ROLE MODEL WITH ZONE DIFFERENTIATION OF ACCESS

Irgashevadurdona Yakubdjanovna[1]

[1]*Senior Lecture, "Information Security" Department, Tashkent University of Information Technology, Tashkent, Uzbekistan*

Abstract

The present article is devoted to development of a role model with zone differentiation of access. For safety of control and management of access, in this work, it is offered to use the approach based on concepts of «information resource» and «the functional module». By means of functional modules and the set of the universal operations called by the interface realized in them, access to information resources is provided. The interface of access to information resources determines a set universal for this type of resources of operations of access to the information maintenance of a resource, and also operations of its creation, destruction and management of properties, including by attributes of safety. All operations are unambiguously displayed on the relations of access regulated by models of safety of a computer network. Also are described, model of administration of access rights of roles. The choice of this type of a role model is caused by its proximity to real organizational and administrative and organizational and technological schemes at the enterprises and the organizations. In work it is offered functionally - a role model of differentiation of access with the zone policy, allowing to establish the relations of bilateral trust. The mechanism of realization of the developed role model with zone differentiation of access is offered.

Keywords: *Synthesis, Computer Network, Metrics of Security, Structural Protection, Database Management System, Role Model of Access Control.*

----------***----------

1. INTRODUCTION

The majority of the corporate computer network (CN), intended for management of the large enterprises, the multiuser hardware-software systems constructed on the basis of the client server technology represent. The server is the database management system (DBMS) realizing mechanisms of storage, processing and information safety. Client parts are established on personal computers of users program modules necessary mechanisms of display providing to users on functional duties and information processing [1].

2. CONCEPTUAL MODEL OF ROLE DIFFERENTIATION OF ACCESS.

For realization of control and management of access it is offered to use the approach based on concepts of «information resource» and «the functional module» [2]. Information resource in this case is understood as any abstract essence possessing the unique identifier, capable to participate in the access relations as a source or information receiver access to which is provided by means of the fixed set of the operations which are working with the maintenance of only one resource and carrying out information transfer only in one direction - or from the consumer to a resource, or from a resource to the consumer. Information resource in a corporate computer network is set of the data characterizing a certain essence of environment and representable in DBMS in the form of a set of records of one or several tables of a relational database as, in relational model, the database represents the centralized storage of tables providing safe simultaneous access to information from many users. Information resources concerning which the security policy works, are called to objects.

The functional module is a set of the subjects united proceeding from scope of carried-out actions and providing some set of universal operations over data. The subject is understood as the active essence, capable to change a condition of system. Among subjects access to which is provided by means of functional modules, procedures of transformation and analytical procedures [2] are allocated.

Procedure of transformation (transformation procedure) is defined as any nonzero sequence of the elementary actions which performance leads to change of data [2]. Elementary action is defined as state transition which can cause change of some elements of data. For example, subjects can eliminate elements of data, change information in elements of data, copy them, etc.

In a corporate computer network procedure of formation and granting to the called user of a subset of information objects of a corporate computer network necessary for it, including with their possible quantitative and structural modification proceeding from problems of differentiation of access to information is called as «submission» of information, or analytical procedure (analytic procedure). During performance of analytical procedure of change of information resources doesn't occur. Analytical procedures are an integral part of functional modules. Analytical procedures can be realized in a look of «stored procedures», «functions of the user» or DBMS «representations».

It should be noted that there is strictly certain relation of procedures of transformation and functional modules. Procedure of transformation can belong to only one functional module, analytical procedure can belong to several functional modules at the same time. Such fixing of procedures of transformation is connected with that addition, in change and transformation of data the users who are carrying out the functional duties within strictly certain activity of the organization to which unambiguously there corresponds a certain functional module are engaged. Analytical procedures are used generally by the administrative and managerial personnel for which information on various activities of the organization [2] is necessary for decision-making.

