Conceptual approach to building information security systems for telecommunication systems using artificial immune systems

L V Stepanov, E V Grechishnikov, V I Novoseltsev and S S Kochedykov
ET Department, Voronezh Institute Federal Penitentiary Service of Russia, 1a Irkutskaya Street, Voronezh, RU

E-mail: infosec36@mail.ru

Abstract. In article, it is shown that distributed nature the infotelecommunication of systems and networks, a large number of users in them leads to considerable increase of "bottlenecks" and because of vulnerabilities of these structures. It steadily lowers the level of information security, increases risks of damage or destruction of data, and negatively affects confidentiality of information. Further, the concept of application at the heart of mechanisms of information security of the distributed system of the principles of functioning of immune system of the person as effective remedy of counteraction to different types of threats is considered. This publication is one more step in the direction of discussion of a possibility of creation of the program technical means imitating functioning of biological systems.

1. Introduction
The problem of ensuring information security is a relevant task for any information system. This task has the special importance for telecommunication systems and networks. The distributed nature of these structures and a large number of users leads to considerable increase of "bottlenecks" and as a result of vulnerabilities of telecommunication systems and networks. It steadily lowers the level of the information security (IS), increases risks of damage or destruction of data, negatively affects confidentiality of information.

2. Entity of a problem of support of information security of telecommunication systems or networks
Under the threat of (IS) we will understand potentially possible action or an event capable to reduce the level of security of information, telecommunication system or network.

At the same time these actions or events often have complex character. So, for example, influence of malicious applications can lead not only to damage or destruction of information, not only to reduction of its confidentiality, but also to failure of technical infrastructure within an information system. Thus, the threat of influence of the malicious software can be considered as complex and containing in the composition not one, and directly three types of the actions having negative effect on the IS level [1, 2].

Any threat is a consequence of vulnerabilities of telecommunication systems. Elimination of these vulnerabilities is impossible owing to a large number objective (for example, absence of money) and subjective (for example, absence of experts or negligence in questions IS) factors.
Let $H$ and $A$ sets of threats and vulnerabilities of IB respectively:

$$H = \{H_j\}, j = 1, m; A = \{A_i\}, i = 1, n,$$

(1)

where $H_j$ – $j$-th threat of IB; $A_i$ – $i$-th vulnerability of IS.

We will define $H_j$ as:

$$H_j = \{h_j^y\}, y = 1, w_j,$$

(2)

where $h_j^y$ – $y$-th characteristic $j$-th threat of IB, that is an action or an event capable to reduce the IS level; $w_j$ – number of characteristics $j$-th threats.

It is offered to divide threats of IS on an entity of their harmful action into the quantitative and qualitative:

$$\forall h_k^y | h_k^y \in C \lor h_k^y \in NC,$$

(3)

where $C$ – quantitative characteristics of harmful action; $NC$ – qualitative characteristics of harmful action of threat.

The same way it is possible to characterize vulnerability of IS. Besides, it is possible to understand set of actions for counteraction to threats of IS from a security system of telecommunication systems and networks as a set of A. If actions from the IS system are understood, then it needs to be considered in the course of formalization of actions as a part of these actions.

Expression (3) has significant character as the difference between quantitative and qualitative parameters is high as only some results of harmful action can be expressed quantitatively. In the example given above failure of the equipment quite can be estimated in value terms (that is quantitatively), and damage of information and the more so decrease in its confidentiality, can be estimated qualitatively in is dependent on the importance of this information.

Characteristics of C can express the quantitative in the numerical form. Unlike the quantitative parameters, qualitative characteristics of NC have no numeric expression and represent linguistic descriptions [3-5]. And for each threat or vulnerability the list of all characteristics can be in advance defined and constant for each telecommunication system or a network. The variable with values in the form of the words of some natural or artificial language is called linguistic.

