APPLIED PROBLEMS OF MATHEMATICS AND MECHANICS

ALGULIYEV R.M.

ARCHITECTURAL BASES OF AUTHORIZED ACCESS SECURITY TO THE CORPORATIVE NETWORKS

Abstract

In the paper the formalized description of the authorized access process between the objects of corporative Network is given and the possibilities of its realization in the frame of conception of form of Adaptive system of information security are considered. The method of selection of the internetwork screen by many criterion for complexion of authorized access control subsystem is suggested.

1. Introduction.

It is known, that in the corporative networks (CN) constructed for the separative organizations, one of the complex problems realized by the adaptive system of information security (ASIS) in the security of the authorized access to the objects - network applications, data base, operation systems and etc., which realization is complexed much more because of disconcentration, non-equality of desires by defence, difference in nature of the objects and generally because of providing interaction with the objects of open computer network (OCN) as a potential source of appearance of different types of threat and non-authorized actions from the plotters [1]. Because of that ASIS need realize the complex of the problems on organization and access security to the objects as inside as by perimeter CN. With this purpose, first of all it is necessary to analyze requests of the politics of by access security to each of these objects and to determine possibilities of interaction (inter-access) between them and also with the objects OCC which are kept for some given time and during the functioning process of CN can be changed by ASIS.

Generally, authorized access to the objects of CN is based on two main principles: «everything banned is allowed» and «everything allowed is banned» which further we will name the allow principle and ban principle, correspondingly [2]. Note that the ban principle in comparison with allow principle stronger desires to access security. In dependence on the level of defence of CN and the components of its objects both these principles can be realized. Thus, if some group of objects of CN is allowed to interchange with some objects of OCN, for example, Internet, then the access on the bound of the two networks it is advisable to realize on the plotters which represent some danger for the network are known, then access for them is banned and the other objects of OCN are allowed to interchange with the known beforehand objects of CN, as for as realization of ban principle at access security to CN because of great deal of the objects of OCN is not possible. If security politics gives higher level of defence of the network and the list of the objects of OCN or some other network which are supposed for interaction with is determined clearly, then access will be provided on the base of ban principle.

The other block of the problems of organization, security and access control in the CN is connected with its inner structure and defence desires of each of its objects. It is known, that all objects of the computer network in sense of accessibility can be divided in two groups. In the first group those undefended objects enter where access

from other objects in the frame of the given network is allowed, but their interactions with the objects of OCN as it has been mentioned above are authorized by ASIS. And the second group is formed by those defended objects access to each of which is realized on the base of one of the abovedescribed principles by the desires to them on defence security. With this deal, CN by the geographical arrange of the objects in all Network is divided in the demilitarized segment (DMZ-segment) and the militarized segment (MZ-segment) for the undefeneable and defeneable objects, correspondingly. Let us note that in dependence on disconcentration of the functional structure CN can be formed several MZ-segments as it is shown in fig.1.

Taking into account the aboveexpressed, the problems of formalized description of access process and complexing ASIS by the corresponding stuffs of access security in CN are considered below.

2. Formalized description of authorized access process and the possibilities of its realization in the corporative Networks

Suppose that CN with purpose of access security as to the undefened as to the defined objects is divided in DMZ-segment B and MZ-segments A_k, $k=\overline{1,K}$. Moreover, we name segment C all OCN which the given network interacts with. Suppose, in each MZ-segment A_k there are great deal of the defined objects where access can be realized on the base of one of the aboveexpressed principles. According to that the set A_k is divided in two non-intersected subsets $A_k^z=\left\{a_{ik}^z\middle|_{ik}=\overline{1,I_k}\right\}$ and $A_k^r=\left\{a_{jk}^r\middle|_{jk}=\overline{1,J_k}\right\}$ to which elements access is realized by ban principle and allow principle, correspondingly. DMZ-segment B consists of be non-protected objects, $l=\overline{1,L}$, that is, $B=\left\{b_l\middle|l=\overline{1,L}\right\}$. Moreover, let us represent in the form of the set $C=\left\{c_m\middle|m=\overline{1,M}\right\}$ those objects c_m, $m=\overline{1,M}$ of OCN which as the defened as the non-protected objects interact with.