Besides, a part of the majority of modern information systems are so-called information and analytical or the information retrieval systems intended for implementation of centralized access to information resources of a corporate computer network. Such systems represent a set of the analytical procedures of the computer network (CN) grouped in various signs concentrated within one functional module, and providing access on reading to all information resources of the corporate CN, necessary users. Thus, users get access to information objects of system by means of the interface [2] realized in functional modules. The generalized structure of functioning of CN is presented in figure 1.

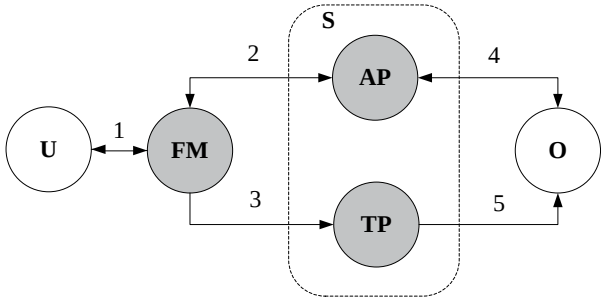

Fig. 1. The generalized structure of functioning of computer networks

U - users; FM - functional modules; AP - analytical procedures; TP - transformation procedures; O - objects.
The structure of functioning of the corporate CN, based on concepts of information resources and functional modules, defines the generalized scheme of functioning of means of protection of corporate CN. Means of authentication provide access to system only the authorized users. The process carrying out from a user name and possessing its powers, provides access to resources of corporate CN under obligatory control of means of identification which define corresponding to it subject of access. All appeals to information resources are carried out under control of control facilities by the access providing implementation of rules of security policies at access to those information resources which are objects. All operations of access to resources (both successful, and unsuccessful) are entered in the audit protocol. Control devices of integrity provide integrity of means of protection and restoration of integrity of information resources [3].

During the carried-out analysis of models of computer systems it is shown that, creation of safety of the information security system (ISS) of corporate CN requires application of models of management by access with ensuring correct division of areas of the objects intended for the organization of groups of users on powers, and also functional duties within a role model of differentiation of access [4].

The role model realizing a role security policy, represents significantly advanced model Harrison-Ruzzo-Ullman. However it can't be carried neither to discretionary, nor to mandatory because control of access in it is exercised both on the basis of a matrix of access rights for roles, and by means of the rules regulating purpose of roles to users and their activation during sessions.

In a role model the classical concept «subject» is replaced with the concepts «user» and «role». The user is the person who is working with system and carrying out certain official duties. The role is abstract essence actively operating in system with which limited, logically connected set of the powers necessary for implementation of a certain activity is connected. Such approach is close to real life where users act not from the personal name, and fulfill certain official duties. Therefore it is quite logical to exercise control of access and to appoint powers not to real users, and the abstract (not personified) roles representing participants of a certain processing of information [5].

When using role policy, control of access is exercised in two stages: at first for each role the set of powers representing a set of access rights to objects is specified, and then to each user the list of roles available to it is appointed.

The role model describes system in the form of the following sets: U - users; R - set of roles; P - set of powers on access to the objects, presented, for example, in the form of a matrix of access rights; S - set of sessions of users with system [2].

For the listed sets the following relations are defined:

$PA \subseteq P \times R$ - displays a set of powers on a set of roles, establishing for each role a set of the powers appropriated to it;

$UA \subseteq U \times R$ - displays a great number of users on a set of roles, defining for each user a set of roles available to it.

Rules of management of access of a role security policy are defined by the following functions:

for each session S this function determines by $user: S \rightarrow U$- the user who carries out this session with system;

$roles: S \rightarrow P(R)$ - for each session of s this function defines a set of roles from a set of R which can be at the same time available to the user in this session;

permissions: S→P - for each session of s this function sets a set of available powers in it which is defined as set of powers of all roles involved in this session.

As criterion of safety of a role model the following rule is used: the system is considered safe if any user of system working in a session of S, can carry out the actions demanding power p only if *p∈permissions(s)*. It means that control of access is exercised mainly not by means of purpose of powers to roles, and by a task of the relation of UA and the roles function.