For transition from high-quality expression of characteristics of harmful action of threat to their numeric expression it is offered to use provisions of the theory of decision-making and indistinct sets, having formulated them in relation to the task of support of IS. However, in these conditions of restriction of "classical" methods for the decision of semi structured tasks are a serious problem. In too time approaches which are based on the theory of indistinct sets and the theory of decision-making are effective in the conditions of similar uncertainty. Qualitative characteristics require formalization in the form of a vector of interval values, that is an indistinct interval. Everyone the interval is characterized by an uncertainty level. For establishment of boundaries of intervals experts on the basis of the available data and also experience can describe these boundaries rather precisely quantitatively.

For each $h^y$ it is possible to specify a set of linguistic designs of $L^y$, precisely and fully describing all values which $y$-th the characteristic of threat of IS can accept:

$$L^y = \{l_b^y\}, b = 1, r,$$

(4)

where $r$ – number of linguistic designs $y$-oh characteristics of threat of IS.

For transition to numerical values of characteristics, it is necessary to give some mark in compliance to each $l_b$. Its weight value has to establish a ratio between linguistic designs:
Estimates of \( o_b \) can be used instead of linguistic terms of \( l_b \) in calculations. Unfortunately, at their large number in practice it is difficult precisely and the main thing proportionally to estimate all characteristics.

It is offered to compare all available \( l_b \) in pairs and to estimate as one \( l_b \) corresponds to other characteristic.

Integer scale of couples "DESCRIPTION: PREFERENCE DEGREE" characterizes difference of characteristics:

\[
SH = \{o : sh_u\}, u = 1, dl,
\]

where \( dl \) – quantity of degrees of preference.

The \( sh_u \) element is set by an integer. The value characterizes difference of \( op \) of two sizes among themselves. Depending on the required accuracy, the scale can be any length of \( dl \). Elements of a scale have to be set with an identical step.

We will create a square matrix [6, 7] of paired comparison of the available linguistic designs:

\[
SR = \begin{bmatrix}
  sr_{11} & ... & sr_{1b} & ... & sr_{1r} \\
  ... & ... & ... & ... & ... \\
  sr_{bl} & ... & sr_{lb} & ... & sr_{lr} \\
  ... & ... & ... & ... & ... \\
  sr_{rl} & ... & sr_{rb} & ... & sr_{rr}
\end{bmatrix}
\]

where

\[
sr = \begin{cases}
  sh, l_b > l_{b'}, \\
  1, l_b = l_{b'}, \\
  1, l_b < l_{b'}.
\end{cases}
\]

The symbol «\(<\)» means that one linguistic design is "more attractive" another.

Using \( SR \), it is possible to define value of weight of each linguistic design \( l_b \) in various ways. For example, we summarize elements of lines of a matrix

\[
Sum_b = \sum_{b=1}^{r} sr_{bb}, b = 1, r,
\]

where \( b \) and \( b' \) – indexes of a line and column respectively.

We determine the sum of \( Sum_{obu} \) of all elements of a matrix of \( SR \).

We normalize values:

\[
o_b = \frac{Sum_b}{Sum_{obu}}.
\]

This and others a way can be realized even at a big matrix of \( SR \) and as a result to receive a vector of \( O' \) of numerical values for each design from \( L' \). Especially as the quantity of linguistic designs applicable even to various slags is most often limited.
Also for further operation with the formalized characteristics of threats and vulnerabilities, it is necessary to execute normalization of the quantitative values of the initial sets.

Each information system and its technical infrastructure have the specifics. These specifics do often-unique conditions of support of the required IS level and, therefore, it becomes necessary to apply special means of information protection.

Despite of development of the basic principles of support of IS, mechanisms of information security it is impossible to read completely effective and capable to provide complete security of data computers and telecommunication networks. The variable nature of threats of information and the increasing significance of information for private and professional activity of the person does relevant development of new approaches to support of IS. One of such approaches is mathematical and program (and it is possible program and technical) implementation of the principles of functioning of immune system of the person. In other words, it is possible to speak about creation of the artificial immune system for counteraction to threats of IS within telecommunication systems and networks.

We will understand set of the mathematical methods modeling basic functions of immunity of biosystem as the artificial immune system (AIS) (for example, the person), and the threats of IS, their parameters and values applied to definition and capable to minimize influence of harmful factors on IS of telecommunication system or network.