Now let as consider various variants of access organization between the objects of the sets C, B and A_k, $k=\overline{1,K}$. It is obvious, that access organization between the objects c_m, $m=\overline{1,M}$ doesn't enter the problem ASIS. Also there is not any necessity in access security between the objects b_l, $l=\overline{1,L}$, as all these objects interact in DMZ-segment. Thus, the main problems of ASIS on access security in CN are:

1) Organization of external access of the objects of set C to the objects of set B and subsets A_k^z, A_k^r, $k=\overline{1,K}$;

Let us note, that at organization of the access of objects C to the objects of set B it is necessary first operate by request to provide defence of objects b_l, $l=\overline{1,L}$, as for as, access to these objects from outside of the network can be organized on the base of one of two principles. By this reason, at organization of the access from OCN the set B is divided beforehand in the intersected subsets $B_r=\left\{b_l^r\middle|l=\overline{1,L'}\right\}$ and $B_z=\left\{b_l^z\middle|l=\overline{L'+1,L}\right\}$ where b_l^r *and* b_l^z are the objects where access from outside is realized by the allow principle and ban principle, correspondingly. Further, with purpose to realize control over the access processes in all CN in every current moment of time ASIS must have in its disposal the corresponding matrices of the access and the blocking

describing the relations between the objects of all abovementioned sets. For description of access process at moment of time t by the allow principle let us introduce the matrix of allow of access $V_t(C,B_r)=\|\vartheta_{ml}(t)\|$ *and* $V_t(C,A_k^r)=\|\vartheta_{mj_k}(t)\|$ which elements are described by the following way:

$$\vartheta_{ml}(t)=\begin{cases}1, \textit{ at any moment } t\in[t'_{ml},t''_{ml}] \textit{ object } c_m \textit{ is allowed}\\ \textit{access to object } b_l^r\ ;\\ 0, \textit{ in opposite case}\end{cases}$$

Here t'_{ml},t''_{ml} are the initial and final moments of time of the authorized access of object C_m to object b_l^r, where $m=\overline{1,M}$ *and* $l=\overline{1,L}$. Further,

$$\vartheta_{mj_k}(t)=\begin{cases}1, \textit{ at any moment } t\in[t'_{mj_k},t''_{mj_k}] \textit{ object } c_m \textit{ is}\\ \textit{allowed access to object } a_{jk}^r;\\ 0, \textit{ in opposite case},\end{cases}$$

where t'_{mj_k},t''_{mj_k} are the initial and final moments of time of authorized access of object c_m to object $a_{j_k}^r$, $m=\overline{1,M}$, $j_k=\overline{1,J_k}$ *and* $k=\overline{1,K}$.

As it has been abovementioned, access of some objects c_m to objects b_l^z *and* $a_{i_k}^z$ because of some reasons (struggle with «spams», blockage of the plotters and etc.) can be banned. So, we reduce the matrices of ban of access: $W_t(C,B_z)=\|w_{ml}(t)\|$ *and* $W_t(C,A_k^z)=\|w_{mi_k}(t)\|$, where $\exists m,\ m=\overline{1,M},\ l=\overline{L'+1,L}$, $i_k=\overline{1,I_k}$, $k=\overline{1,K}$. By analogy to above expressed description,

$$w_{ml}(t)=\begin{cases}1, \textit{ at any moment } t \textit{ of time for the period } [t'_{ml}t''_{ml}]\\ \textit{ access of object } c_m \textit{ to object } b_l^z \textit{ is banned};\\ 0, \textit{in the opposite case}.\end{cases}$$

$$w_{mi_k}(t)=\begin{cases}1, \textit{ at any moment } t \textit{ of time for the period}\\ [t'_{mi_k},t''_{mi_r}] \textit{ access of object } c_m \textit{ object } a_{i_k}^z \textit{ is banned}\ ;\\ 0, \textit{ in the opposite case}.\end{cases}$$

2) Organization of access of the objects of CN to the objects of OCN:
With this purpose let us consider the access of the objects of set B, subsets A_k^r *and* A_k^z, $k=\overline{1,K}$ to the objects of set C. Let us note that the access of the objects which are as in MZ-segments, as in DMZ-segment, to the objects of OCN in most cases is realized by the allow principle, though it is possible access by the ban principle. So we reduce only the matrices of allow of access $V_t^*(B,C)=\|\vartheta_{lm}^*(t)\|$, $V_t^*(A_k^r,C)=\|\vartheta_{j_km}^*(t)\|$ and $V_t^*(A_k^z,C)=\|\vartheta_{i_km}^*(t)\|$, $l=\overline{1,L}$, $m=\overline{1,M}$, $j_k=\overline{1,J_k}$, $i_k=\overline{1,I_k}$ *and* $k=\overline{1,K}$. Let us note that the introduced here and further denotations are interpreted as in point 1.
3) Organization of inner access of DMZ-segment to the objets of MZ-segments of CN:
By analogy, we introduce the matrix of allow of access $V_t(B,A_k^z)=\|\vartheta_{lj_k}(t)\|$ and the

matrix of ban of access $W_t\left(B, A_k^z\right) = \left\| w_{ii_k}(t) \right\|, \ k = \overline{1, K}$.

