# კომპიუტერულ ქსელებში ინფორმაციულ რესურსებზე წვდომის მართვის მოდელები

გულნარა ჯანელიძე, ლილი თვალავაძე
საქართველოს ტექნიკური უნივერსიტეტი

**რეზიუმე**

განხილულია კომპიუტერული ქსელების უსაფრთხოების სისტემის აგების ძირითადი პრინციპები. აღწერილია წვდომის მართვის საბაზო მოდელები. გაანალიზებულია მათი დადებითი და უარყოფითი მხარეები. მეთოდურად არის აღწერილი როლური მოდელის აგების პრინციპები ობიექტ-ორიენტირებული მიდგომის საფუძველზე, რომელსაც გამოყენებით პროგრამებში უპირატესობა ენიჭება ადმინისტრირების სიმარტივის თვალსაზრისით. ინფორმაციულ რესურსებზე წვდომის მართვის დამუშავებული მოდელი თავსებადია ცნობილ საბაზო მოდელებთან, მაგრამ ამავე დროს მას შემოაქვს თავისუფლების დამატებითი ხარისხი, რაც სისტემის ობიექტების იერარქიაზე მომხმარებლების უფლებების მიბმის პროცესის სიმარტივეში მდგომარეობს. ამდენად, იგი გაცილებით მოქნილს ხდის ობიექტებზე წვდომის სქემას.

**საკვანძო სიტყვები:** მანდატური მოდელი. დისკრეციული მოდელი. როლური მოდელი.

## 1. პრობლემის არსი და აქტუალობა

დანართის უსაფრთხოების გონიერი პოლიტიკის რეალიზებისთვის მნიშვნელოვანი როლი უჭირავს დანართის ობიექტებზე წვდომის მართვის მოდელების დამუშავებას. წვდომის მართვის ყველა მოდელის საერთო მიდგომაა სისტემის შემადგენელი მრავალი კომპონენტის განაწილება ობიექტების და სუბიექტების სიმრავლეზე. ამავე დროს ობიექტისა და სუბიექტის ცნება არსებითად განსხვავებულია. ჩავთვალოთ, რომ ობიექტი არის ინფორმაციის კონტეინერი, ხოლო სუბიექტი – მომხმარებელი, რომელიც ობიექტზე ატარებს სხვადასხვა ოპერაციას. სუბიექტსა და ობიექტს შორის ურთიერთდამოკიდებულების ხასიათი განსხვავებულია წვდომის მართვის დისკრეციულ, მანდატურ და როლურ მოდელებში. ამდენად, მიზანშეწონილია გავაანალიზოთ ობიექტზე წვდომის მართვის ძირითადი მოდელების ღირსებები და ნაკლოვანებები.

მომხმარებლის დიდი რაოდენობის შემთხვევაში წვდომის მართვის ტრადიციული როლური სისტემები ადმინისტრირების თვალსაზრისით საკმაოდ რთული ხდება. კავშირების რაოდენობა მომხმარებლებისა და ობიექტების წარმოებულით იზრდება. აღნიშნული სირთულის შემცირების მიზნით მიზანშეწონილია პრობლემის ობიექტ-ორიენტირებული გადაწყვეტა.

## 2. ძირითადი ნაწილი

დისკრეციული წვდომის მართვის (Discretionary Access Control - DAC) ღირსებებს მიეკუთნება შედარებით მარტივი რეალიზაცია და კარგი განსწავლის უნარი, ხოლო რაც შეეხება ნაკლოვან მხარეებს, პირველ რიგში აღსანიშნავია წვდომის შეზღუდვის სტატიკურობა – რაც გამოიხატება იმაში, რომ კომპიუტერული სისტემის მდგომარეობის ცვლილების მიუხედავად, ობიექტის მიმართ სუბიექტის წვდომის უფლება შემდგომში არ შეიცვლება.

წვდომის დისკრეციული მოდელის გამოყენებისას არ ხდება შემოწმება იმისა, გამოიწვევს თუ არა ობიექტზე წვდომის ნებართვა ზოგიერთი სუბიექტისათვის კომპიუტერული სისტემის ინფორმაციული უსაფრთხოების დარღვევას. სხვაგვარად რომ ვთქვათ, წვდომის დისკრეციული მართვა ვერ უზრუნველყოფს კონფიდენციალური ინფორმაციის გაჟონვისგან დაცვას. აღნიშნული მოდელის ნაკლს მიეკუთვნება ასევე, სუბიექტებზე წვდომის უფლების ავტომატური დანიშვნა [1].