It is possible to say that IIS has to create a certain barrier to counteraction to threat of IS. It is possible to understand set of independent measures (actions) which sources is IIS directed to full or partial isolation of telecommunication system from threats of IS as such barrier. In addition, AIS has to be capable to react on external and internal, rather telecommunication network, threat of IS.

It is offered to allocate objective and subjective barriers:

1. Objective barriers don't depend on activity of components of telecommunication network and are the general conditions for all elements of this network.
2. Subjective barriers are framed in response to implication of threat of IS by the framed activity of concrete knot or the participant of network.

Unlike objective barriers subjective barriers can be considered local. Their action shouldn't extend to other participants (knots) of telecommunication network. "Classical" mechanisms of providing IS can't provide such selective action. In it the relevance and the high practical importance of AIS in the sphere of telecommunication systems and networks since this new security system will be adaptive to operating conditions as all structure, and to individual conditions of each concrete knot or a segment consists. At the same time it has to be the distributed system, but at the same time, according to similarity to biological systems, uniform system.

The principle of "counteraction" allows drawing an analogy between processes of information security and processes in biological systems and, in particular, with protective functions of a live organism which source is the immune system. However, the superficial glance on activity of immunity is not enough. Before development of software, the analysis of functional features of activity of immunity is necessary.

3. Immunity as protective function of biological systems

The immunity of biosystems is considered as a way of protection of this system against all alien substances various (external and internal) the nature. His main goal consists in the maximum ensuring steady existence and development of an organism [8, 9].

The immune biosystem is a complex structure, consisting of a large number of functionally different components and subsystems. In the process of development, she constantly learns and is able to distinguish between foreign agents and her own cells, molecules and body substances.

In [8, 9] the following generalized, basic algorithm of action of immune system is considered:

1. Penetration of the alien agent into an organism;
2. Manifestation of allogeneity of the agent through antigens;
3. Immune answer:
   - antigen recognition by specific lymphocytes and their activation;
- an effector phase – lymphocytes coordinating the activity eliminate a source the stranger of antigens;
- phagocytosis – absorption and dissolution of alien agents;

4. A conclusion from an organism of products of activity of immune system.

Thus, the main role of the immune system is to recognize and classify all cells (molecules or substances) in the body into "one's own" or "others". Alien cells are further classified to stimulate the necessary protective mechanism necessary to neutralize them. It is this role of immunity that is the main prerequisite for considering the similarity of biological processes and protective mechanisms in telecommunication systems and networks [10, 11].

| Immune system | Telecommunication system or network |
|---------------|-----------------------------------|
| Penetration of the alien agent into an organism | Emergence of threat of IS |
| Show of antigens | Manifestation of the characteristic (characteristics) of threat |
| Immune answer: | Reaction of AIS: |
| Antigen recognition | Classification of threat of IS and definition of her influence (bears harmful action or not) on telecommunication system or network |
| Effector phase | Definition of the directions (types or sets of measures) counteractions to threat |
| Phagocytosis | Selection of one set of measures of counteraction to threat and realization of these actions for preservation of IS of telecommunication system or network |
| Conclusion of results of activity from an organism | Check of success of counteraction |

Apparent from the table, between biological and artificial immune system there is a considerable similarity. The analogies revealed as a result of the analysis allow to apply the general technology of functioning of immunity to modeling of counteraction to threat of IS of telecommunication system or network.

Thus, in relation to the AIS telecommunication systems has to allow to classify threat of IS and to determine the most effective option of counteraction by her. An additional, but also important task is definition of the direction of application of the chosen counteraction option. I.e. according to technology of action of immunity, for modeling of AIS it is necessary to synthesize mathematical models of three phases of the immune answer.

4. Mathematical model of classification of threat of IS

Sign on which the biological immune system is capable to distinguish the foreign agent influencing an organism is the antigen, that is some specific element of this agent.

In the conditions of threats of IS we will understand any as an antigen $h^j$ -th action or an event capable to lower the IS level, important in this telecommunication system or network [5, 6].

Antibodies are an antigen the binding elements of immune system. In the conditions of telecommunication systems the antibody can represent the certain indicator characterizing vulnerability of IS of system.