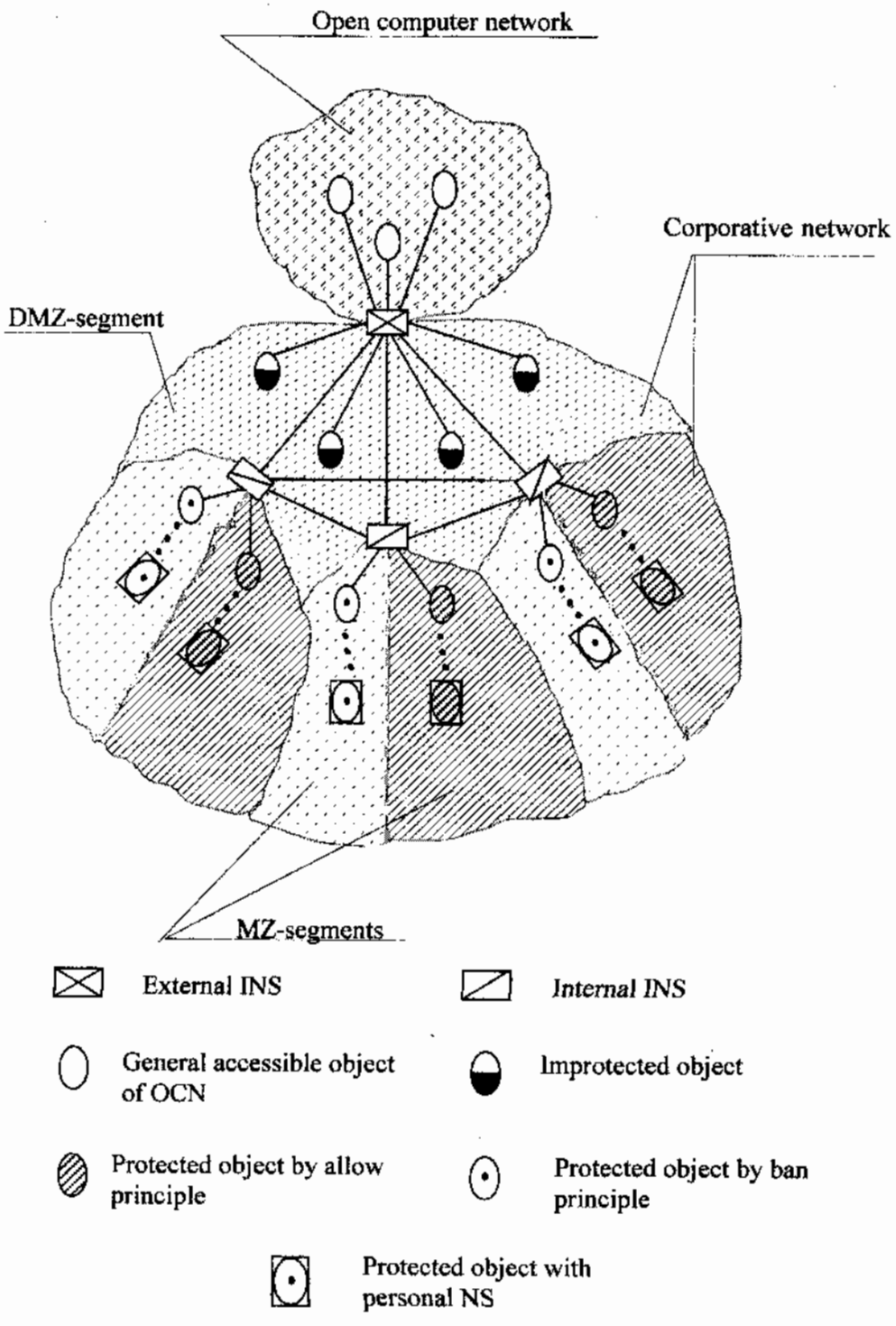

Fig.1. Conceptual scheme of access security to the object of CN

4) Organization of inner access of the objects of MZ-segments to the objects of DMZ-segment of CN.