The role security policy is an integral part of modern control systems of access to CN with difficult organizational and regular structure, a large number of the users carrying out certain functions within the official duties and allocated in this regard with various rights and powers [2].

Application of a role model of differentiation of the access, which structure it is provided on figure2 allows to simplify significantly design and administration of systems of differentiation of access of CN realizing difficult, uncommon organizational and technological and organizational and administrative schemes and processes. Therefore the role policy can be used as the mechanism of management by roles and powers of the users, allowing to ensure effective safety of system [2]

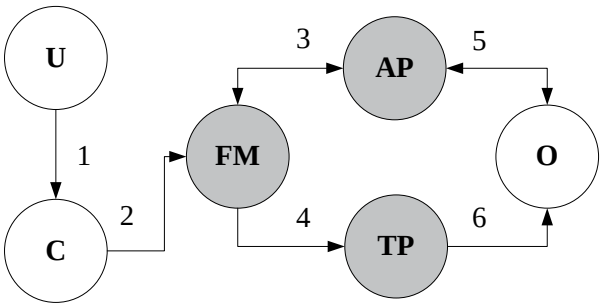

Fig. 2. Structure of a role model of differentiation of access In this structure With - is defined by roles and powers of users.

3. MODEL OF ADMINISTRATION OF ACCESS RIGHTS OF ROLES.

In a functional role model of differentiation management of users and their roles is controlled by access within a role model. And the model based on the hierarchical organization of system of roles is chosen from all kinds of this model. The hierarchical organization of roles reflects the relation of subordination established in the real world between participants of processing of information and division of spheres of responsibility between them. Roles in hierarchy are ordered on level of conferred powers. The above the role is in hierarchy, the more with it is connected powers as it is considered that if some role is appropriated to the user, to him all subordinates to it on hierarchy of a role [3] are automatically appointed also. The hierarchy of roles allows multiple inheritance. The hierarchical role model differs from classical the following relations:

$RH \subseteq R \times R$ - the partial relation of an order on a set of R which defines hierarchy of roles and are set on a set of roles by the operator of domination ≥, such that if $r_1 \geq r_2$, r_1 is in hierarchy above than r_2;

$UA^h \subseteq U \times R$- appoints to each user a set of roles, and together with each role it joins also all roles subordinated by it on hierarchies, i.e. for $\forall r, r' \in R, u \in U: r \geq r' \wedge (u, r) \in UA^h \Longrightarrow (u, r') \in UA^h$.

$roles^h: S \rightarrow P(R)$ - appoints to each session of s a set of roles from hierarchy of roles of the user working in this session:

$$roles^h(s) \subseteq \{r_i \mid (\exists\, r' \geq r_i (users(s), r') \in UA^h)\};$$

$permissions^h: S \rightarrow P$ - defines set of the powers available on all roles, the involved user in this session, taking into account hierarchically subordinated roles:

$$\text{permissions}^h(s) = U_{r \in \text{roles}^h(s)} \{p_i \mid (\exists\, r'' \leq r(p_i, r) \in PA)\}.$$

Powers of users are defined by the right of activationof functional modules. That is the $permissions^h$ defines a set of the functional modules which right of start the user in this session [3] possesses.

As criterion of safety of a role model the following rule is used: the system is considered safe if any user of system working in a session of s, can carry out the actions demanding power p only if by $p \in permissions(s)$.

