TEKA. COMMISSION OF MOTORIZATION AND ENERGETICS IN AGRICULTURE – 2012, Vol. 12, No.4, 196-203

The mechanism of the analysis of entering Internet traffic for the presence of threats

Alexander Ρetrov[1,2], *Sergey Velchenko*[2]

[1]AGH University of Science and Technology, Krakow, Poland
[2] Volodymyr Dahl East-Ukrainian National University, Lugansk, Ukraine

S u m m a r y. The mechanisms of defense of AIS from the external threats are investigated in the article. There have been shown the classification of threats, technology of prognostication of the appearance of the external threats with the help of the Markovskiy processes, and the mechanisms of protecting from them. It is given the mechanism of watching the changes in the development of threats in a virtual network on the base of semantic neuron network for teaching of the system to their counteraction.
K e y w o r d s: external threats, defense of the informative system, Markovskiy processes, semantic neuron networks, virtual networks.

INTRODUCTION

Providing the safety of confidential information (KI) from affecting the automated informative systems (AIS) of the external threats presently acquires the special actuality. The indicated problem is confirmed by the analysis of the present statistical information about the influence of the external threats on safety of KI, circulatory in AIS [Babenko, Makarevich, Peskov, 2003.],[Khayretdinov, 2005], [1. Babenko, Makarevich, Peskov , 2003.], [Rosenko, Kopytov, Lepeshkin, 2004.], [Rosenko, 2000.], [Rosenko, Gricyk, 2001.], [Saveliev, 2000.], [Voronenko, 2000.], [Voyaobuev, 2002.], [Zaegorodny, 2001.] Because of the loss of KI, representing the intellectual property or the information of «know-how», can be inflicted a considerable financial and moral damage to the owner of the information [Internal IT threats in Russia. Research companies InfoWatch. 2006.]. Therefore, the task of the defense of the informative system from the unauthorized division from outside is actual.

Threats can be classified according to the different programmatic factors. For example, on the features of defeat viruses and programmatic failures **[**Foster, Kesselman, Tuecke, 2001.**]** viruses and worms, spam, are selected, attacks of type «refuse in service», financial swindle, gaps in the systems of safety of software.

Threats can be classified according to the different consequences which they render **[**Foster, Kesselman, Tuecke, 2001.**]**: violation of KI; distortion of the information, failures in-process AIS, loss of the information, delete of the information, theft of equipment, etc.

THE ANALYSIS OF THE PREVIOUS PUBLICATIONS

The authors in their previous researches consider the method of counteraction attacks in local calculable network (LCN) in a virtual imitation network, built for discrete stochastic systems with the use of theory of the Markovskiy processes **[**Petrov, 2011.**].** It has been also discussed the model of defense of the up-diffused local network by the queuing systems with the use of network sluice and Internet of sluice with a built-in virtual imitation network, built on the base of the Markovskiy closed system of the mass service**[**Petrov, 2011.**].** It has been also considered the realization of switching of the system of

defense in the case of the appearance of threat in a virtual network **[**Petrov, 2012.**].**

THE PURPOSE AND THE DEFINITION OF THE TASK OF RESEARCHES

The purpose of this work is in the development of the mechanism of the analysis of entering the Internet traffic in the presence of threats. Realization of anti-virus verification and checking is offered by various external - to vulnerability, got from the network of data, on a server. It is more profitable because of wider possibilities and the exception of hit of undesirable and nocuous information or potentially dangerous information. We'll name this block as the administrator the Internet of safety of network (AISN), which analyses the basic parameters of the loaded files and assess the legitimacy of the source of the new data. If a source is doubtful or the information is contained by presence of nocuous code bits, they are fully loaded on proxy-server, their anti-virus scan-out is whereupon conducted. This decision is based on the anti-virus verification, to verification on vulnerability and attack on the side of remote computer or server. Thus, there is the possibility of automatic choice of test of the loaded files algorithm that makes the system of defense more effective and saves resources.