ზემოაღნიშნული ნაკლოვანებები ნაწილობრივ აღმოფხვრილია წვდომის მანდატურ მოდელში (Mandatory Access Control - MAC), რომლის ძირითადი მახასიათებლებიდან გამოვყოთ ზოგიერთი მათგანი:

_ კომპიუტერული სისტემის ყველა ობიექტი და სუბიექტი უნდა იყოს ერთმნიშვნელოვნად იდენტიფიცირებული;

– არსებობს კონფიდენციალობის მაჩვენებლების და მისი შესაბამისი დაშვების ხარისხის წრფივად მოწესრიგებული ნაკრები;

– კომპიუტერული სისტემის ცალკეულ ობიექტს მინიჭებული აქვს კონფიდენციალობის მაჩვენებელი;

– კომპიუტერული სისტემის ცალკეულ სუბიექტს მინიჭებული აქვს ობიექტზე წვდომის ხარისხი.

ზემოაღნიშნულიდან გამომდინარე, წვდომის მართვის მანდატური მოდელის ძირითადი მიზანია კონფიდენციალობის მაღალი მაჩვენებლის ობიექტებიდან კონფიდენციალობის დაბალი მაჩვენებლის ობიექტებში ინფორმაციის გაჟონვის აღმოფხვრა.

აღვნიშნოთ წვდომის მანდატური მოდელის სხვა ღირსებებიც:

– კომპიუტერული სისტემის მუშაობის გაცილებით მაღალი საიმედობა, რამდენადაც ობიექტებზე წვდომის შეზღუდვისას კონტროლდება არა მხოლოდ დადგენილი უფლებების დაცვა, არამედ თვით სისტემის მდგომარეობა;

– წვდომის შეზღუდვის წესების განსაზღვრის სიმარტივე.

რაც შეეხება წვდომის მანდატური მართვის ნაკლოვან მხარეებს, შეიძლება გამოვყოთ:

– პროგრამული რეალიზაციის სირთულე, რაც ზრდის შეცდომების შეტანის ალბათობას და კონფიდენციალური ინფორმაციის გაჟონვის არხების გაჩენას;

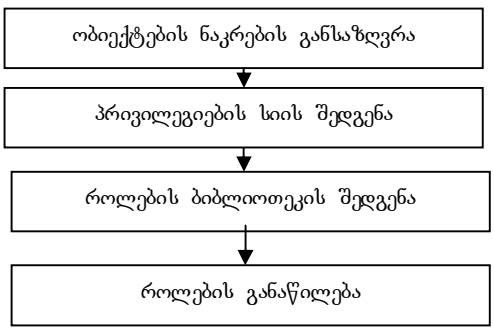
– კომპიუტერული სისტემის მუშაობის ეფექტურობის შემცირება, რამდენადაც ობიექტზე სუბიექტის წვდომის უფლების შემოწმება ხორციელდება არა მხოლოდ ობიექტის გახსნისას, არამედ მასზე ნებისმიერი ოპერაციის შესრულებისას;

– კომპიუტერული სისტემის მომხმარებლის მუშაობაში დამატებითი დისკომფორტის შექმნა, რაც განპირობებულია არაკონფიდენციალურ ობიექტზე ინფორმაციის შეცვლასთან დაკავშირებული პრობლემებით, იმ შემთხვევაში, თუ იგივე პროცესი იყენებს ინფორმაციას კონფიდენციალური ობიექტიდან. ამ უკანასკნელის აღმოფხვრა მოითხოვს კომპიუტერული სისტემის პროგრამული უზრუნველყოფის დამუშავებას მანდატური შეზღუდვის თავისებურებების გათვალისწინებით [2,3].

წვდომის მართვის როლური მოდელი (Role-Based Access Control - RBAC) რამდენადმე მკაცრია, მაგრამ ამავდროულად მოქნილია. ამ უკანასკნელის ღირსებად ჩაითვლება დიდი რაოდენობის მომხმარებლებისა და ობიექტების მქონე რთულ საინფორმაციო სისტემების რესურსებზე ჯგუფური წვდომის ორგანიზაციის შესაძლებლობა [4].

როლური მოდელი ეფუძნება ადამიანის მიერ დაკავებულ თანამდებობას – ანუ როლს. ამდენად, იგი მოითხოვს როლების ნაკრების დამუშავებას, რომელიც შეესაბამება თანამშრომლების მიერ შრომითი ფუნქციის შესრულებას.

