International Journal of Engineering Innovation & Research
Volume 5, Issue 2, ISSN: 2277 – 5668

Designing the Methods and Algorithms of the Estimation Malicious Programs on the Base of Fuzzy Mathematical Models

Babamukhamedova Makhbuba Zakirovna
Email ID : abbts@mail.ru

Abstract **– This article is dedicated to the development of ways to protect computer networks from malicious programs based on fuzzy mathematical models that allow to mathematically is described a sequence of unlawful acts against the protected information system, made with use of malicious program and evaluate security threat level system, depending on the stage of action. Principles for solving mechanisms modeling tasks the impact of malware on secure information systems for evaluation of security threats to their information resources are formed. Also estimate of methods of estimate detection malicious programbased on the aggregation of disparate expertise and fuzzy mathematical models are developed.**

Keywwords **– Malicious Programs, Multistage Strategy, Fuzzy, Artificial Immune System, Connectionist Immune Detectors (CID).**

I. INTRODUCTION

Protection of computer systems from malicious software is currently one of the most urgent tasks in the field of information security. Annual losses from computer viruses estimated at tens and hundreds of billions of dollars. Malicious- a computer program or a portable code designed to implement the threat information stored in the computer system or flush misuse of system resources or other effects, prevents the normal functioning of a computer system. Malicious programs include worms, classical file viruses, Trojans, hacking tools and other software, causing deliberate damage to the computer on which they are launched for execution or other computers on the network. Regardless of the type of malicious can cause significant harm, implementing any threat information - the threat of compromising the integrity, confidentiality and availability.

II. PRINCIPLES MODELING MECHANISM OF INFLUENCES OF THE MALICIOUS PROGRAMS ON PROTECTED INFORMATION SYSTEMS

The analysis of unauthorized influence strategy to information in protected information system, realized with using malicious programs, allows installing the regularity between functional look of malicious programs and stage of the influence on protected information systems, within the framework of which these programs are used. At description stage influences on protected information systems can be received only as a result of structured syntheses generalized functional model of illegal actions, made with using malicious programs. This allows formulating the principles of modeling mechanism influences of malicious programs on protected information systems in interest of the estimation of the threats to their security. For this purpose we will define the row a worker hypothesizes [1]. The background hypothesis at decision given tasks are hypothesis about identity of the influences of malicious programs on protected information systems and hypothesis about multi-staged completion of the illegal actions in respect of protected information systems, made with using malicious programs.

In accordance with the first hypothesis, in spite of applicable malicious program to technologies of the provision to activities and vitality, exist the ways to identifications of their influence. This enables to put in correspondence to influence malicious programs identifying signs that, in turn, allows using these signs as raw data for modeling mechanism influences of malicious programs on protected information systems in interest of the estimation of the threats to their security.

Their own functions realize in accordance with the second hypothesis of malicious programs within the framework of multistage strategy of illegal actions. Multi-staging of these strategies is conditioned by need breaking (opening) of the defense mechanisms protected information systems.

The cardinal principles of modeling mechanism influences of malicious programs result from brought hypothesizes on protected information systems in interest of the estimation of the threats to their security.

The principle of synthesizability of the descriptions of illegal actions, made with using illegal programs, expects as central to shaping the descriptions of the similar sort action their structured syntheses. Logically resulting from given principle functional presentation of illegal actions, made with using illegal programs, brings about need of the use the methods of functional modeling for shaping the descriptions of the similar sort action.

In accordance with principle phased generalizability of the signs of illegal actions, made with using malicious programs, estimation of the threats of the influence of such programs must be realized with provision for multi-staging of strategies of the similar sort action.

The principle of multi-leveling of the functional syntheses of the descriptions of illegal actions, made with using illegal programs, expects presence several levels of the functional look of the similar sort action.

For the reason of decisions of the task of modeling mechanism influences of illegal programs on protected

information systems in the interest of estimation of the threats to their security are defined corresponding to factor [2].

As central to constructing factor of the possibilities of the estimation of the threats to security protected information system on base of modeling mechanism influences of illegal programs on their information facility by given nomenclature M models agree to use probability M such estimations, as probability of the event, under which prototyped illegal actions, made with usage of malicious programs, from their ensemble D uniquely identify the degree of the threat to security protected information system.

At ensemble D will be considered full if each its element$d_i, i = 1,2, \dots, |D|$will correspond to the sign of illegal actions $a_j, j = 1,2, \dots, |D|$ from their ensemble A.

The estimation level U such threats is considered marketed given by nomenclature M models if with probability P is provided participation of each sign of illegal action$a_j, j = 1,2, \dots, |D|$ in shaping of importance U.