It should to remark that in CN which are not segmented by MZ-zones there is no necessity to provide access of the protected objects to the non-protected objects. However, at segmenting of CN there is such necessity by the reason that the protected object arranging in MZ-segment on turning to some non-protected object of DMZ-segment in any case must be autenfitied by the allow principle. Then the autentification process is realized not in the non-protected object itself but on the bound of the corresponding MZ-segment with DMZ-segment. So it is necessary to introduce the matrices of allow of access $V_t^*\left(A_k^r, B\right) = \left\|\vartheta_{i_k l}^*(t)\right\|$ *and* $V_t^*\left(A_k^z, B\right) = \left\|\vartheta_{j_k l}^*(t)\right\|$, $k = \overline{1, K}$.

5) Organization of the inner access of the objects between them in the frame of one MZ-segment of CN.

As it has been above mentioned, the protected objects arranging in the frame of one MZ-segment by the principle of access security are grouped in subsets A_k^r and A_k^z. So, it is necessary to consider the problems of organization of access between the protected objects as in the subsets as between them. So, we introduce the matrices of allow of access $V_t\left(A_k^r, A_k^r\right) = \left\|\vartheta_{j_k j_k'}(t)\right\|$, $j_k \neq j_k'$ and $V_t\left(A_k^z, A_k^r\right) = \left\|\vartheta_{i_k j_k'}(t)\right\|$, the matrices of allow of access $W_t\left(A_k^r, A_k^z\right) = \left\|w_{j_k i_k}(t)\right\|$ and $W_t\left(A_k^z, A_k^z\right) = \left\|w_{j_k i_k'}(t)\right\|$, $i_k \neq i_k'$, $i_k, i_k' = \overline{1, I_k}$, $j_k, j_k' = \overline{1, J_k}$, $k = \overline{1, K}$.

6) Organization of the inner access between the objects of MZ-segments of CN.

With this purpose it is necessary to complete the following matrices of allow and ban of access, correspondingly:

$$V_t\left(A_k^z, A_{k'}^r\right) = \left\|\vartheta_{i_k j_{k'}}(t)\right\|, V_t\left(A_k^r, A_{k'}^r\right) = \left\|\vartheta_{j_k j_{k'}}(t)\right\|, V_t^*\left(A_{k'}^z, A_k^r\right) = \left\|\vartheta_{i_{k'} j_k}^*(t)\right\|$$

and

$$V_t^*\left(A_{k'}^r, A_k^r\right) = \left\|\vartheta_{j_{k'} j_k}^*(t)\right\|, \; k \neq k', \; k, k' = \overline{1, K};$$

$$W_t\left(A_k^z, A_{k'}^z\right) = \left\|w_{i_k i_{k'}}(t)\right\|, \; W_t^*\left(A_{k'}^z, A_k^z\right) = \left\|w_{i_{k'} i_k}^*(t)\right\| \quad \text{and} \quad W_t^*\left(A_{k''}^r, A_k^z\right) = \left\|w_{j_{k'} i_k}(t)\right\| \; k \neq k',$$

$k, k' = \overline{1, K}$.

It is not difficult to notice that in addition $V_t(\cdot)$ and $V_t^*(\cdot)$ of access allow by the matrices of access ban $W_t(\cdot)$ and $W_t^*(\cdot)$ the matrices $\Delta T_v(\cdot)$ and $\Delta T_v^*(\cdot)$ of access allow reglamentation, matrices $\Delta T_w(\cdot)$ and $\Delta T_w^*(\cdot)$ of access ban, correspondingly are formed. For example, to the matrices $V_t\left(C, B_r\right) = \left\|\vartheta_{ml}(t)\right\|$ and $w_t\left(B, A_k^z\right) = \left\|W_{lj_k}(t)\right\|$ by analogy the matrices $\Delta T_v\left(C, B_r\right) = \left\|\left[t_{ml}', t_{ml}''\right]\right\|$ and $\Delta T_w\left(B, A_k^z\right) = \left\|\left[t_{lj_k}', t_{lj_k}''\right]\right\|$. Here the element $\left[t_{ml}', t_{ml}''\right]$ of the matrix $\Delta T_v\left(C, B_r\right)$ means that the authorized access of the object c_m OCN to the object b_l of CN since the moment t_{ml}' to the moment t_{ml}'' of time is reglamentated $m = \overline{1, M}$, $l = \overline{1, L}$. And by matrix $\Delta T_w\left(B, A_k^z\right)$ the access of the object b_l to the object $a_{i_k}^z$ beginning since the moment t_{lj_k}' and finishing at the moment t_{lj_k}'' of time is banned, $l = \overline{1, L}$, $i_k = \overline{1, I_k}$, $k = \overline{1, K}$.

