. Zainal A., Maarof M., Shamsuddin S. et al., (2009), Ensemble Classifiers for Network Intrusion Detection System, *Journal of Information Assurance and Security*, vol. 4, pp. 217 – 222.



Briukhovetskyi
Aleksei Alekseevich,
PhD., Assistant Professor of Cybernetics and Computer Technology, Sevastopol National Technical University,
E-mail:
kvt.sevntu@gmail.com



Skatkov
Alexandr Vladimirovich,
ScD, Professor, Head of Cybernetics and Computer Technology, Sevastopol National Technical University E-mail: kvt.sevntu@gmail.com



Selkin
Andrey Alexandrovich,
Student of Cybernetics and Computer Technology, Sevastopol National Technical University
E-mail:
kvt.sevntu@gmail.com