With provision for stated, task of modeling mechanism influences of malicious programs on protected information systems in interest of the estimation of the threats to their security in profound plan is formulated as follows.

With reference to possibility of the influence of malicious programs on protected information systems and nomenclature of the models, describing of illegal actions, made with using malicious programs, designed algorithms of the estimation to security of these systems on base of modeling of the similar sort influence.

For the reason formalizations of the problem and ways of its decision, in accordance with worded by profound production, will mark through $R(M)$ set rules of the estimation of the threat to security protected information system by given nomenclature M models. Are they herewith provided possibility of the estimation of the threats P(R).

Then task of modeling mechanism influences of malicious programs on protected information systems in interest of the estimation of threats to their security possible to consider as task of the finding the set of the rules R, maxi minimizing possibilities P estimations of the threats to information security at nomenclature m models not exceeding given by M.

This allows formally statement of the problem to present in the manner of

$$R = \arg \max_{m \le M} P(R) \quad (1)$$

Defined a task modeling mechanism influences of the malicious programs on protected information systems in interest of the estimation of the threats to their security reasonable to solve by presentations:

- structuring descriptions of illegal actions, made with using malicious programs;
- the unification of the methods of modeling mechanism influences of malicious programs on protected information systems in interest of the estimation of the threats to their security to achieve the nomenclature of the models, not exceeding given;
- undertaking experiment on estimation of the possibility of estimation of the threats to security protected information system.

The signed methods of estimation can be applying to stage of the audit of information systems (see Fig.1). In general event model can be applying to elementary action, classified as illegal on each stage of audit. However not all parameters of models can be taken into account in step of system designing that obstructs the analysis of models.

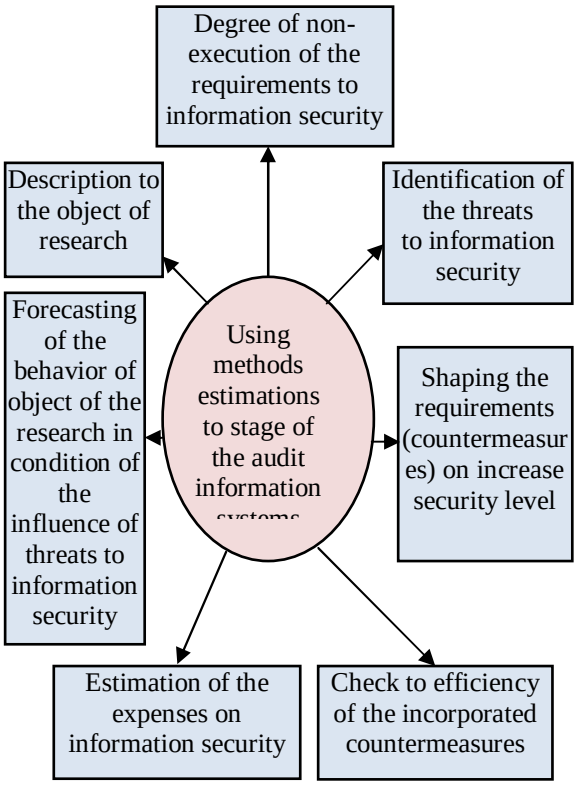

Fig. 1. Methods of the estimation to stage of the audit of information systems

III. The Ways of the Protection to Computer Network from Malicious Programs on the Base of Fuzzy Mathematical Models

The computer networks enterprise are subjected to the serious threat in connection with multiple attack of malicious programs. The attacks bring about interruption of the checking on production process with possible serious consequence. One of the most wide-spread types of malicious programs is classical computer viruses, for protection from which are actively used antiviral programs. Functioning of such type of the means of protection it is impossible value uniquely, such a lot of antiviral programs like viruses.

Thereby, necessary to value the influence of the concrete varieties of malicious programs and defensive facilities on features of the computer network of the

enterprise and on base got result to develop the efficient methods of protection computer network from malicious programs [3]. The most significant feature to network, influencing upon its power, are local: average length queue and average time processing the request in element. For calculation of the features of real networks possible to use the models closed and open network.

The model closed to network. Let it given loop network, consisting of C systems of mass service. It is given by N −amount packet, circulating in network; $P_R = (p_{ji})$ − routing matrix; m_i − amount processing conveyor in i − node; τ_i − average time of processing the packet in one conveyor i − node (see Fig.2).