CN is represented set of the following sets of matter:

- set of objects of $O(o_1, o_2, \ldots, o_N)$;
- great number of subjects of $S(s_1, s_2, \ldots, s_J)$;
- set of procedures of the $TP(tp_1, tp_2, \ldots, tp_B)$, TP ⊆ S;;
- set of the analytical $AP(ap, ap_2, \ldots, ap_H)$, $AP \subseteq S$and $S = TP \cup AP, TP \cap AP = 0$;
- great number of users of $U(u_1, u_2, \ldots, u_K)$;
- set of roles of users of $C(c_1, c_2, \ldots, c_W)$;
- set of access rights and R privileges $(R(r_1, r_2, \ldots, r_Q)$;
- set of thematic categories of subject domain of $T(\tau_1, \tau_2, \ldots, \tau_M)$;;
- set of divisions $D(d_1, d_2, \ldots, d_Z)$;
- set of the functional FM models $FM(fm_1, fm_2, \ldots, fm_X)$, and $(fm_1 \subseteq S, \text{для } \forall i \in (1 \div X))$.

The relations between matter systems are installed by the following displays (fig. 3.):

$F_1: O \times T(D)$- display of a set of objects to a set of thematic categories of subject domain (the set of thematic categories reflects organizational structure of D);

$F_2: S \times T$ - display of a great number of subjects (analytical procedures) to a set of thematic categories of subject domain (the set of thematic categories reflects structure of information resources);
$F_3: S \times FM$-display of a great number of subjects to a set of functional modules;

$F_4: U \times C$ - display of a great number of users to a set of roles;

$F_5: C \times FM$- display of a set of roles to a set of functional modules;

$F_6 C \times T \cup D$- display of a set of roles to a set of thematic categories of subject domain, and a set of thematic categories can reflect both organizational structure, and structure of information resources.

Functioning of system is based on introduction and use of the following functions:

$f_c: U \to C$- value of the function $f_c(u) = \underline{C}$ is a set of roles $\underline{C} = \{c_{u1}, c_{u2}, \dots\} \subseteq C$ in which the user and is included on display F_4.

$f_m: C \to FM$ - value of the function $f_m(c) = \underline{FM}$is a set of functional modules$\underline{FM} = \{fm_{g1}, fm_{g2}, \dots\} \subseteq FM$, to which the role of c is related on the F_5. display.

$f_k C \to T \cup D$- value of function $f_k(c) = \underline{T}$ is a set of subjects of subject domain of $\underline{T} = \{\tau_{e1}, \tau_{e2}, \dots\} \subseteq T$ to which the role of c is related on the F_6display;

$f_s: FM \to S$ - value of the function $f_s(fm) = \underline{S}$, is a great number of subjects, $\underline{S} = \{s_{fm1}, s_{fm2}, \dots\} \subseteq S$included in the functional *fm* module on the F_3 display;

$f_{ap}: T \to AP$- value of the function $f_t(\tau) = \underline{AP}$ is a great number of subjects (analytical procedures) $\underline{AP} = \{ap_{\tau1}, ap_{\tau2}, \dots\} \subseteq AP$ relating to subject τ on the F_2display;
$f_o: T(D) \to O$- value of the function ($f_o(\tau) = \underline{O} f_o(\tau) = \underline{O}$ is a set of information objects of $\underline{O} = \{o_{\tau1}, o_{\tau2}, \dots\} \subseteq T$ relating to subject τ on the F_1display.

In this structure of T - the subject of subject domain, can be used for the organization of safe access to information resources of system by means of analytical procedures [7].

The step-by-step algorithm of functioning of model of differentiation of access looks as follows [3]. After authorization of the user in system the set of role which include the account of this user directly or due to hierarchy of roles ($f_c$function) is formed.

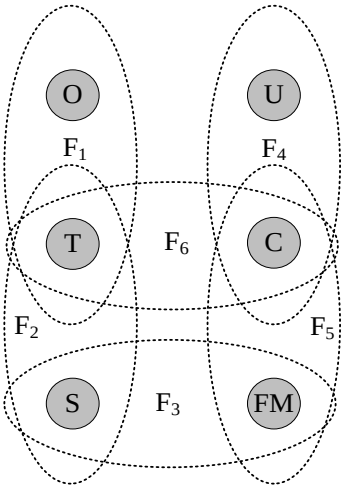

Fig. 3. The relations between sets of model matter.