It should note that the above reduced matrices are not sufficient for access security to the object of CN as properly. Since the elements of these matrices characterize the space-time indicators of access between the objects and don't consider the characteristics and requests of the protected objects network technologies, the corresponding operation systems, politics of security and etc., which must be systematerized in the form of the ordered authentification rules for each pair of objects by the elements of the matrices $V_l(\cdot), V_l^*(\cdot), W_l(\cdot)$ *and* $W_l^*(\cdot)$, which are equal to unit. In connection with that analogously the matrices $P(\cdot), P^*(\cdot), Q(\cdot)$ and $Q^*(\cdot)$ of the authentification rules are introduced which elements are the access between the objects of sets C,B, and $A_k, k=\overline{1,k}$. For example, in the matrix $P\left(A_k^z, B\right) = \left\|P_{i_k l}\right\|$ the element $P_{i_k l}$ is the vector of the authentification rules $P_{\alpha_{i_k l}}, \alpha_{i_k l} = \overline{1, A_{i_k l}}$, which are necessary for providing allow of access of object $a_{i_k}^z$ to object b_l, that is:

$P_{i_k l} = P\left(P_{\alpha_{i_k l}} \middle| a_{i_k l} = \overline{1, A_{i_k l}}\right)$, $i_k = \overline{1, I_k}$, $k = \overline{1, K}$, $l = \overline{1, L}$. On the other hand, in the matrix $Q(C, B_2) = \|q_{ml}\|$ the element q_{ml} includes the ordered rules $q_{\beta_{ml}}$, $\beta_{ml} = \overline{1, B_{ml}}$, requesting for providing ban access of object c_m to object b_l, i.e., $q_{ml} = \left\langle q_{\beta_{ml}} \middle| \beta_{ml} = \overline{1, B_{ml}} \right\rangle, m = \overline{1, M}$, $l = \overline{L' + 1, L}$.

As we see, the access process in CN is represented in the form of the complex oriented graph which is described by the aboveexpressed matrices. Here the objects of CN and OCN correspond to the tops of the graph and the elements of that matrices to the arcs. Let us note in the given graph none of the tops has a loop, since the access of the object to itself has no sense from the point of view of information security. The characteristic property of the considered virtual graph is the fact that it has a dynamic changing structure since the continuity of existence of the arcs is determined by the difference of the final and initial moments of time of security (or ban) of the access between the corresponding objects as of CN as with the objects of OCN and the new, arcs appear in dependence on establishing ASIS of new relations between them.

Therefore, the abovepointed problems of ASIS on organization, security and access control in CN are realized by the separate subsystem which has hierarchical structure and functioning on the base of technology «client/server». Let us name the given functional structure authorized access control subsystem (AACS). AACS consists of the manager part and separate functional units of access security - network screens. (NC) established on the bound of OCN and CN (external internet work screen (INS)) between DMZ and MZ-segments (internal INS $S(k)$, $k = \overline{1, K}$), and also immediately near the protected objects by necessity (personal NS $S\left(a_{i_k}^z\right)$ and $S\left(a_{j_k}^r\right)$, $i_k = \overline{1, I_k}$, $j_k = \overline{1, J_k}$, $k = \overline{1, K}$), as it is shown in fig.1. The main functional unit of manager part of AACS is the centralized data based about authentification rules (CDBAR) which is realized on the base of the abovedescribed matrices of allow (or ban) of access, access reglamentation and authentification rules by all objects of CN. Let us note that CDBZR does not immediately realize access and authentification of graphic in the separate points and segments of the network. As it has already been noted these problems are realized in NS in which at access organization process the corresponding data based about authentification rules (DBAR) taking into account the direction of