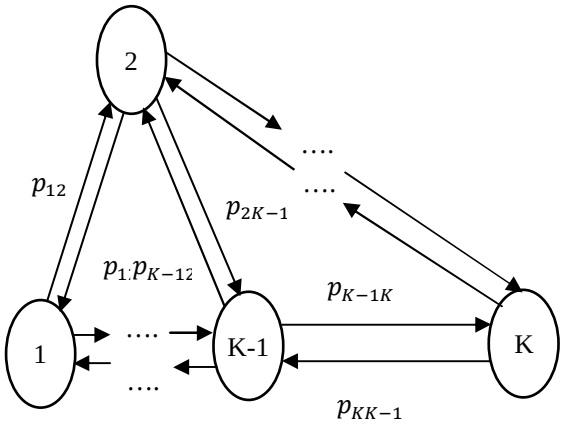

Fig. 2. The graph closed to network

In general event network is assigned by stochastic route matrix:

$$P_R = \begin{pmatrix} p_{11} & p_{12} & \dots & p_{1K} \\ p_{21} & p_{22} & \dots & p_{2K} \\ \dots & \dots & \dots & \dots \\ p_{K1} & p_{K2} & \dots & p_{KK} \end{pmatrix}, \qquad (2)$$

Where P_{ij} −probability of the sending the packet from$i$ − node in j − node, moreover $\sum_{j=1}^{K} p_{ij} = 1 \forall i = \overline{1,K}$.

For stationary mode intensity flow, falling into node is an intensities coming:

$$\lambda_j = \sum_{i=1}^{K} \lambda_i, p_{ij} \forall j = \overline{1,K}. \qquad (3)$$

We'll mark as $\mu_i = 1/\tau_i$intensity of the processing packet in$i$ − node, where τ_i −average time of processing the packet in i − node.

The possible conditions 1- node$\{S_k\} = \{S_0, S_1, S_2, .., S_N\}$, where k − number of packets(processing or expecting) in node. The roaming process on these conditions will be Markov's process to ruins and duplications.

In general event, probability of the finding i- node ableS_k:

$$P_i(n) = \frac{\lambda_i^n}{\mu_i^n(n)} P_i(0) \forall i = \overline{1,K}, \beta_i(n) = \begin{cases} n!, n \le m \\ m!\, m^{n-m}, n > m' \end{cases} \qquad (4)$$

m −number of conveyors in i − node.

The numerator – is the intensities of arrival packet (the duplication), denominator – is the intensities of their service (the ruin).

Possible conditions to network - an ensemble$S(N,K)$: $n = (n_1, n_2, \dots, n_K)$: $n_1 + n_2 + \dots + n_K = N$,where$n_i$ −the number of packets in node.

$$P_i(k) = \sum_{\substack{n_i' \in S(N,K) \\ n_i' = k}} P(n') \forall i = \overline{1,K}, \forall k = \overline{0,N} -$$

The summation over conditions from ensemble S(N, K), for which in i − node fund exactly kpacket

The averagenumber of packetsin$i$ −node:

$$L_i = \sum_{n=0}^{N} n P_i(n) \; \forall \; i = \overline{1,K}. \quad (5)$$

The averagetimestaysthepacketin$i$ −node (The theorem ofLittle):

$$T_i = \frac{L_i}{\lambda_i} \; \forall \; i = \overline{1,K}. \quad (6)$$

Model of unlocked networks. Let it given unclosed network, consisting of the source packet and K systems of the mass service (see Fig. 3).

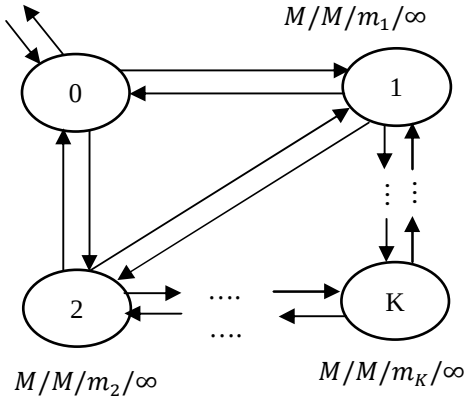

Fig. 3. Scheme of unlockednetworks

It is given $P_R = (p_{ji})$ −routematrix; μ_i −average intensity of the processing the packet in one conveyor i − node, λ_0 −intensity of falling into the network of flow packets.