On the basis of this set the set of identifiers of those divisions which the user and a set of the thematic categories available to the user in structure of information resources ($f_k$function) treats is defined and associates with the account of the user. Further the set of functional modules available to the user ($f_m$function) is formed. The user makes active the functional module demanded to it. In the course of initialization of the module the set of procedures of transformation available to the user and analytical procedures ($f_s$and f_{ap}function) is formed. Basic data thus are the set of the procedures realized in the functional module and structure of information resources [3].

From the formulation of criterion of safety of a role model follows that control of access is exercised mainly not by means of purpose of powers to roles, and by a task of the relation of UA^h, appointing roles to users, and the *roles* function defining a set available in a session of roles.

Besides, in connection with features of a functional role model, the hierarchical role model is used in system for management of users, roles and powers of roles.

From the above it is visible that one of shortcomings of a role model is lack of limited completeness of functions of the user. Therefore there is a need of restriction of a scope of the powers given out to the user and, as a result, simplifications of the scheme of access to objects.

For this purpose in work it is offered functionally - a role model of differentiation of access with the zone policy, allowing to establish the relations of bilateral trust.

Role model with zone differentiation of access and the mechanism of its realization. In an offered role model with zone differentiation of access the role «owner»R_{own} appointed to users in a context of those objects of O_{ijk} which they own [6] is entered. This role on the behavior slightly differs from usual roles. First, only one user can play a role «owner» in a context of any certain object. Secondly, object «owner» from the parent if in his own context such role to someone is appointed shouldn't inherit a role. Thus, in

relation to object of O_{ijk} only one user of $R_{own}(O_{ijk})$ can carry out the given role. If, in an object context the role «owner» of R_own isn't appointed, the owner is considered parental object:

$$O_{ijk} \in (O_{ijk}) else\ O_{ijk} \in R_{own}(O_{ij}) else\ O_{ijk} \in R_{own}(O_i)$$

For restriction of completeness of functions of users it is offered to enter the concept «access class»of f_{OFR}. The class of access contains a set of the rules which are setting the rights of performance of certain operations for certain roles. The class of access is the display connecting the rights of performance of certain functions with certain roles [6].

Performance of function by the user is authorized if this function is defined and as the user of f_{FR}, and in a class of access of object of f_{OFR} in relation to which the f_{FR} function is carried out conditions:

$f_{FR}: F \times R;$
$F_{OFR}: F(O_i) \times R;$
$F_S \Leftrightarrow f_{FR} = f_{OFR}.$

To each object of system exactly one class of access is put in compliance, and any class of access can be appointed to any amount of objects. It allows to have some different schemes of access to objects in system, without forcing us to connect these schemes with types or any other signs of objects. And purposes of classes aren't connected in any way with hierarchy of objects: the affiliated object can have any class of access irrespective of the fact which the class is appointed to parental object [6].

According to uniform hierarchy of objects it is offered to enter inheritance of rules of access from higher objects. The similar mechanism often meets in file systems (discretionary model): the files lying in the folder, cannot have own rules of access, and inherit these rules from the folder. At transfer of these files in other folder, the rights of the user for access to these files can exchange.

At application of a role model with zone differentiation of access it is necessary to enter sets of physical objects of system of $V(v_1, v_2, \dots, v_l)$ - computing installations (workstations, servers), printers, the communication equipment, etc. and also a set of zones of system $Z(z_1, z_2, \dots, z_k)$.

Thus in a computer network set of a subset of users, subsets of objects of access and a subset of the physical objects isolated in a local segment with a separate (intra zone) security policy is called as a zone.

Thus in a computer network set of a subset of users, subsets of objects of access and a subset of the physical objects isolated in a local segment with a separate (intra zone) security policy is called as a zone.