In case of discovering the suspicion on external threats or origins of vagueness, what should be done with this potential threat? There is a version either to block, or to carry out the analysis of uncertain and suspicious data in the so-called virtual mode for a further analysis: both information and record of changes of what is going on in a network with the purpose of accumulation of necessary information. In case of the not confirmed information about nocuity of this software all of these changes happened on a virtual computer can be carried on the real computer with the certain lateness depending on the power of server and desire of user. And, thus, the accumulated information will be analyzed and utilized on teaching the system with the purpose of more effective interpretation of the external traffic. Such technology of work with entrance information will allow to save time in future and the resources of network. In this case the system of exchange is described by the information from each concrete computer of network of enterprise with a network the Internet by an administrator the Internet of safety of network (AISN).

REALIZATION

General statement of the question.

The influence of external threats on the elements of the system of AIS in a general view carries casual character and can result in two ends.

• happy end in case if purpose of influence of external threats, on AIS has not been achieved;

• an unhappy end is in all the other cases.

In this connection as a criterion of estimation of safety of KI it is possible to accept probability of happy end at the influence on AIS of external threats.

We will designate the indicated probability through Probability of opposite event, i.e. probability of unhappy end at influence on AIS of the external threats, will be equal to q. The indicated events make the complete group of independent events. Then

$$p + q = 1. \qquad (1)$$

It ensues from expression (1), that probabilities of **p** and **q** are the analytical criteria of estimation of safety of KI.

For the estimation of safety KI can be used different approaches [Dolgov, Kasatkin, Sretenskiy, 1978.] . However, as the analysis [Gavryushin, 2002.] shows, for such estimation it is necessary to take into account circumstance that as the result of influence on AIS of external threats it can pass from the initial (normal) state in other, special, state, proper the origin of exception condition[Zegzhda, 2002.:]. At the same time the appearance of exception conditions is related to the threat safety of KI, to circulatory in AIS [A. Kusz, P. Maksym, Andrzej W. Marciniak 2011].

A transition of AIS from one state into the other one is the investigation of fully concrete reasons. However, they appear, as a rule, in arbitrary moment of time, that's why their appearance is casual therefore. Every particular situation can result both in happy and unhappy end for KI taking into account success (to not success) of actions of employees on the reflection of consequences of the appearance of exception conditions [G. Bartnik, G. Kalbarczyk, Andrzej W. Marciniak 2011].

We will designate the probability of origin of i-th exception condition through q_i conditional probability of reflection of its consequences through r_i and probability of non-reflection – through $\overline{r_i}$ Then for the determination of probabilities p_i and q_i will present the sequence of transitions of AIS from one (initial) state to the other one by the Markovskiy casual process with

the account number of the states and by continuous time. Such presentation is conditioned by the following assumptions:

• in the initial state AIS is in normal state;

• a sequence of the appearance of exception conditions of i-th kind is the simplest stream with intensity λ_i intensity of happy end is marked through $\lambda_i r_i$, and unhappy - $\lambda_i \overline{r_i}$

The essence of the method of calculation of probabilities p_t and q_t at the use of the Markovskiy process consists of that unknown probabilities are determined from the decision of differential equalizations which describe this process. Such a process should be presented in the form of logical and probabilistic process [Philinov, Boychenko , 2001.]**.**

We will suppose that the possible states of AIS in the process of the influence on them of external threats are defined. Besides, the directions of its casual transitions are known from the state into the state. Then it is possible to build the logical chart (count) of the state of AIS, which at the known probabilities of transition of the system from the state into the state is logical-probabilistic model of AIS (please, see fig. 1, by analogy with [Kornevec, Payachun, Prokofev, 2005.], [Zegzhda, 2002.]).

On the fig. 1 the logical chart of influence is presented on AIS one i-th of external threat.

The competence of such presentation of AIS is based on that possible ends from influence on AIS are random events by virtue of chance of appearance of one or the other external threats.

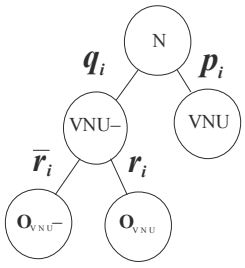

Fig. 1. Logic diagram of the impact on AIS one i-th external threat.