In general event network is assigned stochastic routematrixes:

$$P_R = \begin{matrix} 0 \\ p_{10} \\ p_{20} \\ p_{K0} \end{matrix} \begin{matrix} p_{01} & p_{02} & \dots & p_{0K} \\ p_{11} & p_{12} & \dots & p_{1K} \\ p_{21} & p_{22} & \dots & p_{2K} \\ p_{K1} & p_{K2} & \dots & p_{KK} \end{matrix}, \quad (7)$$

WhereP_{ij} −probability of the sending the packet from$i$ −node in j −node, moreover

$$\sum_{j=1}^{K} p_{ij} = 1 \forall i = \overline{1,K}. \quad (8)$$

The node of networks has m conveyor and unlimited queue. The possible conditions of the node: $\{S_k\} = \{S_0, S_1, S_2, \dots, S_m, S_{m+1}, \dots\}$, where$k$ −the number packet

(processing or expecting) in node. The process roaming on these conditions will be Markov's process to ruins and duplications.

In general case:

$$P_i(n) = \frac{\lambda_i^n}{\mu_i^n \beta_i(n)} P_i(0) \forall i = \overline{1,K}, \beta_i(n) = \begin{cases} n!, n \le m \\ m!\, m^{n-m}, n > m' \end{cases} \quad (9)$$

Where$m$ – number of conveyors in i –node.

Utilised capacity of the node:$\chi_i = \frac{\lambda_i}{m\mu_i}$.

$$P_i(0) = \left(\sum_{n=0}^{m} \frac{p_i^n}{n!} + \frac{p_i^{m+1}}{m!\, m(1-\chi_i)} \right)^{-1} \forall i = \overline{1,K}, \quad (2.10)$$

Where$m$ – number of conveyors in$i$ –node.

The average length of queue:

$$r_i = P_i(0) \frac{p_i^{m+1}}{m!\, m(1-\chi_i)^2} \forall\, i = \overline{1,K}, \quad (11)$$

Where$m$ –number of the conveyors in$i$ –node.

Average number of the packet in node:

$L_i + k_i + r_i$,Wherek_i –average number of working channel.

Average time stay of the packet in$i$ –node is found on theorem of Little:

$$T_i = \frac{L_i}{\lambda_i} \forall\, i = \overline{1,K} \quad (12)$$

Average of the number, that circulating in network, packet:

$$N = \sum_{i=1}^{K} L_i \quad (13)$$

The average time stay of the packet in network:

$$T = \frac{N}{\sum_{i=1}^{K} \lambda_i} \quad (14)$$

The models and algorithms the building systems of protection computer network companies. Let it given unlocked network S, consisting of a source packet (the node 0) and M nodes. Then network is assigned by route matrixes:

$$P_R = \begin{matrix} 0 & p_{01} & p_{02} & \dots & p_{0M} \\ p_{10} & p_{11} & p_{12} & \dots & p_{1M} \\ p_{20} & p_{21} & p_{22} & \dots & p_{2M} \\ p_{M0} & p_{M1} & p_{M2} & \dots & p_{MM} \end{matrix}, \quad (15)$$

Wherep_{ij} –probability of sending the packet from$i$ –nodein$j$ –node, moreover$\forall\, p_{ij} \ge 0$ $(i, j = \overline{0,M})$и$\sum_{j=0}^{M} p_{ij} = 1 \forall\, i = \overline{0,M}$.

The packet – is malicious program, fallen into network through the zero node.

The possible conditions of network S: $s_0, s_1, s_2, .., s_M$,where$M$ –amount of nodes.

Theconditionss_i $(i = \overline{0,M})$means that malicious program is found in$i$ –node.

The breaking process on conditions - Markov's process, transition from condition to condition - in certain moments of time$t_0, t_1, t_2, ..$, (steps of the process) [4]. As a result of casual process of spreading the computer network occurs poisoning the receptive nodes, which correspond to the absorbing conditions.

The model I. 1 protected node and 0 nodes of protection. Let network S has two absorbing conditions - $s_0$ands_M,malicious program or bring back into the source (for instance, Internet) or will infect protected$M$ –node. How much steps will be able to pass the system before stop of the process that is to say absorptions in that or other condition, and as will be a distribution of probability of the conditions. For answer to supplied question use the following algorithm:

The step 1: Build the matrix Q from matrix P, carrying in it corresponding to absorbing conditions:

$$Q = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ p_{10} & p_{11} & p_{12} & \dots & p_{1M} \\ p_{20} & p_{21} & p_{22} & \dots & p_{2M} \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} \quad (16)$$

The step 2: Assign vector of the distribution of probability on zerostep$(t_0 = 0)$:

$$e = (0, p_{01}, p_{02}, \dots, p_{0M}). \quad (17)$$

The step 3: Finddistributionofprobability of the conditions onn –step on formula:

$$q(n) = e \cdot Q^n.$$

We will consider the process of the spreading malicious programs terminated on stepn, if probability of the conditions $s_1, s_2, \dots, s_{M-1}$are zero: $p_1(n) = p_2(n) = \dots = p_{M-1}(n) = 0$..