transform of the graphic in the network. Let us note that all changes relating to AS process in CN are carried in by the unit of access system control in CD BAR. Being in current moment of time in the active condition centralized by CDBAR administrates all DBARs and by appearance of changes in the interrelations of the objects realizes the tuning of authentification rules in them. As it is seen, CDBAK and DBAR of the corresponding receive and transform units of NS form the distributed data base with hierarchic structure which interact through the communication unit with networks screen (CUNS) of manager part of AACS with help of the enchiphered channels of CN in the real scale of time. At the some time it is obvious that in NS different types of threat are fixed (substitution of addresses, non-authorized access try, entering of networks viruses and etc.), representing some danger to the requests of security of those or other objects of CN. In connection with that, in every NS the special data based about access rules break (DBARB) is supposed which accumulates all facts of non-authorized access through the given NS to the objects and other similar events. Further, with purpose of further analysis and generization of report for the corresponding subsystem of ASIS and also for effective realization of the problems on access security on all CN to the composition of the manager port of AACS the centralized data based about access rules break (CDBARB) is introduced which gathers the reports with a certain periodicity from DBARB of all NS through CUNS.

It is known, that in some cases CN in differ from the conceptual scheme given in fig.1., can have more than one foreign INS in their structure in accordance to the amount of the channels of connection which provide interaction with other networks. In such case, administrating of DBAR of foreign methods of routing of the packets or if in CN the method of adaptive routing is used then DBAR of all foreign INS for the given network will be doubled, since the ways of traffic are not known beforehand as out of the network as ouside of it. Contrary, when the method of the static routing by all content of DBAR of all foreign INS will differ from each other. It is obvious, that application of more than one foreign INS INCN increases risk of the non-authorized access and realization of some other types of threat. Though the given technical solution for the first sight let increase productivity and reliability of whole CN. However, in this case the expenses connected with gain of INS and then exploitation at functioning process of ASIS will increase. In differ from foreign INS internal INS and personal NS are used correspondingly as a rule for every MZ-segment of the protected object in one amount which DBAR do not intersect at all.

3. Method of choose of network screens for complexing the authorized access control subsystem.

At present time the market of the equipments for access security in CN is represented by many commercial accessible NS which differ as by architecture as by the set of the functions operated by them [2,3]. In addition analysis of the functional possibilities of NS, opinion of the leading specialists in this field and the results of testing International organizations which occupy with certification of such products show that the intellectual level and characteristics of these NS in some degree correspond to the conceptual requests of construction of AACS in the composition of ASIS. In connection with that the above expressed architectural principles of constructing of as AACS as NS at the result of realization of the complex of important problems by tuning and centralized administrating taking into account the technological properties and politics of security of the considered network can be realized on the base of some known program and apparatus program NS. One of the complex problems for complexing of

AACS is the choose of program or apparatus-program NS replying to the set of criterion. The set of criterion for estimation and choose of NS are formed by subjective reasonings of specialists on security and is connected immediately with the problems of AACS stated before it on security access and functional-technological properties of network construction control. Also some other important factors must be considered. Analysis of scientific-technical references devoted to isvestigation and syntez of NS and opinions of world-wide known «reaction commands», «commands of tigers» and some certification centers for similar products show that in most cases the estimation of the existing NS is realized by the following base criterion which have different degree of importance in dependence on the reasons and problems in CN by access security [2,3]:

- functional possibilities of NS according to standard model; centralized administrating; interoperability; references and recommendations of world-wide known certification centers; the network hardcopy logs and interfaces; cost; experience and reputation of the firm-producer in the market of equipments of access security; keeping VPN-technology; keeping stealth-technology and providing security; class of protection security; keeping functions of identification and audentification of the user; failure stability; tuning and adaptation; kept operation systems; keeping client/server technology; productivity; impossibility of passage to the unsafe condition.

Estimation and choosing NS problem is in that the existing NS are characterized by many numerical and in most of cases non-numerical indicators. By the way, criterion of estimation and selection of NS also have similar nature, at the result of that it is not possible to defermine their functional dependence on the indicators of NS in the analytical form with help of the classic and traditional methods. Relations between the criterion and the considered types of NS not precise and have subjective character [4]. Moreover, as it was above mentioned the selected criterion have different degrees of importance by series of reasons which definition is possible only basing on experiment, knowledge and instuition of the specialists in this subject field. As it is seen, the considered problem on estimation and selection of NS for complexing AACS can be solved by the methods of making solutions on the base of non-precise sets and expert estimations [5].