In difference, for example, from a nervous system of the person which activity the brain controls management isn't performed of functions of immunity of biosystem. All components of immune
system work rather independently, at the same time reacting to "behavior" as each other, and to changes in the whole organism. In this regard, for more adequate modeling of real processes in AIS, we will consider that it is necessary to react to each threat also independently, but taking into account all set of vulnerabilities in the IS systems telecommunication system or networks.

It is important to note that sets of threats and vulnerabilities of \( H \) and \( A \) cannot coincide by quantity of elements. And it is the most probable that the set of threats of \( H \) will be more even the real-life, but not revealed number of vulnerabilities.

In this regard, process of recognition of antigens and antibodies (the alien agent in general) comes down to comparison of sets of \( H \) and \( A \).

Affinity of antibodies to an antigen call force of their interaction realizing forces of an attraction and pushing away between an antibody and antigen [4]. At the same time degree of durability of communication is estimated by coefficient of affinity [4]:

\[
K = \frac{[H \cdot A]}{[H] \cdot [A]},
\]

(11)

where \([H] \cdot [A]\) designate concentration of antibodies and antigens.

Immunology expression (11) is received based on the law of the acting masses and is right only for immune biosystems. Therefore, in relation to IB we will define communication durability degree as the relation of number coincided antigen and antibodies to total number [5], t.i.

\[
K = \frac{|H \cap A|}{c},
\]

(12)

where \(|H \cap A|\) – the number of the coincided parameters of the antibodies and antigens on type that is which have coincided as elements of threat of IS and vulnerabilities of IS of telecommunication system or network.

Transition from (11) to (12) can be justified the fact that the value of threat of IS will significantly not have negative effect on telecommunication system if it matches in all respects vulnerabilities. For example, the harmful attack to the server hardware will have smaller consequences for a telecommunication network if on these servers there is no confidential information though this type of threat can assume confidentiality harming.

From expression (12) it is visible what the more characteristics of threat and vulnerabilities has coincided (and only on type, but not on value), the more than \( K \) [7], t.i.:

1) at \( K \to 1 \) – the threat of characteristics of \( H \) should be considered the alien agent (this condition is necessary, but isn’t sufficient);

2) at \( K = 0 \) – the threat doesn’t bear negative impact to a condition of telecommunication system or network.

Except affinity coefficient, the size of the importance of threat for telecommunication system is estimated with a force of not covalent communication \( F \) [7]. At interaction of antibodies and antigens of force of not covalent communication, we are separately very weak, but at their large number, total energy will be essential. In biological system, she depends on \( d \) distance between the interacting groups of elements. At usual interaction it is inversely proportional \( d^2 \), and at close rapprochement molecules – \( d^3 \). However, at very close rapprochement of molecules of antigen and an antibody between them on the contrary there are pushing away forces inversely proportional \( d^{12} \).

In biosystem, there are also other ways of interaction, which owing to specifics can’t be formalized mathematically or extremely difficult [7].

Apparently from the figure 1, at \( d \to 0 \), the \( F \to \infty \) function, and at \( d \to \infty \), the \( F \to 0 \) function. This option of interaction can be considered under a condition, for example, if values of antigen and an antibody are close.

In relation to the considered task, size \( d \) is offered to be determined how:
\[ d = h - a, \]  

(13)

where \( h \) and \( a \) – values only for the coincided components of threat and vulnerability respectively.

This condition is obligatory for conservation of similarity of activity of immunity of biological system and IIS as at this stage the immune system reacts only to antigens for which it has receptors.

Expression (13) is right if to accept that at estimation of threats of telecommunication network it was accepted that the harmful nature of activity of subjects is higher, than the indicator is closer to unit, and vulnerability, on the contrary, the value is closer to unit, the worse.