The considered algorithm allows to define probability that malicious program will abandon the networkS – $p_0(n)$andprobability of the poisoning the protected node$p_M(n)$.

The model II. One protected node and 1 node of protection. Let i –node of unlocked network is a node of protection [4]. The node of protection will name the node capable with probability and reveal the malicious program and delete. Under destruction will be in given models to understand the surge amalicious program in zero nodes.For determination of probability of the poisoning the protected node possible to use same algorithm, with matrix Q type only:

$$Q = \begin{pmatrix} 0 & 0 & \dots & 0 \\ p_{10} & p_{11} & \dots & p_{1M} \\ p_{i0} + u(1-p_{i0}) & (1-u)p_{i1} & \dots & (1-u)p_{iM} \\ 0 & 0 & \dots & 1 \end{pmatrix} \quad (18)$$

Changing number of the node$i = \overline{1, M-1}$possible obtain best protection for protected by M – node.

IV. Algorithm the Building Connectionist Artificial Immune Systems for Detectionmalicious Programs on the Base of Fuzzy Mathematical Models

In spite of the active actions on the part of producers of antiviral softwares, the computer viruses continue successfully to get into computer systems of the users on the world and execute malicious actions on destruction or theft to information. The traditional methods of finding the malicious programs, applicable today, not capable to provide reliable protection of the computer systems from penetration of computer viruses.

International Journal of Engineering Innovation & Research
Volume 5, Issue 2, ISSN: 2277 – 5668

The methods of the artificial intelligence allow to create in principal new algorithms of the finding malicious programs, allowing vastly raise the security level of computer systems. It is considered processes to generations, education, selection and the operation ofimmune detectors on base of connectionist networks [5]. It is generated initial population ofimmune detectors, each of which presents itself artificial neural network. We will present the connectionistimmune detector (CID) in the manner of black box, which has n-input and two outputs (see Fig.4).

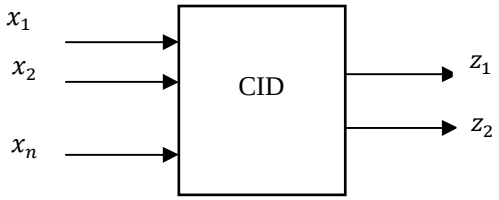

Fig. 4. Connectionistimmunedetector

Output importance of the detector is formed after presenting all images on it in accordance with the following expression:

$$Z_1 = \begin{cases} 1, if\ clear\ file \\ 0, else. \end{cases}$$
$$Z_2 = \begin{cases} 1, if\ virus \\ 0, else. \end{cases} \quad (19)$$

For correct operation connectionist immune detectors (CID) must pass the process of the education. The training sample is formed from clear files (the class of clear programs) and maliciousprograms (the class of malicious programs). The presence of the virus or its labels when learning allows the trained immune detector to find the difference between clear file and computer virus. Obviously that more varied files are presented in training sample, is more immune detectors will be more various. Advisable also have a representatives of all types of malicious programs - a hearts, Trojan programs, macro viruses and etc. However this unnecessary condition since malicious programs structured differ from uninfected files, since imply the destructive functions that influences upon decision of immune detector at scan of the file. Neural network is trained by education with teacher andetc.We indicate artificial neural network where given from clear files, but where from malicious programs.

Let $T-$ensemble ofclear files, but F-ensemble of malicious files. From them the ensemble of input images for learning of $i-$detector is formed at random.

$$X_i = \begin{bmatrix} X_i^1 \\ X_i^2 \\ \dots \\ X_i^L \end{bmatrix} = \begin{bmatrix} X_{i1}^1 & X_{i2}^1 & \dots & X_{in}^1 \\ X_{i1}^2 & X_{i2}^2 & \dots & X_{in}^2 \\ \dots & \dots & \dots & \dots \\ X_{i1}^L & X_{i2}^L & \dots & X_{in}^L \end{bmatrix} \quad (20)$$

Where $L-$ dimensionality of training sample.