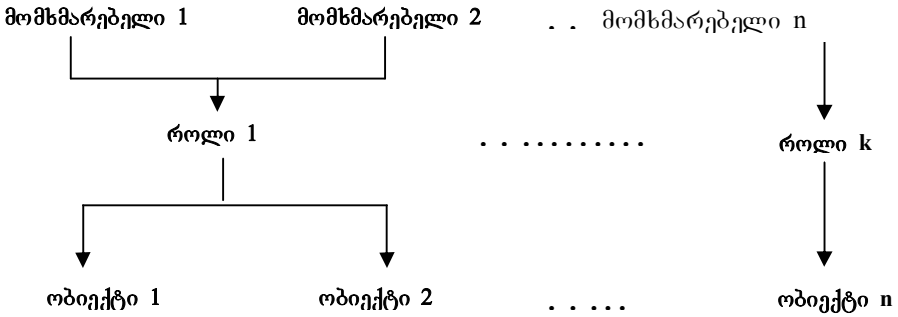
წვდომის მართვის როლური მოდელის რეალიზება შეიძლება წარმოვადგინოთ შემდეგი ბიჯების სახით:




**ნახ.1. როლური მოდელის რეალიზების სქემა**

პირველი ბიჯი ახდენს ობიექტების სიის დაზუსტებას; მეორე ბიჯი ახორციელებს პრივილეგიების განსაზღვრას და სიის შედგენას; მესამე ბიჯზე როლების კონსტრუქტორი ამუშავებს მოცემული სისტემისათვის როლების ბიბლიოთეკას; მეოთხე ბიჯზე როლების დისპეტჩერი სისტემის ცალკეულ მომხმარებელს სტატიკური სახით მიანიჭებს მოცემული მომხმარებლისათვის შესაძლო როლების ნაკრებს.

მომხმარებლის ავტორიზების შემდეგ, მონაცემები დაფიქსირდება აუდიტის ჟურნალში. როლური მოდელი ითავსებს დისკრეციული და მანდატური შეზღუდვის ელემენტებსაც. მომხმარებლებსა და პრივილეგიებს შორის შუალედურ რგოლს წარმოადგენს როლი. თითოეული მომხმარებლისათვის ერთდროულად შეიძლება აქტიური იყოს რამდენიმე როლი, რომელთაგან თითოეული მომხმარებელს აძლევს გარკვეულ უფლებას. მომხმარებლების, ობექტებისა და როლების ურთიერთდამოკიდებულება წარმოდგენილია ნახ. 2.-ზე.

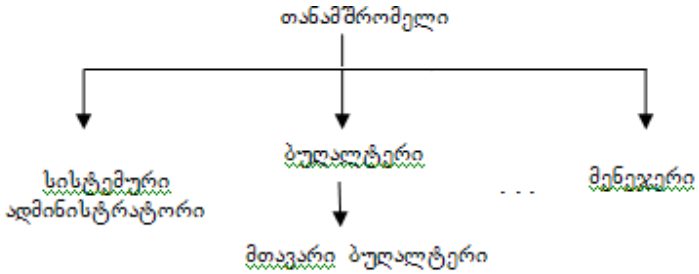



**ნახ.2. ობიექტებზე წვდომის ზოგადი სტრუქტურა**

როლური წვდომა შეიძლება გახვიხილოთ როგორც ობიექტ-ორიეხტირებული კარკასი, რომელიც აადვილებს ადმინისტრირებას, რამდენადაც იგი წვდომის განაწილების სისტემას მართვადს ხდის მომხმარებელთა დიდი რაოდენობისათვის, როლებს შორის კავშირის დამყარების ხარჯზე, რომელიც ობიექტ-ორიენტირებულ სისტემებში მემკვიდრეობითობის ანალოგიურია. გარდა ამისა როლი შეიძლება იყოს გაცილებით მცირე, მომხმარებელთან შედარებით, რომლის შედეგადაც ადმინისტრირების კავშირები ხდება მომხმარებლებისა და ობიექტების ჯამის პროპორციული.

შეიძლება ითქვას, რომ მომხმარებლებსა და უფლებებს შორის არის „მრავალი მრავალთან" დამოკიდებულება. სეანსის პროცესში აქტივირდება მრავალი როლი, ამავდროულად მომხმარებელმა შეიძლება გახსნას მრავალი სეანსი. თუ r2 როლი არის r1 როლის მემკვიდრე, მაშინ r2-ს მიენიჭება r1-ის ყველა უფლება. მემკვიდრეობითობის დამოკიდებულება არის იერარქიული, ამდენად წვდომის უფლებები და მომხმარებლები ვრცელდებიან იერარქიის დონეებზე. ზოგადად, მემკვიდრეობითობა არის მრავლობითი, ანუ ერთ როლს შეიძლება ჰყავდეს რამდენიმე წინაპარი და ასევე, მემკვიდრე.