Suppose that at the result of analysis of the existing stuffs market of access security the set $E = \left\{ e_\delta \middle| \delta = \overline{1,\Delta} \right\}$ NS is determined and it is necessary to select one of them by the given criterion F_λ, $\lambda = \overline{1,\Lambda}$. Moreover, the given criterion F_λ have different coefficients σ_λ of relative importance, correspondingly. Let us note that coefficients σ_λ are not negative numbers, which sum is equal to number Λ and as the criterium is import ant as the value of σ_λ is more. It should be noted that the coefficients σ_λ, $\lambda = \overline{1,\Lambda}$ can be determined with help of one of the methods of expert estimations. At present time the scientific based classification of the methods of expert estimations and more that recommendations on their use don't exist. With this purpose for determination of the values of the coefficients of relative importance we use the pair comparison on the base of the scale of importance estimation of the criterion F_λ *and* $F_{\lambda'}$, $\lambda \neq \lambda'$, $\lambda, \lambda' = \overline{1,\Lambda}$ given in Table 1.

Relative importance of criterion F_λ and $F_{\lambda'}$	Elements of matrix $d_{\lambda\lambda'}$
equal importance	1
a few more important	3
more important	5
noticeable more important	7
much more important	9
interval values	2,4,6,8

With help of this scale let us complete matrix $D = \|d_{\lambda\lambda'}\|$ of pair comparisons which elements satisfy the following conditions $d_{\lambda\lambda'} = 1$ *for* $\lambda = \lambda'$ and coordination providing let us take that $d_{\lambda\lambda'} = 1/d_{\lambda'\lambda}$, λ, $\lambda' = \overline{1,\Lambda}$. Now it is necessary to find the eigen vector $\Psi = \left\langle \psi_\lambda \middle| \lambda = \overline{1,\Lambda} \right\rangle$ of matrix D for which the condition $D\Psi = \tau\Psi$ is fulfilled, where τ is the eigen value of matrix D. Let us turn to the solution of the problem on finding the eigen values $(D - \tau I) = 0$, where I is the unique diagonal matrix. This non-homogenous system has non-trivial solution then and only then when the determinant of matrix $(D - \tau I)$ is equal to zero, i.e. $\det(D - \tau I) = 0$. Hence we determine the eigen values τ_λ of matrix D and select among them $\tau_{\max} = \max_\lambda \left\{ \tau_\lambda \middle| \lambda = \overline{1,\Lambda} \right\}$. Here the cast of $\tau_{\max}$ from Λ can serve a measure of agreement of reasonings of the specialists-experts by estimation of the relative importance of criterion $F_\lambda, \lambda = \overline{1,\Lambda}$ by Table 1. Matrix D where the inverse values of $d_{\lambda'\lambda} = 1/d\lambda\lambda'$ are used reflect the agreed reasonings of the experts then and only then when $\tau_{\max} = \Lambda$. Moreover, always $\tau_{\max} \geq \Lambda$, so the difference $(\tau_{\max} - \Lambda)$ gives the measure of disagreement and points when the reasonings of the experts should be checked. Further, by the system of the linear equations with respect to variables $\Psi_\lambda, \lambda = \overline{1,\Lambda}$ obtained by formula $D\Psi = \tau_{\max}\Psi$ the eigen vector Ψ of matrix D is determined for maximal eigen value $\tau_{\max}$, i.e.:

$$\sum_{\lambda'=1}^{\Lambda} \left[d_{\lambda\lambda'} - \tau_{\max} sign(\lambda - \lambda') \right] \Psi_{\lambda'} = 0, \quad \lambda = \overline{1,\Lambda},$$

where sign $(\lambda - \lambda')$ is signium function which is equal to unit if $\lambda = \lambda'$ and is equal to zero if $\lambda \neq \lambda'$. It is known that the given system of equations has only zero solution. For finding eigen vector Ψ the substitution of one of the equations of the system by the condition of normalizing $\sum_{\lambda'=1}^{\Lambda} \psi_{\lambda'} = 1$ is realized. As the result of solution of the newformed system the values of variables $\psi_\lambda, \lambda = \overline{1,\Lambda}$ are determined. Let us note that on putting the condition of normalizing by turn instead of one of the equations of the system the result of the solution doesn't change. After that the sought values of coefficients σ_λ are determined correspondingly by the formula:

$$\sigma_\lambda = \Lambda\psi_\lambda, \lambda = \overline{1,\Lambda}.$$

Now let us realize many criterion estimation and selection of NS on the base of non-precise sets. In connection with that let us represent the criterium as a fuzzy set described by the following way:

$$F_\lambda = \left\{ \mu_{F_\lambda}(e_\delta) / e_\delta \middle| \delta = \overline{1,\Lambda} \right\}, \ \lambda = \overline{1,\Lambda}, \tag{1}$$