In accordance with the fig. 1 it follows that in the process of functioning of AIS there is some danger, related to affecting it i-th external threats. At such influence AIS can be in the following states (see of fig. 1.1):

• «N» is the initial state of AIS;

• «VNU» is the state, when i-th an external threat does not show up with probability p_i ;

• «VNU-» is the state, when i-th an external threat showed up with probability $q_i = 1 - p_i$;

• « O_{vnu} » it is the state of reflection of external threat with probability of r;

• « O_{vnu-} » it is the state of not reflection of consequences of display of external threat with probability $\overline{r} = 1 - r$.

Final states of «VNU», and « O_{vnu} », correspond to the happy end at the influence on AIS i-th of external threat.

The state « O_{vnu-} » corresponds to the unhappy end at the influence on AIS i-th of the external threat. Then, in accordance with the fig. 2, the probability of happy end from the influence on AIS i-th external is determined by the following way:

$$P_{(vnu)h_i} = p_{(vnu)i} + q_{(vnu)i} r_{(vnu)i}$$

and the probability of unhappy end

$$Q_{(vnu)} = q_{(vnu)i} \overline{r_{(vnu)i}}$$

Because probabilities $P_{(vnu)h_i}$ and $Q_{(vnu)h_i}$ make the complete group of events

$$P_{(vnu)h_i} + Q_{(vnu)} = 1 ; \quad (2)$$

From (2) it follows that

$$P_{(vnu)h_i} = 1 - Q_{(vnu)}$$

$$Q_{(vnu)} = 1 - P_{(vnu)h_i}$$

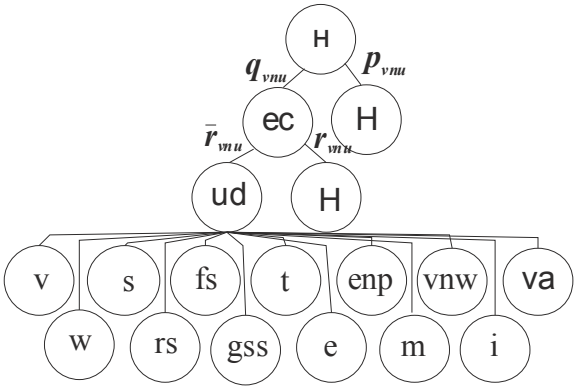

Fig. 2. Logic diagram of the possible states AIS

Thus, from the point of view of the consequences of the influence on AIS of external threats on the basis of analysis of expressions (2) it is possible to come to the following conclusions.

1. By a quantitative measure, characterizing the consequences from the influence (i-th of external threat, on KI, are probability of happy end of P_h and probability of opposite event, I.e. probability of unhappy end as a result of the

influence of i-th of external threat on AIS, I.e., $Q_{(vnu)h_i}$.

2. The analysis of the expression (2) testifies that probabilities $P_{(vnu)h_i}$ and $Q_{(vnu)}$ are the quantitative estimation of the consequences from the influence on AIS i-th of external threat.

3. The analysis of expression (2) shows also, that for the quantitative estimation of consequences of influence external threats on AIS it is enough to define any constituent, for example $Q_{(vnu)h_i}$. The definition of the other constituent from the expression (2) is not complicated.

Let's consider the application of the quantitative estimation for the determination of the probabilities of the consequences from the influence on AIS of external threats. The consequence from affecting of external threats safety of KI can be different.

• «N» is the initial (initial) state of AIS;

• «H» - an external threat did not show up with probability p_{vnu} ;

• «EC» - an external threat showed up $q_{ec} = 1 - p_{vnu}$ with probability, that had resulted in the origin of exception condition;

• an exception condition with probability r_{ec} is reflected;

• an exception condition with probability $\overline{r_{ec}} = 1 - r_{ec}$ is not reflected, that resulted in outgrowing of exception condition in the unauthorized division of NSD to KI;

• $q_v, q_w, q_s, q_{rs}, q_{fs}, q_{gss}, q_t, q_e, q_{enp}, q_m, q_{vnw}, q_i, q_{va}$ — according to probability there are viruses and worms, spam, attacks of type «refuse in service», financial swindle, gaps in the systems of safety of software, theft, elimination (destructions), errors and misconducts of personnel, substitution (modifications), violation of normal work of AIS intercept and violation of access to KI.

The definition of probabilities of such states of AIS is carried out taking into account that the casual display of external threats, as potentially hazardous occurrence, and also not the reflection of exception condition, accompanied an unauthorized division to information.