Accordingly, the ensemble of master image looks as follows:

$$l_i = \begin{bmatrix} l_i^1 \\ l_i^2 \\ \dots \\ l_i^L \end{bmatrix} = \begin{bmatrix} l_i^1 & l_{i2}^1 \\ l_i^2 & l_{i2}^2 \\ \dots & \dots \\ l_{i1}^L & l_{i2}^L \end{bmatrix} \quad (21)$$

Master output importance for $i-$detector so:

$$l_{i1}^k = \begin{cases} 1, if\ X_i^K \in T \\ 0, else. \end{cases}$$
$$l_{i2}^k = \begin{cases} 1, if\ X_i^K \in F \\ 0, else \end{cases} \quad (22)$$

Education of each detector is realized for the reason minimization of the total square-law mistake of the detector. The Total square-law mistake $i-$detector is defined as follows:

$$E_i = \frac{1}{2}\sum_{k=1}^{L}\sum_{j=1}^{2}(Z_{ij}^k - l_{ij}^k)^2, \quad (23)$$

Where $Z_{ij}^k -$ importance of the $j-$output of $i-$detector when presenting on entry to its $k-$ image. The value of the total square-law error characterizes the fitness of detector to finding malicious files. The less importance of detector is more fitness. So value of the total square-law error is possible to use for selection best detector. The set of trained neural networks forms the population of the immune detector, which circulate in computer system and produce finding the malicious programs [6-7]. Presence of the varied files for learning and element to accidents in shaping input vector enables to get the big amount different on its structure of immune detector. In process of the scan of an unknown file neural network identifies the unknown image with the result that immune detector comes to a conclusion about accessories of the file to class malicious programs or to class clear files. The general algorithm of the operation connectionist immune systems, possible present in the manner of the following sequence:

The generation to initial population of the immune detectors, each of which presents itself artificial neural network with casual synaptic connections:

$$D = \{D_i, i = \overline{1,r}\} (24)$$

Where $D_i - i-$ connectionist immune detector,$r-$ total amount of detectors.

The education of formed immuneconnectionist detectors. The training sample is formed by casual image from collection of clear files (as a rule, this varied system utilities of the operating system) and from collection of malicious programs or their labels. Master output importance of neural network are formed accordingly (22).

The selection (the breeding) of theconnectionist immune detectors on test sample. On given iterations are destroyed that detectors, which turned out to be unapt to education, and detectors, in work which exist the different defect (for instance, false response). For this each detector is checked on test sample. As a result for each detector is defined importance of the square-law mistake E_i (24).

The breeding of the detector is produced as follows:

$$D_i = \begin{cases} 0, if\ E_i \neq 0 \\ D_i, else \end{cases}, \quad (25)$$

Where $0-$operation of deleting the detector.

Each detector is provided with by time to lives and casual image chooses the file for scan from collection of the files, which he did not check. The Scan by each detector of the selected file, as a result which are defined output importance of the detector $Z_{i1}, Z_{i2}, i = 1, r$.

If i −detector has not found the virus in scanned file, i.e. $Z_{i1} = 1$ and $Z_{i2} = 0$, that he chooses the following file for scan. If lifetime i − detector ended, that he is deleted, instead of he is generated new detector.

If i −detector has found the virus in scanned file i.e. $Z_{i1} = 0$and $Z_{i2} = 1$,that is flashed a signal about finding malicious file and are realized operations of cloning and mutations corresponding to detector [9]. The operation to mutations is concluded in additional education detector-clones on discovered malicious file. So the collection of detectors, adjusted on discovered malicious program. The selection cloned detectors, which are the most adapting to finding malicious programs. If$E_{ij} < E_i$, that detector passed the selection. Here E_{ij} −total square-law error of j −clone of i −detector, which is computed on maliciousfile.

The detectors-clones realize the scan of the file space of computer system until will occur the destruction of all manifestations of malicious programs.

Forming the detectors of immune memories. On these iterations are defined connectionist immune detectors, shown best results when finding being present in computer system of the virus. The detectors of immune memories are found in system it is enough long time and provide protection from the repeated contamination [8]. The particularity of the offered algorithm is that each connectionist immune detector is completely independent object (the autonomous agent) i.e. chooses itself area of the scan itself. For this he gets the list of the files, keeping in space of the memories, and casual image chooses the file from list forits check.

After checking a file of detector goes to the following file, also chosen by casual image from existing list. The scan of the files of connectionist immune detector lasts until detector finds the malicious program, or prior to the expiration of time, conducted for operating given detector. The Broad population ofconnectionist immune detector provides well-timed finding malicious programs. Thereby, is kept principle to decentralizations of the system to security, built on base of the combinations of the methods ofneural networks and artificial immune systems that vastly raises intolerance and security of systems as a whole.