where $\mu_{F_\lambda}(e_\delta)$ is estimation of NS of e_δ type by criterium F_λ which characterizes the degree of correspondence (membership function) of the given type of NS to the concept defined by criterium F_λ. Values $\mu_{F_\lambda}(e_\delta)$ can be determined too analogously to the procedure of determination of coefficients σ_λ of the relative importance with help of the method of expert estimations on the base of the results of pair comparisons of all types NS by criterium F_λ included in set E. In connection with that criterion F_λ have relative importance σ_λ the fuzzy sets represented by formula (1) will be modificated for the following form:

$$F_\lambda^{\sigma_\lambda} = \left\{ \mu_{F_\lambda}^{\sigma_\lambda}(e_\delta) / e_\delta \middle| \delta = \overline{1,\Lambda} \right\}, \ \lambda = \overline{1,\Lambda}. \tag{2}$$

According to the theory of fuzzy sets if there are Λ criterion: F_λ, $\lambda = \overline{1,\Lambda}$ then the is considered the type of NS from set E which satisfies criterium F_1 *and* F_2 and ... and F_Λ. Then the rule for selection of the best type of NS can be written in the form of intersection of the corresponding modificated fuzzy sets reduced by formula (2), i.e.

$$F = \bigcap_{\lambda=1}^{\Lambda} F_\lambda^{\sigma_\lambda}.$$

It is known that to the operations of intersection of fuzzy sets the operation **min** fulfilled at their membership functions:

$$\mu_F(e_\delta) = \overline{\min_{\lambda=1,\Lambda}} \mu_{F_\lambda}^{\sigma_\lambda}(e_\delta), \ \delta = \overline{1,\Delta}$$

As the NS of type e_{δ^*} is selected which has maximal value of membership function among $\mu_F(e_\delta)$, $\delta = \overline{1,\Delta}$, i.e.:

$$\mu_F(e_{\delta^*}) = \max_{\delta=1,\Delta} \mu_F(e_\delta)$$

Therefore, with help of the given method the manycriterion estimation and selection NS on the base of fuzzy sets are realized and realization of selection does not represent any difficulty for calculations on modern personal computers.

By the above expressed it is possible to realize selection of NS for external INS S, internal INS S(K), personal NS $S(a_{i_k}^z)$ and $S(a_{i_k}^r)$ for 30 $a_{i_k}^z$ *and* $a_{j_k}^r$ on the base of own criterion of estimation and the coefficients of their relative importance, $i_k = \overline{1,I_k}$, $j_k = \overline{1,J_k}$, $k = \overline{1,K}$. As it is seen from fig. 1., in difference from personal NS, external and internal INS are supposed in those functional blocks of CN where in addition to the realization of the functions of packets routing is requested. So, for realization of external and internal INS it is necessary to select the apparatus-program NS and for personal NS it is necessary to select the program NS.

4. Conclusion.

As it is seen, formalization of the relations between the objects gives the complecte representation about the authorized access process at every moment of time on all CN without whose help it is not possible to realize tuning and the cenralized administrating of NS as at entering the exploitation as their functioning in the composition of AACS of ASIS. Further, the suggested method of selection of NS by

many criterion have been realized on personal computer and the effective results have been obtained.

References

[1]. Алгулиев Р.М. *Модели синтеза распределенной системы аутентификации виртуальной частной сети с перестраиваемой структурой.//* Известия РАН. Сер. Теория и системы управления, Москва, №2, 2000, сс. 138-147.
[2]. К.Пьянзин. *Классификация межсетевых экранов.* //LAN// Журнал сетевых решений, сентябрь, 1999, сс.81-92.
[3]. С.Нестеров. *Межсетевые экраны: надежная защита стоит дорого.//* Мир Internet, №9, 1999, сс. 82-89.
[4]. Орлов А.И. *Статистика объектов нечисловой природы и экспертные оценки.* В сб. «Экспертные оценки. Вопросы кибернетики, вып. 58». М.: Научный Совет АН СССР по комплексной проблеме «Кибернетика», 1979, сс. 17-33.
[5]. Борисов А.Н., Крумберг О.А., Федоров И.П. *Принятие решений на основе нечетких моделей:* Примеры использования. - Рига: Зинатне, 1990-184 с.

Alguliev R.M.
Information-Telecommunication Scientific Center of AS Azerbaijan.
9, F.Agayev str., 370141, Baku, Azerbaijan.

Received March 27, 2000; Revised June 7, 2000.
Translated by Soltanova S.M.