In accordance with the fig. 2.3, the probabilities of the consequences from affecting of external threats safety of KI are determined by the following way:

• the probability of happy end from the influence on AIS of external threats

$$P_{ph} = p_{vnu} + q_{vnu} r_{ec} ; \quad (3)$$

• the probability of the opposite event, that the probability of unhappy end from influence on AIS of external threats viruses and worms, spam, attacks of type «refuse in service», financial swindle, gaps in the systems of safety of theft, elimination (destructions), errors and misconducts of personnel, substitution (modifications), violation of normal work of AIS, intercept and violation of access to KI software.

$$Q_{vnu} = q_{vnu} \overline{r_{ec}} ; \quad (4)$$

• the probability of infection viruses

$$p_v = Q_{vnu} q_v \quad (5)$$

• the probability to be infected by worms

$$p_w = Q_{vnu} q_w \quad (6)$$

• the probability of the appearance of the spam

$$p_s = Q_{vnu} q_s \quad (7)$$

• the probability of attack of type «refuse in service»

$$p_{rs} = Q_{vnu} q_{rs} \quad (8)$$

• the probability of financial swindle

$$p_{fs} = Q_{vnu} q_{fs} \quad (9)$$

• the probability of gap is in the systems of safety software

$$p_{gss} = Q_{vnu} q_{gss} \quad (10)$$

• the probability of theft of KI

$$p_t = Q_{vnu} q_t \quad (11)$$

• the probability of elimination (destructions) of KI

$$p_e = Q_{vnu} q_e \quad (12)$$

• the probability of errors and misconducts of personnel

$$p_{enp} = Q_{vnu} q_{enp} \quad (13)$$

• the probability of substitution (modifications) of KI

$$p_m = Q_{vnu} q_m \quad (14)$$

• the probability of violation of normal work of AIS

$$p_{vnw} = Q_{vnu} q_{vnw} \quad (15)$$

• the probability of intercept of KI

$$p_i = Q_{vnu} q_i \quad (16)$$

• the probability is violation of access of KI

$$p_{va} = Q_{vnu} q_{va} \quad (17)$$

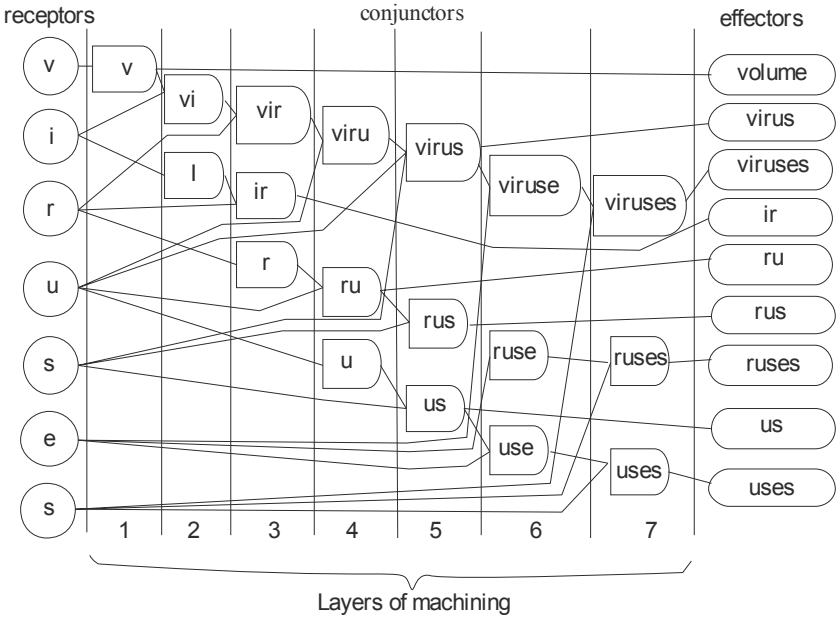

Fig. 3. Fragment processing layers of linear tree

The expression (3) allows to define the probability of happy end, and the expression (4) – of unhappy end on the whole from the influence of external threats on AIS. The expressions (5)-(17) allow to define strength of KI security on the types of the consequences from the influence on AIS of external threats.