The intra zone security policy is realized by intra zone monitoring of safety which provides all set of functions of safety (authentication and generation of primary subjects of access of users of a zone, differentiation and management of access, audit of processes) [6]. Intra zone monitoring of safety (fig. 4.) is the system subject who realizes concerning objects of a zone $z \epsilon Z P_L(z)$, resolved set accesses which in a general view is association of intra zone accesses (S_{zk} relation - the subject being in *k*-that zone, O_{zk} - object being in k-that zone), regulated by rules (criteria) of intra zone policy of users of a zone to objects of other zones, users by rules (to criteria,

$$P_L(z) = P_L^{in}(z) \cup P_L^{out}(z), \quad (1)$$

where $P_L^{in}(z)$ - a set of safe intra zone accesses;

$P_L^{out}(z) = P_L^{out}(z\rightarrow) \cup P_L^{out}(z \leftarrow)$- a set of safe remote accesses for a zone $z \epsilon Z$ which is association of a set of remote accesses of users of a zone *z* with objects of the zone z $P_L^{out}(z \leftarrow)$.

The zone structure of system is defined by displays of sets of the matter, expressed following functions:

$f_{phys}: V \rightarrow Z$ – value of the $z = f_{phys}(v)$ function is the zone $z \epsilon Z$ in which there is a physical object of $v \in V$;

$f_{user}: U \rightarrow Z$ – value of the $z = f_{user}(u)$ function is the zone $z \in Z$ in which it is authorized for work of users of $u \in U$;

$f_{fobject}: O \rightarrow V$– value of the $v = f_{fobject}(o)$ function is physical object of $u \in U$ in which there is an object of $o \in O$.

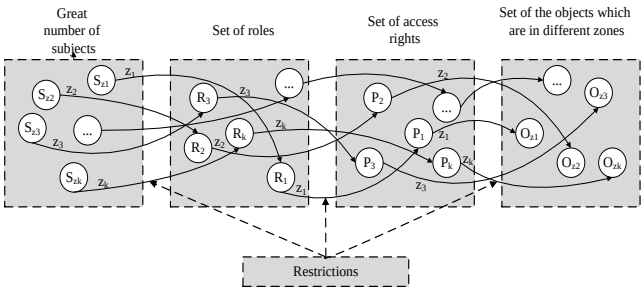

Fig. 1.5. Model of intra zone monitoring of safety

It should be noted that set of the $v_{fobject}(o)$ and $z = f_{phys}(v)$ functions realizes the $z = f_{iobject}(o)$ function defining accessory of object of access of $o \in O$ to the certain zone z∈Z that it is possible to treat as «a zonal – coloring » all objects of access zonal - the distributed system [6].

On a set of zones of system Z the partial mild order installing system of the interzonal confidential relations is defined: $f_{zz}: Z \times Z$- the relation defining a priority of trust of one safety zones in relation to another and setting the operator of domination «≤», such that:

1. If for $S_{zk}, O_{zk}, \in Z$ and $S_{zk}" = "O_{zk}$, between the zone S_{zk} and the zone O_{zk} are established the relations of

bilateral trust, i.e. the zones S_{zk}, O_{zk} trust each other, in other words, remote accesses of users of the zone S_{zk} to objects of the zone O_{zk}, and vice versa, users of the zone O_{zk} to objects of the zone S_{zk} -are essentially possible

$$P_L^{out}(S_{zk} \longrightarrow O_{zk}) \neq \emptyset \wedge P_L^{out}(S_{zk} \leftarrow O_{zk}) \neq \emptyset \quad (2)$$

2. If for $S_{zk}, O_{zk}, \in Z \text{and} S_{zk} > O_{zk}$ between the zone S_{zk} and the zone O_{zk} are established the relations of unilateral trust, the zone O_{zk} trusts the zone S_{zk}, but the zone S_{zk} doesn't trust the zone O_{zk}, in other words, remote accesses of users of the zone S_{zk} to objects of the zone O_{zk} are essentially possible, but remote accesses of users of the zone O_{zk} to objects of the zone S_{zk} are essentially impossible –

$$P_L^{out}(S_{zk} \longrightarrow O_{zk}) \neq \emptyset \wedge P_L^{out}(S_{zk} \leftarrow O_{zk}) = \emptyset \quad (3)$$