V. Estimation of the Methods Detectionmalicious Programs on Base of the Ill-defined Mathematical Models

Estimation of the methods of finding the malicious programs on base of the ill-defined mathematical models comprises of itself following stages:

- choice of the testes of antiviral programs, determination their weight by means of method of the fresh comparisons and highlighting of the scales estimation different test (checkout);
- choice of the united scale, shaping the requirements to scale;
- transformation the estimation of results of the test in estimations on chosen universal scale. The reception of the estimation in the manner of fuzzy set, which element are a variants estimation on universal scale, corresponding to estimation on scale result test;
- reception of estimation of the antiviral programs on chosen to scale. On base of e generalised estimation in the manner of fuzzy set by method centre of gravity is computed total estimation antiviralpacket.

The scales estimateof the methods detection malicious programs. The Universal scale must satisfy the following requirements:

1. The scale must be a strong type to when turning to universal scale did not occur the loss to information.
2. For ensuring comfort perceptions of the got result universal scale must be quantitative and its maximum estimation must be not too much.
3. To at transformation of the scales not add big amount of information chosen scale must have not too big maximum importance.

As universal scale is chose scale of the relations, minimum estimation which - 0, maximum - 10.

The transformation estimation of results of the test in estimations on chosen universal scale. The data got as a result of undertaking different test (checkout), in general event, have a different logical sense, are measured in miscellaneous scale and, generally speaking, incomparable between itself on range of importance [10]. For adduction of different scales of the united comparable type (the uniform space sign) can be used normalization. The normalization often conducts by fissions of all importance on greatly possible importance criterion. Given normalization has a row defect: first, it is applicable only for scales of the relations and absolute scales, secondly, is expected that preferences evenly increase that not always so. At transformation of the scales for each scale necessary to define the factors of fuzziness. Also, the factors hang from criterion, priced at test; for instance, amount of demodulated virus is valued moreobjectively, than comfort of the use, thereby, test, evaluating comfort of the use corresponds to the greater factor of fuzziness. For given methods of importance factor offuzziness are chosen from 1 before 2.

For each estimationis on scale of the results of tests possible to build the fuzzy set with function accessories triangular or trapezoid type (see Fig.5).

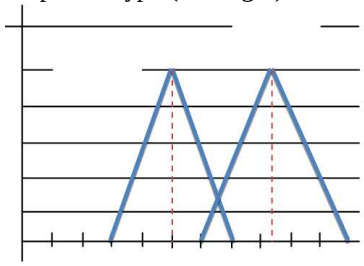

Fig. 5. Correspondence of points on source and on universal scale

In connection with chosen source scale will enter the following algorithms of transformation:

The scales of relations. The estimation of the methods of the finding malicious programs on universal scale is assigned by means of modes (the expected importance) and fuzziness factor - a parameter, characterizing degree of blurriness ill-defined number [11].

The most probable importance (mode) on the universal scale is calculated on formula:

$b = \frac{K \cdot q}{K_{max}}$, if greater amount of points corresponds to the best estimation;

$b = q - \frac{K \cdot q}{K_{max}}$, if smaller amount of points corresponds to the best estimation;

where$b$ – mode;

q – Maximum estimation in universal scale;

K – Amount of taken points in source scale;

K_{max} – Greatly possible the amount of points in source scale.

Thereby, mode – a real number from gap $[0, q]$ (where q – is maximum estimation in universal scale), in general event is not integer.

The fuzziness factor is chosen in accordance with type of the scale of results of the test and particularity of the concrete test. Each estimation on the scale of results of the test corresponds to the fuzzy set, which elements are variants of the estimation of chosen universal scale. To build this ensemble it's necessary to calculate the importance of function of the accessories for each variant of the estimation of universal scale. The importance of function of the accessories for each variant estimation universal scale is calculated on formula:

$$\mu(i) = \max\left\{1 - \frac{|b - i|}{k}; 0\right\} \quad (26)$$

Where$i$ – variant of the points of universal scale;

b – Mode, computed on previous step;

k – Coefficient of fuzziness.

If mode is an integer number, maximum importance of the function accessories got fuzzy set is 1. Otherwise, importance of the function accessories is necessary to normalize. Normalization is executed on the following formula:

$$\mu^*(i) = \frac{\mu(i)}{sup\,\mu\,(i)}, i \in [0; q] \quad (27)$$

Where$\mu^*(i)$ – importance of the function accessories for estimation i after standardization;

$\mu^*(i)$ – Importance of the function accessories for estimation i;

q – Greatly possible estimation on universal scale.

For the further calculations will be used normalized importance of the function accessories.

For scales of order. The point of the methods of findingmalicious programs on universal scale is assigned by means of the expected importance and factor of fuzziness, but if and when gradation on scale of the order small quantity, that the expected importance will not number, but some gap (the gap of tolerance). For calculation of the borders oftolerance of the points in ordinal scale will convert to estimation from. For calculation of the borders oftolerance of the estimations in ordinal scale will convert to points from 0 to K_{max}, whereK_{max} – amount of gradation-1 (for scales of the order of such transformation possible). Hereinafter compute the mode similarly way for quantitative scales.