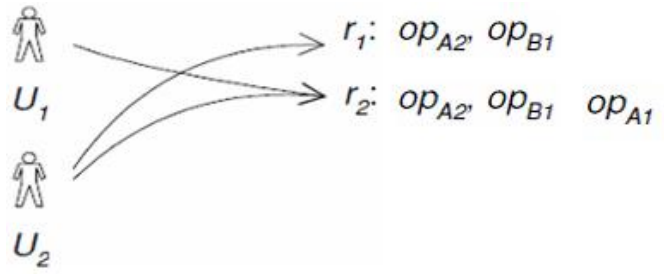
როლების იერარქიის ფორმირება დავიწყოთ მინიმუმი უფლებებიდან, რომელსაც მივაკუთვნოთ როლი „თანამშრომელი", თანდათან დავაზუსტოთ მომხმარებლების შემადგენლობა და დავამატოთ როლები, მაგალითად: როლი „სისტემური ადმინისტრატორი", „ბუღალტერი", „მენეჯერი" და ა.შ. როლების იერარქია მოცემულია მე-3 ნახაზზე.




**ნახ.3. როლების იერარქიის ფრაგმენტი**

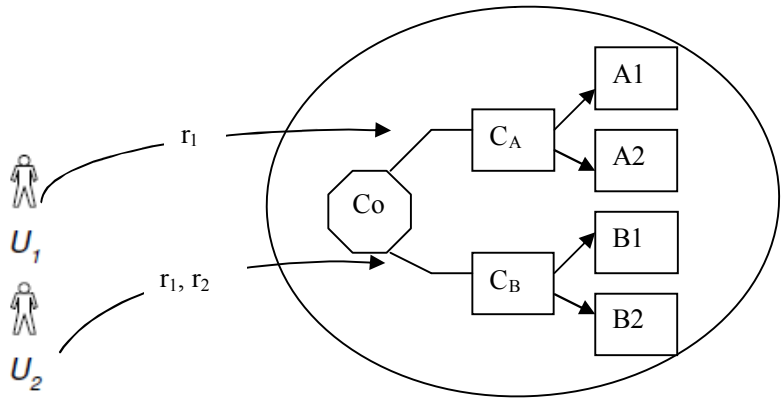
ერთი მომხმარებელი შეიძლება ასრულებდეს ორ როლს, მაგალითად მოლარის და ბუღალტრის როლს, მაგრამ არა ერთდროულად. ბუღალტრის როლამდე, მან უნდა დახუროს სალარო. ამ სახით რეალიზდება ე.წ. ნდობის დროებითი შეზღუდვა, რომელიც წარმოადგენს პრივილეგიების მინიმიზების ძირითად ასპექტს.

ავაგოთ ობიექტზე წვდომის როლური მოდელი, თუ მოცემული გვაქვს ოთხი სხვადასხვა ობიექტი: A1, A2, B1, B2, გვაქვს ორი ოპერაცია, რომელიც უნდა შესრულდეს A ტიპის ობიექტზე და ერთი ოპერაცია, რომელიც უნდა შესრულდეს B ტიპის ობიექტზე. ოპერაციები ობიექტების მიმართ აღვნიშნოთ: $OP_{A1}$, $OP_{A2}$, $OP_{B1}$. სისტემაში დარეგისტრირებულია ორი მომხმარებელი: $U_1$, $U_2$. $r_1$ როლი მოიცავს $OP_{A2}$, $OP_{B1}$ ოპერაციებს, ხოლო $r_2$ როლი მოიცავს $r_1$ როლის ყველა ოპერაციას დამატებულს $OP_{A1}$-ს. დავუნიშნოთ როლებს მომხმარებლები: $U_1$ ასრულებს სისტემაში $r_2$ როლს, ხოლო $U_2$ - ორივე როლს. მომხმარებლებზე როლების განაწილება მოცემულია ნახ.4.-ზე.




**ნახ.4. მომხმარებლებზე როლების განაწილება**

დანართის ყველა ობიექტი მოვიყვანოთ ერთიან იერარქიაში, რისთვისაც შემოვიტანოთ Co ფესვური ობიექტის კლასი, რომლის პირდაპირი მემკვიდრეები იყოს A და B ობიექტების კლასები, ანუ $C_A$ და $C_B$ კლასები. ობიექტებზე როლების დამოკიდებულება წარმოდგენილია ნახ.5.-ზე.