At the practical use of the expressions (3)-(17) it is necessary, for the verification of the competence of the got results, to utilize expression (1). It is related to that for a branching out process the sum of probabilities of the subsequent states of AIS, outgoing from proceeding, is equal to unit.

We analyze the traffic by a neuron network, built with conjunctors and disjunctors. Let's suppose that all of the neurons are identical, and they realize one transmission function, and the weight and thresholds will be realized by equal and general possibilities. It is required to build a neuron network under this task.

This network must analyze the traffic and reflect attacks, and in the case of non-reflection the attack or suspicious application, to pass from the real network into the virtual one, and there to make the analysis of vulnerabilities and attacks, as well as the training of the neural network for these vulnerabilities.

The information about what is going on is written down in a text file. Therefore the typical method of the text processing with the purpose of determination of his maintenance consists in a text translation in human language in the internal form of the system and possible leading out from this presentation of new information [Gerasimenko, Mayayuk, 1997.]. The process of treatment will be realized on three levels: morphological, syntactic and semantic. On morphological and syntactic levels from a text separate words which are divided into separate morphemes are selected. Syntactic copulas are determined interword after it. The purpose of the first two stages is a receipt of word-parts with the cut completions. To the each inter word belongs every word-part in accordance of value of certain grammatical signs. The purpose of semantic interpretation is an exposure of maintenance of words and combinations of words [Luger, 2003.]. In the process of semantic interpretation the knowledge which are in the simulation model are compared with the facts, presented in the text [Shuklin, 2003.]. The result of comparison becomes the internal, from the point of view of the system treatment, structured presentation of text [Tereykovsky, 2007.]. That determination of the maintenance of text is the process of comparison of the encoded denotations of the phenomena of subject domain, which are contained directly in the text corresponding to these phenomena by the fragments of simulation model of that subject domain. The information about the syntactic structure of text is the criterion of decision of possible dissimilarities of the indicated comparison. The final result of the analysis of text is a semantic network which is considered for today as the most complete and reliable description of its maintenance.

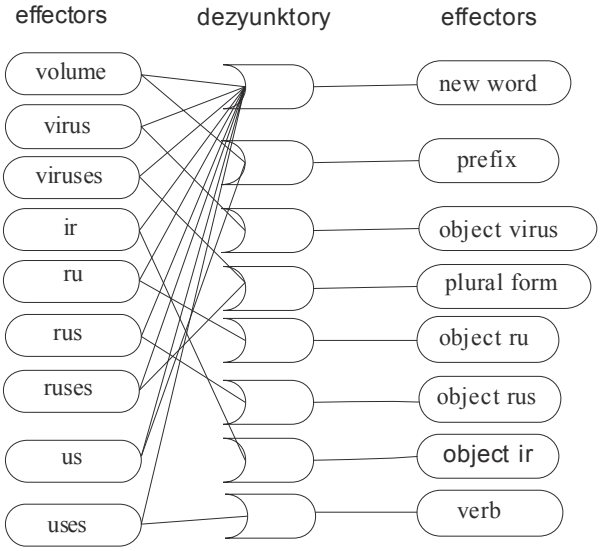

Fig. 4. Structure of an aggregating layer neurons

In general case under the concept of semantic neuron network is understood the network of the dynamically CPLD between itself neurons, that parallel or kvazi parallel execute the operations of fuzzy logic, exchanged between the information itself and organized in the unique unit by the certain mechanisms. As well as for the other types of neuron networks, base operations of the treatment information are executed by separate neurons. Thus, for perception the semantic neuron network of information from an external environment are used receptors (entrance neurons). For passing the information from a network on external are used receptors (initial neurons). Organizing mechanisms can have own calculable activity and co-operate with neurons. Accordance of some elements of semantics of subject domain or model of text is appointed inter neurons. Thus, an element can present separate character, aggregate of some characters of text or aggregate of concepts and relations between the concepts, that can be abstracted as the unique unit.