We realize accounting of forces of an attraction and pushing away proceeding from value \( d \). If \( d > 0 \), then we consider that, there is attraction force. It means that parameters of threats advance similar parameters of vulnerabilities. If \( d < 0 \), then arises pushing away force – the current parameter of threat concedes to a vulnerability indicator.

\[ \text{Figure 1. Dependence of force of not covalent communication on distance} \]

On condition of a small difference (for example, \( d < 0.5 \)) between parameters of threat and vulnerability force of communication will be defined as [5]:

\[
F_{\text{v}} = \begin{cases} 
\frac{1}{d^2} + \frac{1}{d^7} = \frac{d^7 + d^2}{d^9}, & \text{with } 0.5 \geq d > 0; \\
\frac{1}{d^{12}}, & \text{with } -0.5 \leq d < 0; \\
0, & \text{with } d = 0,
\end{cases} 
\]

(14)

where \( F_{\text{v}} \) – force of communication of an antibody and antigen.

On condition of a big difference (for example, \( d \geq 0.5 \)) between parameters of threat and vulnerability force of communication is offered to be defined how:
The first method (14) of determination of function value of communication is most sensitive to insignificant deviations of $a$ and $h$ unlike the second (15).

Taking into account an entity of the solvable task the value of force of communication allows to describe threat precisely:

1. $F_{ys} > 0$ – the threat should be considered the alien agent;
2. $F_{ys} \leq 0$ – threat does not bear negative impact on network or system.

![Figure 2. Recognition process antigen](image)

It is important to note that parameters of threats and vulnerabilities can be set in different scales therefore it is necessary to execute their preliminary normalization. Their preliminary formalization and representation in a numerical form is necessary for determination of force of communication when using qualitative characteristics of threats and vulnerabilities.

5. **Mathematical modeling of an effector phase**

Whether at a stage of classification of threats preliminary definition is carried out the threat bears the valid harmful influence on IS of telecommunication system and network. The problem of this phase of the answer of immune system consists in exact definition of need of the directions of necessary reaction to set of antigens of the alien agent (threat of IS).

As appears from expressions above only at $K \to 0$ and $\forall F \leq 0$ the immune answer isn't required, that is the threat doesn't break the developed IS level. The value of function $F$ pays off only for each of the coincided couples "antigen antibody", that is for the coincided activities of threat and vulnerability of telecommunication system or couple "threat action on IS". At the same time for some couples function can be more, and for some couples it is less than zero.

In other words, for a part of the coincided couples the threat of IS of telecommunication system will exist, and for some will not be. On some positions the appeared threat can be dangerous, and on some – insignificant. Anyway, there can be directions of threats (the antigens that are not connected...
with antibodies), counteraction to which won't be or vulnerability in relation to which in a security system hasn't been revealed. In practical cases such situation can follow from a circumstance of constant improvement of threats of IS and their sources, or from the insufficient level of reliability of the IS system. In this case, even if $\forall F \leq 0$, threat, appear at telecommunication system or network, it is impossible to refer to category "isn't harmful". It confirms need of check of two conditions in the course of recognition antigen and proves importance in addition that is an effector phase.

Indispensable condition of transition to an effector phase is $K > 0$, t.i. characteristics of threat and the characteristic of vulnerability are crossed and for them the value of force of communication $F_{ys} > 0$ is calculated. The result of a stage of recognition antigen can be illustrated as follows (figure 3) [10].

| Threat | Antigen | $h_1$ | $h_2$ | $h_3$ | $h_4$ | $h_5$ | $h_6$ |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Value | 3 | 5 | 4 | 1 | 7 | 8 |

| Vulnerability | Antibody | $a_1$ | $a_2$ | $a_3$ |
| --- | --- | --- | --- | --- |
| Value | 3 | 2 | 7 |

$K = 3/6 = 0.5$

| $F$ | $F > 0$ | $F < 0$ | $F > 0$ |

*Figure 3. Initial condition of an effector phase*

The threat has five directions of influence (antigens), three of which have coincided with vulnerabilities (antibodies). At the same time the coefficient of affinity of $K$ will be equal to 0.5. It means that this threat should be considered as harmful to telecommunication system. Having defined $d$, it is possible to find values of force of communication, which in the second and sixth direction it is more than zero. On the first, third and fifth direction the telecommunication system in general has no receptors that is these directions can be unimportant for this system because of lack of these vulnerabilities. It confirms that the threat is harmful (the alien agent).