3. If for $S_{zk}, O_{zk}, \in Z \text{and} S_{zk}$ " $\neq$ " O_{zk},, the trust relations between the zones S_{zk}, O_{zk} aren't established, i.e. the zones S_{zk}, O_{zk} don't trust each other, in other words, remote accesses of users of the zone S_{zk} to objects of the zone O_{zk} and remote accesses of users of the zone O_{zk} to objects of the zone S_{zk} are essentially impossible –

$$P_L^{out}(S_{zk} \longrightarrow O_{zk}) \neq \emptyset \wedge P_L^{out}(S_{zk} \leftarrow O_{zk}) = \emptyset \quad (4)$$

We will note that the relation of a partial mild order on a set of Z adequately reproduces the confidential relations as possesses properties of a reflectivity, anti-symmetry and transitivity:

$\forall z \in Z : z \leq z;$
$\forall z_1, z_2 \in Z: (z_1 \leq z_2 \wedge z_2 \leq z_1) \Longrightarrow z_1$ " = "$z_2;$
$\forall z_1, z_2, z_3 \in Z: (z_1 \leq z_2 \wedge z_2 \leq z_3) \Longrightarrow z_1 \leq z_3;$

CONCLUSIONS

In the offered role model with zone differentiation of access any zone trusts to itself, i.e. intra zone accesses aren't forbidden (reflectivity). If one zone trusts another (remote accesses of users of the first zone to objects in the second zone are possible) and, at the same time, other zone trusts the first (remote accesses of users of the second zone to objects of the first zone are possible), it means existence of the relations of bilateral trust (anti-symmetry). And, at last, if one zone trusts another, and another trusts the third, it doesn't make sense to forbid remote accesses of users of the first zone to objects of the third zone as on a chain of remote accesses information can be transferred from the third zone to first (transitivity).

ACKNOWLEDGEMENT

The authors can acknowledge any person/authorities in this section. This is not mandatory.

REFERENCES

[1]. Sandhu Ravi S., Coyne Edward J, Feinstein Hal L. Youman Charles E. Role-Based Access Control Models // IEEE Computer, Volume 29, Number 2, February 1996. - p.38-47.

[2]. Ganiev S.K., Irgasheva D.Y., Abramov A.S. The conceptual model of role-based access control for computer networks //International Conference on IT Promotion in Asia 2011 / Tashkent University of IT, 2011. - p. 140-142.

[3]. Ganiyev S. K. Irgasheva D. Ya. To a question of administration of access rights of roles in corporate computer networks//Republican scientifically – technical conference of young scientists, researchers, undergraduates and students «Problems of information technologies and telecommunications». Collection of reports, Tashkent, 2012. Volume No. 1 - page 215-216.

[4]. Devyanin P. N. of Model of safety of computer systems: Studies. grant for Higher Education Institutions. - M.: Publishing tsentr:Akademiya, 2005. - page 144.

[5]. Ganiyev S. K. Irgasheva D. Ya. Tashev K.A. Creation of model of safety in telecommunication networks and computer systems//the Republican seminar / Information security in the communication and informatization sphere. Problems and ways of their decision: Collection of reports - Tashkent, 2010. - page 48-50.

[6]. Irgasheva D. Ya. Role model with zone differentiation of access//the Magazine the TSIU Bulletin. 2011, No. 4 - page 21-23.

[7]. Sandhu Ravi S., Coyne Edward J, Feinstein Hal L. Youman Charles E. Role-Based Access Control Models // IEEE Computer, Volume 29, Number 2, February 1996. - p.38-47.

BIOGRAPHIES

DurdonaIrgasheva was born in Uzbekistan. She has received M.Tech in Computer Science from Tashkent state technical university at 1999y. and is currently pursuing PhD in Computer Science with Specialization in area Information Security in Tashkent university of information technology. Her areas of interest include Data Security and her research interest includes Data and Network Security