The borders of tolerance are calculated on the following formula:

$$a_1 = \max\left\{b - \frac{l}{2}; 0\right\}$$
$$a_2 = \min\left\{b + \frac{l}{2}; q\right\} \quad (28)$$

Wherea_1 anda_2 – left and right borders of tolerance;

l – the length of the gap of tolerance;

b – mode;

q – themaximum mark in universal scale.

Importance of the function accessories for each variant estimation universal scale is calculated on formula:

$$\mu(i) = \begin{cases} \max\left\{1 - \frac{|a_1 - i|}{k}; 0\right\}, i < a_1 \\ \max\left\{1 - \frac{|a_2 - i|}{k}; 0\right\}, i < a_2 \\ 1, i \in [a_1, a_2] \end{cases}, \quad (29)$$

Where$i$ – variant of the marks of universal scale;

a_1 anda_2 – left and right borders of tolerance;

k – coefficient of fuzziness.

If maximum importance of the function accessories got fuzzy set less 1 (this possible if and when gap of tolerance less 1), that got importance of the function accessories necessary to normalize.

VI. CONCLUSIONS

1. The layered presentation for phased modelling not only illegal actions, but also strictly acts of the information system and software in particular is offered.

2. Manners of the protection computer network from malicious programs on the base of fuzzy mathematical models, allowing value the influence malicious programs and means of protection on features of the computer networks and build the optimum system of the protection of computer network of the enterprise frommalicious programsare brought.

3. There were researched algorithms of the building and operation connectionist artificial immune systems for finding malicious programs.

4. Estimation of the methods of finding malicious program on base aggregating disembodied ill-defined mathematical modelsis designed.

REFERENCES

[1] Barry L. Williams. «Information Security Policy Development for Compliance»: ISO/IEC 27001, NIST SP 800-53, HIPAA Standard, PCI DSS V2.0, and AUP V5.0. 2013 year.

[2] Gorniak, S., Ikonomou, D., Saragiotis, P. et al., Priorities for Research on Current and Emerging Network Trends. European Network and Information Security Agency. 2010. ttp://www.enisa.europa.eu.

[3] Aycock J. Computer Viruses and Malware on based mathematical models. Advances in information security. - Calgary: Springer, 2006. - 227 p.
[4] Mashevsky Y.V., Namestnikov Y.V., Denishchenko N.V. Method and system for detection and prediction of computer virus-related epidemics. – US Patent No. 7,743,419 B1, 2010.
[5] Timothy J. Ross. F Fuzzy Logic with Engineering Applications. 3rd Revised edition. Publication City/Country Hoboken, United States., 2010. ISBN10 047074376X.
[6] Bezobrazov S., V. Golovko. Neural Networks for Artificial Immune Systems: LVQ for Detectors Construction// IDAACS'2007: proceedings of the 4 IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. - Dortmund, 2007. - P. 180-184.
[7] Bezobrazov S. V.Golovko. Neural networks and artificial immune systems - malware detection tool // ICNNAI'2008: proceedings of the 5 International Conference on Neural Networks and Artificial Intelligence, Minsk, 27-30 May 2008. /Brest State University of Informatics and Radioelectronics.- Minsk, 2008. - P. 49-52.
[8] Michael Sikorski. Andrew Honig. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software 1st Edition. No Starch Press; (March 3, 2012) ISBN-13: 978-1593272906, ISBN-10: 1593272901, 800 pages.
[9] Nachenberg C., Ramzan Z., Seshadri V. Reputation: a new chapter in malware protection // Virus Bulleti Conference. – 2009. – P. 185–191.
[10] Elovici Y.M., Tachan G.O., Shabtai A.C. A system that provides early detection, alert, and response to electronic threats. – European patent app. No. 07015353.1, 2008.
[11] Mashevsky Y.V., Namestnikov Y.V., Denishchenko N.V. Detection and minimization of false positives in anti-malware processing. – US Patent No. 7,640,589 B1, 2009.

AUTHORS PROFILE

Babamukhamedova Makhbuba Zakirovna
Assistant Professor was born January 25, 1953 year in Tashkent city, Republic of Uzbekistan. In 1975 graduated «Applied Mathematics» faculty of Tashkent Polytechnic Institute. Has more than 40 published scientific works in the form of articles, journals, theses and tutorials. Currently works of the department «Information technology software» in Tashkent University of Information Technologies.