The immune biosystem is capable to distinguish antigens antibodies of separate cages on all organism. Therefore, it is quite possible to expand activity of the considered phases on various levels of telecommunication system:

1) on microlevel – the level of a separate component of telecommunication system;
2) on macrolevel – the level of knot of network;
3) on megalevel – the level of system or network.

In the course of the functioning AIS has to be capable to react to different types of threats. In terms of immunity of biosystem accumulate such set of antibodies which is the most rational. Therefore, the situation of "untied" antigens is improbable, but a chance.

To model the effector phase, let us use the realization of the diversity mechanism for the antigen-recognition structures of the biosystem [7]. Most of these processes occur at biochemical level and are highly complex. The biochemical level and complexity do not allow complete formalization of the mechanism of diversity in the form of a mathematical model.

One of the most explored ways of realizing the mechanism of diversity are somatic recombination’s and the synthesis of additional nucleotides [7]. The essence of these methods is to supplement the already existing structure of the antibody with additional components. In the case of the IS, a number of vulnerabilities (antibodies) of the telecommunication system need to be supplemented with a new component (antibody) for each new threat component (Figure 4).
problem of "complementarity" of the list of vulnerabilities is important and needs a separate discussion, since it is quite possible that some characteristic component of the threat activity may not be relevant or simply inapplicable to the conditions of a particular telecommunications system.

Elements of synthesis are characteristics of antibodies of $a_1$ and $a_4$. It is important to note that availability of untied antigens ($h_2$) is manifestation of the natural (already available) barriers.

| Antigen | $h_1$ | $h_2$ | $h_4$ | $h_6$ |
|---------|------|------|------|------|

( recombination)

| Antibody | $a_1$ | $a_2$ | $a_3$ | $a_5$ | $a_6$ |
|----------|------|------|------|------|------|

Then $F(x)$:

\[
\begin{array}{cccccc}
4 & 2 & -4 & -1 & 2 & 1 \\
\end{array}
\]

Figure 4. Recombination antigen and antibodies

After end of this phase, it is necessary to define total value of force of communication:

\[
F_{\Sigma} = \sum_{x \in X} F(x),
\]

(16)

Figure 5. Process of an effector phase
For example, for the reviewed example:

\[ F_{\Sigma} = 4. \]  
(17)

Therefore, if \( F > 0 \), then the appeared threat is harmful for IS of telecommunication system.

Acceptance of the final decision on the nature of threat of IS is possible only upon termination of an effector phase and leaning on total value of function of force (16). If for some couples of antigens and antibodies of \( F_{ss} > 0 \), these components of threat can be compensated by other couples for which \( F_{ss} < 0 \). The total \( F_{\Sigma} \) value less than zero can be as a result received, and it will mean that the threat has no harmful value for IS. This situation needs special consideration in separate work.

Having established the nature of new threat ( \( F_{ss} > 0 \)), on the basis of the first stages of the answer of AIS, it is possible to pass to definition of counteraction to this threat, that is to a stage of a phagocytosis of biosystem.

6. Mathematical modeling of a phagocytosis

The threat is an alien agent in telecommunication system if values of antigens surpass antibodies. The directions of action of threats of IS exceed on the formalized value similar values of measures for counteraction to these threats or the formalized values of vulnerabilities of telecommunication system below values of threat. Otherwise the threat will not affect a condition of IS and work of AIS on reaction to this threat ends.

In the first case of AIS has to develop such option of counteraction to threat at which her influence will exist partially or completely is eliminated.

In other words, it is necessary to correct values of antibodies from \( A \) to provide performance of a condition:

\[ F_{\Sigma} = 0. \]  
(18)

From the point of view of the biosystem \([6, 7]\) of an antibody strengthen activity of phagocytes on alien agents. The Fagotsitarny cage absorbs the alien agent.