**ნახ.5. როლების დამოკიდებულება ობიექტებზე**

## 3. დასკვნა

ამდენად, დისკრეციულთან შედარებით მართვის როლური მოდელის უპირატესობას წარმოადგენს ადმინისტრირების სიმარტივე, რამდენადაც როლებზე მომხმარებლების დანიშვნა და ასევე ახალი როლების შექმნა სირთულეს არ წარმოადგენს. ამიტომაც როლური მოდელის რეალიზება მიზანშეწონილია გამოყენებით პროგრამებში. თუმცა, აღნიშნული მოდელის ნაკლს მოეკუთვნება კომპიუტერული სისტემის უსაფრთხოების ფორმალური მტკიცებულების არარსებობა, დუბლირების შეტანის შესაძლებლობა და დანაკლისი მომხმარებლებზე წვდომის უფლებების წარდგენისას, როლების კონსტრუირების სირთულე.

წვდომის მართვის წარმოდგენილი მოდელი ეფუძვნება საბაზო მოდელს, რაც მეტად მნიშვნელოვანია. იგი აფართოებს მას მომხმარებლების როლებზე დანიშვნის შესაძლებლობით სისტემის ნებისმიერი ობიექტის მიმართ. ამდენად, როლების სიმრავლე, რომელსაც მომხმარებელი ასრულებს დროის რაღაც მომენტში არ არის ერთიდაიგივე დანართის ყველა ობიექტისთვის. იგი შეივსება ახალი როლებით ობიექტების იერარქიაში სიღრმისეული პრინციპით.

ზემოაღნიშნულის საფუძველზე ჩნდება შესაძლებლობა მომხმარებლებისთვის მაქსიმალურად ბუნებრივი სახით შეიზღუდოს დანართის განსაზღვრულ ნაწილზე მოქმედების არე. როლების მიმართ ობიექტ-ორიენტირებული მიდგომა როლების ოპტიმიზაციის და ობიექტებზე წვდომის სქემის გამარტივების საშუალებას იძლევა. ყოველივე ზემოთქმულიდან გამომდინარე წარმოდგენილი მოდელი ფლობს დანართის ობიექტებზე არასანქცირებული წვდომის შეზღუდვის აუცილებელ შესაძლებლობებს, ამდენად, იგი მიზნად ისახავს მოქნილი უსაფრთხოების პოლიტიკის შექმნას.

**ლიტერატურა:**

1. შონია ო., ჯანელიძე გ., მეფარიშვილი ბ. ინფორმაციული და ქსელური რესურსების უსაფრთხოების ურუნველყოფა, სტუ, თბ., 2009

2. Хорев П.Б. Программно-аппаратная защита информации, М., изд. ФОРУМ, 2009

3. Зегжда Д.П. Общая схема мандатных моделей безопасности и ее применение для доказателства безопасности систем обработки информации . Ст-ПБГ ТУ. 2002.

4. Mohan Rao Cavale. Role-Based Access Control Using Windows Server 2003 Authorization Manager. http://msdn.microsoft.com/library/en-us/dnnetserv/html/AzManRoles.asp

## MANAGEMENT MODELS OF ACCESS INFORMATION RESOURCES IN COMPUTER NETWORKS

Djanelidze Gulnara, Tvalavadze Lili
Georgian Technical University

### Summary

In the article the main principles of construction of safety systems for computer networks are discussed. Base models of access management are described, and also advantages and disadvantages are in details considered. The principle of construction of a role model on the basis of objective focused approach is methodologically defined, which, due to its simplicity in administration, is preferencial one for the use in applied programs. The developed model of access management is compatible to known base models, but it releases an additional degree of latitude expressed in user-friendly application of hierarchy of system objects. Thus, the given approach makes schemes of access to objects considerably flexible.

## МОДЕЛИ УПРАВЛЕНИЯ ДОСТУПОМ К ИНФОРМАЦИОННЫМ РЕСУРСАМ В КОМПЬЮТЕРНЫХ СЕТЯХ

Джанелидзе Г., Твалавадзе Л.
Грузинский Технический Университет

### Резюме

Рассматриваются основные принципы построения систем безопасности компьютерных сетей. Описаны базовые модели управления доступом, а также детально рассматриваются их преимущества и недостатки. Методически описан принцип построения ролевой модели на основе объектно- ориентированного подхода, который из-за простоты администрирования является предпочтительным к использованию в прикладных программах. Разработанная модель управления доступом совместима с известными базовыми моделями, но она вводит дополнительную степень свободы, которая выражается в простоте привязки пользовательских полномочий к иерархии объектов системы. Данный подход делает схемы доступа к объектам значительно гибкими.