The studies of semantic neuron network with the structure of type of the synchronized linear tree consist in memorizing, by it to new information, to forbidden for a reception/transmission. Thus selection of separate words from a text it is expedient to conduct by the preprocessor dissociated from a neuron network. In the mode of studies, information a symbol-by-symbol is given at the entrance of the synchronized linear tree. On each stage of studies the search of the excited neurons is conducted in a neuron network. If such neurons are, it is considered that a network is already taught this character sequence, and to bring in it additional information it is not needed. In opposite case to the network the new disjunctors are added, that at once translated in the excited state. Thus, not only the weighing coefficients of connections but also neuron network structure itself changes at the studies of the synchronized linear tree.

Educational information, given at the entrance of networks, due to present a database and base of knowledge of simulation model of subject domain in the complement of which information enters forbidden for a reception/transmission. A simulation model will be formed as a result of studies of semantic neuron network. As a database and base of knowledge of simulation model for the synchronized linear tree, adjusted for the morphological and syntactic analysis of the text, the grammatical dictionaries of language which the text is written can be used The conducted calculations show that the volume of depository information of the synchronized linear tree for the analysis of text in Ukrainian or Russian languages make less than 10 gigabyte. For the basis of calculations is taken one size of the most complete grammatical dictionaries [Grammatical Dictionary of the Russian language: inflection 1980.].

CONCLUSIONS

The conducted researches specify the possibility of construction realization of anti-virus verification and checking for various external - to vulnerability, got from the network of data, on the side of server of AIBS. Due to the application of semantic neuron networks with the purpose of rich in content analysis of the text of written in the file changes, happened on a virtual computer, started virtually suspicious applications, and also conduct of monitoring of threats.

It is formed the general methodic of work of AIBS, analyzing the changes made by suspicious applications. On their basis it is formed the teaching of semantic neuron networks. Afterwards the specification of this threat appears and the block of conduct is formed at these threats. Monitoring is carried out and the strategy of conduct of the system is forecast on external threats on the frame of base, used for teaching of the network. The accumulated statistics allows the system to be self taught taking into account the accumulated information.

This method gives more flexible adaptation of AIBS to the concrete network, and also adequate and reliable system of reflection of external threats. The basic prospects of subsequent

researches in this direction consist in application of modifications of AIBS for protecting from the different type of threats - external, internal and hidden.