In AIS option the problem of this stage consists in "dissolution" of different parameters values of characteristics which are possessed by the IS system of telecommunication network. Taking into account that at a recombination of a set of antigens \( H \) and antibodies of \( A \) becomes identical, and the structure of these sets is unique for each couple: "the threat – vulnerability" or "threat – an action for counteraction", is offered to realize the mechanism of "dissolution" of antigens in antibodies on the basis of a genetic algorithm \([12]\) which general principles doesn't demand special specifications in this task.

Initial population is formed on the basis of only one couple of chromosomes \([12]\)

\[ \{x^h_1(h, a); x^a_1(h, a)\}, \]  
(19)

where \( x^h, x^a \) – sets of already recombined characteristics of threat and vulnerability respectively.

If at a recombination the characteristic of action of threat or vulnerability (or actions for counteraction) was absent, then its value is accepted equal 1 for vulnerability and 0 for actions for counteraction. Thanks to it the quantity of elements at both participants will be equal in chromosomes.

The genetic algorithm allows transition from a phenotype to a genotype, that is replacement of real numerical values with a binary code and also can be realized at the level of a phenotype. This need is defined by the initial stage of formalization of threats and vulnerabilities. In case of distinction of scales normalization of values of chromosomes is required.
There are differences only in an algorithm stop condition. As this condition it is offered to use

\[ F_{\sum} \leq 0. \]  

(20)

At achievement of this condition the threat ceases to bear harmful character to telecommunication system or network.

As a result of application of a genetic algorithm it is possible to define values of characteristics of actions for counteraction or the vulnerability level which will dominate over parameters of threat [7]:

\[ A^{opt} = \{ x_s^H (h, \alpha) \}. \]  

(21)

Further actions for formalization need to execute the return process.

The set of the offered models forms IIS allowing to react to change of threat of IS to telecommunication system or network.

7. Conclusion

Application of AIS will lead to correction of the IS system and its actions for ensuring security of information or infrastructure of telecommunication system or network. It can be connected not always is connected with additional expenses for the enterprise owing to the fact that this system is adaptive to change of threats of IS.

Definition of the direction of improvement of system of information security and the analysis of dynamics of her existence can quite reveal expensive actions for providing IS which in the conditions of the current situation can be not realized and saved. Adaptability – an important indicator of the developed system of models in the form of AIS.

References

[1] Dushkin A V, Novoseltsev V I and Sumin V I 2016 Methodological bases of creation of the protected automated systems: monograph (Voronezh: Scientific book) p 76.

[2] Balan V P, Dushkin A V, Novoseltsev V I and Sumin V I 2016 Risk and reflection: monograph (Moscow: Hot line – Telecom) p 136

[3] Barkalov S A, Dushkin A V, Kolodyazhny V I and Sumin V I 2017 Introduction to system analysis: Monograph (Moscow: Hot line – Telecom) p 234

[4] Dushkin A V, Kravchenko A S, Novoseltsev V I, Smolentseva T E and Sumin V I 2014 Mathematical models and information processes of complex object control: Monograph (Voronezh: Scientific book) p 125

[5] Barkalov S A, Dushkin A V, Kolodyazhny S A and Sumin V I 2017 Introduction to the system design of intellectual knowledge bases: monograph (Moscow: Hot line – Telecom) p 108

[6] David G 1978 Method of steam rooms comparison The lane with English under the editorship of Yu. Adler (M.: Statistics) p 144

[7] Borisov A N, Alekseev A V and Merkuryev G V 1989 Processing of indistinct information in the systems of decision-making (M.: Radio and communication) p 304

[8] Galaktionov V G 2004 Immunology: Textbook (M.: Academia) p 528

[9] Roit A, Brostoff J and Mail D 2000 Immunology; the lane from english V I Kandror (M.: World) p 582

[10] Stepanov L V 2010 Modeling of market barriers on the basis of methodology of artificial immune systems Intellectual systems in production 2 pp 42-50

[11] Stepanov L V, Serbulov Yu S, Glukhov D A 2013 Modeling of market barriers on the basis of artificial immune system Logging journal 4(12) pp 223-231

[12] Stepanov L V 2008 Modeling of assessment of a condition of the perfect competition on the basis of a genetic algorithm Problems of the theory and practice of management 8 pp 111-118