REFERENCES

1. **Babenko L.K., Makarevich O.B., Peskov O. U., 2003.:** Development of an integrated intrusion detection system. Information security. Of the V International scientific-practical conference of Taganrog, RAL. tech. Univ. Taganrog pp. 194-197.
2. **Bartnik G., Kalbarczyk G., Andrzej W. Marciniak 2011.:** Application of the operational reliability model to the risk analysis in medical device production TEKA Kom. Mot. i Energ. Roln. – OL PAN, 11c, pp. 361–377
3. **Dolgov V. A., Kasatkin A, S., Sretenskiy V. N., 1978.:** Radio electronic automatic control systems (systems analysis and implementation techniques). Moscow: Soviet radio. 384 p.
4. **Foster I., Kesselman C., Tuecke S. 2001.:** The Anatomy of the Grid: Enabling Scalable Virtual Organizations. International Journal of High Performance Computing Applications, 15 (3).pp. 200-222.
5. **Gavryushin E. I., 2002.:** The human factor in ensuring the security of information, http// www.ii26.ru/it263.view2.page22.h4nl
6. **Gerasimenko V.A., Mayayuk A.A., 1997.:** Fundamentals of information security. M., MiFi. 538 p.
7. Grammatical Dictionary of the Russian language: inflection 1980.: / [comp. Zaliznyak A.A.] M. : Rus. lang., 880 p.
8. Internal IT threats in Russia. Research companies InfoWatch. 2006.: www.info Watch.ru.
9. **Khayretdinov R. 2005.:** Internal threats and fight against them // Computers. №7-8. pp. 15-18.
10. **Kornevec I. G., Payachun. B.P., Prokofev A. S., 2005.:** The ways of the increase of the efficiency are sewn up acoustic information in the selected apartments. Informative safety. Materials of the VII International Scientific and Practical Conference. Taganrog, RAL. tech. Univ. Taganrog, pp. 231-232.
11. **Kusz A., Maksym P., Andrzej W. Marciniak 2011.:** Bayesian networks as knowledge representation system in domain of reliability engineering TEKA Kom. Mot. i Energ. Roln. – OL PAN, 11c, pp.173–180.
12. **Luger F., 2003.:** Artificial Intelligence: Strategies and methods for solving complex problems, 4th Edition / F. Luger, trans. from English. N.I. Galagan M. Williams, 864 p.
13. **Pankratova I. D., 2002.:** The formation and development of analysis of the systems as the applied scientific discipline. // System research & information technologies IASA. № l. pp. 65-94.
14. **Petrov A.S., 2011.:** Method of counteraction attacks in LVS in a virtual imitation network / A.S. Petrov, S.A Velchenko. // Informative safety. №1(5). pp. 8-14.
15. **Petrov A.S., 2011.:** Model of defense of the up-diffused local network built on the basis of the Markovskikh queuing systems / A.S. Petrov, S.A. Velchenko // Informative safety. №2(6). pp. 88-93.
16. **Petrov A.S., 2012.:** Method of management defense of the informative system in off-wire sets on the base of game theory / A.S. Petrov, S.A. Velchenko // Announcer of SLEEP the name of Dalya. №.8(1),- pp 69-79.
17. **Philinov E.I., Boychenko A. V., 2001.:** Standards of protection of information in the draft IP. Proceedings of the scientific-practical conference "Information Security". Taganrog, rad. tech. Univ. Taganrog. pp. II-I9.
18. **Rosenko A. P., Kopytov V. V., Lepeshkin O. M., 2004.:** Security Threats North Caucasus region in the field of information and ways of reducing them. Threats safety of Russia in North Caucasus; Monograph. Stavropol. pp. 136-188.
19. **Rosenko. P., 2000.:** Methodological aspects of the dynamic of the expert system of information protection. A mathematical design is in scientific researches. Materials of the All-Russian scientific conference. 4.2. Stavropol. pp. 206-208.
20. **Rosenko A. P., Gricyk B. A., 2001.:** Analysis of existent approaches on the selection of personnel, working with KI. Informative safety. Sat works of the scientific-practical conference of Taganrog, rad. tech. Univ. Taganrog, 243 p.
21. Research on mitigating the insider threat to information systems. RAND - Conference Proceedings, August, 2000.
22. **Shuklin D. E., 2003.:** Models of semantic neuron networks and their application are in the intelligence systems: dis. . kan. tekhn. sciences: 05.13.23 / D. E. Shuklin. - X.,. 196 p.
23. **Saveliev M., 2000.:** Systems analysis and modeling of protection of information. The second regional scientific-practical seminar "Information Security-South Russia." Taganrog, rad. tech. Univ. Taganrog, pp. 136-137.
24. **Tereykovsky I., 2007.:** Neuron borders in the means of defense computer information/ I. Tereykovsky K.: PoligraphConsulting - 209 p.
25. **Voronenko P. A., 2000.:** Security. Situation in the world and in Russia // news-letter of «Jet Info». № 8 (87). P. 14-16.
26. **Voyaobuev C B., 2002.:** Systems analysis object security information. Scientific Session MIFI-2002. IX International Scientific and Practical Conference "Problems of security in a higher school) *. Collection of scientific works MIFI. Moscow, pp. 31-33.
27. **Zaegorodny V.I., 2001.:** Integrated protection of information in computer systems: the manual. Moscow: Logos, 264 p.
28. **Zegzhda P.D., 2002.:** Modern technology trends to ensure the security of computer systems. Scientific Session MIFI-2002. IX International Scientific and Practical Conference "Problems of security in higher education." Collection of scientific works MIFI. M.. pp. 40-41.

МЕХАНИЗМ АНАЛИЗА ВХОДЯЩЕГО ИНТЕРНЕТ ТРАФИКА НА НАЛИЧИЕ УГРОЗ

Александр Петров, Сергей Вельченко

Аннотация. В статье исследуется механизмы защиты АИС от внешних угроз. Показаны классификация угроз, технология прогнозирования появления внешних угроз с помощью Марковских процессов, и механизмы защиты от них. Приведен механизм отслеживания изменений в развитии угроз в виртуальной сети на базе семантической нейронной сети для обучения системы их противодействию.

Ключевые слова: внешние угрозы, защита информационной системы, Марковские процессы, семантические нейронные сети, виртуальные сети.